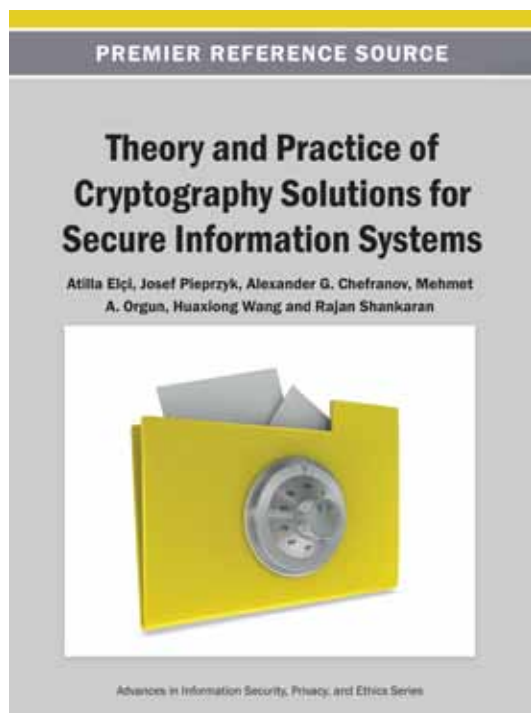


An Excellent Addition to Your Library!

Released: May 2013

Theory and Practice of Cryptography Solutions for Secure Information Systems



ISBN: 9781466640306; © 2013; 351 pp.

Print: US \$195.00 | Perpetual: US \$295.00 | Print + Perpetual: US \$390.00

Pre-pub Discount:*

Print: US \$185.00 | Perpetual: US \$280.00

* Pre-pub price is good through one month after publication date.

Part of the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

Atilla Elçi (Aksaray University, Turkey), Josef Pieprzyk (Macquarie University, Australia), Alexander G. Chefranov (Eastern Mediterranean University, North Cyprus), Mehmet A. Orgun (Macquarie University, Australia), Huaxiong Wang (Nanyang Technological University, Singapore) and Rajan Shankaran (Macquarie University, Australia)

Information Systems (IS) are a nearly omnipresent aspect of the modern world, playing crucial roles in the fields of science and engineering, business and law, art and culture, politics and government, and many others. As such, identity theft and unauthorized access to these systems are serious concerns.

Theory and Practice of Cryptography Solutions for Secure Information Systems explores current trends in IS security technologies, techniques, and concerns, primarily through the use of cryptographic tools to safeguard valuable information resources. This reference book serves the needs of professionals, academics, and students requiring dedicated information systems free from outside interference, as well as developers of secure IS applications. This book is part of the Advances in Information Security, Privacy, and Ethics series collection.

Topics Covered:

- Agent and Multi-Agent System Security
- Authentication and Authorization
- Copyright Protection
- Cryptographic Protocols
- Cryptography and Security
- Data Protection
- Engineering Secure Information Systems
- Forensics and Ethical Hacking
- Key Management
- Privacy of Information Systems

Market: This premier publication is essential for all academic and research library reference collections. It is a crucial tool for academicians, researchers, and practitioners. Ideal for classroom use.

Atilla Elçi is full professor and chairman of the Department of Electrical and Electronics Engineering at Aksaray University, Aksaray, Turkey, since August 2012. He was full professor and chairman of computer and educational technology at Süleyman Demirel University, Isparta, Turkey (May 2010 - June 2012). He served as full professor of computer engineering, the founding director of the Graduate School of Science and Technology, and the dean of Engineering Faculty at Toros University, Mersin, Turkey (July 2010 - June 2011); with the Computer Engineering Program, Middle East Technical University (METU NCC, Spring 2010); Eastern Mediterranean University (2003-2009) where he established the Internet Technologies Research Center and semantic robotics lab; Haliç University, Istanbul, Turkey, founder and chair of the Computer Engineering Department (2000-2003); the International Telecommunication Union, Geneva, Switzerland, as chief technical advisor (1985-1997); METU Ankara, Turkey, where he was chair and assistant chair of Computer Engineering Department (1976-1985); Purdue University, W. Lafayette, Indiana, USA, as research assistant (1974-5). He has organized or served in the committees of numerous international conferences. He has been organizing IEEE Engineering Semantic Agent Systems Workshops since 2006, Security of Information and Networks Conferences since 2007; and, IJRCs Symposiums 2007&9. He has published over a hundred journal and conference papers; edited the book titled *Semantic Agent Systems* (Springer 2011), *Theory and Practice of Cryptography Solutions for Secure Information Systems* (IGI 2013); proceedings of SIN 2007, 9 - 12 by ACM, ESAS 2006-12 by IEEE CS, and IJRCs 2009; special issues. He was the program chair for the 36th COMPSAC (2012). He obtained B.Sc. in Computer/Control Engineering at METU, Ankara, Turkey (1970), M.Sc. & Ph.D. in Computer Sciences at Purdue University, USA (1973, 1975). Website: His research and experience encompass web semantics, agent-based systems, robotics, machine learning, knowledge representation and ontology, information security, software engineering, and natural language translation.



www.igi-global.com

Publishing Academic Excellence
at the Pace of Technology Since 1988

Section 1: Cryptographic Methods Analysis

Chapter 1

Ontology-Based Analysis of Cryptography Standards and Possibilities of Their Harmonization
Atiskov Alexey Y. (St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, Russia)
Novikov Fedor A. (St. Petersburg State Polytechnical University, Russia)
Fedorchenko Ludmila N. (St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, Russia)
Vorobiev Vladimir I. (St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, Russia)
Moldovyan Nickolay A. (St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences, Russia)

Chapter 2

GOST Encryption Algorithm and Approaches to its Analysis
Babenko Ludmila (Southern Federal University, Russia)
Ishchukova Evgeniya (Southern Federal University, Russia)
Maro Ekaterina (Southern Federal University, Russia)

Chapter 3

Cryptography for the Forensics Investigator
Martin Thomas (Khalifa University, UAE)

Chapter 4

Search in Encrypted Data:
Tang Qiang (University of Luxembourg, Luxembourg)

Section 2: Cryptographic Systems

Chapter 5

Encryption Schemes with Hyper-Complex Number Systems and Their Hardware-Oriented Implementation
Doukhnich Evgueni (Istanbul Aydin University, Turkey)
Chefranov Alexander G. (Eastern Mediterranean University, North Cyprus)
Mahmoud Ahmed (Al-Azhar University-Gaza, Palestine)

Chapter 6

Design Time Engineering of Side Channel Resistant Cipher Implementations
Barengi Alessandro (Politecnico di Milano, Italy)
Breveglieri Luca (Politecnico di Milano, Italy)
De Santis Fabrizio (Technische Universität München, Germany)
Melzani Filippo (STMicroelectronics, Italy)
Palomba Andrea (Politecnico di Milano, Italy)
Pelosi Gerardo (Politecnico di Milano, Italy)

Section 3: Cryptographic Solutions for Distributed Systems

Chapter 7

An Efficient Attribute-Based Signature with Application to Secure Attribute-Based Messaging System
Yang Piyi (University of Shanghai for Science and Technology, China)
Zia Tanveer A (Charles Sturt University, Australia)

Chapter 8

Secure Neighbor Discovery:
AlSa'deh Ahmad (Hasso-Plattner-Institute, Germany)
Rafice Hosnich (Hasso-Plattner-Institute, Germany)
Meinel Christoph (Hasso-Plattner-Institute, Germany)

Chapter 9

Offline/Online Security in Mobile Ad Hoc Networks
Hsin Wen-Jung (Park University, USA)
Harn Lein (University of Missouri – Kansas City, USA)

Chapter 10

A Survey on Security in Wireless Sensor Networks:
Korkmaz Ilker (Izmir University of Economics, Turkey)
Dagdeviren Orhan (Ege University, Turkey)
Tekbaeck Fatih (Izmir Institute of Technology, Turkey)
Dalkilic Mehmet Emin (Ege University, Turkey)

Section 4: Cryptographic Trust Solutions

Chapter 11

Secure Multiparty Computation via Oblivious Polynomial Evaluation
Özazar Mert (Middle East Technical University, Turkey)
Özgit Attila (Middle East Technical University, Turkey)

Chapter 12

PKI Trust Models
Josang Audun (University of Oslo, Norway)

Chapter 13

Entity Authentication and Trust Validation in PKI Using Petname Systems
Ferdous Md. Sadek (University of Glasgow, UK)
Josang Audun (University of Oslo, Norway)

Chapter 14

Building a Trusted Environment for Security Applications
Cabiddu Giovanni (Politecnico di Torino, Italy)
Lioy Antonio (Politecnico di Torino, Italy)
Ramunno Gianluca (Politecnico di Torino, Italy)

Chapter 15

Enhancing Security at Email End Point:
Sokouti Babak (Tabriz University of Medical Sciences, Iran)
Sokouti Massoud (Shahid Beheshti University, Iran)

Section 5: Engineering Secure Information Systems

Chapter 16

Cryptography in Electronic Mail
Rafice Hosnich (Hasso Plattner Institute, Germany)
von Löwis Martin (Hasso Plattner Institute, Germany)
Meinel Christoph (Hasso Plattner Institute, Germany)

Chapter 17

Theory and Practice of Secure E-Voting Systems
Peng Kun (Institute for Infocomm Research, Singapore)

Chapter 18

Sealed-Bid Auction Protocols
Peng Kun (Institute for Infocomm Research, Singapore)

Chapter 19

Preserving the Privacy of Patient Records in Health Monitoring Systems
Elkhodr Mahmoud (University of Western Sydney, Australia)
Shahrestani Seyed (University of Western Sydney, Australia)
Cheung Hon (University of Western Sydney, Australia)

Order Your Copy Today!

Name: _____

Organization: _____

Address: _____

City, State, Zip: _____

Country: _____

Tel: _____

Fax: _____

E-mail: _____

Enclosed is check payable to IGI Global in
US Dollars, drawn on a US-based bank

Credit Card Mastercard Visa Am. Express

3 or 4 Digit Security Code: _____

Name on Card: _____

Account #: _____

Expiration Date: _____