



Topics in Coding, Cryptography and Information Security

Editors:

Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa



IIUM PRESS

2011



Topics in Coding, Cryptography and Information Security

Editors:

**Mohammad Umar Siddiqi
Sigit Puspito Wigati Jarot
Othman Omran Khalifa**



**IIUM Press
2011**

Published by:
IIUM Press
International Islamic University Malaysia

First Edition, 2011
©IIUM Press, IIUM

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without any prior written permission of the publisher.

Perpustakaan Negara Malaysia

Cataloguing-in-Publication Data

Mohammad Umar Siddiqi, Sigit Puspito Wigati Jarot and Othman Omran
Khalifa: Topics in Coding, Cryptography and Information Security

ISBN: 978-967-418-169-7

Member of Majlis Penerbitan Ilmiah Malaysia – MAPIM
(Malaysian Scholarly Publishing Council)

Printed by :
IIUM PRINTING SDN. BHD.
No. 1, Jalan Industri Batu Caves 1/3
Taman Perindustrian Batu Caves
Batu Caves Centre Point
68100 Batu Caves
Selangor Darul Ehsan

Topics in Coding, Cryptography and Information Security

Contents

| | |
|------------------------|----|
| List of Contributors | ii |
| Editorial Introduction | vi |

PART I: SOURCE CODING

| | |
|--------------------------------------------------------------------------------------|----|
| 1. Performance Analysis of Image Data Compression using Zero-Tree Wavelet Transform | 2 |
| <i>Othman O. Khalifa, Emir Tabakovic, Zlatko Memisevic and Aisha-Hassan Abdullah</i> | |
| 2. Scalable and Robust Streaming Video System Challenges | 12 |
| <i>Othman O. Khalifa, Sinzobakwira Issa and Mohammad Umar Siddiqi</i> | |

PART II: CHANNEL CODING

| | |
|--------------------------------------------------------------------|----|
| 3. Golay Codec: An Overview | 23 |
| <i>Othman O. Khalifa</i> | |
| 4. Reed-Muller Codes: An Overview | 35 |
| <i>Othman O. Khalifa</i> | |
| 5. Viterbi Decoder: A Review and Implementation | 42 |
| <i>Noorainani Ainina Bt. Md Noor Albakri and Othman O. Khalifa</i> | |

| | | |
|-----|---------------------------------------------------------------------------------------------------------------|-----|
| 6. | Zigzag Codes: High Rate Low Complexity Iterative Codes <i>Sigit P.W. Jarot</i> | 53 |
| 7. | Convolutional Coded OFDM in Broadband Mobile Communication <i>Sigit P.W. Jarot</i> | 66 |
| 8. | Channel Coding Techniques in Mobile Communication Systems <i>Othman O. Khalifa and Rashid A. Saeed</i> | 77 |
| 9. | Channel Coding in CDMA 2000 <i>Othman O. Khalifa</i> | 85 |
| 10. | Channel Coding in Mobile WiMAX <i>Rashid A. Saeed and Othman O. Khalifa</i> | 91 |
| 11. | Turbo Codes: An Error Correction Technique for 4G <i>Mosharraf Hussain Masud and Mohammad Umar Siddiqi</i> | 99 |
| 12. | Combined Source Channel Decoding for Image Transmission over Noisy Channels <i>Jalel Chebil</i> | 108 |

PART III: CRYPTOGRAPHY AND INFORMATION SECURITY

| | | |
|-----|-----------------------------------------------------------------------------------------------------------------------------------|-----|
| 13. | Cryptographic Boolean Functions: Transform Domain Perspective <i>Hashum Mohamed Rafiq and Mohammad Umar Siddiqi</i> | 120 |
| 14. | Implementation of RSA Algorithm <i>Hafizul Azizi Rasid, Mohd Azmi Jabar and Othman O. Khalifa</i> | 141 |
| 15. | GSM Security: Problems and Solutions <i>Rashid A. Saeed and Othman O. Khalifa</i> | 152 |
| 16. | Recent Approaches to Wireless Physical Layer Security <i>M. Tahir, Sigit P.W. Jarot and M.U. Siddiqi</i> | 161 |
| 17. | Securing OFDM-based Systems from the Physical Layer <i>Sigit P.W. Jarot</i> | 169 |
| 18. | Simulation of Artificial Noise based Physical Layer Security <i>Muhammad Izzat bin Zurkiple and Sigit Puspito Wigati Jarot</i> | 174 |

19. Secure IPv6 Address Generation 183
Nashrul Hakiem, Mohammad Umar Siddiqi, and Sigit Puspito Wigati Jarot
20. Video Streaming and Encrypting Algorithms 190
Mohammed Abumuala, Othman O. Khalifa, and Aisha-Hassan A. Hashim
21. Wireless IP Camera based on Motion Detection Surveillance System 217
Zeeshan Shahid and Khaizuran Abdullah
22. Design of Mobile Phone Jammer 223
Fauzum Abdullah Asuhaimi, Nur Fatin Mohd Zakki, and Khaizuran Abdullah

Index

Chapter 14

Implementation of RSA Algorithm

Hafizul Azizi Rasid, Mohd Azmi Jabar and Othman O. Khalifa

14.1. Introduction

14.1.1. Background

The algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman at Massachusetts Institutes of Technology (MIT). The letters RSA are the initials of their surnames. Originally, it was invented at a Passover Seder in Schenectady, New York. Clifford Cocks is a British mathematician working for one of the United Kingdom intelligence agency known as GCHQ, as a head mathematician. He described an equivalent system in an internal document in 1973, but given the relatively expensive computers needed to implement it at that time. It was mostly considered a curiosity invention and it was never deployed as far as publicly known. However, his discovery was not revealed until 1997 due to its top secret classification and Rivest, Shamir and Adleman formulated RSA independently of Cocks' work.

MIT was granted US patent 4405829 for a "Cryptographic communications system and method" that used the algorithm in 1983. The patent expired on 21 September 2000. Since a paper describing the algorithm had been published in August 1977, prior to the December 1977 filing date of the patent application, regulations in much of the rest of the world prohibited patents elsewhere and only the United States patent was granted. Had Cocks' work been publicly known, a patent in the United States would not have been possible either [2].

14.1.2. Problem

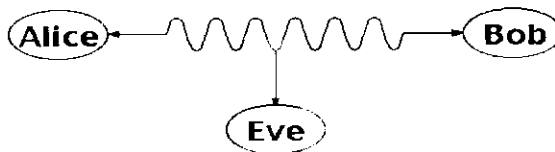


Fig.14. 1: Illustration of Alice-Bob communication