Efficient Certificateless Anonymous Multi Receiver

The recent explosion of digital media, online networking, and e-commerce has generated great new opportunities for those Internet-savvy individuals who see potential in new technologies and can turn those possibilities into reality. It is vital for such forward-thinking innovators to stay abreast of all the latest technologies. Web-Based Services: Concepts, Methodologies, Tools, and Applications provides readers with comprehensive coverage of some of the latest tools and technologies in the digital industry. The chapters in this multi-volume book describe a diverse range of applications and methodologies made possible in a world connected by the global network, providing researchers, computer scientists, web developers, and digital experts with the latest knowledge and developments in Internet technologies.

This book constitutes the refereed proceedings of the 8th International Workshop on Theory and Practice in Public Key Cryptography, PKC 2005, held in Les Diablerets, Switzerland in January 2005. The 28 revised full papers presented were carefully reviewed and selected from 126 submissions. The papers are organized in topical sections on cryptanalysis, key establishment, optimization, building blocks, RSA cryptography, multivariate asymmetric cryptography, signature schemes, and identity-based cryptography.

This book constitutes the refereed proceedings of the 13th International Conference on Provable Security, ProvSec 2019, held in Cairns, QLD, Australia, in October 2019. The 18 full and 6 short papers presented were carefully reviewed and selected from 51 submissions. The papers focus on provable security as an essential tool for analyzing security of modern cryptographic primitives, including a special theme on “Practical Security.”

In today’s world, data must be sent around the world cheaply and securely, and that requires origin authentication, integrity protection, and confidentiality – the recipient of a message should be able to ascertain who sent the message, be sure that the message has not been changed en route, and be sure that the data arrives without having been read by anyone else. The second editor invented signcryption, an area of cryptography that studies systems that simultaneously provide origin authentication, integrity protection and confidentiality for data. Signcryption schemes combine the features of digital signature schemes with those of public-key encryption schemes and aim to provide security guarantees in a way that is provably correct and significantly less computationally expensive than the “encrypt-then-sign” method most commonly adopted in public-key cryptography. This is the first comprehensive book on signcryption, and brings together leading authors from the field of cryptography in a discussion of the different methods for building efficient and secure signcryption schemes, and the ways in which these schemes can be used in practical systems. Chapters deal with the theory of signcryption, methods for constructing practical signcryption schemes, and the advantages of using such schemes in practical situations. The book will be of benefit to cryptography researchers, graduate students and practitioners.

Building on previous editions, this third edition of the Smart Card Handbook offers a completely updated overview of the state of the art in smart card technology. Everything you need to know about smart cards and their applications is covered! Fully revised, this handbook describes the advantages and disadvantages of smart cards when compared with other systems, such as optical cards and magnetic stripe cards and explains the basic technologies to the reader. This book also considers the actual status of appropriate European and international standards. Features include: New sections on: smart card applications (PKCS #15, USIM, Tachosmart). smart card terminals: M.U.S.C.L.E., OCF, MKT, PC/SC. contactless card data transmission with smart cards. Revised and updated chapters on: smart cards in the telecommunications industry (GSM, UMTS, (U)SIM application toolkit, decoding of the files of a GSM card). smart card security (new attacks, new protection methods against attacks). A detailed description of the physical and technical properties and the fundamental principles of information processing techniques. Explanations of the architecture of smart card operating systems, data transfer to and from the smart card, command set and implementation of the security mechanisms and the function of the smart card terminals. Current applications of the technology on mobile telephones, telephone cards, the electronic purse and credit cards. Discussions on future developments of smart cards: USB, MMU on microcontroller, system on card, flash memory and their usage. Practical guidance on the future applications of smart cards, including health insurance cards, e-ticketing, wireless security, digital signatures and advanced electronic payment methods. “The book is filled with information that students, enthusiasts, managers, experts, developers, researchers and programmers will find useful. The book is well structured and provides a good account of smart card state-of-the-art technology… There is a lot of useful information in this book and as a practicing engineer I found it fascinating, and extremely useful.” Review of second edition in Measurement and Control. 'The standard has got a lot higher, if you work with smart cards then buy it! Highly recommended.’ Review of second edition in Journal of the Association of C and C++ Programmers. Visit the Smart Card Handbook online at www.wiley.co.uk/commstech/

This book constitutes the refereed proceedings of the Workshops and Symposiums of the 15th International Conference on Algorithms and Architectures for Parallel Processing, ICA3PP 2015, held in Zhangjiajie, China, in November 2015. The program of this year consists of 6 symposiums/workshops that cover a wide range of research topics on parallel processing technology: the Sixth International Workshop on Trust, Security and Privacy for Big Data, TrustData 2015; the Fifth International Symposium on Trust, Security and Privacy for Emerging Applications, TSP 2015; the Third International Workshop on Network Optimization and Performance Evaluation, NOPE 2015; the Second International Symposium on Sensor-Cloud Systems, SCS 2015; the Second International Workshop on Security and Privacy Protection in Computer and Network Systems, SPPCN 2015; and the First International Symposium on Dependability in Sensor, Cloud, and Big Data Systems and Applications, DependSys 2015. The aim of these symposiums/workshops is to

provide a forum to bring together practitioners and researchers from academia and industry for discussion and presentations on the current research and future directions related to parallel processing technology. The themes and topics of these symposiums/workshops are a valuable complement to the overall scope of ICA3PP 2015 and give additional values and interests.

This book provides a broad overview of the many card systems and solutions that are in practical use today. This new edition adds content on RFIDs, embedded security, attacks and countermeasures, security evaluation, javacards, banking or payment cards, identity cards and passports, mobile systems security, and security management. A step-by-step approach educates the reader in card types, production, operating systems, commercial applications, new technologies, security design, attacks, application development, deployment and lifecycle management. By the end of the book the reader should be able to play an educated role in a smart card related project, even to programming a card application. This book is designed as a textbook for graduate level students in computer science. It is also as an invaluable post-graduate level reference for professionals and researchers. This volume offers insight into benefits and pitfalls of diverse industry, government, financial and logistics aspects while providing a sufficient level of technical detail to support technologists, information security specialists, engineers and researchers.

Advances in Artificial Intelligence and Security7th International Conference, ICAIS 2021, Dublin, Ireland, July 19-23, 2021, ProceedingsSpringer Nature

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.

A atudy of mobile agents and security. The mobile agents paradigm integrates a network of computers and reduces networking to program construction. A mobile agent can travel from one place to another, and, subject to the destination's approval, interact programmatically with the place it visits.

This book presents the proceedings of the International Computer Symposium 2014 (ICS 2014), held at Tunghai University, Taichung, Taiwan in December. ICS is a biennial symposium founded in 1973 and offers a platform for researchers, educators and professionals to exchange their discoveries and practices, to share research experiences and to discuss potential new trends in the ICT industry. Topics covered in the ICS 2014 workshops include: algorithms and computation theory; artificial intelligence and fuzzy systems; computer architecture, embedded systems, SoC and VLSI/EDA; cryptography and information security; databases, data mining, big data and information retrieval; mobile computing, wireless communications and vehicular technologies; software engineering and programming languages; healthcare and bioinformatics, among others. There was also a workshop on information technology innovation, industrial application and the Internet of Things. ICS is one of Taiwan's most prestigious international IT symposiums, and this book will be of interest to all those involved in the world of information technology.

This book constitutes the refereed proceedings of the 7th International Conference on Cryptology in India, INDOCRYPT 2006, held in Kolkata, India in December 2006. The 29 revised full papers and 2 invited papers cover such topics as symmetric cryptography, provable security, fast implementation of public key cryptography, id-based cryptography, as well as embedded systems and side channel attacks.

This book reports on the latest advances in mobile technologies for collecting, storing and processing mobile big data in connection with wireless communications. It presents novel approaches and applications in which mobile big data is being applied from an engineering standpoint and addresses future theoretical and practical challenges related to the big data field from a mobility perspective. Further, it provides an overview of new methodologies designed to take mobile big data to the Cloud, enable the processing of real-time streaming events on-the-move and enhance the integration of resource availability through the ‘Anywhere, Anything, Anytime’ paradigm. By providing both academia and industry researchers and professionals with a timely snapshot of emerging mobile big data-centric systems and highlighting related pitfalls, as well as potential solutions, the book fills an important gap in the literature and fosters the further development in the area of mobile technologies for exploiting mobile big data.

This book discusses recent advances and contemporary research in the field of cryptography, security, mathematics and statistics, and their applications in computing and information technology. Mainly focusing on mathematics and applications of mathematics in computer science and information technology, it includes contributions from eminent international scientists, researchers, and scholars. The book helps researchers update their knowledge of cryptography, security, algebra, frame theory, optimizations, stochastic processes, compressive sensing, functional analysis, and complex variables.

This book constitutes the refereed proceedings of the 22nd International Conference on Information and Communications Security, ICICS 2020, held in Copenhagen, Denmark*, in August 2020. The 33 revised full papers were carefully selected from 139 submissions. The papers focus in topics about computer and communication security, and are organized in topics of security and cryptography. *The conference was held virtually due to the COVID-19 pandemic.

This two volume set LNCS 10602 and LNCS 10603 constitutes the thoroughly refereed post-conference proceedings of the Third International Conference on Cloud Computing and Security, ICCCS 2017, held in Nanjing, China, in June 2017. The 116 full papers and 11 short papers of these volumes were carefully reviewed and selected from 391 submissions. The papers are organized in topical sections such as: information hiding; cloud computing; IOT applications; information security; multimedia applications; optimization and classification.

This book addresses topics related to cloud and Big Data technologies, architecture and applications including distributed computing and data centers, cloud infrastructure and security, and end-user services. The majority of the book is devoted to the security aspects of cloud computing and Big Data. Cloud computing, which can be seen as any subscription-based or pay-per-use service that extends the Internet's existing capabilities, has gained considerable attention from both academia and the IT industry as a new infrastructure requiring smaller investments in hardware platforms, staff training, or licensing software tools. It is a new paradigm that has ushered in a revolution in both data storage and computation. In parallel to this progress, Big Data technologies, which rely heavily on cloud computing platforms for both data storage and processing, have been developed and deployed at breathtaking speed. They are among the most frequently used technologies for developing applications and services in many fields, such as the web, health, and energy. Accordingly, cloud computing and Big Data technologies are two of the most central current and future research mainstreams. They involve and impact a host of fields, including business, scientific research, and public and private administration. Gathering extended versions of the best papers presented at the Third International Conference on Cloud Computing Technologies and Applications (CloudTech'17), this book offers a valuable resource for all Information System managers, researchers, students, developers, and policymakers involved in the technological and application aspects of cloud computing and Big Data.

It has been a real pleasure to have taken part in organizing the 12th Inter- tional Conference on Practice and Theory in Public Key Cryptography (PKC 2009). PKC 2009 was held March 18-20, 2009, on the campus of the Univ- sity of California, Irvine (UCI). As usual, it was sponsored by the International Association for Cryptologic Research (IACR) in cooperation with: – UCI Secure Computing and Networking Center (SCONCE) – UCI Donald Bren School of Information and Computer Sciences (DBSICS) – California Institute for Telecommunications and Information Technology (CalIT2) The PKC 2008 Program Committee (PC) consisted of 33 internationally r- ognized researchers with combined expertise covering the entire scope of the conference. Recent growth in the number of cryptography venues has resulted in sti? competition for high-quality papers. Nonetheless, PKC's continued success is evident from both the number and the quality of submissions. PKC 2009 - ceived a total of 112 submissions. They were reviewed by the PC members and a highly quali?ed team of external reviewers. Each submission was refereed by at least three reviewers. After deliberations by the PC, 28 submissions were accepted for presentation. Based on extensive discussions, the PKC 2009 best paper awardwas givento Alexander Mayand MaikeRitzenhofen for their paper "Implicit Factoring: On Polynomial Time Factoring Given Only an Implicit Hint".Theconferenceprogramalsoincluded twoinvited talks,byAnna Lysy- skaya (Brown University) and Amit Sahai (UCLA).

Thisbookcontainsthepostproceedingsofthe6thEuropeanWorkshoponPublic Key Services, Applications and Infrastructures, which was held at the CNR Research Area in Pisa, Italy, in September 2009. The EuroPKI workshop series focuses on all research and practice aspects of public key infrastructures, services and applications, and welcomes original research papers and excellent survey contributions from academia, government, and industry. Previous events of the series were held in: Samos, Greece (2004); Kent, UK (2005); Turin, Italy, (2006); Palma de Mallorca, Spain, (2007); and Trondheim, Norway (2008). From the original focus on public key infrastructures, EuroPKI interests - panded to include advanced cryptographic techniques, applications and (more generally) services. The Workshops brings together researchersfrom the cryp- graphiccommunity as well as fromthe applied security community, as witnessed by the interesting program. Indeed, this volume holds 18 refereed papers and the presentation paper by the invited speaker, Alexander Dent. In response to the EuroPKI 2009 call for papers, a total of 40 submissions were received. All submissions underwent a thorough blind review by at least three ProgramCommittee members, resulting in careful selection and revision of the accepted papers. After the conference, the papers were revised and improved by the authors before inclusion in this volume.

This book constitutes the refereed proceedings of the 12th International Workshop on Security, IWSEC 2017, held in Hiroshima, Japan, in August/September 2017. The 11 regular papers and 3 short papers presented in this volume were carefully reviewed and selected from 37 submissions. They were organized in topical sections named: post-quantum cryptography; system security; public key cryptosystems; cryptanalysis; and cryptographic protocols.

The book provides a comprehensive guide to vehicular social networks. The book focuses on a new class of mobile ad hoc networks that exploits social aspects applied to vehicular environments. Selected topics are related to social networking techniques, social-based routing techniques applied to vehicular networks, data dissemination in VSNs, architectures for VSNs, and novel trends and challenges in VSNs. It provides significant technical and practical insights in different aspects from a basic background on social networking, the inter-related technologies and applications to vehicular ad-hoc networks, the technical challenges, implementation and future trends.

This book presents several novel approaches to model the interaction between the attacker and the defender and assess the security of Vehicular Ad Hoc Networks (VANETs). The first security assessment approach is based on the attack tree security assessment model, which leverages tree based methods to analyze the risk of the system and identify the possible attacking strategies the adversaries may launch. To further capture the interaction between the attacker and the defender, the authors propose to utilize the attack-defense tree model to express the potential countermeasures which could mitigate the system. By considering rational participants that aim to maximize their payoff function, the brief describes a game-theoretic analysis approach to investigate the possible strategies that the security administrator and the attacker could adopt. A phased attack-defense game allows the reader to model the interactions between the attacker and defender for VANET security assessment. The brief offers a variety of methods for assessing the security of wireless networks. Professionals and researchers working on the defense of VANETs will find this material valuable.

This book constitutes the proceedings of the 7th International Conference on Security and Cryptography for Networks held in Amalfi, Italy, in September 2010.

This book constitutes the refereed proceedings of the 11th International Conference on Provable Security, ProvSec 2017, held in Xi'an, China, in October 2017. The 24 full papers and 5 short papers presented were carefully reviewed and selected from 76 submissions. The papers are grouped in topical sections on secure cloud storage and computing; digital signature and authentication; authenticated encryption and key exchange; security models; lattice and post-quantum cryptography; public key encryption and signcryption; proxy re-encryption and functional encryption; protocols.

This book gathers selected research papers presented at the AICTE-sponsored International Conference on IoT Inclusive Life (ICIIL 2019), which was organized by the Department of Computer Science and Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India, on December 19–20, 2019. In contributions by active researchers, the book presents innovative findings and important developments in IoT-related studies, making it a valuable resource for researchers, engineers, and industrial professionals around the globe.

This book constitutes the refereed proceedings of the 10th International Conference on Security, Privacy and Anonymity in Computation, Communication, and Storage, SpaCCS 2017, held in Guangzhou, China, in December 2017. The 47 papers presented in this volume were carefully reviewed and selected from 140 submissions. They deal with research findings, achievements, innovations and perspectives in information security and related fields covering topics such as 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.

As an intermediate model between conventional PKC and ID-PKC, CL-PKC can avoid the heavy overhead of certificate management in traditional PKC as well as the key escrow problem in ID-PKC altogether. Since the introduction of CL-PKC, many concrete constructions, security models, and applications have been proposed during the last decade. Differing from the other books on the market, this one provides rigorous treatment of CL-PKC. Definitions, precise assumptions, and rigorous proofs of security are provided in a manner that makes them easy to understand.

This book constitutes the refereed proceedings of the 12th International Conference on Practice and Theory in Public-Key Cryptography, PKC 2009, held in Irvine, CA, USA, in March 2009. The 28 revised full papers presented were carefully reviewed and selected from 112 submissions. The papers are organized in topical sections on number theory, applications and protocols, multi-party protocols, identity-based encryption, signatures, encryption, new cryptosystems and optimizations, as well as group signatures and anonymous credentials.

This book constitutes the refereed proceedings of the 13th Australasian Conference on Information Security and Privacy, ACISP 2008, held in Wollongong, Australia, in July 2008. The 33 revised full papers presented were carefully reviewed and selected from 111 submissions. The papers cover a range of topics in information security, including authentication, key management, public key cryptography, privacy, anonymity, secure communication, ciphers, network security, elliptic curves, hash functions, and database security.

The 3-volume set CCIS 1422, CCIS 1423 and CCIS 1424 constitutes the refereed proceedings of the 7th International Conference on Artificial Intelligence and Security, ICAIS 2021, which was held in Dublin, Ireland, in July 2021. The total of 131 full papers and 52 short papers presented in this 3-volume proceedings was carefully reviewed and selected from 1013 submissions. The papers were organized in topical sections as follows: Part I: artificial intelligence; Part II: artificial intelligence; big data; cloud computing and security internet; Part III: cloud computing and security; encryption and cybersecurity; information hiding; IoT security.

This book constitutes the refereed proceedings of 11 symposia and workshops held at the 10th International Conference on Security, Privacy and Anonymity in Computation, Communication, and Storage, SpaCCS 2017, held in Guangzhou, China, in December 2017. The total of 75 papers presented in this volume was carefully reviewed and selected from a total of 190 submissions to all workshops: UbiSafe 2017: The 9th IEEE International Symposium on UbiSafe Computing ISSR 2017: The 9th IEEE International Workshop on Security in e-Science and e-Research TrustData 2017: The 8th International Workshop on Trust, Security and Privacy for Big Data TSP 2017: The 7th International Symposium on Trust, Security and Privacy for Emerging Applications SPIoT 2017: The 6th International Symposium on Security and Privacy on Internet of Things NOPE 2017: The 5th International Workshop on Network Optimization and Performance Evaluation DependSys 2017: The Third International Symposium on Dependability in Sensor, Cloud, and Big Data Systems and Applications SCS 2017: The Third International Symposium on Sensor-Cloud Systems WCSSC 2017: The Second International Workshop on Cloud Storage Service and Computing MSCF 2017: The First International Symposium on Multimedia Security and Digital Forensics SPBD 2017: The 2017 International Symposium on Big Data and Machine Learning in Information Security, Privacy and Anonymity

This valuable handbook is a comprehensive compilation of state-of-art advances on security in computer networks. More than 40 internationally recognized authorities in the field of security and networks contribute articles in their areas of expertise. These international researchers and practitioners are from highly-respected universities, renowned research institutions and IT companies from all over the world. Each self-contained chapter covers one essential research topic on security in computer networks. Through the efforts of all the authors, all chapters are written in a uniformed style; each containing a comprehensive overview, the latest pioneering work and future research direction of a research topic.

This handbook introduces the basic principles and fundamentals of cyber security towards establishing an understanding of how to protect computers from hackers and adversaries. The highly informative subject matter of this handbook, includes various concepts, models, and terminologies along with examples and illustrations to demonstrate substantial technical details of the field. It motivates the readers to exercise better protection and defense mechanisms to deal with attackers and mitigate the situation. This handbook also outlines some of the exciting areas of future research where the existing approaches can be implemented. Exponential increase in the use of computers as a means of storing and retrieving security-intensive information, requires placement of adequate security measures to safeguard the

entire computing and communication scenario. With the advent of Internet and its underlying technologies, information security aspects are becoming a prime concern towards protecting the networks and the cyber ecosystem from variety of threats, which is illustrated in this handbook. This handbook primarily targets professionals in security, privacy and trust to use and improve the reliability of businesses in a distributed manner, as well as computer scientists and software developers, who are seeking to carry out research and develop software in information and cyber security. Researchers and advanced-level students in computer science will also benefit from this reference.

Contains papers from a May 2000 symposium, covering all areas of computer security and electronic privacy. Papers were selected on the basis of scientific novelty, importance to the field, and technical quality. Material is in sections on access control, applications to cryptography, achievability of electronic privacy, protocol analysis and design, open source in security, intrusion detection, assurance, and key management. Specific topics include efficient authentication and signing of multicast streams over lossy channels, engineering tradeoffs and the evolution of provably secure protocols, and robust nonproprietary software. Lacks a subject index. Annotation copyrighted by Book News, Inc., Portland, OR.

This book constitutes the post-conference proceedings of the 15th International Conference on Information Security and Cryptology, Inscrypt 2019, held in Nanjing, China, in December 2019. The 23 full papers presented together with 8 short papers and 2 invited papers were carefully reviewed and selected from 94 submissions. The papers cover topics in the fields of post-quantum cryptology; AI security; systems security; side channel attacks; identity-based cryptography; signatures; cryptanalysis; authentication; and mathematical foundations.

The two-volume set LNCS 11944-11945 constitutes the proceedings of the 19th International Conference on Algorithms and Architectures for Parallel Processing, ICA3PP 2019, held in Melbourne, Australia, in December 2019. The 73 full and 29 short papers presented were carefully reviewed and selected from 251 submissions. The papers are organized in topical sections on: Parallel and Distributed Architectures, Software Systems and Programming Models, Distributed and Parallel and Network-based Computing, Big Data and its Applications, Distributed and Parallel Algorithms, Applications of Distributed and Parallel Computing, Service Dependability and Security, IoT and CPS Computing, Performance Modelling and Evaluation.

Pairing-based cryptography is at the very leading edge of the current wave in computer cryptography. That makes this book all the more relevant, being as it is the refereed proceedings of the First International Conference on Pairing-Based Cryptography, Pairing 2007, held in Tokyo, Japan in 2007. The 18 revised full papers presented together were carefully reviewed and selected from 86 submissions. The papers are organized in topical sections including those on applications, and certificateless public key encryption.

How the enabling technologies in 5G as an integral or as a part can seamlessly fuel the IoT revolution is still very challenging. This book presents the state-of-the-art solutions to the theoretical and practical challenges stemming from the integration of 5G enabling technologies into IoTs in support of a smart 5G-enabled IoT paradigm, in terms of network design, operation, management, optimization, privacy and security, and applications. In particular, the technical focus covers a comprehensive understanding of 5G-enabled IoT architectures, converged access networks, privacy and security, and emerging applications of 5G-eabled IoT.