

SELECTED TOPICS IN ADVANCED ELECTRONICS

Edited by
Khalid A. S. Al-Khateeb



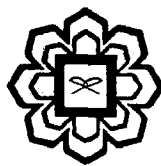
IIUM Press

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

SELECTED TOPICS IN ADVANCED ELECTRONICS

Edited by

Khalid A. S. Al-Khateeb



IIUM Press
International Islamic University Malaysia
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

Khalid A. S. Al-Khateeb: Selected Topics in Advanced Electronics

ISBN: 978-967-418-153-6

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
Tel: +603-6188 1542 / 44 / 45 Fax: +603-6188 1543
EMAIL: iiumprinting@yahoo.com

SELECTED TOPICS IN
ADVANCED ELECTRONICS

CONTENTS

Chapter 1	1
WIRELESS CONNECTIVITY OF PC PERIPHERALS USING ULTRAWIDE BAND (UWB) PULSES	
Khalid A. S. Al-Khateeb and Ahmed Ramzi Mohammed	
Chapter 2	11
VOLTAGE CONTROLLED OSCILLATOR FOR STANDARD GSM USING MEMS	
Khalid A. S. Al-Khateeb	
Chapter 3	23
MEMS SURFACE ACOUSTIC WAVES OSCILLATOR	
Jamilah Karim, Anis Nurashikin Nordin and AHM Zahirul Alam	
Chapter 4	37
USING MEMS IN CLASS D AMPLIFIERS FOR STANDARD GSM CARRIER	
Khalid A. S. Al-Khateeb	
Chapter 5	52
MEMS CAPACITIVE ULTRASONIC TRANSDUCERS	
Khalid A. S. Al-Khateeb	
Chapter 6	57
DESIGN OF MEMS CANTILEVER ENERGY HARVESTER	
Anis Nurashikin Nordin and Aliza Aini Md Ralib	
Chapter 7.....	67
THEORY OF QUANTUM CRYPTOGRAPHY	
Ali Sallami and Khalid A. S. Al-Khateeb	
Chapter 8.....	77
QUANTUM KEY DISTRIBUTION PROTOCOLS	
Ali Sallami and Khalid A. S. Al-Khateeb	

Chapter 9.....	84
FPGA CONTROL OF QUANTUM CHANNEL SECURITY	
Khalid A. S. Al-Khateeb and Mohammed Munther A. Majeed	
Chapter 10.....	97
THE DECOY STATE METHOD IN QUANTUM KEY DISTRIBUTION	
Ali Sallami, Khalid A. S. Al-Khateeb and Mohamad Ridza Wahiddin	
Chapter 11.....	120
EAVESDROPPING ATTACKS ON QKD CHANNELS	
Ali Sallami and Khalid A. S. Al-Khateeb	
Chapter 12.....	126
SECURITY PERFORMANCE OF QKD	
Sellami Ali and Khalid A. S. Al-Khateeb	
Chapter 13.....	132
THEORETICAL ANALYSIS OF A DOUBLE STAGES ERBIUM DOPED FIBER AMPLIFIER	
Khalid A. S. Al-Khateeb and M. A. Mohammed	
Chapter 14.....	142
THEORY OF ERBIUM DOPED FIBER LASERS (EDFLS) AND ERBIUM DOPED FIBER AMPLIFIERS (EDFAS)	
Sallami Ali and Khalid A. S. Al-Khateeb	
Chapter 15	175
ERBIUM DOPED FIBER LASERS WITH DOUBLE TUNABLE BANDPASS FILTER	
Ali Sallami, Khalid Al-Khateeb and Bouzid Billoui	
Chapter 16.....	181
ERBIUM DOPED FIBER AMPLIFIER WITH A QUADRUPLE PASS	
Sellami Ali, Khalid A. S. Al-Khateeb and Bouzid Billoui	
Chapter 17.....	189
TRANSPARENT ELECTRODES FOR OPTOELECTRONIC DISPLAYS	
Khalid A. S. Al-Khateeb	
Chapter 18.....	201
EPITAXIAL GROWTH OF THIN ZnS FILMS	
Khalid A. S. Al-Khateeb	
Chapter 19.....	211
MODERN ELEECTRONIC DISPLAY SYSTEMS	
Khalid A. S. Al-Khateeb and Moaaz Elhag Ali	

Chapter 20.....	230
AVALANCHE PHOTO DIODES AS SINGLE PHOTON DETECTORS	
Khalid A. S. Al-Khateeb	
Chapter 21.....	243
COOLING TECHNIQUES FOR SINGLE PHOTON AVALANCHE DIODE	
Nurul Fadzlin Hasbullah, Nurul Izzati Samsuddin and Salmiah Ahmad	
Chapter 22.....	256
SUPERVISORY CONTROL AND DATA AQUISITION SYSTEM (SCADA)	
USING MICROCONTROLLER	
Khalid A. S. Al-Khateeb and Mohamad Azman Shah	
Chapter 23.....	268
ELECTRONIC REMOTE MONITORING OF INDUSTRIAL SYSTEMS	
Khalid A. S. Al-Khateeb	
Chapter 24.....	276
MEDICAL CARE SYSTEM FOR REMOTE MONITORING OF FOETAL	
ECG	
Khalid A. S. Al-Khateeb and Mohammed I. Ibrahimy	
Chapter 25.....	287
INTELLIGENT AUTO TRACKING IN 3D SPACE BY IMAGE	
PROCESSING	
Khalid A. S. Al-Khateeb and Othman O. Khalifa	
Chapter 26.....	300
CIRCUIT DESIGN FOR RADIO FREQUENCY IDENTIFICATION	
DEVICES (RFID)	
Aisyah Jaafar, Nurul Syuhadah Izwar Arfani and Othman O. Khalifa	
Chapter 27.....	309
DYNAMIC TRAFFIC LIGHT SEQUENCE ALGORITHM USING RFID	
Khalid A. S. Al-Khateeb, Jaiz A.Y. Johari and Wajdi F. Al-Khateeb	
Chapter 28.....	326
ADVANCED RFID SECURITY FRAMEWORK FOR DYNAMIC TRAFFIC	
MANAGEMENT	
Khalid A. S. Al-Khateeb, Jaiz A. Y. Johari	
Chapter 29.....	337
MODELING CMOS WAFER PRODUCTION LINE USING PROMODEL	
SOFTWARE	
Khalid A. S. Al-Khateeb and Khairul Hakim B. Zainiddin	

Chapter 30.....	348
ASIC DESIGN FLOW	
Sreedharan Baskara Dass, Aisha_Hassan A. Hashim and Loay Faisal	
Chapter 31.....	355
ELECTRONIC DESIGN AUTOMATION TOOLS	
Sreedharan Baskara Dass, Aisha_Hassan A. Hashim and Loay Faisal	
Chapter 32.....	365
CIRCUIT DESIGN OF A CLOCK DATA RECOVERY	
Z. M. Ashari and Anis N. Nordin	
Chapter 33.....	376
EFFECTS OF NEUTRON IRRADIATION ON VARIOUS ELECTRONIC DEVICES	
Nuurul Iffah Che Omar and Nurul Fadzlin Hasbullah	
Chapter 34.....	384
NEUTRON SOURCE AND NEUTRON SHIELDING	
Nuurul Iffah Che Omar and Nurul Fadzlin Hasbullah	
Chapter 35.....	390
QUANTUM DOTS AS A SOLUTION TO RADIATION HARDNESS	
Nuurul Iffah Che Omar and Nurul Fadzlin Hasbullah	

CHAPTER 11

EAVESDROPPING ATTACKS ON QKD CHANNELS

By

¹Ali Sallami and ²Khalid A. S. Al-Khateeb

¹Department of Science in Engineering

²Department of Electrical and Computer Engineering

Kulliyah of Engineering

International Islamic University Malaysia

Gombak, Selangor, Malaysia

Synopsis

For the security of QKD, it is crucial to determine as precisely as possible the amount of information that might have leaked to Eve. Its knowledge allows Alice and Bob to choose such security parameter t that privacy amplification will safely obliterate Eve's information on the distilled key. Let us first take a closer look at two simple attacks that Eve could mount, intercept/resend and beam splitting.

1. Introduction

One of the most formidable tasks to safeguard against intruder attacks on secure messaging systems is to recognize the technique used by the attacker. The attacker on the other hand will also try to avoid being detected. One of the methods used by the attackers is to intercept the message and resend it to mislead the corresponding parties that their channel of communications is safe. Another method would be to steal part of the signals carrying the message by beam splitting. Of course there is variety of other methods and techniques.

It is customary in the security of messaging systems to refer to the intruder or eavesdropper as (Eve), to the sender as (Alice) and the receiver as (Bob).