Smart Card Applications 3rd Edition

Advances in hardware, software, and audiovisual rendering technologies of recent years have unleashed a wealth of new capabilities and possibilities for multimedia applications, creating a need for a comprehensive, up-to-date reference. The Encyclopedia of Multimedia Technology and Networking provides hundreds of contributions from over 200 distinguished international experts, covering the most important issues, concepts, trends, and technologies in multimedia technology. This must-have reference contains over 1,300 terms, definitions, and concepts, providing the deepest level of understanding of the field of multimedia technology and networking for academicians, researchers, and professionals worldwide.

Intended for Java Card applet developers, platform implementers, and technical managers seeking an overall understanding of Java Card technology, this guide provides an introduction to the development of applications with Java Card technology based on Java Card version 2.1. Includes an introduction to the platform, an overview and discussion of the technology, a programming guide, and tips. Annotation copyrighted by Book News, Inc., Portland, OR

This volume constitutes the thoroughly refereed post-proceedings of the Third International Conference on Smart Card Research and Advanced Applications, CARDIS'98, held in Louvain-la-Neuve, Belgium in September 1998. The 35 revised full papers presented were carefully reviewed and updated for inclusion in this book. All current aspects of smart card research and applications development are addressed, in particular: Java cards, electronic commerce, efficiency, security (including cryptographic algorithms, cryptographic protocols, and authentication), and architecture.

Welcome to the proceedings of the 2005 International Conference on Emb- ded Software and Systems (ICESS 2005) held in Xian, China, December 16-18, 2005. With the advent of VLSI system level integration and system-on-chip, the center of gravity of the computer industry is now moving from personal c- puting into embedded computing. Embedded software and systems are incre- ingly becoming a key technological component of all kinds of complex technical systems, ranging from vehicles, telephones, aircraft, toys, security systems, to medical diagnostics, weapons, pacemakers, climate control systems, etc. The ICESS 2005 conference provided a premier international forum for - searchers, developers and providers from academia and industry to address all resulting profound challenges; to present and discuss their new ideas, - search results, applications and experience; to improve international com- nication and cooperation; and to promote embedded software and system - dustrialization and wide applications on all aspects of embedded software and systems.

9th IFIP WG 8.8/11.2 International Conference, CARDIS 2010, Passau, Germany, April 14-16, 2010, Proceedings

Public-key Cryptography

Smart Card. Research and Applications

Radio Frequency Identification System Security

Web Commerce Security

Security and Protection in Information Processing Systems

Guide to RBI Grade B Officers Exam 2019 Phase 1 - 3rd Edition

CRYPTO is a conference devoted to all aspects of cryptologic research. It is held each year at the University of California at Santa Barbara. Annual meetings on this topic also take place in Europe and are regularly published in this Lecture Notes series under the name of EUROCRYPT. This volume presents the proceedings of the ninth CRYPTO meeting. The papers are organized into sections with the following themes: Why is cryptography harder than it looks?, pseudo-randomness and sequences, cryptanalysis and implementation, signature and authentication, threshold schemes and key management, key distribution and network security, fast computation, odds and ends, zero-knowledge and oblivious transfer, multiparty computation.

Briefly, we review the basic elements of computability theory and prob ability theory that are required. Finally, in order to place the subject in the appropriate historical and conceptual context we trace the main roots of Kolmogorov complexity. This way the stage is set for Chapters 2 and 3, where we introduce the notion of optimal effective descriptions of objects. The length of such a description (or the number of bits of information in it) is its Kolmogorov complexity. We treat all aspects of the elementary mathematical theory of Kolmogorov complexity. This body of knowledge may be called algo rithmic complexity theory. The theory of Martin-Lof tests for random ness of finite objects and infinite sequences is inextricably intertwined with the theory of Kolmogorov complexity and is completely treated. We also investigate the statistical properties of finite strings with high Kolmogorov complexity. Both of these topics are eminently useful in the applications part of the book. We also investigate the recursion theoretic properties of Kolmogorov complexity (relations with Godel's incompleteness result), and the Kolmogorov complexity version of infor mation theory, which we may call "algorithmic information theory" or "absolute information theory. " The treatment of algorithmic probability theory in Chapter 4 presup poses Sections 1. 6, 1. 11. 2, and Chapter 3 (at least Sections 3. 1 through 3. 4).

Presents an illustrated A-Z encyclopedia containing approximately 600 entries on computer and technology related topics.

Our reliance on ever more sophisticated computer systems for the management of data and information means that the field of security and privacy technology continues to be of crucial importance to us all. This book presents ten peer-reviewed papers from the 2013 workshop Radio Frequency Identification/Internet of Things Security (RFIDsec'13 Asia) held in Guangzhou, China, in November 2013. This is the fifth of a series of workshops organized by the Asian branch of RFIDsec, which provides a platform for researchers, enterprises and governments to investigate, discuss and propose new solutions for the security and privacy issues related to RFID/IoT technologies and applications. Topics covered include RFID authentication, mutual authentication and ownership transfer, security of RFID applications, NFC and the Internet of Things, as well as side channel attacks. The book will be of interest to all those whose work involves the security aspects of information management.

IFIP 18th World Computer Congress : TC11 19th International Information Security Conference, 22-27 August 2004, Toulouse, France

The Developer's Toolkit

Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday
Java Card Technology for Smart Cards
19th International Conference, CARDIS 2020, Virtual Event, November 18–19, 2020, Revised Selected Papers
Encyclopedia of Information Science and Technology, Third Edition
Smart Card Programming

"This 10-volume compilation of authoritative, research-based articles contributed by thousands of researchers and experts from all over the world emphasized modern issues and the presentation of potential opportunities, prospective solutions, and future directions in the field of information science and technology"--Provided by publisher.

Recognized as one of the best tools available for the information security professional and especially for candidates studying for the (ISC)2 CISSP examination, the Official (ISC)2® Guide to the CISSP® CBK®, Third Edition has been updated and revised to reflect the latest developments in this ever-changing field. Endorsed by the (ISC)2, this book provides unrivaled preparation for the certification exam that is both up to date and authoritative. Compiled and reviewed by CISSPs and (ISC)2 members, the text provides an exhaustive review of the 10 current domains of the CBK.

This is the third revised edition of the established and trusted RFID Handbook; the most comprehensive introduction to radio frequency identification (RFID) available. This essential new edition contains information on electronic product code (EPC) and the EPC global network, and explains near-field communication (NFC) in depth. It includes revisions on chapters devoted to the physical principles of RFID systems and microprocessors, and supplies up-to-date details on relevant standards and regulations. Taking into account critical modern concerns, this handbook provides the latest information on: the use of RFID in ticketing and electronic passports; the security of RFID systems, explaining attacks on RFID systems and other security matters, such as transponder emulation and cloning, defence using cryptographic methods, and electronic article surveillance; frequency ranges and radio licensing regulations. The text explores schematic circuits of simple transponders and readers, and includes new material on active and passive transponders, ISO/IEC 18000 family, ISO/IEC 15691 and 15692. It also describes the technical limits of RFID systems. A unique resource offering a complete overview of the large and varied world of RFID, Klaus Finkenzeller’s volume is useful for end-users of the technology as well as practitioners in auto ID and IT designers of RFID products. Computer and electronics engineers in security system development, microchip designers, and materials handling specialists benefit from this book, as do automation, industrial and transport engineers. Clear and thorough explanations also make this an excellent introduction to the topic for graduate level students in electronics and industrial engineering design. Klaus Finkenzeller was awarded the Fraunhofer-Smart Card Prize 2008 for the second edition of this publication, which was celebrated for being an outstanding contribution to the smart card field.

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.

ECIW2010
Design models for using and programming smart cards
Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication
10th IFIP WG 8.8/11.2 International Conference, CARDIS 2011, Leuven, Belgium, September 14-16, 2011, Revised Selected Papers
Second International Workshop Worcester, MA, USA, August 17-18, 2000 Proceedings
Power Analysis Attacks
Smart Cards

A state-of-the-art guide to middleware technologies, and their pivotal role in communications networks. Middleware is about integration and interoperability of applications and services running on heterogeneous computing and communications devices. The services it provides - including identification, authentication, authorization, soft-switching, certification and security - are used in a vast range of global appliances and systems, from smart cards and wireless devices to mobile services and e-Commerce. Qusay H. Mahmoud has created an invaluable reference tool that explores the origins and current uses of middleware (highlighting the importance of such technologies as CORBA, J2EE and JMS) and has thus compiled the roadmap to future research in this area. Middleware for Communications: discusses the emerging fields of Peer-to-Peer (P2P) and grid middleware detailing middleware platforms such as JXTA and the Globus middleware toolkit. shows how Middleware will play a significant role in mobile computing. presents a Platform Supporting Mobile Applications (PLASMA) - a middleware platform that consists of components for location, event, and profile handling of Location-Based Services. introduces middleware security focusing on the appropriate aspects of CORBA, J2EE, and .NET and demonstrates how to realize complex security capabilities such as role-based access control (RBAC) and mandatory access control (MAC). discusses how Quality of Service (QoS) component middleware can be combined with Model Driven Architecture (MDA) technologies to rapidly develop, generate, assemble and deploy flexible communications applications. This incomparable overview of middleware for communications is suitable for graduate students and researchers in communications and computing departments. It is also an authoritative guide for engineers and developers working on distributed systems, mobile computing and networked appliances.

Umar provides a collection of powerful services to support the e-business andm-business

initiatives of today and tomorrow. (Computer Books)

Public-key Cryptography provides a comprehensive coverage of the mathematical tools required for understanding the techniques of public-key cryptography and cryptanalysis. Key topics covered in the book include common cryptographic primitives and symmetric techniques, quantum cryptography, complexity theory, and practical cryptanalytic techniques such as side-channel attacks and backdoor attacks.Organized into eight chapters and supplemented with four appendices, this book is designed to be a self-sufficient resource for all students, teachers and researchers interested in the field of cryptography.

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.

Smart Card Application Development Using Java

Cryptographic Hardware and Embedded Systems - CHES 2000

Smart Card Research and Advanced Applications

ECIW2010-Proceedings of the 9th European Conference on Information Warfare and Security

EUC 2006 Workshops: NCUS, SecUbiq, USN, TRUST, ESO, and MSA, Seoul, Korea, August 1-4, 2006, Proceedings

Encyclopedia of Computer Science and Technology

In today's world, smart cards play an increasingly important role in everyday life. We encounter them as credit cards, loyalty cards, electronic purses, health cards, and as secure tokens for authentication or digital signature. Their small size and the compatibility of their form with the magnetic stripe card make them the ideal carriers of personal information such as secret keys, passwords, customization profiles, and medical emergency information. This book provides a guide for the rapid development of smart card applications using Java and the OpenCard Framework. It gives you the basic information you need about smart cards and how they work. It shows in detail how to develop applications that use smart cards by guiding you through examples step by step. A smart card provided along with the book will help you to quickly get some first hands-on experience. Das Buch bietet erstmals einen Leitfaden zur Entwicklung von Smartcard-Anwendungen mit Java (JDK ab Version 1.1.6) und OCF 1.1.1 auf dem Computer, sowie zur Entwicklung von Java Applets, die direkt auf einer Karte (Java Card) ausgeführt werden. Der erste Teil führt konzise in Grundlagen, Technologie und Anwendungsmöglichkeiten von Smartcard ein. Im zweiten Teil werden Ziel, Konzept, Architektur und Komponenten des OpenCard Framework detailliert beschrieben. Der dritte Teil demonstriert anhand einfacher Beispiele Aufbau und Design komplexer Anwendungen für den Karten- und den Host-Teil. Mit der beiliegenden Multi Function Card lassen sich die beschriebenen Beispiele leicht ausführen und weiterentwickeln.

Communications and Multimedia Security is an essential reference for both academic and professional researchers in the fields of Communications and Multimedia Security. This state-of-the-art volume presents the proceedings of the Eighth Annual IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, September 2004, in Windermere, UK. The papers presented here represent the very latest developments in security research from leading people in the field. The papers explore a wide variety of subjects including privacy protection and trust negotiation, mobile security, applied cryptography, and security of communication protocols. Of special interest are several papers which addressed security in the Microsoft .Net architecture, and the threats that builders of web service applications need to be aware of. The papers were a result of research sponsored by Microsoft at five European University research centers. This collection will be important not only for multimedia security experts and researchers, but also for all teachers and administrators interested in communications security.

A practical guide to the specification, design, and programming of smart card systems for working applications. More than 3 billion smartcards are produced every year. Generally defined as any pocket-sized card with embedded integrated circuits or chips, they have a huge number of applications including travel cards, chip and pin cards, pet tags, mobile phone SIMs and pallet trackers. Now with modern Smart Card technology such as Java Card and Basic Card it is possible for everyone to create his or her own applications on a smart card. This book provides generic solutions for programming smart cards, enabling the creation of working applications and systems. Key features: Presents a comprehensive introduction to the topic of smart cards, explaining component elements and the smart card microcontrollers. Sets out information on operating systems with case studies of a range of applications including credit card security, mobile phones and transport payment cards. Gives detailed advice on the monitoring of smart card applications, recognizing potential attacks on security and improving system integrity. Provides modules and examples so that all types of systems can be built up from a small number of individual components. Offers guidelines on avoiding and overcoming design errors. Ideal for practising engineers and designers looking to implement smart cards in their business, it is also a valuable reference for postgraduate students taking courses on embedded system and smart card design.

Security is probably the most critical factor for the development of the "Information Society". E-government, e-commerce, e-healthcare and all other e-activities present challenging security requirements that cannot be satisfied with current technology, except maybe if the citizens accept to waive their privacy, which is unacceptable ethically and socially. New progress is needed in security and privacy-preserving technologies. On these foundations, the IFIP/SEC conference has been established from the eighties as one of the most important forums for presenting new scientific research results as well as best professional practice to improve the security of information systems. This balance between future technology improvements and day-to-day security management has contributed to better understanding between researchers, solution providers and practitioners, making this forum lively and fruitful. Security and Protection in Information Processing Systems contains the papers selected for presentation at the 19th IFIP International Conference on Information Security (SEC2004), which was held in August 2004 as a co-located conference of the 18th IFIP World Computer Congress in Toulouse, France. The conference was sponsored by the International Federation for Information Processing (IFIP).This volume is essential reading for scholars, researchers, and practitioners interested in keeping pace with the ever-growing field of information security.

Cyber Crime: Concepts, Methodologies, Tools and Applications
Smart Card Research and Advanced Applications VI
Design and Development
Proceedings
8th IFIP WG 8.8/11.2 International Conference, CARDIS 2008, London, UK, September 8-11, 2008, Proceedings
Smart Card Handbook
RFIDsec'13 Asia Workshop Proceedings

With Smart Card Programming the reader will have the expert guidance he need to work with smart cards. The book offers a comprehensive guide, to the technological aspects related to smart cards, providing an high level overview of the technological panorama and giving an in-depth technical coverage about the related architectures, programming paradigms and APIs. The first part of the book introduces the smart card technologies, the general concepts and a few case studies. It is addressed also to non-technical reader who wishes an high level overview on smart card world. The second part of the book is a technical guide to smart card specifications and programming paradigms. It dives into technical topics about smart card programming and applications development in C/C++, C#, Visual Basic and Java. Key features include: - Contact and Contactless Cards - ISO 7816 - NFC - JavaCard Framework - PC/SC - PKCS#11 - OpenCard Framework - Java - Smart Card I/O - GlobalPlatform - EMV

This book constitutes the thoroughly refereed post-proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2000, held in Worcester, MA, USA in August 2000. The 25 revised full papers presented together with two invited contributions were carefully reviewed and selected from 51 submissions. The papers are organized in topical sections on implementation of elliptic curve cryptosystems, power and timing analysis attacks, hardware implementation of block ciphers, hardware architectures, power analysis attacks, arithmetic architectures, physical security and cryptanalysis, and new schemes and algorithms.

This book constitutes the proceedings of the 19th International Conference on Smart Card Research and Advanced Applications, CARDIS 2020, which took place during November 18-20, 2020. The conference was originally planned to take place in Lübeck, Germany, and changed to an online format due to the COVID-19 pandemic. The 12 full papers presented in this volume were carefully reviewed and selected from 26 submissions. They were organized in topical sections named: post-quantum cryptography; efficient implementations; and physical attacks.

Smart Card HandbookJohn Wiley & Sons
An Introduction to Kolmogorov Complexity and Its Applications
Middleware for Communications
Fundamentals of Information Technology (Third Edition)
Third International Conference, CARDIS'98 Louvain-la-Neuve, Belgium, September 14-16, 1998 Proceedings
Smart Cards, Tokens, Security and Applications
Smart Card Applications
8th IFIP TC-6 TC-11 Conference on Communications and Multimedia Security, Sept. 15-18, 2004, Windermere, The Lake District, United Kingdom

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.

Smart cards have been driven by the need for a secure, portable, computing platform. Hence it is no surprise that security considerations dominated their research. The CARDIS conferences were created to provide a forum for this research. CARDIS 1998 is the third international conference on Smart Card Research and Advanced Applications, held in Louvain-la-Neuve, Belgium, 14-16 Sept- ber 1998. The ?rst CARDIS was held in Lille, France in November 1994, and the second was held in Amsterdam, The Netherlands in September 1996. The fourth CARDIS is scheduled to take place in Bristol, UK in September 2000 (http://www.cardis.org). This volume contains the refereed papers presented at CARDIS 1998. These 35 papers were ?rst published in a pre-proceedings and distributed to the - tendees at the conference; they have subsequently been revised and updated for this volume. The papers discuss all aspects of smart-card research: Java cards, elect- nic commerce applications, e?ciency, security (including cryptographic al- rithms, cryptographic protocols, and authentication), and architecture. Subm- sions from Europe, the U.S., Asia, and Australia show that this is indeed an international area of research, and one that is becoming more popular as pr- tical demand for smart cards increase. We wish to thank the Program Committee members who did an excellent job in reviewing papers and providing feedback to the authors.

The explosive demand for mobile communications is driving the development of wireless technology at an unprecedented pace. Unfortunately, this exceptional growth is also giving rise to a myriad of security issues at all levels-from subscriber to network operator to service provider. Providing technicians and designers with a critical and comprehens

This book constitutes the refereed proceedings of the EUC 2005 workshops held in conjunction with the IFIP International Conference on Embedded and Ubiquitous Computing, EUC 2005, in Nagasaki, Japan in December 2005.The 132 revised full papers presented were carefully reviewed and selected from 352 submissions. Topics covered by the five workshops are ubiquitous intelligence and smart worlds (UISW 2005), network-centric ubiquitous systems (NCUS 2005), security in ubiquitous computing systems (SecUbiq 2005), RFID and ubiquitous sensor networks (USN 2005), and trusted and autonomic ubiquitous and embedded systems (TAUES 2005).

Second International Conference, ICESS 2005, Xi'an, China, December 16-18, 2005, Proceedings

Embedded and Ubiquitous Computing - EUC 2005 Workshops

Official (ISC)2 Guide to the CISSP CBK, Third Edition

Third Generation Distributed Computing Environments

Emerging Directions in Embedded and Ubiquitous Computing

Architecture and Programmer's Guide

Security of Mobile Communications

This volume constitutes the refereed proceedings of the 7th International Conference on Smart Card Research and Advanced Applications, CARDIS 2006, held in Tarragona, Spain, in April 2006. The 25 revised full papers presented were carefully reviewed and updated for inclusion in this book. The papers are organized in topical sections on smart card applications, side channel attacks, smart card networking, cryptographic protocols, RFID security, and formal methods.

This book constitutes the refereed proceedings of the 9th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Application, CARDIS 2010, held in Passau, Germany, in April 2010. The 16 revised full papers presented were carefully reviewed and selected from numerous submissions. The papers are organized in topical sections on mathematical algorithms; side channel analysis; systems; logical attacks; fault analysis; and privacy.

Since1994,CARDIShasbeentheforemostinternationalconferencededicatedto smart card research and applications. Every two years, the scienti?c community congregates to present new ideas and discuss recent developments with both an academicandindustrialfocus.Followingtheincreasedcapabilitiesofsmartcards anddevices,CARDIS has becomea majoreventfor the discussionofthe various issuesrelatedtotheuseofsmallelectronictokensintheprocessofhuman-machine interactions.Thescopeoftheconferenceincludesnumeroussub?eldssuchasn-working,e?cientimplementations,physicalsecurity,biometrics,andso on. This year's CARDIS was held in London, UK, on September 8–11, 2008. It was organized by the Smart Card Centre, Information Security Group of the Royal Holloway, University of London. Thepresentvolumecontainsthe21papersthatwereselectedfromthe51s- missions to the conference. The 22 members of the program committee worked hard in order to evaluate each submission with at least three reviews and agree on a high quality ?nal program. Additionally, 61 external reviewers helped the committee with their expertise. Two invited talks completed the technical p- gram. The ?rst one, given by Ram Banerjee and Anki Nelaturu, was entitled "Getting Started with Java Card 3.0 Platform". The second one, given by Aline Gouget, was about "Recent Advances in Electronic Cash Design" and was c- pleted by an abstract provided in these proceedings.

Here are the refereed proceedings of the EUC 2006 workshops, held in conjunction with the IFIP International Conference on Embedded and Ubiquitous Computing in Seoul, Korea, August 2006. The book presents 102 revised papers spanning six workshops: network-centric ubiquitous systems (NCUS 2006), security in ubiquitous computing systems (SecUbiq 2006), RFID and ubiquitous sensor networks (USN 2006), trustworthiness, reliability and services in ubiquitous and sensor networks (TRUST 2006), embedded software optimization (ESO 2006), and multimedia solution and assurance in ubiquitous information systems (MSA 2006).

Embedded Software and Systems

Concepts, Methodologies, Tools and Applications

7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006, Tarragona, Spain, April 19-21, 2006, Proceedings

IFIP 18th World Computer Congress TC8/WG8.8 & TC11/WG11.2 Sixth International Conference on Smart Card Research and Advanced Applications (CARDIS) 22–27 August 2004 Toulouse, France

RFID Handbook

Encyclopedia of Multimedia Technology and Networking, Second Edition

Communications and Multimedia Security

This Festschrift volume, published in honor of Jean-Jaques Quisquater on the occasion of his 65th Birthday, contains 33 papers from colleagues all over the world and deals with all the fields to which Jean-Jaques dedicated his work during his academic career. Focusing on personal tributes and re-visits of Jean-Jaques Quisquater's legacy, the volume addresses the following central topics: symmetric and asymmetric cryptography, side-channels attacks, hardware and implementations, smart cards, and information security. In addition there are four more contributions just "as diverse as Jean-Jacques' scientific interests".

This book provides readers with an overview to the design of multiapplication smart card environments including the selection of a platform, the creation of applications and the logistics of initial deployment.

Provides information on designing effective security mechanisms for e-commerce sites, covering such topics as cryptography, authentication, information classification, threats and attacks, and certification.

In the Information Society, the smart card, or smart device with its processing power and link to its owner, will be the potential human representation or delegate in Ambient Intelligence (Pervasive Computing), where every appliance or computer will be connected, and where control and trust of the personal environment will be the next decade challenge. Smart card research is of increasing importance as the need for information security grows rapidly. Smart cards will play a very large role in ID management in secure systems. In many computer science areas, smart cards introduce new dimensions and opportunities. Disciplines like hardware design, operating systems, modeling systems, cryptography and distributed systems find new areas of applications or issues; smart cards also create new challenges for these domains. CARDIS, the IFIP Conference on Smart Card Research and Advanced Applications, gathers researchers and technologists who are focused in all aspects of the design, development, deployment, validation and application of smart cards or smart personal devices.This volume contains the 20 papers that have been selected by the CARDIS Program Committee for presentation at the 6th International Conference on Smart Card Research and Advanced Applications (CARDIS 2004), which was held in conjunction with the IFIP 18th World Computer Congress in Toulouse, France in August 2004 and sponsored by the International Federation for Information Processing (IFIP). With 20% of the papers coming from Asia, 20% from America, and 60% from Europe, the competition was particularly severe this year, with only 20 papers selected out of 45 very good submissions. Smart Card Research and Advanced Applications VI presents the latest advances in smart card research and applications, and will be essential reading for developers of smart cards and smart card applications, as well as for computer science researchers in computer architecture, computer security, and cryptography.

Advances in Cryptology - CRYPTO '89

Theory and Practice

EUC 2005 Workshops: UISW, NCUS, SecUbiq, USN, and TAUES, Nagasaki, Japan, December 8-9, 2005

Cryptography and Security: From Theory to Applications

Revealing the Secrets of Smart Cards

This book constitutes the thoroughly refereed post-conference proceedings of the 10th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications, CARDIS 2011, held in Leuven, Belgium, in September 2011. The 20 revised full papers presented were carefully reviewed and selected from 45 submissions. The papers are organized in topical sections on smart cards system security, invasive attacks, new algorithms and protocols, implementations and hardware security, non-invasive attacks, and Java card security.

The most comprehensive book on state-of-the-art smart card technology available Updated with new international standards and specifications, this essential fourth edition now covers all aspects of smart card in a completely revised structure. Its enlarged coverage now includes smart cards for passports and ID cards, health care cards, smart cards for public transport, and Java Card 3.0. New sub-chapters cover near field communication (NFC), single wire protocol (SWP), and multi megabyte smart cards (microcontroller with NAND-Flash). There are also extensive revisions to chapters on smart card production, the security of smart cards (including coverage of new attacks and protection methods), and contactless card data transmission (ISO/IEC 10536, ISO/IEC 14443, ISO/IEC 15693). This edition also features: additional views to the future development of smart cards, such as USB, MMU, SWP, HCI, Flash memory and their usage; new internet technologies for smart cards; smart card web server, HTTP-Protocol, TCP/IP, SSL/TSL; integration of the new flash-based microcontrollers for smart cards (until now the usual ROM-based microcontrollers), and; a completely revised glossary with explanations of all important smart card subjects (600 glossary terms). Smart Card Handbook is firmly established as the definitive reference to every aspect of smart card technology, proving an invaluable resource for security systems development engineers. Professionals and microchip designers working in the smart card industry will continue to benefit from this essential guide. This book is also ideal for newcomers to the field. The Fraunhofer Smart Card Award was presented to the authors for the Smart Card Handbook, Third Edition in 2008.