Premier Reference Source

Multidisciplinary Perspectives in Cryptology and Information Security

IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE

Sattar B. Sadkhan Al Maliky and Nidaa A. Abbas

Multidisciplinary Perspectives in Cryptology and Information Security

Sattar B. Sadkhan Al Maliky
University of Babylon, Iraq

Nidaa A. Abbas
University of Babylon, Iraq

A volume in the Advances in Information Security, Privacy, and Ethics (AISPE) Book Series

Information Science
REFERENCE
An Imprint of IGI Global

Managing Director:	Lindsay Johnston
Production Editor:	Jennifer Yoder
Development Editor:	Erin O'Dea
Acquisitions Editor:	Kayla Wolfe
Typesetter:	John Crodian
Cover Design:	Jason Mull

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Multidisciplinary perspectives in cryptology and information security / Sattar B. Sadkhan Al Maliky and Nidaa A. Abbas, editors.
pages cm
Includes bibliographical references and index.
ISBN 978-1-4666-5808-0 (hardcover) -- ISBN 978-1-4666-5809-7 (ebook) -- ISBN 978-1-4666-5811-0 (print & perpetual access) 1. Data encryption (Computer science) 2. Wireless communication systems--Security measures. 3. Computer networks--Security measures. I. Al Maliky, Sattar B. Sadkhan, 1954- editor of compilation. II. Abbas, Nidaa A. editor of compilation.
QA76.9.A25M846 2014
005.8'2--dc23

2014011686

This book is published in the IGI Global book series Advances in Information Security, Privacy, and Ethics (AISPE) (ISSN: 1948-9730; eISSN: 1948-9749)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

For electronic access to this publication, please contact: eresources@igi-global.com.

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

ISSN: 1948-9730
EISSN: 1948-9749

Mission

As digital technologies become more pervasive in everyday life and the Internet is utilized in ever increasing ways by both private and public entities, concern over digital threats becomes more prevalent.

The **Advances in Information Security, Privacy, & Ethics (AISPE) Book Series** provides cutting-edge research on the protection and misuse of information and technology across various industries and settings. Comprised of scholarly research on topics such as identity management, cryptography, system security, authentication, and data protection, this book series is ideal for reference by IT professionals, academicians, and upper-level students.

Coverage

- Access Control
- Device Fingerprinting
- Global Privacy Concerns
- Information Security Standards
- Network Security Services
- Privacy-Enhancing Technologies
- Risk Management
- Security Information Management
- Technoethics
- Tracking Cookies

IGI Global is currently accepting manuscripts for publication within this series. To submit a proposal for a volume in this series, please contact our Acquisition Editors at Acquisitions@igi-global.com or visit: http://www.igi-global.com/publish/.

The Advances in Information Security, Privacy, and Ethics (AISPE) Book Series (ISSN 1948-9730) is published by IGI Global, 701 E. Chocolate Avenue, Hershey, PA 17033-1240, USA, www.igi-global.com. This series is composed of titles available for purchase individually; each title is edited to be contextually exclusive from any other title within the series. For pricing and ordering information please visit http://www.igi-global.com/book-series/advances-information-security-privacy-ethics/37157. Postmaster: Send all address changes to above address. The views expressed in this series are those of the authors, but not necessarily of IGI Global.

Titles in this Series

For a list of additional titles in this series, please visit: www.igi-global.com

Cases on Research and Knowledge Discovery Homeland Security Centers of Excellence
Cecelia Wright Brown (University of Baltimore, USA) Kevin A. Peters (Morgan State University, USA) and Kofi Adofo Nyarko (Morgan State University, USA)
Information Science Reference • copyright 2014 • 357pp • H/C (ISBN: 9781466659469) • US $215.00 (our price)

Multidisciplinary Perspectives in Cryptology and Information Security
Sattar B. Sadkhan Al Maliky (University of Babylon, Iraq) and Nidaa A. Abbas (University of Babylon, Iraq)
Information Science Reference • copyright 2014 • 334pp • H/C (ISBN: 9781466658080) • US $245.00 (our price)

Analyzing Security, Trust, and Crime in the Digital World
Hamid R. Nemati (The University of North Carolina at Greensboro, USA)
Information Science Reference • copyright 2014 • 281pp • H/C (ISBN: 9781466648562) • US $195.00 (our price)

Research Developments in Biometrics and Video Processing Techniques
Rajeev Srivastava (Indian Institute of Technology (BHU), India) S.K. Singh (Indian Institute of Technology (BHU), India) and K.K. Shukla (Indian Institute of Technology (BHU), India)
Information Science Reference • copyright 2014 • 279pp • H/C (ISBN: 9781466648685) • US $195.00 (our price)

Advances in Secure Computing, Internet Services, and Applications
B.K. Tripathy (VIT University, India) and D.P. Acharjya (VIT University, India)
Information Science Reference • copyright 2014 • 405pp • H/C (ISBN: 9781466649408) • US $195.00 (our price)

Security Engineering Techniques and Solutions for Information Systems Management and Implementation
Noureddine Boudriga (Engineering School of Communications, Tunisia) and Mohamed Hamdi (Engineering School of Communications, Tunisia)
Information Science Reference • copyright 2014 • 359pp • H/C (ISBN: 9781615208036) • US $195.00 (our price)

Trust Management in Mobile Environments Autonomic and Usable Models
Zheng Yan (Xidian University, China and Aalto University, Finland)
Information Science Reference • copyright 2014 • 288pp • H/C (ISBN: 9781466647657) • US $195.00 (our price)

Network Security Technologies Design and Applications
Abdelmalek Amine (Tahar Moulay University, Algeria) Otmane Ait Mohamed (Concordia University, USA) and Boualem Benatallah (University of New South Wales, Australia)
Information Science Reference • copyright 2014 • 330pp • H/C (ISBN: 9781466647893) • US $195.00 (our price)

Editorial Advisory Board

Chapter 1 provides an introduction to the disciplinary, multidisciplinary, and their general structure (interdisciplinary, trans-disciplinary, and cross-disciplinary). It also gives an introduction to the applications of the multidisciplinary approaches to some of the cryptology and information security fields.

Chapter 2 contains a survey of current and proposed spam-filtering techniques with particular emphasis on how well they work. The primary focus is spam-filtering in email, but the role of the spam filter is only one component of a large and complex information universe.

Chapter 3 aims to emphasize the multidisciplinary nature of the research in the field of Quantum Key Distribution Networks (QKDNs). Such networks consist of a number of nodes that can perform security protocols protected by some basic laws of physics. The operation of QKDNs requires the integration of Quantum Key Distribution (QKD) protocols with the already-existing network security infrastructures.

Chapter 4 reviews most of the encryption techniques that adopt chaos-based cryptography and illustrates the use of chaos-based voice encryption techniques in wireless communication as well. The review in this chapter summarizes the traditional and modern techniques of voice/speech encryption and demonstrates the feasibility of adopting chaos-based cryptography for wireless communications.

Chapter 5 shows the progress of cryptography based on error-correcting codes. In contrast to the number-theoretic problems typically used in cryptography nowadays, certain instances of the underlying problems (the code-based cryptography problem) remain unbroken, even when employing quantum cryptanalysis. The chapter surveys the more recent developments in code-based cryptography as well as implementations and side channel attacks. This work also recalls briefly the basic ideas and provides a roadmap to readers.

Chapter 6 provides a "security evaluation method based on fuzzy logic" for pseudo-random sequences used (mainly) in stream cipher systems. The designed Fuzzy rules consider two main parameters, which are the length of the maximum period of the key sequence obtained from Linear Feedback Shift Register (LFSR) and the entropy of the result in sequences obtained from different lengths of the shift registers.

Chapter 7 introduces nano and bio techniques in cryptography to enhance the information security systems. Tasks unfeasible on a classical computer can now be performed by quantum computers and could have a big impact on online security. Threats of exponentially fast quantum algorithms on business transactions could be overcome by this new technology. Based on biological observations, the exploration of biometric cryptography and authentication to determine individuals' authenticity can be done through numeric measurements.

Chapter 8 provides Independent Component Analysis (ICA) and Principal Component Analysis (PCA) as categories of the Blind Source Separation (BSS)-based method for encrypting images and speech, since the encryption technologies depend on many intractable mathematical problems. Using key signals, the authors build a suitable BSS underdetermined problem in the encryption and then circumvent this problem with key signals for decoding.

Chapter 9 presents a new area-efficient composite field inverter of the form $GF(q^l)$ with $q = 2^{n.m}$ suitable for the hardware realization of an Elliptic Curve (EC) cryptosystem. Considering both the security aspect and the hardware cost required, the authors propose the utilization of the composite field $GF(((2^2)^2)^{41})$ for EC cryptosystem.

Chapter 10 provides illustration of the variants of RSA-Public Key Cryptosystems based on quadratic equations in finite field, describing their key generation, encryption, and decryption processes. In addition, the chapter illustrates a proposed general formula for the equation describing these different types and a proposed generalization for the Chinese Remainder Theorem.

Chapter 11 describes the real-world problems related to cryptographic key distribution and management and presents existing solutions as well as future directions in their solving. The chapter presents the cryptographic key management and distribution problems from a multidisciplinary point of view by looking at its economic, psychological, usability, and technological aspects.

Chapter 12 offers an overview of new developments in quasigroup-based cryptography, especially of new defined quasigroup-based block ciphers and stream ciphers, hash functions and message-authentication codes, PRNGs, public key cryptosystems, etc. Special attention is given to Multivariate Quadratic Quasigroups (MQQs) and MQQ public key schemes, because of their potential to become one of the most efficient pubic key algorithms today.

Chapter 13 presents a comprehensive study on the influence of the intra-modal facial information for an identification approach. A biometric identification system was developed and implemented by merging different intra-multimodal facial features: mouth, eyes, and nose. The principal component analysis, independent component analysis, and discrete cosine transform were used as feature extractors.

Chapter 14 focuses on biometrics (types and technologies), personal identification, and specifications, and then how to implement these performances in security. Two approached are proposed: a novel thinning algorithm for fingerprint recognition and a novel e-passport based on personal identification.

Chapter 15 shows the three security metrics that have been derived from important issues of network security. Each metric demonstrates the level of achievement in preserving one of the security goals. Routing algorithms based on these metrics have been implemented to test the proposed solution. Computational effort and blocking probability were used to assess the behavior and the performance of these routing algorithms.

Chapter 16 highlights the virtues of volatile memory analysis by demonstrating how key material and passphrases can be extracted from memory and reconstructed to facilitate the analysis of encrypted data. The chapter also shows current methods for identifying encryption keys in memory and discusses possible defeating techniques and cryptosystem implementation strategies that could be used to avoid the key extraction.

The book can be considered as an introduction on multidisciplinary aspects and their importance in implementation of the new methods and algorithms designed for cryptography, cryptanalysis, and complexity evaluation of the designed algorithms. It improves the ability to process and manage information and knowledge-related processes in order to create new knowledge. In the fields of information security, information transmission, knowledge security management, cryptology, etc., there exists a need for an edited collection of articles in this area.

Sattar B. Sadkhan Al Maliky
University of Babylon, Iraq

Nidaa A. Abbas
University of Babylon, Iraq

Acknowledgment

The editors of the book *Multidisciplinary Prospective in Cryptology and Information Security* would like to thank to all authors for their ideas and the excellent work in their chapters. We appreciate the originality of their works. Moreover, we would like to express our deep appreciation to the editorial advisory board for their excellent review of the book chapter. The editors acknowledge the remarkable collaboration and the efforts of all the reviewers to ensure the technical quality of this book.

Finally, this book is the result of great teamwork. For this reason, we would like to thank all the efforts of IGI Global.

Sattar B. Sadkhan Al Maliky
University of Babylon, Iraq

Nidaa A. Abbas
University of Babylon, Iraq

Table of Contents

Detailed Table of Contents

To reach the high depths of knowledge and expertise that are required nowadays, scientists focus their attention on minute areas of study. However, the most complex problems faced by scientists still need the application of different disciplines to tackle them, which creates a necessity for multi-disciplinary collaboration. Cryptology is naturally a multidisciplinary field, drawing techniques from a wide range of disciplines and connections to many different subject areas. In recent years, the connection between algebra and cryptography has tightened, and established computational problems and techniques have been supplemented by interesting new approaches and ideas. Cryptographic engineering is a complicated, multidisciplinary field. It encompasses mathematics (algebra, finite groups, rings, and fields), probability and statistics, computer engineering (hardware design, ASIC, embedded systems, FPGAs), and computer science (algorithms, complexity theory, software design), control engineering, digital signal processing, physics, chemistry, and others. This chapter provides an introduction to the disciplinary, multidisciplinary, and their general structure (interdisciplinary, trans-disciplinary, and cross-disciplinary). And it also gives an introduction to the applications of the multidisciplinary approaches to some of the cryptology fields. In addition, the chapter provides some facts about the importance of the suitability and of the multidisciplinary approaches in different scientific, academic, and technical applications.

This chapter deals with using soft computing methods in information security. It is engaged in two big areas: (1) information security and spam detection and (2) cryptography. The latter field is covered by a proposal of an artificial neural network application, which represents a way of further development in this area. Such a neural network can be practically used in the area of cryptography. It is a new approach, which presents a development of automatic neural networks design. The approach is based on

Blind Source Separation (BSS) represented by Independent Component Analysis (ICA) has been used in many fields such as communications and biomedical engineering. Its application to image and speech encryption, however, has been rare. In this chapter, the authors present ICA and Principal Component Analysis (PCA) as a category of BSS-based method for encrypting images and speech by using Blind Source Separation (BSS) since the security encryption technologies depend on many intractable mathematical problems. Using key signals, they build a suitable BSS underdetermined problem in the encryption and then circumvent this problem with key signals for decoding. The chapter shows that the method based on the BSS can achieve a high level of safety right through building, mixing matrix, and generating key signals.

This chapter presents a new area-efficient composite field inverter of the form GF(q1) with q=2n.m suitable for the hardware realization of an elliptic curve (EC) cryptosystem. Considering both the security aspect and the hardware cost required, the authors propose the utilization of the composite field GF(((22)2)41) for EC cryptosystem. For efficient implementation, they have derived a compact inversion circuit over GF(2164)=GF(((22)2)41) to achieve an optimal saving in the hardware cost required. Furthermore, the authors have also developed a composite field digit serial Sunar-Koc multiplier for the multiplication in the extension field. All of the arithmetic operations in the subfield GF(24) are performed in its isomorphic composite field, GF((22)2), leading to a full combinatorial implementation without resorting to the conventional look-up table approach. To summarize the work, the final hardware implementation and the complexity analysis of the inversion is reported towards the end of this chapter.

The importance of Public Key Cryptosystems (PKCs) in the cryptography field is well known. They represent a great revolution in this field. The PKCs depend mainly on mathematical problems, like factorization problem, and a trapdoor one-way function problem. Rivest, Shamir, and Adleman (RSA) PKC systems are based on factorization mathematical problems. There are many types of RSA cryptosystems. Rabin's Cryptosystem is considered one example of this type, which is based on using the square order (quadratic equation) in encryption function. Many cryptosystems (since 1978) were implemented under such a mathematical approach. This chapter provides an illustration of the variants of RSA-Public Key Cryptosystems based on quadratic equations in Finite Field, describing their key generation, encryption, and decryption processes. In addition, the chapter illustrates a proposed general formula for the equation describing these different types and a proposed generalization for the Chinese Remainder Theorem.

It is important to know that absolute security does not exist, and the main goal of the security system is to reach an optimal approach that satisfies the customer requirements. Biometrics is a small part of the security system that aims to replace a traditional password or a key. Biometrics offer higher security levels by simply ensuring that only the authorized people have access to sensitive data. It is easy to copy or get a traditional password using different methods (legal or illegal), but it is difficult to copy a key of biometric pattern such as iris or fingerprint or other patterns. Recent years have seen a boom in the use of biometric techniques in the design of modern equipment to maintain the information and personal identification. This chapter focuses on biometrics (types and technologies), personal identification, and specifications, and then how to implement these performances in security. Finally, a future aspect of merging technologies and disciplines is a good issue to treat via a specific concentration of information technology. In this chapter, two approached are proposed: a novel thinning algorithm for fingerprint recognition and a novel e-passport based on personal identification.

Even though it is an essential requirement of any computer system, there is not yet a standard method to measure data security, especially when sending information over a network. However, the most common technique used to achieve the three goals of security is encryption. Three security metrics are derived from important issues of network security in this chapter. Each metric demonstrates the level of achievement in preserving one of the security goals. Routing algorithms based on these metrics are implemented to test the proposed solution. Computational effort and blocking probability are used to assess the behavior and the performance of these routing algorithms. Results show that the algorithms are able to find feasible paths between communicating parties and make reasonable savings in the computational effort needed to find an acceptable path. Consequently, higher blocking probabilities are encountered, which is the price to be paid for such savings.

The increasing portability of computing devices combined with frequent reports of privacy breaches and identity theft has thrust data encryption into the public attention. While encryption can help mitigate the threat of unintentional data exposure, it is equally capable of hiding evidence of criminal malfeasance. The increasing accessibility and usability of strong encryption solutions present new challenges for digital forensic investigators. Understanding forensic analysis as a multidisciplinary field that searches evidence of crime, the authors focus their topic on particularity of cross-disciplinary issues arising in this area: Forensic analysis uses cryptology, information technology and mathematics in extracting encryption keys from memory. The chapter highlights the virtues of volatile memory analysis by demonstrating how key material and passphrases can be extracted from memory and reconstructed to facilitate the analysis of encrypted data. The authors show current methods for identifying encryption keys in memory and discuss possible defeating techniques and cryptosystem implementation strategies that could be used to avoid the key extraction.