Secure Communication in 802.11 Networks with a Novel Protocol Using Quantum Cryptography

Xu Huang Shirantha Wijesekera Dharmendra Sharma

Abstract— **It is the fact that wireless local area networks are increasingly deployed by businesses, government and SOHO users as they offer many advantages to its customers with mobility, flexibility, convenience etc. It opened a wide range of new commercial areas for hardware vendors, at low cost. This justifies why wireless networks have become one of the most widely used communication systems in the world. However, since there are no boundaries in wireless networks, they are vulnerable to security threats than wired networks. Therefore, providing secure communication for wireless networks has become one of the prime concerns. Quantum cryptography, to be precise, Quantum Key Distribution (QKD), offers the promise of unconditional security. In this paper, we extend our previous research work of how QKD can be used in IEEE 802.11 wireless networks to ensure secure key distribution. Our contributions in this paper are as follows: (1) We discussed how QKD can be used in IEEE 802.11 wireless networks to securely distribute the keys. (2) We use new protocol QKD. (3) We introduced a method that take the advantage of mutual authentication features offered by some EAP variants of 802.1X Port-Based Network Access Control. (4) Finally, we present a new code called Quantum Message Integrity Code (Q-MIC) which provides mutual authentication between the two communication parties. Also experimental results are presented with Simulink Model.**

Keywords-quantum key distribution (QKD), wireless communication, IEEE 802.11X, security system

I. INTRODUCTION

Wireless communication has gone through rapid advancements during the last few decades, an increasing number of government agencies, businesses and home users are either using, or considering using, wireless technologies in their environments [24]. Therefore wireless networks are becoming ubiquitous in homes, offices and enterprises with its ability to provide high-speed, high-quality information exchange between portable devices. It is obvious that in the near future wireless technology will dominate the communication industry. While wireless networks and its applications are becoming popular every day, security issues associated with it have become a great concern. Due to the nature of wireless communications, it is possible for an attacker to snoop on confidential communications or modify them to gain access to the wireless networks more easily than with wired networks. In this paper we are going to make a novel method to create an implementation of quantum cryptography for key distribution in 802.11 networks.

This paper comprises of 8 sections. In this section we provide some introduction to wireless security, quantum cryptography and discuss advantages of using Quantum Key Distribution (QKD) in wireless networks. Section 2 gives some background to IEEE 802.11i standard, including 4-way handshake, key hierarchy and IEEE 802.1X authentication. Both sections 1 and 2 only provides details with respect to exploit the facts on how QKD can integrate with the 802.11 networks. Section 3 describes the proposed new protocol merging QKD with 802.11 wireless networks. Section 4 provides the details of the protocol implementation. In section 5 talks about future related research works. The last three sections, sections 6, 7 and 8 are for Acknowledgements, Conclusions, and References respectively.

As wireless communications use the airwaves, they are intrinsically more vulnerable to interceptions and attacks than its wired counterparts. As the service become more popular, the risks to users of wireless technology have increased significantly. Thus, there are a great number of security risks associated with the current wireless protocols and encryption methods [6, 8]. Some of the common types of attacks against wireless networks are: Denial of Service (DoS) attacks, Identity theft (MAC spoofing), Man-in-the-middle attacks, ARP poisoning, Network injection etc.

Based on the laws of physics, quantum cryptography allows exchange of cryptographic key between two remote parties with unconditional security. The foundation of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from simultaneously knowing the value of the other. So that, act of an eavesdropper intercepting a photon will irretrievably change the information encoded on that photon, thereby detecting any security breach. It uses quantum states of photons to transfer cryptographic key material.

The classical public-key cryptography uses asymmetric keys, with one that is private and another one that is public. During the encryption process, the sending station uses a public key to encrypt the data before transmission. The receiving

978-0-7695-4159-4/10 $26.00 © 2010 IEEE
DOI 10.1109/NSS.2010.17

station uses the matching private key to decrypt the data upon reception. Each station keeps their private key hidden in order to avoid compromising encrypted information. In addition, to protecting information from hackers, stations can use public key cryptography to authenticate themselves to other stations or access points. The major weakness of this classical public-key cryptography is based on the fact that the private key is always linked mathematically to the public key [14]. Due to this reason, it is always possible to attack a public-key system if the eavesdroppers equipped with sufficiently large computational resources. Therefore, the mathematical problem to derive the private key from public key must be as difficult as possible. Hence those systems cannot provide any indication of eavesdropping or guarantee of key security.

Hence it is clear that the main problem of secret or public-key cryptography is secure distribution of keys. This is where the quantum mechanics offers a solution. Quantum cryptography provides "unconditional security" in key distribution. In contrast to traditional public-key cryptography, which relies on the computational difficulty of certain mathematical functions, the security of quantum cryptography relies on the foundations of quantum mechanics. Quantum cryptography exploits the fundamental laws of quantum physics where nobody can measure a state of an arbitrary polarized photon carrying information without introducing disturbances. Classical key distribution can always be passively monitored, without the legitimate users being aware that any eavesdropping has taken place. Whereas in quantum mechanics, any projective measurement will induce disturbances hence eavesdropping can be detected. Due to this reason, use of QKD in wireless key distribution will provide huge advantage with respect to data security.

Quantum cryptography is only used to produce and distribute a key, known as Quantum Key Distribution (QKD), but not to transmit any message data. Several QKD protocols such as BB84 [7], B92 [20] and six-state [18] exist as of now. Out of those, BB84 is more popular and widely used in practical networks [25]. We have chosen a variation of BB84 called SARG04 (Scarani, Acin, Ribordy, and Gisin) [21] to use in our work. SARG04 is robust against photon-number splitting (PNS) attacks [21, 22].

QKD has gone through significant advancements in both optical and wireless networks. There are lots of research work in progress in this area and even commercial QKD networks exited as of now [17, 19, 26, 27, 28]. In QKD, the transmitter (Alice) sends the key as a series of polarized photons via quantum channel towards the receiver (Bob).

Bob measures these photons using randomly selected bases to generate his version of the key. Once the photon transmission is over, the rest of the communication takes place in public channel (eg: internet, wireless medium). This communication is split into 4 main stages: *Sifting, error estimation, reconciliation* and *privacy amplification*. These 4 stages help Alice and Bob to recover identical with "unconditionally" secure key to be used for the subsequent data encryption.

II. IEEE 802.11I STARNDARD

IEEE 802.11 [2] specifies an over-the-air interface between client and base station or between two wireless clients. IEEE 802.11i [3], an amendment to 802.11, describes two new confidentiality algorithms, namely, Temporal Key Integrity Protocol (TKIP) and Counter-mode/CBC-MAC Protocol (CCMP) respectively [12]. IEEE 802.11i separates the authentication and encryption key management. For authentication 802.11i uses IEEE 802.1X [4] and pre-shared key.

IEEE 802.1X offers an effective framework for authenticating, managing keys and controlling user traffic to protect large networks. It employs the Extensible Authentication Protocol (EAP) [13] to allow a wide variety of authentication mechanisms.

802.1X authentication process happen between three main elements. The user or the client that wants to be authenticated is known as Supplicant or Station. The actual server doing the authentication is called Authentication Server (eg: RADIUS, DIAMETER). The Authenticator or the Access Point allows only the supplicants who are authorized by the authentication server to gain access to the network.

At the end of IEEE 802.1X authentication, the Supplicant and Authentication Server generate a shared key called Pairwise Master Key (PMK). The Authentication Server then transmits PMK to the Authenticator through a secure channel (eg: TLS). This PMK is used to derive Pairwise key hierarchy through an exchange of IEEE 802.1X EAPOL-Key frames, often called as 4-Way Handshake in the IEEE 802.11 standard.

Figure 1 shows the Pairwise key hierarchy [3]. The PMK received from the Authentication Server during 802.1X authentication is used to generate PTK by applying Pseudo Random Function (PRF). The PTK gets divided into three keys. The first key is the EAPOL-key confirmation key (KCK). The KCK is used by the EAPOL-key exchanges to provided data origin authenticity. KCK is also used to calculate Message Integrity Code (MIC). The second key is the EAPOL-key encryption key (KEK). The KEK is used by the EAPOL-key exchanges to provide for confidentiality. KEK is used to encrypt the Group Temporal Key (GTK). The third key is the Temporal Key (TK), which is used by the data-confidentiality protocols to encrypt unicast data traffic**.**

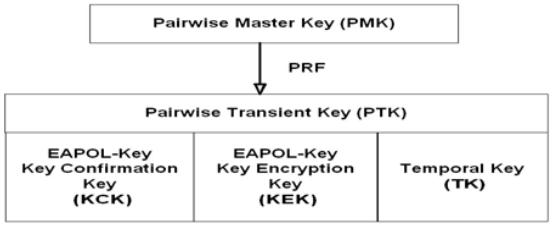

Figure 1: Pairwise Key Hierarchy of IEEE 802.11i

Figure 2 shows the 4-way handshake process.

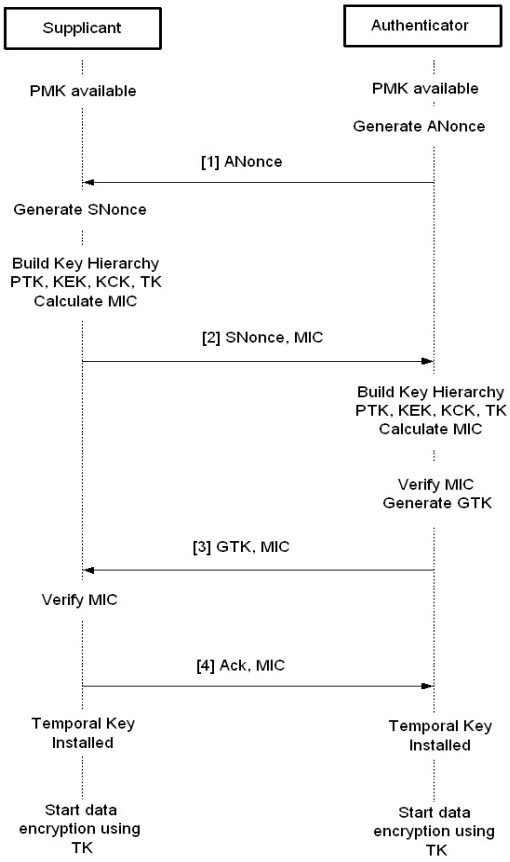

Figure 2: 4-way Handshake

As described in section 1.1, wireless networks are subject to various security risks. Exchanging data over a wireless network must be done with great care because traffic interceptions in wireless networks are much easier. Therefore, in order to provide privacy for the users, it is essential to authenticate users with the network elements. Although there are lots of research works happening to improve this daunting task of providing secure data communication to its users, they are still subject to security attacks. Quantum cryptography or QKD is one area which did not get much attention in wireless networks so far with regards to security.

III. PROPOSED PROTOCOL

Out of many different varieties of wireless networks such as GSM, GPRS, CDMA, UMTS etc, the coverage offered by Wi-Fi networks is only in the range of 100 meters. Wi-Fi networks are very popular in places like coffee shops, air ports, conference halls etc. As our main focus is to offer secured key distribution in wireless networks using QKD, we found that IEEE 802.11i family (Wi-Fi) best suits to marry with QKD. The environmental conditions impacting quantum transmissions in Wi-Fi networks can be minimized as the coverage area is very small.

The overall communication of this new protocol takes place in two channels: *Wireless Channel (Wi-Fi* and *Quantum Channel.*

From the point onwards the SARG04 quantum key distribution process takes place as shown in flows 3 - 6 of Figure 3. As the first step, the transmission switches over to the Quantum Channel. Supplicant then sends series of photons towards the Authenticator. Authenticator keeps track of all the photons that it received along with the bases it used to measure the photons. As soon as the photon transmission finishes, the Wireless Channel resumes for the rest of the protocol execution.

As briefly discussed in section 1.3, the keys obtained by both parties will contain errors due to various atmospheric conditions, eavesdropping etc. The subsequent 3 stages of QKD remove all these errors in order to obtain the final secured key. The Sifting process (flow 3 of figure 4) removes all the bits which recorded against incorrect bases used by the Authenticator. The Error Correction process (flow 4 of figure 3) determines the amount of errors discovered during the transmission. If this error level in within the threshold level, the communication continues.

To achieve this, the quantum transmission should ensure to send sufficient number of photons in order to recover Q-Key at least equal or greater than the PMK. For CCMP, PTK is 256 bits, while TKIP occupies 384 bits for PMK. Therefore, at this stage, we strip any extra bits of Q-Key so that it will have same length as PTK. We get this stripped Q-Key as the PTK. Once PTK is available, we can retrieve the key hierarchy containing all other keys using the PRF as described in section 2.2.

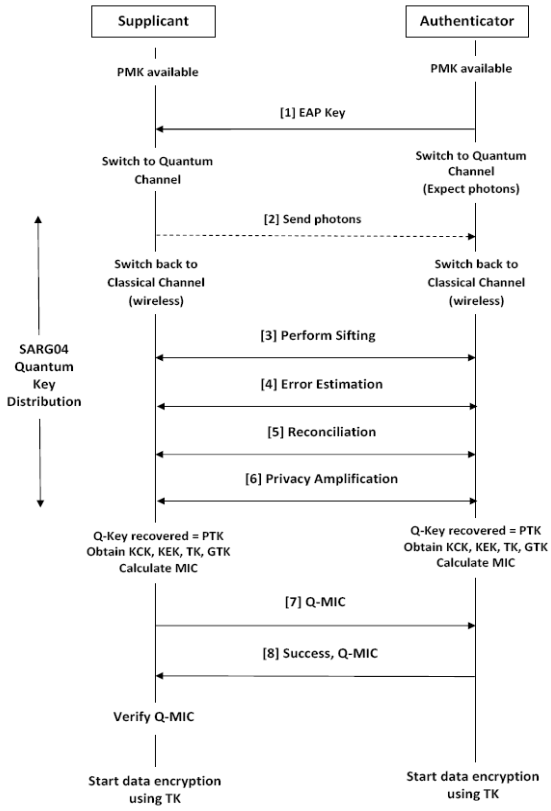

Figure 3: The Proposed Protocol

From PTK, we can derive KEK, KCK and TK, while from KCK, MIC can be calculated. We use this MIC in our subsequent protocol messages to implement mutual authentication. At this stage, Supplicant performs XOR operation with the MIC and the first set of bits of equal length in PMK. We call this resulted MIC as Quantum MIC (Q-MIC).

Q-MIC = (MIC) XOR (first bits of PMK equivalent to the length of MIC)

Supplicant then sends Q-MIC to Authenticator as shown in flow 7 of Figure 3. Upon receiving Q-MIC, Authenticator verifies the Q-MIC. Since the Authenticator is in possession of all the key hierarchy, it can calculate its own Q-MIC and compares with the one came from the Supplicant. If they match, the Supplicant is authenticated.

Recent research work explores some of the flaws of 4-way handshake [5, 6, 8, 16]. It was shown that the message 1 of 4-way handshake is subject to DoS attacks. Intruders can flood message 1 to the supplicant after the 4-way handshake has completed, causing the system to fail. Since key distribution of our protocol is done by the QKD, use of nonce values in the message flows are not required.

Present hardware devices for quantum transmission require Line of Sight (LOS) between the Supplicant and the Authenticator in order to transfer photons. However, there has been lot of new advancements happening in this area to eliminate the requirement of LOS for quantum transmission. One such research work is done by Kedar and Arnon [9] to have Non Line Of Sight (NLOS) system for optical communication by using wireless sensor network.

IV. The Implementation

The implementation of this set up can be divided into two main communication phases: *Quantum Communication* and *Wireless Communication*. The quantum communication is only used for a short time to transmit the quantum key in the form of series of polarized photons. This transmission is fully controlled by hardware devices such as photon transmitter and the detector at either ends.

Our implementation is twofold: Setting up the quantum channel, implementing the wireless communication. The implementation is currently happening in both streams (hardware and software) in parallel. University of Canberra has past research activities on QKD [15]. During that project, a QKD system was successfully established between university of Canberra and Telstra tower. We choose this hardware setup as our quantum transmission between the Supplicant and Authenticator. We plan to have this hardware set up for a short distance to suit for Wi-Fi networks. We would like to emphasize that we do not pay much attention in converting the present bulky quantum hardware to fit in comparatively small Wi-Fi apparatus. There are lots of new developments taking place to include quantum devices in small gadgets [28]. Our aim in this research is to demonstrate a working QKD based key distribution process for Wi-Fi using the proposed protocol. For simplicity, we use both Authenticator and Authentication Server as one entity. The high level view of this test set up is shown in Figure 4.

The Supplicant is running on Windows XP, while the Authenticator/Authentication Server machine is running on Windows Server 2000. We have chosen Microsoft "Native WiFi" product with its user Application Programming Interfaces (API) to be used for software developments.

We start from the place where the 802.1X process deliver the PMK to the Authenticator and the Supplicant. At this stage both parties switch to hardware channel to start the photon transmission. Once the photon transmission finishes, they switch back to wireless channel. Both Supplicant and Authenticator store the states of the photons that they used during the communication.

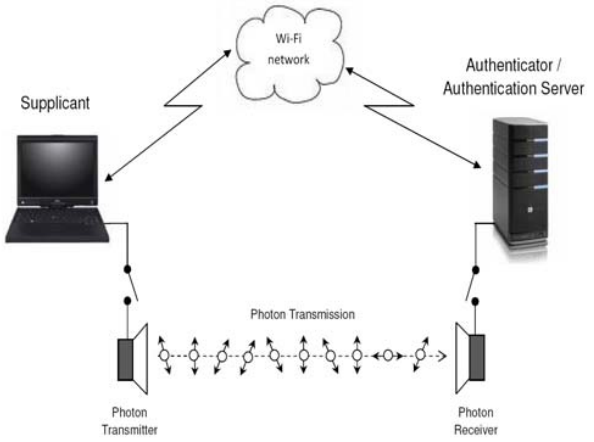

Figure 4: Test set up of QKD based key distribution for Wi-Fi

In the next message, Supplicant sends the bases it used to polarize the photons. Upon receiving the bases, the Authenticator extracts the bits based on the information it has. (We recall that describing the operation of SARG04 is not in scope of this paper). During this stage, the two parties estimate the error introduce during the transmission. This error could result due to atmospheric noise [23], dark counts in the photon detectors, eavesdropping etc. To estimate this error level, the Supplicant chooses a sample from its key and reveals to the Authenticator. This message frame consist of the start bit position and the length of the sample. The authenticator compares the bits it extracted and if it is below the threshold level, the Authenticator informs Supplicant with Success message to proceed with. Otherwise it sends out Fail message asking the Supplicant to reattempt the Photon transmission. The threshold value for error estimation has been set as a configurable parameter at the Authenticator.

Unlike in normal QKD systems, the key used is Wi-Fi is not very long. The maximum length of the key that will be transmitted via quantum link is 256 for CCMP and 384 for TKIP. Therefore the whole key of SARG04 can easily be

accommodated into these message flows. Due to this reason, the key exchange does not require any indexing to maintain long keys spanning across multiple files. In our set up, all key manipulations, comparisons etc are done in memory enabling faster operation.

Figure 5 shows the software architecture of main modules of protocol implementation. We use Windows XP (SP2) for Authenticator while Windows Server 2000 for Authenticator/Authentication Server. The reason to choose these OS platforms is due to basic requirements by "Native WiFi" product. The software applications running on both machines interact with 3 main wrappers classes: Native WiFi, Quantum Transmission and SARG04.

IEEE 802.11 standard defines Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless LANs (IEEE Std 802.11, 2007). Since the changes we made under the new QKD protocol are directly on the Physical and MAC layers, it is really difficult to rewrite those layers from scratch to reflect the changes within the research time frame. Therefore, the best possible way of experimenting the new protocol is by simulation. Thus, most of the QKD processing has been coded using C++ language. For simulation, we have chosen Simulink as it provides S-Functions to incorporate C++ programs into Simulink.

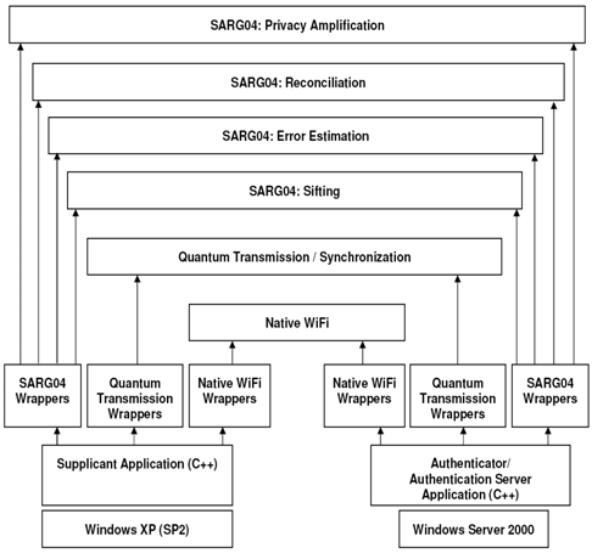

Figure 5: Software Communication Architecture

Authenticator and Supplicant state machine procedures that used to implement QKD in IEEE 802.11 standard are described below.

Authenticator State machine procedures

The procedure that used to receive photons:

ReceivePhotons()

PMK = TRUE

// Receive photons

qcTransmissions++

if (QCFinished and qcTransmissions)

<= qcTransmissionsThreshold

then

basesRecorded = TRUE

else if QCTimeOutEvt

then

EAPOL(reattemptTransmission)

else

QCError // unable to setup

// quantum transmission

end if

The procedure that used for reconciliation:

reconciliationAuthenticator()

if (QKD Phase = 0000 0101) then

if ReconciliationCounter == 0 then

1 Divide the raw key

into blocks

2 Calculate parity of

each block

else if (ReconciliationCounter == MaxSubLevel) or (no more parity mismatches)

then

end of reconciliation

else

//A new EAPOL reconciliation

//frame has received

1 compare the parities received

against corresponding block(s)

2 discard the last bit of the

blocks compared

3 identify blocks sub-blocks

with parity differences

4 bisect the blocks with

parity differences

5 Calculate sub-block parity

6 Set Sub-Block Level field

7 ReconciliationCounter + 1

end if

end if

end if

V. CONCLUSION

Wireless networks are subject to various security risks. Most significant source of risk in wireless networks is that the technology's underlying communication medium, the airwave, is open to intruders. Due to this reason, lots of efforts have been put in to address security issues in wireless networks. To address the same issue, we figure out the usage of quantum cryptography for key distribution in 802.11 networks. The advantage of quantum cryptography over traditional key exchange methods is that the exchange of information can be shown to be secure in a very strong sense, without making assumptions about the intractability of certain mathematical problems. In our work, we take advantage of the "unconditional security" offered by QKD to merge with IEEE 802.11i wireless network. For small wireless networks such as IEEE 802.11, quantum cryptography can serve better to provide secure data communications. With the recent advancements on MIMO technology for quantum transmissions, shows us a better way towards eliminating the LOS restriction. Although present technology does not extend to provide quantum transmissions in 802.11 apparatus so far, we believe our work will contribute to develop secure communications for future wireless networks.

REFERENCES

[1] Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma, "Implementation of Quantum Key Distribution in Wi-Fi (IEEE 802 11) Wireless Networks," IEEE the 10th International Conference on Advanced Communication Technology, Feb 17-20, 2008 Phoenix Park, Korea. Proceedings ISSN 1738-9445, ISBN 978-89-5519-135-6, Vol. II, p865.

[2] ANSI/IEEE 802.11, 1999 Edition (R2003), Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[3] IEEE Std 802.11i, IEEE Standard for Information Technology – Telecommunication and information exchange between systems – Local and metropolitan area networks – Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements, 2004.

[4] IEEE Std 802.1X, 2004, IEEE Standard for Local and metropolitan area networks, Port-Based Network Access Control

[5] Changhua He, John C Mitchell, Analysis of the 802.11i 4-way Handshake.

[6] Floriano De Rango, Dionogi Lentini, Salvatore Marano, Statis and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i, June 2006.

[7] Bennett, C. H. and Brassard, G., "Quantum cryptography: Public-key distribution and coin tossing", Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, December 1984, pp. 175 – 179.

[8] Changhua He, John C. Mitchell, Security Analysis and Improvements for IEEE 802.11i.

[9] Debbie Kedar, Shilomi Arnon, Non-line-of-sight optical wireless sensor network operating in multiscattering channel, 2006.

[10] Debbie Kedar, Shilomi Arnon, Quantum Key Distribution by a Free-Space MIMO System, May 2006.

[11] Bob O'Hara, Al Petrick, IEEE 802.11 Handbook, A Designer's Companion,2005.

[12] D. Whiting, R. Housley, N. Ferguson, Request for Comments: 3610, Counter with CBC-MAC (CCM), September 2003.

[13] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, , RFC – 3748, Extensible Authentication Protocol (EAP), 2004.

[14] Matthias Scholz, Quantum Key Distribution via BB84, An Advanced Lab Experiment, August 2005.

[15] Paul J. Edwards, The University of Canberra – Telstra Tower Quantum Crypto-Key Telecommunications Link, Advanced Telecommunications and Electronics Research Centre, http://www.ips.gov.au/IPSHosted/NCRS/wars/wars2002/proceedings/invited/print/edwards.pdf.

[16] ChangHua He, John C. Mitchell, 1 Message Attack on the 4-Way Handshake, May 2004.

[17] http://www.computerworld.com/securitytopics/security/story/0,10801,96111,00.html, Quantum cryptography gets practical.

[18] Dagmar Bruß, Optimal Eavesdropping in Quantum Cryptography with Six States, Physical Review Letters, 81.3018, October 1998.

[19] M.S. Goodman, P. Toliver, R.J. Runser, T.E. Chapuran, J. Jackel, R.J. Hughes, C.G. Peterson, K. McCabe, J.E. Nordholt, K. Tyagi, P. Hiskett, S. McNown, N. Nweke, J.T Blake, L. Mercer, H. Dardy, Quantun Cryptography for Optical Networks: A Systems Perspective.

[20] C.H. Bennett, Phys. Rev. Lett. 68, 3121 (1992).

[21] Valerio Scarani, Antonio Acin, Grégoire Ribordy and Nicolas Gisin, Quantum cryptography protocols robust against photon number splitting attcks.

[22] Valerio Scarani, Antonio Acin, Grégoire Ribordy and Nicolas Gisin, Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations, Phys. Rev. Lett., Vol 92, 057901, 2004.

[23] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, Barry C. Sanders, Limitations on Practical Quantum Cryptography, February 2000.

[24] Tom Karygiannis, Les Owens, Wireless Network Security, 802.11, Bluetooth and Handheld Devices, NIST, Special Publication 800-48, November 2002.

[25] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, Harald, Weinfurter, Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, Phys. Rev. Lett. 98, 010504, January 2007.

[26] http://www.secoqc.net/, SECOQC, Development of a Global Network for Secure Communication based on Quantum Cryptography.

[27] http://www.technologynewsdaily.com/node/8985, http://www.idquantique.com/, id Quantique, Quantum Cryptography.

[28] New Scientist, Quantum ATM rules out fraudulent web purchases, 10 November 2007