

**Quantum Cryptography for Secure Communication in
IEEE 802.11 Wireless Networks**

Shirantha Wijesekera

Faculty of Information Sciences and Engineering

University of Canberra ACT 2601

A thesis submitted in fulfilment of the requirements of the

Degree of Doctor of Philosophy

June 2011

Abstract

IEEE 802.11 is the Wireless Local Area Networks (WLAN) standard developed by the IEEE LAN/MAN Standards Committee. WLANs are increasingly deployed by businesses, government and SOHO users as they offer many advantages to customers with mobility, flexibility and convenience. Wi-Fi is a trademark of the Wi-Fi Alliance that has been used with certified products that belong to a class of WLANs based on the IEEE 802.11 standards. WLANs have become one of the widely used communication systems in the world. It is estimated that there are over 4,00,000 hotspots and millions of Wi-Fi users across the world as of now.

Since there are no boundaries in wireless networks, they are more vulnerable to security threats than their wired counterparts. It is possible for an attacker to snoop on confidential communications or modify them to gain access to the wireless networks more easily. Therefore, providing secure communication for wireless networks has become one of the prime concerns. IEEE has made amendments to the initial release of 802.11 standard with the 2004 release of 802.11i, since the former version was found to having security weaknesses in the way it handles authentication and privacy.

Quantum Key Distribution (QKD), based on quantum cryptography, offers the promise of unconditional security. QKD enables two parties to distribute a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages.

This research implements a novel method of integrating QKD to distribute the secret key in WLANs. IEEE 802.11i standard uses a *4 way handshake* procedure to distribute the key used to encrypt the data communication. In this research, instead of using the 4 way handshake procedure, QKD based key distribution for IEEE 802.11 has been implemented targeting the Counter mode with CBC-MAC Protocol (CCMP) of the Robust Security Network Association (RSNA). Necessary communication flows of existing IEEE 802.11 protocol have been indentified and modified. These modifications are done in such a way that only some of the selected fields of the existing protocol have been used to carry QKD specific information. Existing frame formats are not changed, keeping the overall modifications to a minimum. The

resulting QKD based novel protocol offers unconditional security to the wireless networks with the use of key distributed via QKD.

The key distribution process splits into two main communication channels. Firstly, it uses quantum channel to transmit the photons where both parties interpret each photon to a bit (0 or 1) depending on the bases and polarisation used. Secondly it uses classical channel, in this case it is the existing wireless channel, to retrieve the final secured key.

Further, a number of possible extensions to IEEE 802.16 (WiMax) and also possibility of merging with IEEE 802.21 standard are also discussed. Several possible enhancements of this research are presented. One such enhancement is the use of Multi Agent Systems (MAS) to deploy the same solution with better control and more efficiently.

Acknowledgements

First and foremost I would like to thank Associate Professor Xu Huang for supervision and support over the course of my PhD program. His selfless perseverance, consistent attention to my work and many insightful comments has been a great aid to me in completing this research. He has been instrumental in providing me the guidance through his academic experience which was always there when I needed. This research would never have taken shape without his support.

I would also like to express my humble gratitude to Professor Dharmendra Sharma for his supervision, inspiration and kindness right throughout this research which has been invaluable to me.

I am extremely grateful to my previous supervisors Assistant Professor Bala Balachandran, Dr Sajal Palit, Dr Adrian Whichello for their support towards my studies.

I am indebted to emeritus Professor Paul Edwards for his supervision, enthusiasm and inspiration given to me during the initial stage of this research. I would also like to thank him for granting me CATQER top up scholarship.

I must also thank the IT support staff for their timely interventions to resolve my network issues.

I am heartily thankful to administration staff of ISE, specially Serena Chong, Coral Suthern and Kylie Reece for their support given to me in many ways.

I am grateful for University of Canberra for choosing me for a RTS scholarship, which was an invaluable aid to me in completing my PhD.

Last, but not least, I would like to thank my wife and daughter for their support and understanding right throughout the course of my studies.

List of Acronyms

ACK	Acknowledgement
AES	Advanced Encryption Standard
AK	Authorisation Key
ANonce	random or pseudo-random value generated by the Access Point
AP	Access Point
APD	Silicon Avalanche Photodiode
ARP	Address Resolution Protocol
B92	QKD protocol developed by C. H. Bennett in 1992
BB84	QKD protocol developed by Bennett and Brassard 1984
BS	Base Station
BSS	Basic Service Set
CA	Certificate Authority
CCMP	Counter mode with CBC-MAC Protocol
CR	Cognitive Radio
CTS	Clear to Send
DES	Data Encryption Standard
DoS	Denial of Service
DS	Distribution System
EAP-AKA	EAP for UMTS Authentication and Key Agreement)
EAPOL	Extensible Authentication Protocol over LAN
EAP-SIM	EAP for GSM Subscriber Identity
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP-Tunnelled Transport Layer Security
ECC	Elliptic Curve Cryptography
ESS	Extended Service Set
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTK	Group Temporal Key
IBSS	Independent Basic Service Set
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers

IPsec	Internet Protocol Security
IV	Initialization Vector
KCK	Key Confirmation Key
KEK	Key Encryption Key
L2TP	Layer 2 Tunnelling Protocol
LEAP	Lightweight Extensible Authentication Protocol
MAC	Media Access Control
MAS	Multi Agent System
MIC	Message Integrity Check
MIMO	Multiple-Input Multiple-Output
MLME	MAC Sublayer Management Entity
NAT	Network Address Translation
NIC	Network Interface Controller
P2P	Peer to Peer
PHY	Physical layer
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PKM	Privacy Key Management
PMK	Pairwise Master Key
PPTP	Point-to-Point Tunnelling Protocol
PRF	Pseudo Random Function
PTK	Pairwise Transient Key
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
Q-Key	Quantum Key
Qubit	Quantum Bit
RADIUS	Remote Authentication Dial In User Service
RSA	Rivest-Shamin-Adleman
RSN	Robust Security Networks
RSNA	Robust Security Network Association
RTS	Request to Send
SAID	Security Association IDs
SARG04	QKD protocol (derived from BB84)

SNonce	random or pseudo-random value generated by the Station
SS	Subscriber Station
SSID	Service Set Identifier
SSL	Secure Sockets Layer protocol
TEK	Traffic Encryption Keys
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TSN	Transition Security Network
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over IP
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Networks
WMAN	Wireless Metropolitan area networks
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPAN	Wireless Personal Area Networks

Nomenclature:

- **IEEE 802.1X** standard provides authentication mechanism to clients accessing the IEEE 802.11 wireless network. IEEE 802.1X uses three main parties of its architecture: *Authenticator*, *Supplicant* and *Authentication Server*. These entities have been referred to in the network documentation by various other terms as well.

Widely used terms for the *Authenticator* are: *Access Point (AP)*, *Base Station (BS)* etc.

Widely used terms for the *Supplicant* are: *Station (STA)*, *Client*, *Subscriber Station (SS)* etc.

For consistency, throughout this thesis, these entities have been referred as **AP** (*Authenticator*) and **STA** (*Supplicant*).

Also for simplicity, the functionalities of the *Authentication Server* has been assumed to be implemented within the AP.

- **Wi-Fi** is the industry standard for products as defined by the Wi-Fi Alliance and conforming to IEEE 802.11 standard. Because of the relationship with the underlying standards, the term Wi-Fi is often used as a synonym for IEEE 802.11 technology. Further IEEE 802.11i standard specifies security mechanisms for wireless networks done as an amendment to the original IEEE 802.11. Throughout this thesis, the term **Wi-Fi** has also been referred as **IEEE 802.11** and **IEEE 802.11i**.

Table of Contents

Abstract	iii
Certificate of Authorship of Thesis	v
Acknowledgements	vii
List of Acronyms	ix
Table of Contents	xv
List of Tables	xxi
List of Figures	xxiii
Chapter 1 Introduction	1
1.1 Motivation of the research	1
1.2 Wireless Networks	2
1.3 Cryptography	5
1.4 Secret Key and Public Key systems	7
1.5 Quantum Cryptography	8
1.6 Why 802.11 Wireless Networks?	9
1.6.1 Security issues in WEP	10
1.6.2 The 802.11i Standard	11
1.7 Research problems and proposed methodology	12
1.8 Experimental Procedure	13
1.9 Specific Contributions of the research	14
1.10 Structure of the thesis	15
Chapter 2 Research Content: A Survey	17
2.1 802.11 Network Architecture	17

2.2	Security in 802.11 Networks	21
2.3	IEEE 802.11i Standard	22
2.3.1	Management Frames impacted by proposed modifications	22
2.3.2	RSNA Key Hierarchy	32
2.3.3	4-Way Hand Shake Protocol	34
2.3.4	Security Issues in 4-Way Hand Shake Protocol	35
2.4	802.1X Port Based Network Access Control	35
2.4.1	IEEE 802.1X Authentication	36
2.4.2	EAPOL-Key frames	38
2.5	Use of EAP methods for Mutual Authentication	40
2.6	One-Time Pad.....	42
2.7	Use of Virtual Private Network in Wi-Fi Networks	42
2.8	Security Improvements of IEEE 802.11 Networks	44
2.9	Quantum Cryptography	45
2.9.1	Quantum Bit Error Rate of Quantum Channel	47
2.9.2	Quantum Key Distribution.....	48
2.9.3	Probability of Errors Introduced by Eavesdropping	55
2.9.4	QKD Protocols and Networks	56
2.9.5	Attacks on quantum cryptography networks.....	57
Chapter 3	Methodology	59
3.1	Classical Cryptography vs. Quantum Cryptography	59
3.2	Advantages of using QKD in 802.11 networks.....	60
3.3	QKD Based Solution for Key Distribution in Wi-Fi	61

3.3.1	Proposed protocol	61
3.3.2	STA State transition diagrams	68
3.3.3	STA EAPOL Frame Pseudo-codes.....	72
3.3.4	AP State transition diagrams	75
3.3.5	EAPOL Frame Pseudo-codes for AP.....	79
3.3.6	Packet Level Changes	82
3.3.7	Quantum communication channel.....	97
Chapter 4	Implementation	99
4.1	Implementation of Quantum Channel.....	99
4.2	Implementation of Wireless Channel	104
4.3	Simulink Approach	106
4.3.1	QKD Software Implementation	107
4.4	Full Model of the System	123
Chapter 5	Evaluation of Results	125
5.1	Analysis of Sifting Phase.....	127
5.2	Analysis of Error Estimation.....	130
5.2.1	Error Estimation – Successful Scenario	132
5.2.2	Error Estimation – Unsuccessful Scenario	134
5.2.3	Improved Error Estimation for Wireless QKD.....	135
5.3	Analysis of Reconciliation	138
5.3.1	Performance of Proposed Bisect Reconciliation Protocol.....	144
5.4	Analysis of Privacy Amplification	145
5.5	Analysis of Overall QKD based Wi-Fi Protocol	147

5.6	Analysis of the Quantum Channel	151
5.7	Summary	152
Chapter 6	Multi Agents for QKD in 802.11 Networks	153
6.1	Why Multi Agent System?	153
6.2	QKD based Multi Agent System Approach	155
6.2.1	The Operational Procedure	158
6.3	Implementation of MAS Solution	161
6.4	Adding intelligent behaviour	164
6.4.1	Possible Attacks on 802.11 and 802.1X Protocol Standards	164
6.4.2	How to use Agents to detect attacks.....	166
6.5	Future Work of MAS approach	167
6.5.1	Implement the Intelligence to detect attacks	168
6.5.2	Extending to Support Multiple EAP types	168
6.5.3	Extending to Support Multiple QKD Protocols	169
6.5.4	Use of Mobile Agents for Wider Coverage.....	170
6.5.5	Communication between agents	171
6.6	Summary of MAS Approach.....	174
Chapter 7	Conclusion and Future Work	177
7.1	Use of One Key for Multiple Sessions.....	181
7.2	Multi Agent Solution	183
7.3	Overcoming Line-of-Sight Issues.....	184
7.3.1	Use of MIMO Technology.....	184
7.3.2	Use of Cognitive Radio Communications	185

7.3.3	Other Solutions for Line-of-Sight.....	186
7.4	Use of Virtual Private Network in Wi-Fi Networks	186
7.5	Extending QKD for WiMAX	187
7.5.1	WiMAX Security	188
7.5.2	Security issues with WiMAX	192
7.5.3	Use of QKD for Key Distribution in WiMAX	193
7.6	Universal Architecture for Key Distribution in Wireless Networks	194
7.7	Achievements and Contributions against research questions	195
	Bibliography.....	197
	Appendices A: <i>Research Papers Published</i>.....	213
	Appendices B: <i>Patents Granted</i>.....	215
	Appendices D: <i>Universal Hash Function</i>.....	217

List of Tables

Table 1 : Wireless Networks - A Comparison	4
Table 2 : Beacon Frame Body [56]	24
Table 3 : Probe Request Frame Body [56].....	25
Table 4 : Probe Response Frame Body [8]	26
Table 5 : Element IDs [56]	29
Table 6 : Association Request Frame Body [56].....	30
Table 7 : Association Response Frame Body [8].....	30
Table 8 : Reassociation Request Frame Body [8]	31
Table 9 : Reassociation Response Frame Body [8].....	32
Table 10 : Beacon Frame Body (only the first 10 fields are shown).....	84
Table 11 : New Element IDs for QKD.....	86
Table 12 : Reconciliation parity check EAPOL frame details	93
Table 13 : Bases Representation in STA Buffer	103
Table 14 : Bits available to recover the final key after removing errors	127
Table 15 : Time taken (ms) to complete Sifting phase for various error rates	129
Table 16 : Summary of Polarised Photon Propagation Trial Data [27].....	131
Table 17 : Time taken to complete Error Estimation – Successful Scenario	133
Table 18 : Time taken to complete Error Estimation – Unsuccessful Scenario.....	135
Table 19 : Time Taken for Reconciliation for Block Size 8.....	140
Table 20 : Total time for proposed protocol (Error Rate=10%, Initial Block size=8 bits)	148
Table 21 : Total time for proposed protocol (Error Rate=20%, Initial Block size=8 bits)	148
Table 22 : Total time for proposed protocol (Error Rate=10%, Initial Block size=16 bits)	149
Table 23 : Total time for proposed protocol (Error Rate=20%, Initial Block size=16 bits)	149

List of Figures

Figure 1 : ESS Architecture [1].....	18
Figure 2 : Relationship between state variables and services [1]	20
Figure 3 : Capability information field [8]	25
Figure 4 : Request Information element [1].....	27
Figure 5 : Information Element Format [1]	28
Figure 6 : Pairwise Key Hierarchy of IEEE 802.11i of CCMP [30].....	33
Figure 7 : 4-Way Handshake [5]	34
Figure 8 : IEEE 802.1X Authentication [34]	37
Figure 9 : EAPOL-Key Frame [8]	39
Figure 10 : Key Information bit layout [8].....	39
Figure 11 : Polarisation by Filters [144].....	46
Figure 12 : Quantum Communication Setup [6]	49
Figure 13 : Example of Key Recovery of QKD Protocol	50
Figure 14 : Simplified diagram of final key retrieval	55
Figure 15 : The Proposed QKD Based Wi-Fi Protocol [6].....	63
Figure 16 : Successful Error Estimation Communication Flow.....	65
Figure 17 : Unsuccessful Error Estimation Communication Flow	66
Figure 18 : RSNA STA key management state machine – QKD Phase.....	69
Figure 19 : RSNA AP key management state machine (QKD Phase) – Part 1.....	76
Figure 20 : AP State Machine (QKD Phase) - Part 2.....	77
Figure 21 : Modified Capability information field of Beacon	84
Figure 22 : QKD Parameters Element Format	86
Figure 23 : Modified EAPOL-Key Frame to implement QKD [6].....	89
Figure 24 : Modified Key Information bit layout.....	90
Figure 25 : Key Data field values of EAPOL frame during reconciliation phase of QKD	92
Figure 26 : Example of reconciliation via EAPOL (where; A = AP, S = STA)	93
Figure 27 : Key Data for block 6	94
Figure 28 : Reconciliation Process using Parity Check	96
Figure 29 : High Level Set Up of Quantum Channel [10].....	100
Figure 30 : Schematic Diagram of QKD System [19], [30]	101
Figure 31 : QKD Experimental Setup.....	104
Figure 32 : C++ Class Structure of AP	109

Figure 33 : C++ Class Structure of STA	111
Figure 34 : Simulink Model of Sifting Phase for Access Point	113
Figure 35 : Main C++ Function used for Sifting Implementation at AP (scaled image).....	114
Figure 36 : Simulink Model of Sifting Phase for STA	115
Figure 37 : Simulink Model of Error Estimation Phase for STA	116
Figure 38 : Simulink Model of Error Estimation Phase for AP	117
Figure 39 : Simulink Model of Reconciliation Phase for Access Point.....	118
Figure 40 : Simulink Model of Reconciliation Phase for STA.....	119
Figure 41 : Main C++ Function for Parity Check Algorithm (scaled image).....	121
Figure 42 : Simulink Model of Privacy Amplification Phase for AP	122
Figure 43 : Simulink Model of Privacy Amplification Phase for STA.....	122
Figure 44 : Full Simulink model of Access Point	123
Figure 45: Full Simulink model of STA.....	124
Figure 46 : Communication Flows of Sifting Phase	128
Figure 47 : Time taken for Sifting phase	129
Figure 48 : Error Estimation – Successful Scenario	132
Figure 49 : Time taken for Error Estimation.....	133
Figure 50 : Estimation – Unsuccessful Scenario	134
Figure 51 : Comparison of Traditional and Proposed Error Estimation	138
Figure 52 : Key sizes Vs Time for block size = 8	141
Figure 53 : Time to complete Reconciliation for Key Length = 500 bits.....	142
Figure 54 : Time to complete Reconciliation for Error Rate of 30%.....	143
Figure 55 : Comparison of Traditional and Proposed Methods	145
Figure 56 : Time taken for Privacy Amplification	146
Figure 57 : The enterprise [3].....	156
Figure 58 : The Agent Society [3]	158
Figure 59 : The Process Flow of Wireless QKD [9].....	160
Figure 60 : Architecture diagram of MAS Solution.....	161
Figure 61 : High level C++ class diagram of the MAS application	162
Figure 62: Session Hijack by MAC address Spoofing.....	165
Figure 63 : Agent Architecture to Detect Attacks	167
Figure 64 : The extended architecture to support multiple EAP types	168
Figure 65 : Extended architecture to support multiple QKD Protocols	169
Figure 66 : Modified Enterprise supporting multiple QKD protocols and EAP types.....	170

Figure 67 : An example of KQML block for communication.....	172
Figure 68 : Agent UML interactions of QKD	173
Figure 69 : Scenario of One Quantum Key for Multiple Sessions	182
Figure 70 : AK Management in BS and SS [85]	190
Figure 71 : TEK management in BS and SS [85].....	191