Novel Protocol for Quantum Cryptography of Secure in Wireless Communications

Xu Huang, Shirantha Wijesekera, and Dharmendra Sharma
Faculty of Information Sciences and Engineering
University of Canberra, ACT 2601,
Australia

{Xu.Huang, Shirantha.Wijesekera, Dharmendra.Sharma}@canberra.edu.au

***Abstract*— Wireless networks have become one of the most widely used communication systems in the world. However, providing secure communication for wireless networks has become one of the prime concerns. Quantum cryptography, namely Quantum Key Distribution (QKD), offers the promise of unconditional security. In our paper, we shall extend our previous research work to a new method of integrating quantum cryptography for key distribution in 802.11 wireless networks. Our contributions, based on our previous results [1], are as follows: (1) We shall show how QKD can be used in IEEE 802.11 wireless networks to securely distribute the keys. (2) We shall introduce a method that take the advantage of mutual authentication features offered by some EAP variants of 802.1X Port-Based Network Access Control. (3) Finally, we present a new code called Quantum Message Integrity Code (Q-MIC) which provides mutual authentication between the two communication parties and its implementation**

1. Introduction

It is obviously fact we face that wireless networks are becoming ubiquitous in homes, offices and enterprises with its ability to provide high-speed high-quality information exchange between portable devices. As the 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 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. 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.

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, 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, etc. DoS attacks are typically associated with 802.11 wireless communications [24].

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. Quantum cryptography is used to produce and distribute a key, known as Quantum Key Distribution (QKD). 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 employ in our work. SARG04 is robust against photon-number splitting (PNS) attack [21, 22]. Explaining how SARG04 protocol works is not in scope of this paper. QKD has gone through significant advancements in optical networks [17, 19, 26, 27]. However, QKD with respect to free-space is showing rather slow progress. One of the main reasons for this slow progress in free space photon transmission is the difficulty in providing Line-Of-Sight (LOS) between the transmitter and the receiver for long distances. In addition, free-space photon transmission is also impacted by environmental conditions such as noise [23].

In our work, we target the IEEE 802.11 wireless network to integrate with quantum cryptography. Since the coverage area of 802.11 network small, the line-of-sight issue between the participating entities can be minimized. Also, for such a small distances, the impact to the photon transmission from environmental conditions such as noise is very low.

Wireless networks can be divided into three main categories in terms of the coverage: Wide Area Networks (WAN), Wireless Local Area Networks (WLAN) and Personal Area Networks (PAN). WLANs and PANs cater for small indoor coverage areas.

The IEEE 802.11 [2] wireless local area networks seem to present high interest to be used with quantum cryptography due to various reasons [7]. One of the main advantages is the range of coverage offered by IEEE 802.11 networks. The range of a typical WLAN node is about 100 m. So that 802.11 networks deployed in places like coffee shops, air ports, conference halls etc. This offers the line-of-sight path, which is one of the key requirements for quantum cryptography, between the users and network apparatus.

On the other hand the applications that make use of 802.11 requires secured communication path with the service provider. Quantum cryptography has the potential to offer this much needed secured data communications for 802.11 wireless networks. Hence it is worth exploring the possibility of using Quantum Cryptography in 802.11 WLANS.

2. IEEE 802.11i Standard

Before we introduce our new protocol, we need to have a closer look at IEEE 802.11i standard. The security of 802.11 is defined by Wired Equivalent Privacy (WEP). However WEP was identified by cryptanalysts to have severe security weaknesses. As a result of this, an amendment to the IEEE 802.11 standard called IEEE 802.11i [3] was approved in 2004.

IEEE 802.11i is designed to provide enhanced security in the Medium Access Control (MAC) layer for 802.11 networks. It defines two classes of security algorithms: Robust Security Network Association (RSNA) and Transition Security Network (TSN). IEEE 802.11i describes two new confidentiality algorithms to address those two cipher suites, 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.

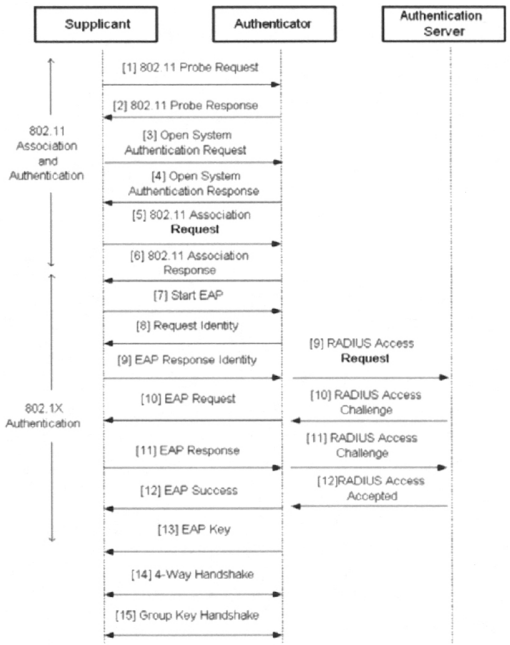

Figure 1: RSN Association, IEEE 802.1X Authentication and Key Establishment process

802.1X authentication process happen between three main elements. The Authenticator or the Access Point allows only the supplicants who are authorized by the authentication server to gain access to the network. Figure 1 shows the RSN Association, IEEE 802.1X authentication and key establishment process [11]. This assumes the pre-shared key is not used. Flows 1 to 6 in Figure 1 illustrate the IEEE 802.11 association and authentication process. Once the IEEE 802.11 association is completed, the IEEE 802.1X authentication starts. This is shown by flows 7 to 13 in Figure 1.

RSNA defines two types of key hierarchies to divide initial key material into useful keys. The two key hierarchies are: Pairwise key hierarchy, which is used to protect unicast traffic and, Group key hierarchy which is used to protect multicast and broadcast traffic. Figure 2 shows the Pairwise key hierarchy [3].

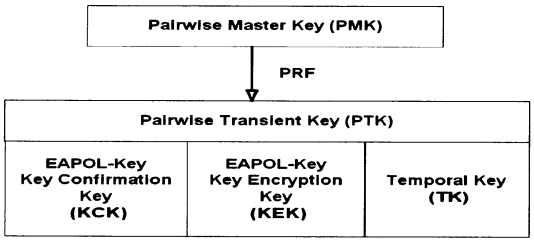

Figure 2: IEEE 802.11i Pairwise Key Hierarchy

3. QKD for Wireless Networks

As described in above, 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 researches are happening to improve this daunting task of providing secure data communication to users, they are still subject to security attacks. Quantum cryptography or QKD is one area that did not get much attention in wireless networks so far with respect to providing secrete key distribution.

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 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 the key security.

Hence it is clear that the main problem of secrete 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.

One of the main security issues in wireless networks is verifying the authenticity of participating elements to the data communication. This is achieved via mutual authentication, which refers to two parties authenticating each other suitably.

In 802.11i networks there are two places where the mutual authentication can be employed. Firstly, by selecting a correct EAP type such as EAP-TLS, EAP-TTLS that offer mutual authentication during IEEE 802.1X authentication process. Secondly, the IEEE 802.11i 4-way handshake makes the mutual authentication happens in second and third messages. In the second message of 4-way handshake, authenticator receives the reply and MIC from the supplicant. Authenticator checks the received and calculated MIC values to authenticate the Supplicant. In the third message, Authenticator sends the calculated MIC to the Supplicant. Supplicant then checks the MIC to authenticate the Authenticator, achieving mutual authentication.

4. The Proposed Protocol

In our work, we paid special attention on the stage where the mutual authentication takes place in 802.11i networks. Therefore, we shall take the advantage of EAP types such as EAP-TLS, EAP-TTLS which offer mutual authentication, to merge 802.11i networks with QKD. In order to make QKD well match wireless communications, i.e. our aim is to introduce quantum key transmission soon after the 802.1X authentication is completed. The proposed protocol is shown in figure 3.

At the end of the IEEE 802.1X authentication, both the supplicant and the authenticator hold PMK. As described in flow 13 of figure 1, the last message of 802.1X protocol is the EAPOL message giving the EAP Key from Authenticator to the Supplicant. Since the two parties are mutually authenticated at this stage, we know that this message is genuine. We use this message as the starting point of quantum transmission. By this way we can safely start the quantum key exchange. As soon as the Supplicant receives the EAP Key message, the communication switches to quantum channel.

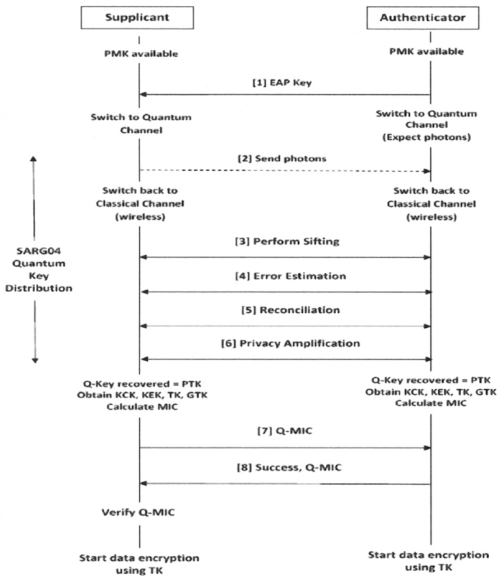

Figure 3: The Proposed Protocol

Supplicant then starts SARG04 key distribution, by sending series of photons towards the Authenticator. Once the photon transmission finishes, the communication switches back to classical wireless channel. Afterwards they complete the SARG04 quantum key exchange as shown in flows 3 to 6 of Figure 3. In QKD, the length of the final key cannot be known before the quantum transmission. This is because, due to atmospheric noise, dark counts in the photon detectors etc, lot of errors have been introduced into the transmission. Therefore, some of the transferred bits will get discarded during the final key recovery process of SARG04 protocol. Our aim is to set the length of Q-Key equal to the length of PTK. For CCMP, PTK is 256 bits, while TKIP occupies 384 bits for PMK. So that we have to make sure the derived Q-Key will contain bits greater than or equal to the number of bits of PTK. Therefore, at this stage we strip the 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.

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. In order to simplify the operation in wireless networks 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) and make the following protocol:

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

The Supplicant then sends the 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 keys, it can calculate its own Q-MIC and compares with the one came from the Supplicant. If they match, the Supplicant is authenticated.

The Authenticator then sends Success message along with Q-MIC to Supplicant as shown in flow 8 of Figure 3. Supplicant verifies the Q-MIC to authenticate the Authenticator, thus achieving the mutual authentication. From now on, both parties use TK to encrypt the data and start secure communication and also use the GTK for multicast applications if needed.

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 SARG04 protocol.

It was shown that BB84, hence SARG04, is subjected to man-in-the-middle attacks [15]. Even though the Supplicant and Authenticator are mutually authenticated during the EAP authentication, an eavesdropper can fake a photon transmission towards Authenticator after seen the EAP Key message. Let's assume an eavesdropper send a fake photon transmission towards Authenticator soon after the EAP Key message (flow 2 of Figure 3). Then once the Q-Key is derived by SARG04 process, supplicant sends Q-MIC to Authenticator in flow 7. Authenticator can check this Q-MIC value as it has all the ingredients to generate its own Q-MIC. Therefore, any fake SARG04 processes can be known at this stage.

5. Implementation of QKD

The Quantum key transmission happens in two stages, in terns of concepts, which can be shown in Figure 4. It is noted that in Figure 4 the Wi-Fi connections are classical channels and the "optical Fiber" channels are quantum channels.

Those two stages are as follows:

Stage 1: Quantum channel (one way communication)

This transmission could happen in either through free space or optical fiber. At present this implementation is being done at the Lab.

Stage 2: Classical channel (two way communication)

This phase deals with recovering identical secrete keys at both ends.

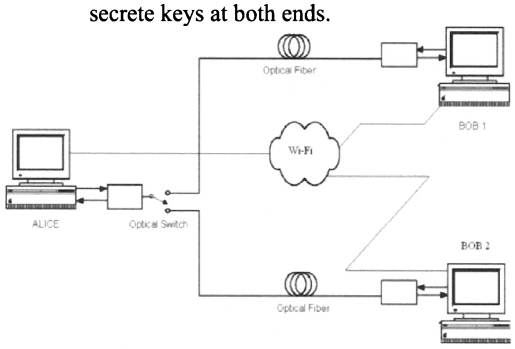

Figure 4. Simplified block diagram of a point-to-point QKD link in concept.

Regarding the implantation, as shown in Figure 5, the quantum channel is taking the task that using quantum cryptography to establish the key used for the encryption of user data in 802.11i, which is the TK. It is noted that TK is part of the PTK, as shown in Figure 1, which is established during the four-way handshake, we shall modify the four-way handshake to integrate the B92/BB84 protocol, as a case study, and make it as quantum handshake.

When the quantum handshake completion the wireless Wi-Fi will either refuse the subscriber station to communicate data via the classical channel or take the subscriber station to access the Wi-Fi and the system becomes "normal" Wi-Fi working states, which will run the communications in the defined classical channels.

The quantum channel between Alice and Bob1 is shown in Fig. 5, the channel between Alice and Bob2 is similar. At Alice, laser pulses are generated by vertical cavity surface emitting lasers (VCSELs) and attenuated into single photon level. The polarization states of photons are set by polarizers according to corresponding protocol (B92 or BB84). Then photons are combined and sent into a fiber through a non-polarizing beam splitter (NPBS). The polarizers Pol. 0A, 0B, 1A, and 1B are oriented to 0°, 90°, +45°, and -45° respectively. Only two channels, 0A and 1A, are used for B92, while all four channels are used for BB84.

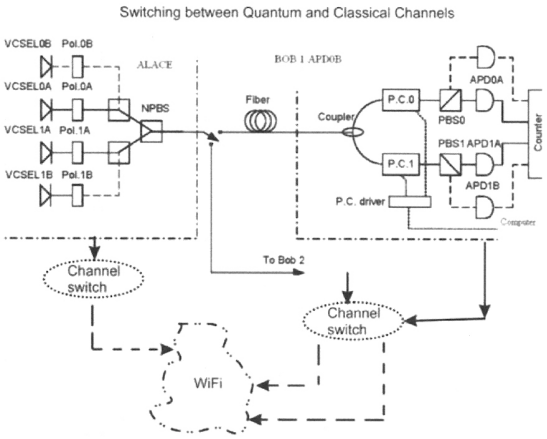

Figure 5. Quantum channel implementing by optical fibers: schematic diagram of the QKD system with PRAC sub-systems. VCSEL: Vertical Cavity Surface Emitting Laser ; Pol.: Polarizer; NPBS: Non-Polarizing beam splitter; P.C.: Polarization Controller; PBS: Polarizing beam splitter; APD: Silicon avalanche photodiode.

Then photons are combined and sent into a fiber through a non-polarizing beam splitter (NPBS). The polarizers Pol. 0A, 0B, 1A, and 1B are oriented to 0°, 90°, +45°, and -45° respectively. Only two channels, 0A and 1A, are used for B92, while all four channels are used for BB84. At Bob, polarization controllers recover the polarization state of photons to their original state at Alice. The 3-dB coupler randomly chooses the detection base and the polarization beam splitter (PBS) helps to determine the key value via an agent-oriented. Finally the photons are detected by single photon detectors (APDs). Two APDs, 0A and 1A, are used for B92, while four APDs are all used for BB84.

The further analysis for the experimental results will be discussed in our other papers, which is beyond the scope of this paper.

6. Conclusions

Risks are inherent in wireless technology. Most significant source of risks in wireless networks is that the technology's underlying communication medium, the airwave, is open to intruders. Due to this reason a lot of efforts have been put 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. Regarding the line of sight (LOS) problem occurring from the QKD to the wireless networks, we have noted the there are three models can be discussed [20] namely, less scattered LOS short-rang indoor propagation environments, log-normal distributed channel, quasi-LOS links may be well modeled by Nakagami distributed channel and Gaussian distributed channel with highly-scattered outdoor NLOS propagation environments. Due to the conference paper size the analyses will be presented in another paper.

7. 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 O(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] Thi Mai Trang Nguyen, Mohamad Ali Sfaxi, Solange Ghernaouti-Helie, 802.11i Encryption Key Distribution Using Quantum Cryptography, 2006.

[10] Yang Xiao, Jie Li, Yi Pan, 2005. Security and Routing in Wireless Networks,

[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] Kenneth G. Paterson, Fred Piper, Rudiger Schack, Why Quantum Cryptography? , June, 2004.

[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, Quantu Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations, Phys. Rev. Lett., Vol 92, 057901, 2004. m

[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] Enzo Baccarelli, Mauro Biagi, Cristian Pelizzoni, and Nivola Cordeschi, "Optimal MIMO UWB-IR Transceiver for Nakagami-fading and Poisson-Arrivals," Journal of Communications, vol.3, no.1 January 2008 pp27-40