



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 <i>Othman O. Khalifa, Emir Tabakovic, Zlatko Memisevic and Aisha-Hassan Abdullah</i>	2
2. Scalable and Robust Streaming Video System Challenges <i>Othman O. Khalifa, Sinzobakwira Issa and Mohammad Umar Siddiqi</i>	12

PART II: CHANNEL CODING

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

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 16

Recent Approaches to Wireless Physical Layer Security

M. Tahir, Sigit P.W. Jarot and M.U. Siddiqi

16.1. Introduction

Although the layered approach to communication system design, as corresponds to the general Open Systems Interconnection (OSI) reference model, is often referred to in the design of network security protocols, the resulting protocols tend to be layer-specific and ignore the most fundamental of communication layers—the physical layer, whereby devices communicate over a wireless or wired medium. This means that the approaches taken to secure modern communication systems are incomplete. Figure 16.1 illustrates the various layers considered in a typical wireless communication protocol, and indicates their specific security measure employed at each level. For instance, cryptographic tools are used at application layer, which focuses on making the data unintelligible, and admission control is handled at the Medium Access Control (MAC) layer using WEP or WPA. Wireless systems face very specific security vulnerabilities caused by the inherent openness of wireless media.

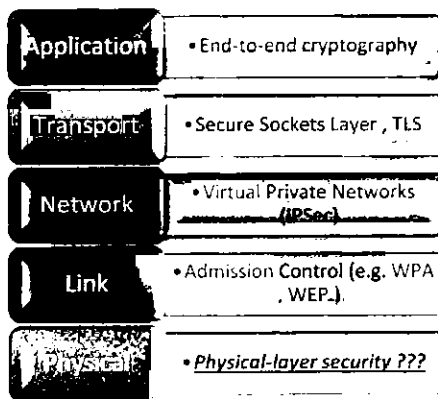


Fig.16. 1: Layered communication architecture from security point of view.

First, wireless channels are susceptible to channel jamming. An attacker can easily jam physical communication channels and prevent legitimate users from ac-