



UNIVERSITI PUTRA MALAYSIA

**QUANTUM KEY DISTRIBUTION PROTOCOLS IN TRANSMISSION
CONTROL PROTOCOL**

NUR HANANI BINTI KAMARUL AIZAN

FSKTM 2012 4

**QUANTUM KEY DISTRIBUTION PROTOCOLS IN TRANSMISSION
CONTROL PROTOCOL**

NUR HANANI BINTI KAMARUL AIZAN

MASTER OF SCIENCE

UNIVERSITI PUTRA MALAYSIA

2012

**QUANTUM KEY DISTRIBUTION PROTOCOLS IN TRANSMISSION
CONTROL PROTOCOL**

By

NUR HANANI BINTI KAMARUL AIZAN

**Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in
Fulfillment of the Requirements for the Degree of Master Science**

January 2012

To my parents...

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

**QUANTUM KEY DISTRIBUTION PROTOCOLS IN TRANSMISSION
CONTROL PROTOCOL**

By

NUR HANANI BINTI KAMARUL AIZAN

January 2012

Chairman : Zuriati Ahmad Zukarnain, PhD

Faculty : Faculty of Computer Science and Information Technology

A quantum key distribution (QKD) system produced shared secret key and transmitted the key between the sender and receiver in a highly secured transmission. QKD uses the fundamental of quantum properties of a single photon to provide a secured communication channel with absolute security guaranteed by the laws of physics.

This research has developed a simulator software for BB84 and B92 protocols which implemented both protocols in 802.11i WLAN environment. The parameters used for this research are with attack and without attack, where measured by three measurements for both protocols which are final key length, expected key length by eavesdropper and error rate estimation. The 802.11i WLAN is consider as insecure because the tendency to be intercepted by intruders is high. Furthermore, the interference from other consumer devices such as cordless phone and microwave can contribute to degradation of WLAN performance. This type of noise can generate different numbers of final key length and

different levels of error rate estimation. Thus, the level of the error rate estimation determined the secrecy of the secret key. The discussion of security issue between BB84 and B92 protocols also discussed in terms of secrecy and strength of the secret key between both protocols in 802.11i WLAN.



Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

**PROTOKOL PENGAGIHAN KEKUNCI KUANTUM DALAM PROTOKOL
KAWALAN PENGHANTARAN**

Oleh

NUR HANANI BINTI KAMARUL AIZAN

Januari 2012

Pengerusi : Zuriati Ahmad Zukarnain, PhD

Fakulti : Fakulti Sains Komputer dan Teknologi Maklumat

Satu sistem penyebaran kunci kuantum (QKD) boleh menghasilkan perkongsian kunci rahsia dan menghantar kunci di antara pengirim dan penerima di dalam transmisi keselamatan yang tinggi. QKD menggunakan asas sifat kuantum foton tunggal untuk menyediakan satu saluran komunikasi yang selamat dengan keselamatan mutlak yang dijamin selamat oleh undang-undang fizik.

Kajian ini telah membangunkan perisian simulasi untuk protokol BB84 dan B92 yang mana kedua-dua protokol ini dilaksanakan dalam persekitaran WLAN 802.11i.

Parameter yang digunakan untuk kajian ini adalah dengan serangan dan tanpa serangan, di mana ianya diukur oleh tiga jenis pengukur bagi kedua-dua protokol seperti saiz panjang akhir kunci, anggaran saiz kunci yang berjaya diperoleh oleh pengancam dan anggaran kadar kesilapan yang berlaku semasa komunikasi sedang berlaku 802.11i WLAN dikatakan tidak selamat kerana kecenderungannya untuk dipintas oleh

penceroboh adalah tinggi. Tambahan pula, gangguan dari peranti pengguna yang lain seperti telefon tanpa wayar dan gelombang mikro boleh menyumbang kepada kemerosotan prestasi WLAN. Gangguan jenis ini boleh menghasilkan bilangan panjang akhir kunci yang berbeza dan perbezaan tahap anggaran kadar kesilapan. Oleh itu, tahap anggaran kadar kesilapan menentukan kekuatan kerahsiaan kunci rahsia. Perbincangan isu keselamatan antara BB84 dan B92 protokol juga dibincangkan dari segi kerahsiaan dan kekuatan kunci rahsia antara kedua-dua protokol dalam 802.11i WLAN.

ACKNOWLEDGEMENTS

Praise to God for all the things throughout my voyage of knowledge exploration to complete this research.

I would like to express my sincere gratitude to my supervisor Associate Professor Dr. Zuriati Ahmad Zukarnain and also my supervisory committee members Associate Professor Dr. Hishamuddin Zainuddin for their guidance and advices throughout this work to make it successful.

My deepest appreciation to my family especially my parents for their utmost support and encouragement without them all these would not be possible. Last but not least, many thanks and appreciation to Mohd Amirza b. Kamarudin for helping me with a lot of ideas, motivations and encouragements during the research.

Thanks to all who have directly or indirectly helped me in the completion of my works.

I certify that a Thesis Examination Committee has met on (the date of viva voce) to conduct the final examination of Nur Hanani Kamarul Aizan on her thesis entitled “Implementation of BB84 and B92 Protocols on 802.11i WLAN” in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Name of Chairperson, PhD
Title (e.g. Professor/Associate Professor/ Ir)
Name of Faculty
University Putra Malaysia
(Chairman)

Name of Examiner 1, PhD
Title (e.g. Professor/Associate Professor/ Ir)
Name of Faculty
University Putra Malaysia
(Internal Examiner)

Name of Examiner 2, PhD
Title (e.g. Professor/Associate Professor/ Ir)
Name of Faculty
University Putra Malaysia
(Internal Examiner)

Name of External Examiner 1, PhD
Title (e.g. Professor/Associate Professor/ Ir)
Name of Department and/or Faculty
Name of Organization (University/Institute)
Country
(External Examiner)

Bujang Kim Huat, PhD
Professor and Deputy Dean
School of Graduate Studies
University Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirement for the degree of Master of Science. The members of the Supervisory Committee were as follows:

Zuriati Ahmad Zukarnain, PhD

Associate Professor

Faculty of Computer Science and Information Technology

University Putra Malaysia

(Chairman)

Hishamuddin Zainuddin, PhD

Associate Professor

Faculty of Science

Universiti Putra Malaysia

(Member)

BUJANG BIN KIM HUAT, PhD

Professor and Dean

School of Graduate Studies

University Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations, which have been duly acknowledged. I also declare that it has not been previously, and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or other institutions.

NUR HANANI BINTI KAMARUL AIZAN

Date: 15 January 2012

TABLE OF CONTENTS

	Page
DEDICATION	ii
ABSTRACT	iii
ABSTRAK	v
ACKNOWLEDGEMENTS	vii
APPROVAL	viii
DECLARATION	x
LIST OF TABLES	xiv
LIST OF FIGURES	xv
LIST OF ABBREVIATIONS	xvii

CHAPTER

1	INTRODUCTION	1
1.1	Cryptographic System before Quantum Cryptography	2
1.2	Introduction to Quantum Cryptography	3
1.3	Problem Statement	4
1.4	Research Objectives	5
1.5	Research Scope	5
1.6	Contribution of Research	6
1.7	Organization of Thesis	6
2	LITERATURE REVIEW	
2.1	Introduction	8
2.2	Fundamental of Classical Cryptography	8
2.2.1	Data Encryption Standard (DES)	9
2.2.2	One-Time Pad	11
2.2.3	Diffie-Hellman Key Exchange	12

2.3	Fundamental of Quantum Cryptography	14
2.4	QKD Protocols	14
2.4.1	BB84 Protocol	15
2.4.2	B92 Protocol	18
2.5	Error Rate Estimation	20
2.6	Error Correction and Privacy Amplification	22
2.7	IEEE 802.11i WLAN Overview	25
2.7.1	Wireless LAN Operating Mode	26
2.7.2	WLAN Security	28
2.7.3	IEEE 802.11i Components	28
2.7.4	Signals and Noise on WLAN	31
2.8	Related Research on QKD in Wireless Network	32
2.9	Summary	41
3	RESEARCH METHODOLOGY	
3.1	Introduction	42
3.2	QKD Simulator	42
3.2.1	Software Structure	43
3.3	Testbed Architecture	45
3.4	The Internal Structure of QKD Protocol	46
3.4.1	Testbed Process of QKD Protocol on 802.11i WLAN	47
3.5	Performance Parameters	57
3.6	Summary	59
4	RESULTS AND DISCUSSION	
4.1	Introduction	60
4.2	Benchmarking of QKD Protocol Simulator	60
4.3	BB84 and B92 Protocols on 801.11i WLAN	62
4.4	Result and Analysis	63
4.4.1	Error Rate Estimation of BB84 and B92 Protocols	63

4.4.2	Eavesdropper's Expected Key Length of BB84 and B92 Protocols	66
4.4.3	Final Key Length of BB84 and B92 Protocols	68
4.4.4	Percentage of Wireless Interference	70
4.5	Summary	74
5	CONCLUSION	
5.1	Conclusion	76
5.2	Recommendation for Future Works	77
	REFERENCES	79
	BIODATA OF STUDENT	82
	LIST OF PUBLICATIONS	83