SELECTED TOPICS IN ADVANCED ELECTRONICS

Edited by

Khalid A. S. Al-Khateeb

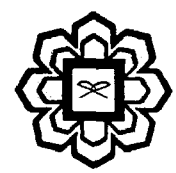
IIUM Press

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 12

SECURITY PERFORMANCE OF QKD

By

Sellami Ali and Khalid A. S. Al-Khateeb
[1]Department of Science in Engineering
[2]Department of Electrical and Computer Engineering
Kulliyyah of Engineering
International Islamic University Malaysia
Gombak, Selangor, Malaysia

Synopsis

The goal of quantum key distribution (QKD) is to enable two distant parties, conventionally called ***Alice*** and ***Bob***, to establish a common ***secret key***, which is a string of random bits, which are unknown to an adversary, ***Eve***. The most important difference between QKD and classical key distribution (CKD) schemes is that the security of the final key of the QKD can actually be proven. The number of logical assumptions that have to be made is very limited. The strong reasoning that backs the notion of ***unconditional security*** is the guarantee that an adversary does not get any information correlated with the key, except with negligible probability. A weaker level of security is computational security, which is difficult to break i.e. time-consuming, but not impossible. This kind of security is typically sought-after in classical cryptographic algorithms.

1. Introduction

With the huge revolution in the speed and computational capacity, if ***Alice*** and ***Bob*** are connected by a classical authenticated communication channel alone, secret communication and thus the generation of a secret key is impossible [25]. This changes dramatically when quantum mechanics form the basis for the security scheme. Bennett and Brassard were the first to introduce a quantum key distribution scheme, which uses a