SELECTED TOPICS IN ADVANCED ELECTRONICS

Edited by

Khalid A. S. Al-Khateeb

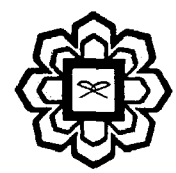
IIUM Press

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 11

EAVESDROPPING ATTACKS ON QKD CHANNELS

By
[1]Ali Sallami and [2]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

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 steel 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).