



---

# **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 17

## Securing OFDM-based Systems from the Physical Layer

Sigit P.W. Jarot

### 17.1. Introduction

Mobile communication industry has been growing at an unexpectedly rapid pace in last decade, much faster than all predictions, and it is expected that the growth will continue and accelerate at least over this decade. Orthogonal Frequency Division Multiplexing (OFDM) is one of the most promising choices for air interfaces. Many standards have been official selected OFDM for the physical layer solution such as LTE, 802.11, WiMax, etc. The widespread use of OFDM in those standards will survive at least in the coming decades of evolution of all that standards.

On the other hands, in recent years, there is increasing attention to an emerging research area that explores the possibility of achieving perfect-secrecy for data transmission among intended network, known as *physical layer security*. In the beginning, research on physical layer security is more on the information theoretical aspects such as: secrecy capacity in wiretap channel models, wireless secret key agreement, and wireless secret codes. However, some recent approaches have been shifting toward more practical physical layer security, such as the possibility of implementations in OFDM systems, the anechoic-chamber experimentations, and so on. In this chapter, we will be discussing about several approaches of securing physical layer in OFDM-based systems.

### 17.2. Typical OFDM System Model

A system model of Convolutional Coded OFDM considered is depicted in Figure 17.1. At the transmitter, the binary information data symbols are encoded using channel code. The encoded sequence is serial-to-parallel (S/P) converted into a number of parallel sequences, which equals to the number of subcarriers. In each parallel stream, the data symbols are. Pilot symbols are time-multiplexed to the data sequence to form a packet. Frequency interleaving is applied to the parallel sequences, in order to decrease fading correlation between adjacent parallel sequences, namely between successive symbols. The interleaved sequence is applied to Inverse Fast Fourier Transform (IFFT), to generate OFDM symbol. Guard interval is inserted between successive OFDM symbols to avoid inter-symbol interference. Then, the signals are transmitted over multipath fading channel.