SELECTED TOPICS IN ADVANCED ELECTRONICS

Edited by

Khalid A. S. Al-Khateeb

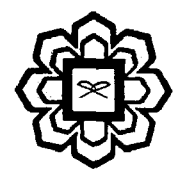
IIUM Press

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

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 9
FPGA CONTROL OF QUANTUM CHANNEL SECURITY

By

Khalid A. S. Al-Khateeb and Mohammed Munther A. Majeed
Department of Electrical and Computer Engineering
Kulliyyah of Engineering
International Islamic University Malaysia
Gombak, Selangor, Malaysia

Synopsis

Quantum Security can be established when two parties generate Quantum Bits (qubits) simultaneously by using different quantum states. The control process of the security protocol is based on the natural inviolability of the laws of quantum mechanics. An adversary can neither successfully tap the transmission nor evade detection. The viability of such a system is proven. There is already hardware, which has been designed, implemented and tested successfully in the laboratory. It is however not fully commercialized although filed patents are pending. Some practically viable systems are already in existence. The implementation of these systems has demonstrated that a secure free space quantum optical link can be established. The control hardware is based on a specially adapted FPGA. The sender end uses FPGA to control the settings of the quantum states. A built in random generator facilitates the generation of a random sequence of bits, which is non repeatable. This is in contrast with the pseudo-random sequence, whose code can soon be broken irrespective how complicated it may be, due to the ever increasing speed and computing capacity. The pulse timing and the detector gating procedures prevent eavesdropping from compromising the security and hence authentication is established.

1. Introduction

The privacy of communications has interested communicating parties since the beginning of time. Therefore, the massages that involve secret exchange of information were