SELECTED TOPICS IN
ADVANCED ELECTRONICS

Edited by
Khalid A. S. Al-Khateeb

IIUM Press
International Islamic University Malaysia
2011
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 Ramli

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)
Sellami 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 ELECTRONIC DISPLAY SYSTEMS
Khalid A. S. Al-Khateeb and Moaaz Elhag Ali
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 10

THE DECOY STATE METHOD IN QUANTUM KEY DISTRIBUTION

By

1Ali Sallami, 2Khalid A. S. Al-Khateeb and 3Mohamad Ridza Wahiddin

1Department of Science in Engineering
2Department of Electrical and Computer Engineering
Kulliyyah of Engineering
and
3Department of Computer Science
Kulliyyah of Information and Communications Technology
International Islamic University Malaysia
Gombak, Selangor, Malaysia

Synopsis

Single photon sources may be useful for quantum computing, but they are rather impractical for QKD. Attenuated light pulses are more useful as signals in practical QKD systems. However employing attenuated pulses instead of perfect single photons brings another attack strategy; the photon-number splitting (PNS) attacks [125,126,127]. This does not apply only to pulse schemes, but affects all sources, which have a finite probability of emitting multiple photons. If all the signal photons are emitted with the same qubit encoding, Eve can steal a copy of the information without Alice and Bob noticing it.

The beam splitting attack is based on the concept that a lossy quantum channel can be described as a combination of a lossless channel and a beam splitter. The photons of the incoming signal states are redirected statistically to Eve and Bob. In principle, Eve could arrange an eavesdropping method by first measuring the number of photons in each pulse without disturbing the degree of freedom encoding the qubits using a quantum non-demolition measurement. The measurement does not perturb the qubit, and does not destroy the photons. The measurement is performed in the photon number Hilbert space.