

802.11i Encryption Key Distribution Using Quantum Cryptography

Thi Mai Trang Nguyen, Mohamed Ali Sfaxi and Solange Ghernaoui-Hélie
 University of Lausanne, HEC-INFORGE, CH-1015 Lausanne, Switzerland
 Email: trnguyen@ieee.org, {mohamedali.sfaxi, sgh}@unil.ch

Abstract—Quantum cryptography is a promising solution towards absolute security in long term cryptosystems. While the use of quantum cryptography in fiber optical networks gets significant advances, research on the application of quantum cryptography in mobile wireless network is still premature. In this paper, we analyze the interests of using quantum cryptography in 802.11 wireless networks, and propose a scheme integrating quantum cryptography in 802.11i security mechanisms for the distribution of the encryption keys. The use of an apparatus network to provide alternative line-of-sight paths is also discussed.

Index Terms—802.11i, quantum cryptography, network security.

I. INTRODUCTION

The uncertainty principle in quantum mechanics created a new paradigm for cryptography: Quantum cryptography, or more specifically Quantum Key Distribution (QKD). Unlike the classical cryptography which relies on mathematical complexity, quantum cryptography is based on the laws of quantum physics. These laws ensure that nobody can measure a state of an arbitrary polarized photon carrying information without introducing disturbances which will be detected by legitimate users. As all eavesdropping can be detected, quantum cryptography is considered as a promising key distribution means towards long term unconditionally secure cryptosystems.

Since the first QKD protocol proposed in 1984 with the name of BB84 [19], research on quantum cryptography gets significant advances. Experiments of different QKD systems have been realized in fiber networks and over free space [1-4]. Especially, a turnkey service using quantum cryptography to frequently generate fresh secret key has been commercialized in Switzerland [5].

While the use of quantum cryptography in fiber optical networks is successfully deployed in practice, the application of quantum cryptography in mobile wireless networks is still premature. Most research and

experiments aim at providing QKD service outdoor for a long distance in satellite networks [6] or between buildings in a city [35]. In these works, communication entities of the QKD protocol are mainly system devices but not final mobile users. For instance, communication entities in satellite networks are ground stations and the satellite. Our motivation of integrating quantum cryptography in mobile wireless networks is quite different. We aim at providing mobile wireless user's terminals with QKD service. In a mobile environment, one technical challenge in addition to those of free space environment is the maintenance of a line-of-sight path between mobile user and the fixed part of the network when the user moves around.

There are a large variety of kinds of mobile wireless networks. Table I compares GSM (Global System for Mobile communications), 802.11, and Bluetooth regarding four aspects: user mobility level, area of use, terminals, and applications.

As indicated in Table I, GSM or cellular networks in general is a wide area network, used essentially outdoor to provide mobile users with telephone service. As voice call is the main application of GSM networks, the terminals are small size cell phones allowing mobile users to move with a high level of mobility. The speed of mobile users in a GSM network can be at step speed or vehicle speed. With this level of mobility and the outdoor environment, cellular network presents some disadvantages for the use of quantum cryptography. It will be difficult to provide a line-of-sight path with a high user mobility level. The outdoor environment is not ideal for free space quantum cryptography. Noise level can be

TABLE I.
COMPARISON OF MOBILE WIRELESS NETWORKS

Mobile wireless network	User mobility level	Coverage area	Terminals	Applications
GSM	high	Outdoor (order of kilometers)	cell phone	Voice calls
802.11	low	Indoor (<100m)	laptop, PDA	Internet, e-commerce
Bluetooth	low	Indoor (< 10 meters)	peripheral devices	Replacement of wires connecting devices in close proximity of each other

Based on "Integration of Quantum Cryptography in 802.11 Networks", by T.M.T. Nguyen, M.A. Sfaxi, and S. Ghernaoui-Hélie which appeared in the Proceedings of the First International Conference on Availability, Reliability and Security, ARES 2006, Vienna, Austria, April 2006. © 2006 IEEE Computer Society Press.

raised because of rain or smoke. The large coverage area of the GSM network and the presence of natural obstacles such as trees or houses do not facilitate the provision of alternative line-of-sight paths.

In contrast to cellular networks, 802.11 networks [7] present many interests relating to the use of quantum cryptography. First, 802.11 is a wireless local area network, mainly used in offices and campus such as, class rooms, meeting rooms, universities, and halls in hotels or in airports. For the limited coverage area, 802.11 networks are mainly used indoor, reducing noise and natural obstacles caused by the outdoor environment. This building-oriented environment also facilitates the deployment of a high density of quantum apparatus to provide alternative line-of-sight paths. Second, 802.11 terminals are mainly laptops or PDAs (Personal Digital Assistant) which have more computational capacity and more energy for the autonomy than cell phones in cellular networks. Quantum key distribution in mobile networks is a task requiring significant amount of computational resource and energy for the control protocol and the QKD protocol. Third, as 802.11 terminals are not small like cell phones and 802.11 applications usually requires that users watch the screen, the mobility level of users in WLAN 802.11 is low and sometimes static, promising a solution to provide line-of-sight paths between quantum transmitters and receivers. Fourth, from an application point of view, WLAN 802.11 is usually used to provide Internet access through an access point installed by an organization or by a wireless ISP (Internet Service Provider). This kind of application is critical from a network security point of view because users can realize e-commerce or banking transactions via the Internet. These applications need a very strong security that quantum cryptography can offer.

Different from cellular and 802.11 networks, Bluetooth is a personal area network which is mainly used to interconnect peripheral devices such as mouse, desktop, keyboard, and computer which are in close proximity of each other. As the coverage area is small, the eavesdropping can be controlled within the vision of users. The contribution of quantum cryptography is less significant in such an environment. From a network security point of view, the application of replacing wires connecting devices in a close proximity is also less critical than the application of Internet access of 802.11 networks.

For this analysis, our first tentative of integrating QKD in mobile networks is towards the 802.11 network. As a first step of the integration of quantum cryptography in 802.11 networks, we have defined the Quantum handshake [29] to establish the 802.11i encryption keys using the BB84 protocol. In this paper, we present an enhanced version of this Quantum handshake and discuss in detail the use of an apparatus network for the provision of alternative line-of-sight paths.

The organization of the remainder of the paper is as follows. In section II, we provide an overview on security mechanisms specified by the 802.11i standard. The procedure of authentication and key management will be

presented in detail because it is where the quantum cryptography is integrated. Section III familiarizes the readers with quantum cryptography and gives a state-of-the-art on the related works. In section IV, we describe the Quantum handshake, a scheme integrating QKD with 802.11i, and its enhanced version. Discussion on open issues and future works are also presented in section IV. Finally, we conclude the paper in section V.

II. 802.11i SECURITY MECHANISMS

A. The failure of WEP and the arrival of 802.11i

The first standard of 802.11 security defines WEP [10] (Wired Equivalent Privacy) for the authentication and data confidentiality of user data over the wireless link. Unfortunately, WEP was not well designed and presents serious vulnerabilities as follows.

- WEP uses only one secret key for both authentication and encryption. This is not a good security strategy. If the encryption key is discovered, we also lose the authentication key. In this case, the authentication key cannot be used to authenticate the user and generate a new encryption key.
- WEP is based on the RC4 algorithm [16], a stream cipher which has a set of weak keys and becomes especially vulnerable if one part of the key is disclosed to attackers. In WEP, the RC4 key is the concatenation of an Initialization Vector (IV) of 24 bits which is sent in plain text together with the encrypted frame, and a WEP key of 40 bits. Attackers can collect IVs to detect weak keys. In addition, because IV is directly used as a part of the RC4 key, passive attacks can be easily realized to reveal the WEP key.
- The IV is not necessary to be secret but it should be used only once together with a given secret key. Unfortunately, WEP does not have any mechanism to avoid repeated IV during the use of a given secret key. In addition, with the bit rate of 11Mb/s of 802.11b, the space of IV is exhausted after about 8 hours. This fact requires a renewal of the secret key every 8 hours which is impossible in WEP because WEP does not define any mechanism to dynamically establish new secret key between mobile device and access point.
- WEP uses CRC-32 to protect messages from undesired modifications. CRC-32 is not a good message integrity protection algorithm, especially when the encryption algorithm is vulnerable.

The failure of WEP leads to the need of a new standard for the 802.11 security. In this context, 802.11i [8] is defined to rectify the flaws of WEP.

802.11i received much attention from specialists in cryptography and network security. All the four above mentioned flaws are addressed and rectified. First, authentication key and encryption key are separated. While the authentication key is a long term secret, encryption keys are temporal keys and dynamically generated during the authentication process. Second, a

new encryption algorithm, CCMP (Counter mode with CBC-MAC Protocol) based on AES (Advanced Encryption Standard) [17], is used to replace the WEP algorithm based on RC4. AES is much stronger than RC4 but it requires a hardware modification for the transition from WEP-based systems. For the transition from WEP to CCMP, 802.11i defines also another encryption algorithm, TKIP (Temporal Key Integrity Protocol), which is based on the RC4 algorithm [16] and only requires a software upgrade on WEP-based systems. The support of TKIP in 802.11i system is optional and only used for the transition from WEP-based system to CCMP. Third, mechanisms to avoid the reuse of IV and to dynamically establish new encryption keys are defined. Fourth, a MAC (Message Authentication Code), also called a MIC (Message Integrity Code) is used for message integrity protection in place of the CRC-32 checksum. Using a MIC is much better than using CRC-32 because the calculation of MIC requires a secret key shared between the communicating parties.

B. 802.11i authentication and key management

In this section, we present in detail the 802.11i authentication and key management, especially the 4-way handshake, to facilitate the understanding of the integration of quantum cryptography in 802.11i presented in section III.

In 802.11i, the authentication and the cryptographic keys establishment procedures are strongly tied together. A summary of the authentication and key management process in 802.11i is shown in Fig. 1. Three elements participating to the authentication and key management are the supplicant, the authenticator, and the authentication server. The supplicant corresponds to the mobile terminal which wants to joint a network. The authenticator corresponds to the access point which realizes the access control and only admits data traffic from supplicants who are authenticated by the authentication server. The authentication server is a centralized server which can access the authentication key database to authenticate mobile users. The authentication and key management can be divided into two parts. The first part aims at the distribution of the Pairwise Master Key (PMK) to the supplicant and the authenticator. The second part consists of the mutual authentication and the establishment of the Pairwise Transient Key (PTK) between the supplicant and the authenticator based on the obtained PMK.

802.11i defines two authentication and key management methods: 802.1X authentication and

preshared key. 802.1X authentication is suitable for large network having an important number of access points. An authentication server is used to avoid the duplication of authentication key database into access points. The 802.1X authentication is based on EAP (Extensible Authentication Protocol) [11] which allows supporting various authentication methods. Depending on the EAP method used, we can have a strong or weak, simple or mutual authentication. For instance, the EAP-TLS method [12] allows a mutual authentication while the EAP MD5-CHALLENGE method [13] only provides the authentication of mobile terminal. The choice of EAP method depends on the available security infrastructure and the level of security required by the organization. During the EAP-based authentication between the supplicant and the authentication server, the PMK is derived by the mobile device and the authentication server from the AAA (Authentication, Authorization and Accounting) key. The EAP-based authentication and PMK establishment between the supplicant and the authentication server corresponds to step 1 in Fig. 1. Once established, the PMK is sent from the authentication server to the access point serving the mobile terminal (step 2 in Fig.1), accomplishing the task of distribution of the PMK to the supplicant and the authenticator. Upon having the PMK, the access point starts the 4-way handshake for the mutual authentication and the derivation of the Pairwise Transient Key (PTK) with the mobile terminal (step 3 in Fig.1).

The preshared key authentication method is suitable for small network. There is not authentication server and no EAP-based authentication is needed. A preshared secret key is installed in both the supplicant and the authenticator by some means outside the 802.11i standard. This preshared key is used as the PMK. The authenticator and the supplicant only need to execute the 4-way handshake for the mutual authentication and the derivation of the PTK between them based on the PMK configured. In other words, only step 3 in Fig.1 is involved in the authentication and key management using preshared key.

C. 4-way handshake

802.11i uses many keys at different levels, constituting a key hierarchy. Fig. 2 presents the Pairwise Key Hierarchy containing the keys related to the encryption of unicast traffic. At the top level, we have the master key called Pairwise Master Key (PMK) which is used to derive the other keys. There are two ways to establish the PMK, one based on the preshared key, and one based on

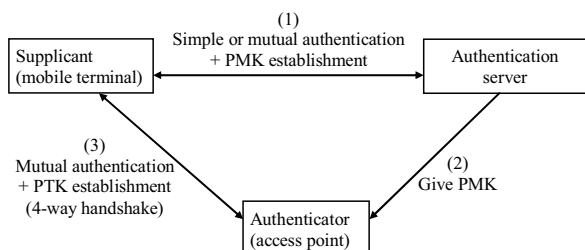


Figure 1. Summary of authentication and key distribution

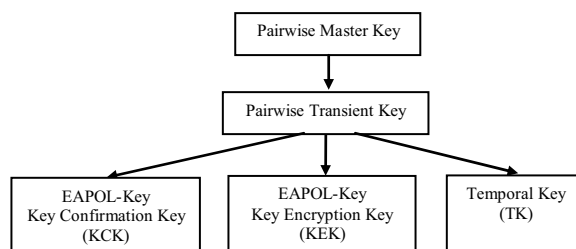


Figure 2. Pairwise Key Hierarchy.

the use of authentication server as presented in section B. The Pairwise Transient Key (PTK) is established between the access point and the mobile terminal during the 4-way handshake. This PTK is then split into three final temporal keys: EAPOL-Key Key Confirmation Key (KCK), EAPOL-Key Key Encryption Key (KEK), and Temporal Key (TK).

The information exchanged between the supplicant and the authenticator during the 4-way handshake is carried by the EAPOL-Key messages, a message type of the EAPOL (EAP over LAN¹) protocol [14]. The KCK is used to calculate the MIC (Message Integrity Code) of EAPOL-Key messages during the 4-way handshake. The KEK is used to encrypt the Group Temporal Key (GTK), the key related to the encryption of the multicast traffic, when the access point distributes the GTK to mobile terminals using EAPOL-Key messages. The TK is used to encrypt unicast user data traffic.

We recall that 802.11i separates authentication key and encryption key. Only the authentication key used for the EAP-based authentication (in case of 801.1X authentication) or for the preshared key configured in the mobile terminal and the access point (in case of preshared key authentication) is static and long term secret. Encryption key is a temporal key which has a limited lifetime. The encryption key distribution process is the 4-way handshake presented in Fig. 3.

At the beginning, the supplicant and the authenticator are not authenticated to each other and the key hierarchy is not established. The only secret shared between the supplicant and the authenticator is the PMK. The 4-way handshake is started by the Authenticator by sending a value ANonce (Authenticator Nonce) to the Supplicant. Upon receiving the value ANonce, the Supplicant generates the value SNonce (Supplicant Nonce) and has all materials to build the key hierarchy. To build the Pairwise key hierarchy, the Supplicant uses a Pseudo Random Function (PRF) to derive the PTK of 384 bits (for CCMP) or 512 bits (for TKIP) from the PMK, the MAC (Medium Access Control) address of the Authenticator (A-MAC), the MAC address of the Supplicant (S-MAC), the ANonce, and the SNonce. The PTK is then split into a KEK of 128 bits, a KCK of 128 bits, and a TK of 128 bits (for CCMP) or 256 bits (for TKIP). However, this key hierarchy is not used until the Authenticator is authenticated and ready to use these keys.

In the second message of the 4-way handshake, the Supplicant sends to the Authenticator the value Snonce and a MIC calculated based on the content of the message and the KCK which has just derived. The algorithm used to calculate the MIC is HMAC-MD5 [13, 26] or HMAC-SHA1-128 [26, 27] depending on the cipher suite chosen for the system. Upon receiving this message, the Authenticator has all materials to build the same key hierarchy. Then it uses the KCK to check the MIC. If the MIC is correct, that means that the Supplicant obtains the PMK, and thus the Supplicant is authenticated.

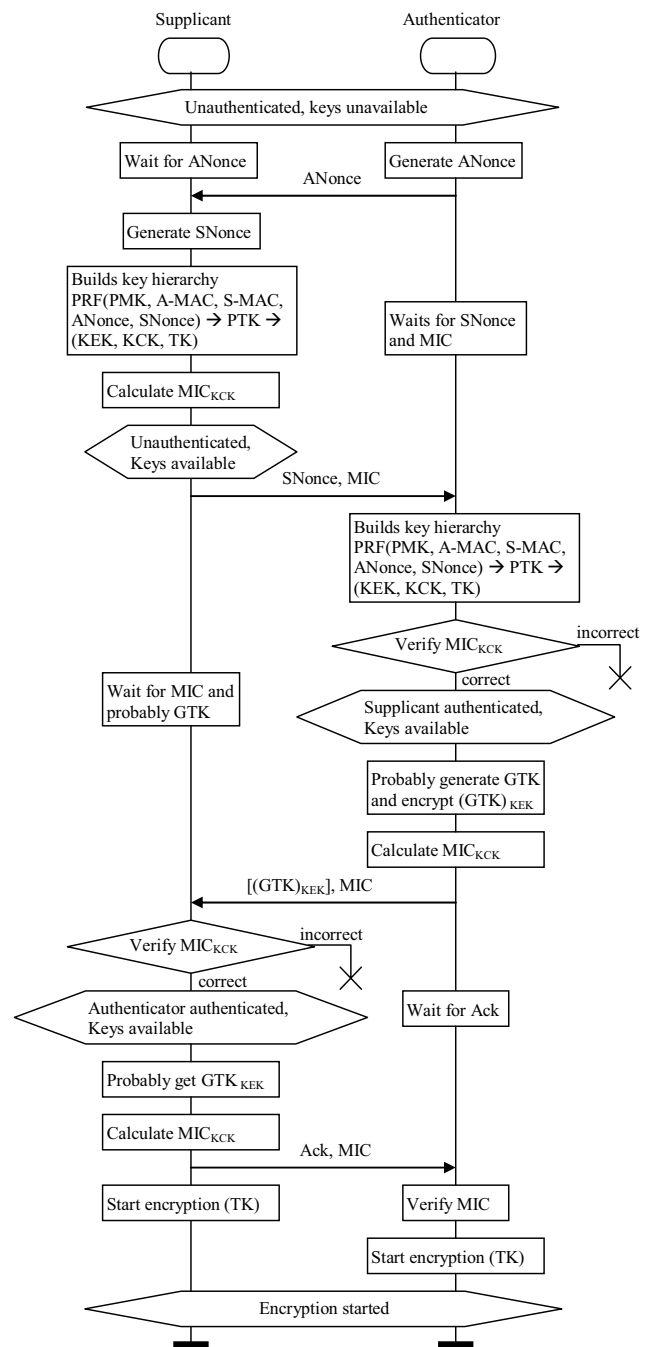


Figure 3. The 4-way handshake.

In the third message of the 4-way handshake, the Authenticator tells the Supplicant that it has finished the derivation of the key hierarchy. It also sends a MIC calculated based on the content of the message and the KCK which has just derived. Upon receiving this message, the Supplicant checks the MIC in order to verify that the Authenticator obtains the PMK, and thus authenticates the Authenticator. Then, the key hierarchy can be used without the doubt about the authenticity of the access point. The third message of the 4-way handshake can be used by the access point as a means to distribute the GTK to the mobile terminal. In this case,

¹ LAN stands for Local Area Network

the GTK is sent encrypted using the KEK in the key hierarchy just derived.

The last message of the 4-way handshake is for the purpose of synchronization. The Supplicant tells the Authenticator that the 4-way handshake is now successfully completed and both can turn on the encryption of user data. This message also includes a MIC to assure the Authenticator that this message is sent by the Supplicant and that it is not modified.

After the 4-way handshake, the Temporal Key (TK) is used by the encryption algorithm to provide confidentiality and the integrity of user data.

III. QUANTUM KEY DISTRIBUTION

A. Quantum cryptography

Quantum cryptography aims at exploiting the laws of quantum physics in order to carry out a cryptographic task. For the moment, the use of quantum physics at cryptographic ends is limited mainly to the distribution of secret keys. That's why we very often use the more precise term of quantum key distribution. The quantum key distribution rests on a common function of the whole protocols, namely the combined use of a traditional channel and a quantum channel. The quantum nature of the data carrier ensures Alice and Bob that the information conveyed on the quantum channel could be spied only by taking measurements, and thus by introducing disturbances. This sensitivity of the quantum channel to espionage is based on various points. First, it is impossible to duplicate an arbitrary quantum state, like that was shown by W. Zurek and W. K. Wootters in 1982 [18]. Second, the encoding of the quantum bits can be made sensitive to espionage since information is coded on at least two non-orthogonal states. Indeed, any measurement of a quantum object carried out in a basis other than the basis of which the quantum state is created will have an effect on the measured object. For that reason, the sender and receiver could obtain a real secret key, providing the use of some protocols including key distribution, key reconciliation and privacy amplification protocols. The quantum key distribution (QKD) is said "unconditionally secure", i.e. independent of the computation power of the spy, and more generally of the technology that he has.

B. BB84 and other QKD protocols

Up to now, several QKD protocols have been proposed since the birth of the first one BB84. BB84 was introduced by Bennet and Brassard in 1984, thus it was named BB84 [19]. In 1994, this protocol was proved to be secure against eavesdropping by Dominic Mayers, Eli Biham, and Michael Ben-Or [20, 21]. BB84 is a non-deterministic protocol, which means that it is useful only for the distribution of a random sequence. BB84 is a four-state protocol. Other protocols can be a two-state protocol (e.g. the B92 [15]), a three-state protocol or a six-state protocol. The BB84 and B92 protocols are nowadays widely used. These protocols are securely proven and largely experimented.

Multiple techniques have been developed enabling quantum cryptography. We will in particular mention three techniques:

- Autocompensating weak laser pulse systems [22]: This technique has been extensively studied and is used in commercially available products. Its particularity is that it is invariant to the polarization rotation of the photon induced by the use of fiber optic.
- Entangled photons [23]: Two photons are generated in a manner that their states are conjointly defined. One is sent to Alice, the other to Bob. Each person then measures the photons' polarization.
- Continuous Variable [24]: In this technique the information is not based on the photons' polarization but coded on the phase or amplitude of the light pulses.

As we use the BB84 for the integration of quantum cryptography in 802.11 networks, the remainder of this section is dedicated to the description of this protocol. The operating mode of BB84 as published in 1984 in the International Conference on Computers, Systems and Signal Processing (in Bangalore, India), consists on two main steps [19]: Quantum transmission as presented in Fig. 4, and public discussion.

In the phase of quantum transmission, the information is encoded in non-orthogonal quantum states. This could be a single photon with a polarization direction of 0 (\leftrightarrow), $\pi/4$ (\nearrow), $\pi/2$ (\updownarrow) or $3\pi/4$ (\searrow). The sender and the receiver must agree first on the meaning of the photon polarizations for instance 0 or $\pi/4$ for a binary 0, and $\pi/2$ or $3\pi/4$ for a binary 1. The sender (Alice) generates a random bit string and a random sequence of polarization bases then sends the receiver (Bob) photon by photon. Each photon represents a bit of the generated bit string polarized by the random basis for this bit position. When receiving photons, Bob selects the polarization filters (rectilinear or diagonal) to measure the polarization of the received photon.

In the phase of public discussion, after finishing the quantum transmission Bob reports the bases that he picked for each received photon. Alice checks Bob bases and says which ones were correct as described in Fig. 5. Bob and Alice take the bits resulting from these correct bases, these bits are only known by Alice and Bob. At this moment Alice and Bob share a secret bit string. This

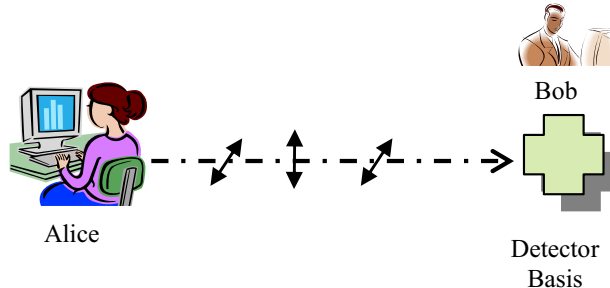


Figure 4. Photon exchange.

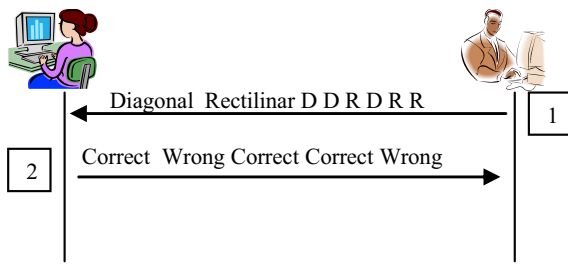


Figure 5. Validation of Bob bases.

exchange is unconditionally secure providing that there is no eavesdrop or active attack and that the quantum channel is perfect. However, as an attack is always possible and the quantum channel is usually imperfect, an additional step is used to estimate the error rate [19]. In this step, Bob chooses a random sequence of testing bits and sends it back to Alice. Alice checks whether these bits are in conformity with those sent by Alice originally. If there is an attack on the quantum channel the error rate will be about 25% or higher. In this case, Alice and Bob detect the eavesdropper. Otherwise, i.e. the error rate is less than 25%, the two parties discard the revealed bits and take the resulting stream as the secret key. The secrecy of this final stream is unconditional [20, 21].

Other steps could be applied to enhance the secrecy and generalize the unconditional security of key exchange. These steps are done mainly by error correction and privacy amplification.

C. Related works using quantum cryptography in mobile wireless networks

Free space QKD uses the air as the medium for the transmission of photons between the quantum sender and receiver. The feasibility of QKD over the air is considered problematic because of a medium with varying properties and a high error rate. However, the study and experiments of QKD systems showed that these problems are tractable [33]. In contrast to the optical fibers, free space has a high transmission window where photons can be easily detected and a non-birefringent characteristic which does not alter the polarization state of the photon [34].

Although preliminary research and experiments on free space QKD start from a short distance and indoor environment, the final objective of these research and recent experimental systems is towards long distance and outdoor systems such as satellites [4] or laser communication systems. The two approaches the most used in free space QKD studies are single qubit scheme based on faint-laser pulses and entanglement based quantum cryptography. Some recent results of the research on free-space QKD systems that can be cited as examples are the practical free-space QKD system over 10km on mountains using laser pulses and the BB84 protocol [25], the practical free space QKD system over 500m between two buildings in a city using weak coherent pulse and the BB84 protocol [35], the proposed free-space QKD system between satellites using entangled photons [16], and the experimental free space

QKD system over 7.8 km between buildings using entangled photons [36].

Different from above mentioned studies, our proposal [29] aims at a short distance and an indoor environment, the wireless local area network 802.11. In comparison to the presented related work, our work has some advantages of the shorter distance and a better environment against bad weather conditions. The apparatus in our system may have a smaller size and 802.11 access points can be found almost everywhere indoor. For a QKD system used together with a satellite or laser based data communication system, the outdoor environment can be much noisy. The large distance may need a bigger size apparatus, and the final mobile users who are inside a building cannot directly have a line-of-sight optical path with the satellite or with the communicating point of a laser data transmission path, which is usually installed at the top of a high building. In fact, our proposal is final mobile user centric while previous related works are communication system centric. Hence, our work is not contradictory to the previous works but very complementary. The final mobile user can use our approach to establish a quantum key with the access point and secure the wireless link. The remainder part of the end-to-end communication can be secured also by quantum cryptography but realized by a fiber-based, satellite-based or laser-based communication system.

The disadvantage that we can encounter in comparison with the other related work is the problem of maintaining a line-of-sight path between the apparatus of the mobile user and the apparatus of the access point. A solution to this issue will be discussed in the next section of the paper. In satellite or laser communication system, the communicating entities (e.g. ground station, satellite, or laser communicating point) are usually installed in a well chosen place and have a relatively stable line-of-sight path.

IV. INTEGRATING QKD IN 802.11i

A. How to integrate QKD in 802.11i ?

Our main objective is using quantum cryptography to establish the key used for the encryption of user data in 802.11i, which is the TK. As the TK is part of the PTK which is established during the 4-way handshake, we modify the 4-way handshake to integrate the BB84 protocol and call it the Quantum handshake.

Fig. 6 summarizes how different keys are generated during the Quantum handshake. The KCK is generated from the PMK to serve the mutual authentication of the supplicant and the authenticator and protect the BB84 protocol from the man-in-the-middle attack. Once the mutual authentication finished, the supplicant and the authenticator starts the BB84 protocol for the establishment of the Q-PTK of 256 bits (for CCMP) or 384 bits (for TKIP). The Q-PTK is then splits into the KEK of 128 bits and the TK of 128 bits (for CCMP) or 256 bits (for TKIP).

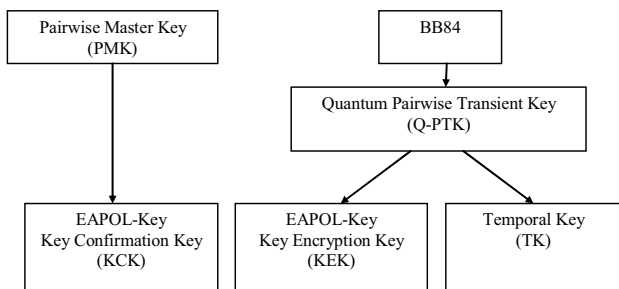


Figure 6. Keys establishment schema in the Quantum handshake

It is easy to see that we can use quantum cryptography to establish the PTK, thus all KEK, KCK and TK are established using quantum cryptography. However, the BB84 protocol itself needs an authentication method to append a MIC to every messages exchanged. Otherwise, the BB84 protocol is vulnerable to the man-in-the-middle attack [9]. We decide to keep the authentication related elements unchanged for the moment. The integration of quantum cryptography into 802.11i should be step in step and changes should be minimized at the beginning. A step in step and modular integration will facilitate the experiment and testing process. For this reason, the principle of generating the KCK remains unchanged. That means that the KCK is generated from the PMK within the mutual authentication process between the mobile terminal and the access point. Once the KCK is generated and both the supplicant and the access point are authenticated, the BB84 protocol is used to establish the encryption key TK.

As the GTK, the key used for the encryption of group traffic, is distributed from the access point to the mobile terminal via the encryption using the KEK, we decide to establish also the KEK by quantum cryptography to secure more the GTK distribution process.

B. Quantum handshake

In the first design of the Quantum handshake [29] presented in Fig. 7, the BB84 protocol is started when the Supplicant is authenticated by the authenticator but the Authenticator has not been authenticated yet. The authenticator is only authenticated after the fifth message of the Quantum handshake. This design presents a problem of potential waste of resources. If the access point is a fake one, the photons are exchanged before the fake access point is detected.

Fig. 8 presents the enhanced version of the Quantum handshake. The three first messages of the Quantum handshake allow the Supplicant and the Authenticator to derive a fresh KCK and authenticate each other before starting the BB84 protocol.

In the first message of the Quantum handshake, the Authenticator sends the ANonce value in order for the Supplicant to be able to generate the KCK. Upon receiving this message, the Supplicant generates the SNonce value. The PRF function is used to derive the KCK of 128 bits from the PMK in a way similar to the generation of the PTK in the 4-way handshake.

In the second message, the Supplicant sends to the Authenticator the SNonce value and a MIC calculated

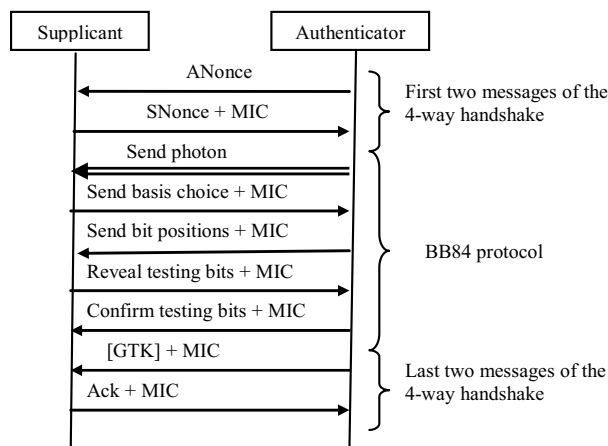


Figure 7. The first design of the Quantum handshake.

based on the message content and the KCK just derived. When this message arrives at the Authenticator, the access point has all materials to build the KCK and use it to authenticate the Supplicant via the verification of the MIC received.

If the Supplicant is authenticated, the Authenticator sends the third message of the Quantum handshake appending a MIC allowing the Supplicant to authenticate the authenticator. This message can also be used as a control message for the QKD process. For example, this message can send a QKD-start signal to inform the Supplicant that the access point is ready to receive photons from the mobile terminal.

If the Authenticator is authenticated, the Supplicant starts the photon transmission step of the BB84 protocol. The BB84 procedure is described in Fig. 9. The roles of quantum sender (Alice) and quantum receiver (Bob) are interchangeable for the supplicant and the authenticator. In this paper, the supplicant corresponds to Alice and the authenticator corresponds to Bob. The other design in which the supplicant corresponds to Bob and the authenticator corresponds to Alice is possible providing that all steps of the BB84 protocol [19] are respected.

At the beginning of the quantum transmission step, the supplicant sends to the authenticator a series of polarized photons. The number of photons to be sent depends on the length of the desired Q-PTK, the key reconciliation algorithm and the privacy amplification algorithm used. Let's call the number of photon to be sent N. For the generation of each photon, the supplicant randomly chooses a bit value of 0 or 1 and encodes this information by the polarization of the photon using a basis which is randomly chosen. We recall that the possible bases and information coding rules are agreed between the supplicant and the authenticator beforehand. They are usually defined in the technical specification of the system.

For the reception of each photon, the authenticator measures each photon using a basis which is randomly chosen and decodes the polarized photon to obtain the carried information. After receiving all N photons, the system finishes the quantum transmission step. Only this step uses the quantum channel which is described as a double line arrow in Fig. 9. Further steps are realized over the radio link as other above mentioned Quantum

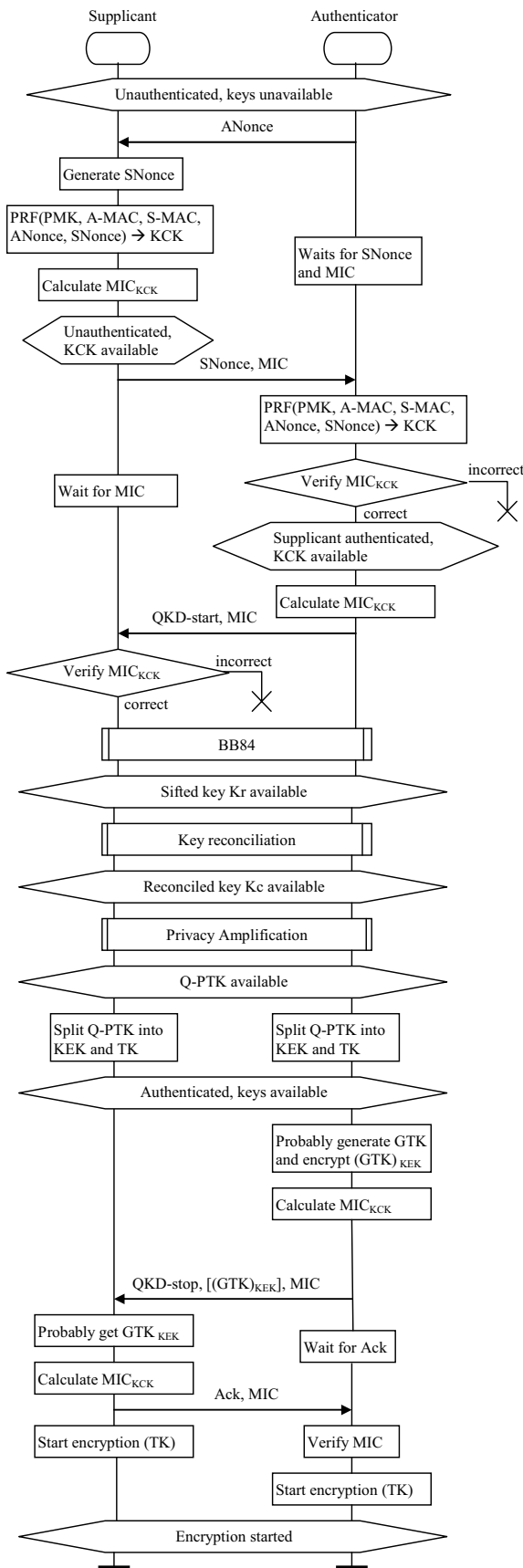


Figure 8. Enhanced version of the Quantum handshake.

public discussion of the BB84 protocol can be easily carried by EAPOL-Key frames.

The authenticator starts the public discussion step by announcing the N bases that it used to receive the N photons. The first message of the public discussion is sent to the supplicant over the radio link and appended with a MIC calculated based on the content of the message and the KCK just established. This MIC assures the integrity and the authenticity of the message.

Upon receiving the bases announcement of the authenticator, the supplicant compares the bases used for the sent photon and those used for the received photons. Assuming that there are M (M < N) photons which are sent and received with the same basis. In the second message of the public discussion, the supplicant tells the authenticator the M bases which were correct. This message as well as further messages during the public discussion are protected by a MIC calculated using the KCK.

The supplicant and the authenticator keep only the M bits corresponding to the M correct bases. These bits can be the shared secret information if there is no eavesdrop and the quantum channel is perfect without noise. However, eavesdrop is always possible and the quantum channel is usually noisy. The supplicant and the

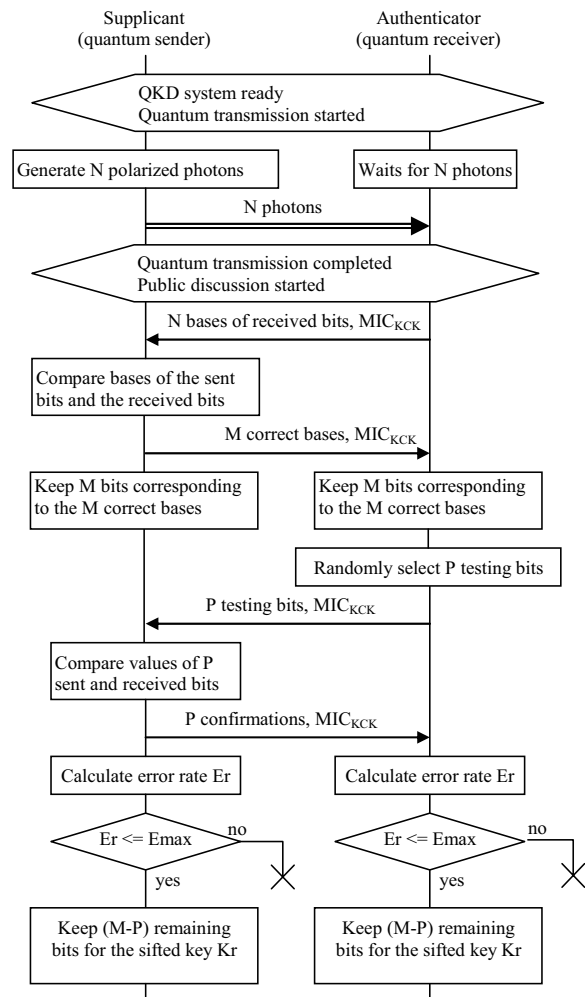


Figure 9. The BB84 procedure.

handshake messages. The information exchanged in the

authenticator will detect the probably happened eavesdrop based on an error rate estimation. For this task, the authenticator randomly selects P testing bits ($P < M$) among the remaining M bits. P can be one third of M following the BB84 protocol [19]. In the third message of the public discussion, the authenticator reveals the values of the P testing bits to the supplicant.

In theory, the photons sent and received with the same basis should yield the same information value. The authenticator and the supplicant should have the same values for the P testing bits. In practice, the photon's polarization can be changed during the transmission over the quantum channel by the presence of eavesdropping or the noise of the quantum channel, leading to the disagreement on the values of the testing bits. A bit 1 encoded by a photon which is sent and received with the same basis can be decoded into a bit 0. Upon receiving of the values of the P testing bits, the supplicant compares them with the values of their original values. In the fourth message of the public discussion, the supplicant confirms the values of the P testing bits with the authenticator. The error rate is calculated as follows.

$$Er = \frac{\text{Number of disagreed testing bits}}{P}$$

If the error rate Er is smaller than a threshold E_{max} , we can conclude that there was no eavesdrop and the error bits are caused by the imperfection of the quantum channel. Otherwise, the quantum transmission was eavesdropped and the photon measurement of the eavesdropper caused an unusual high error rate to quantum transmission. The value of E_{max} depends on the quantum transmission quality of specific QKD systems. If the quantum transmission is concluded "no eavesdropping" after the estimation of the error rate Er , the P testing bits are removed from the M bits. The remaining $M-P$ bits are used as the sifted keys K_r shared between the supplicant and the authenticator, finishing the BB84 procedure. If eavesdropping is detected, the transmitted photon cannot be used. The Quantum handshake is terminated without establishing necessary keys.

After the BB84 procedure resulting in the sifted key K_r , the two versions of this key at the supplicant and the authenticator sides may be still different because of a small error rate caused by the noisy quantum channel. Two procedures need to follow the BB84 procedure as presented in Fig. 8 are key reconciliation and privacy amplification. The key reconciliation procedure is a public discussion between the supplicant and the authenticator to correct errors between the two versions of the key K_r . There are several reconciliation approaches in the literature. The Cascade protocol [28] is the most used in experimental and commercial QKD systems for its simplicity and efficiency. The privacy amplification procedure [30] is also a public discussion between the supplicant and authenticator to lower the amount of information about the final key that an eavesdropper can get from the messages exchanged during the key reconciliation procedure. For the sake of simplicity and

the available space of the paper, we leave the key reconciliation and privacy amplification procedures as implementation dependent and do not present in detail any reconciliation or privacy amplification protocol in this paper. As some bits of the sifted key K_r can be removed during the key reconciliation process, the reconciled key K_c can have a reduced length ($K_c \leq K_r$). However, once established, the two versions of the K_c at the supplicant and the authenticator will be the same. After the privacy amplification procedure, length of the reconciled K_c is reduced again to build the final key $Q-PTK$ ($Q-PTK < K_c$).

Once the $Q-PTK$ is established, it is split into the KEK and the TK. Until this step, the Quantum handshake achieves its goal of mutual authentication and keys distribution between the supplicant and authenticator. In the next message, the authenticator can profit this handshake to distribute the GTK which is encrypted using the KEK just derived. This message can be also used to carry some control signal of the QKD system such as a QKD-stop signal to synchronize some internal state of the supplicant's and authenticator's finite state machines. After receiving the QKD-stop signal and probably getting the GTK from the authenticator, the supplicant sends the last message to synchronize the starting of user data encryption.

C. Discussion on open issues and future works

In this section, we discuss about the way towards an unconditionally secure cryptosystem for 802.11 networks, the apparatus network solution to the line-of-sight problem, and future implementations of the Quantum handshake.

The Quantum handshake is our first tentative to integrate quantum key distribution in 802.11 wireless network. This integration is designed with the intention of keeping minimal changes for 802.11i. The 802.1X authentication, the method used for mutual authentication between the supplicant and the authenticator, as well as the algorithm for the MIC calculation during the Quantum handshake remain unchanged in comparison with 802.11i. In fact, the use of EAP and an authentication server in 802.1X authentication allows flexibility in the deployment of 802.11 systems. Various authentication methods can be used. Client authentication and authorization information does not need to be distributed to every access points. As an unconditionally secure cryptosystem needs an authentication mechanism, a key distribution means, and an encryption algorithm which are unconditionally secure [9], we will consider, in the next step, how to support an unconditionally secure authentication method for 802.11 and how this support impacts this flexibility. A promising approach is the use of an initial short secret distributed to mobile user via smartcard together with an unconditionally secure authentication such as the Wegman-Carter authentication [31]. The use of an unconditionally secure encryption algorithm in 802.11 is also a future work towards a long-term absolutely secure cryptosystem. An issue imposed by the use of the One Time Pad (OTP) [16], the unconditionally secure encryption algorithm, is that the

bit rate of user data can be considerably reduced. As OTP requires that the length of the key must be equal to the length of the message, the key rate is equal to the data rate. Current practical free space QKD systems can provide a key rate of 60 kb/s for a distance of 500m outdoor. However, hope that the shorter distance together with the indoor environment of 802.11 networks can allow a higher key rate. When QKD systems cannot satisfy the key rate demand, some early system can add OTP to 802.11 encryption library and use it for only some critical traffic. For instance, the distribution of the GTK (128 bits) in a CCMP system can be realized by the encryption of this key using OTP and the KEK (128 bits) generated by QKD during the Quantum handshake.

From the quantum transmission point of view, the line-of-sight path can be an open issue. The movement of mobile users and other people in the room can make an ongoing quantum channel become unavailable. In a mobile network, the quantum apparatus should be turnable as illustrated in Fig. 10. That means that quantum apparatus can flexibly adjust their directions to maintain a line-of-sight path in a hall or in a room. A protocol communicating between the mobile terminal and the fixed part of the apparatus network is necessary to control the direction of the mobile and the fixed serving apparatus. To facilitate the find of alternative line-of-sight paths, the fixed apparatus can be implemented with a sufficiently high density. The control protocol will help the mobile apparatus to choose the most appropriate fixed apparatus for the providing of the best line-of-sight path.

The realization of the apparatus network is an interdisciplinary issue requiring the collaboration of scientists at least in physics and telecommunications. At the beginning, the mobile apparatus can be an external module connecting to the laptop via an USB port and have a capability to turn around a support like a webcam. With the progress in optical technologies, we hope that the apparatus will have a reasonably small size. An automatic alignment protocol is necessary to obtain a maximal quantum transmission [32]. The control protocol of the apparatus network should be able to detect the presence of a new mobile device. A positioning technique with a high precision probably up to centimeters is

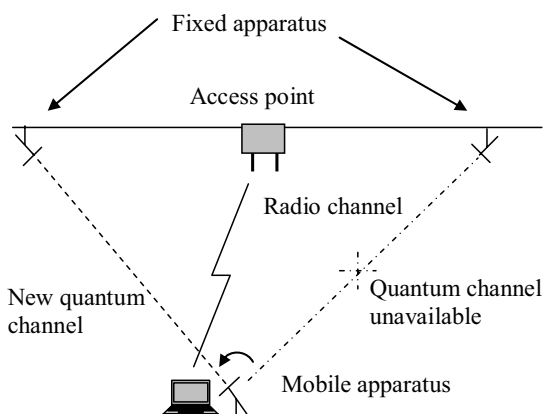


Figure 10. Apparatus network.

needed to locate the mobile apparatus in the hall. This is a difficult problem and needs a very detail location database. Once the position of the mobile apparatus is determined, the control protocol chooses one of the available fixed apparatus which would provide the best line-of-sight for the transmission of photons. If an obstacle is detected during the use of a quantum channel, the system gives instructions to the mobile terminal to use another available fixed apparatus.

The control protocol should have interaction with the Quantum handshake. In case the system is exchanging photons and the ongoing line-of-sight becomes unavailable, the control protocol should inform the Quantum handshake in order to synchronize the photon transmission procedure via the new line-of-sight path. If the system received x photons ($x < N$, N is the total number of photons to be exchanged) before the corruption of the ongoing quantum channel, only $N-x$ new photons must be sent via the new quantum channel. In fact, the quantum apparatus is just the means to send photons. The photon parameters such as the polarisation state of the photon to be sent are controlled and decided by the access point or the mobile device depending on which one is the sender. When the ongoing quantum channel is corrupted, the Quantum handshake is hanged on. The receiver uses a control message to inform the sender the number of photons it successfully received. When the new quantum channel is ready, the Quantum handshake continues the photon exchange procedure.

The implementation of the Quantum handshake is needed to test the first step in the integration of quantum cryptography in 802.11 networks. A specification of detail parameters such as the number of photons to be transmitted N , the number of testing bits P , and the quantum bit error rate threshold E_{max} as described in section IV-B should be realized. The choice of reconciliation protocol and privacy amplification method taking into account the impact of wireless networks, the simulation of the system for resulting in numerical results, and the evaluation of performance of the system are also a future work. The comparison between the results obtained from the experimental system and those from theoretical study is important to the system design verification, the reflection on open issues, and the determination of future research directions.

V. CONCLUSIONS

In this paper, we present an enhanced version of the Quantum handshake, a scheme integrating quantum key distribution in 802.11 networks proposed by our previous works. The Quantum handshake, a modified version of the 4-way handshake, is defined to integrate the BB84 protocol for the distribution of the cryptographic keys used by 802.11i. In the enhanced version, the mutual authentication between communicating parties must be done before the photon exchange to avoid potential waste of resources. The quantum handshake is our first step in the integration of quantum cryptography in mobile wireless networks. Open issues and future works related

to the integration of unconditionally secure authentication and encryption algorithm, the apparatus network to provide alternative line-of-sight paths, and the future implementation of the proposed system have been discussed. When the research on the application of quantum cryptography in mobile wireless networks is still very premature, we hope that the work presented in this paper can contribute to the evolution of this research field.

ACKNOWLEDGMENT

This work was supported by the EC-Integrated Project SECOQC, Project Number: FP6-2002- IST-1 -506813.

REFERENCES

[1] N. Namekata, S. Mori, and S. Inoue, "Quantum key distribution over an installed multimode optical fiber local area network", *Optical Express*, 2005.

[2] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug and play system," *New Journal of Physics*, Vol. 4, 2002, pp. 41.1–41.8.

[3] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, and K. Nakamura, "Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector", *Electronics Letters*, Vol. 39, 2003, pp. 1199–1200.

[4] C. Kurtsiefer, P. Zarda, M. Halder, P.M. Gorman, P.R. Tapster, J.G. Rarity and H. Weinfurter. "Long Distance Free Space Quantum Cryptography", 2003.

[5] <http://www.idquantique.com>

[6] M. Aspelmeyer, T. Jennewein, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites", *IEEE Journal of Selected Topics in Quantum Electronics*, Vol. 9, Issue 6, November 2003.

[7] ANSI/IEEE Standard 802.11, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999 Edition, Reaffirmed June 2003.

[8] IEEE Standard 802.11i, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 6: Medium Access Control (MAC) Security Enhancements, July 2004.

[9] K. G. Paterson, F. Piper, and R. Schack, "Why quantum cryptography ?", *Quantum physics*, quant-ph/0406147, June 2004.

[10] J. Edney, and W..A. Arbaugh, *Real 802.11 Security - Wi-Fi Protected Access and 802.11i*, Addison-Wesley, 2004.

[11] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowitz, "Extensible Authentication Protocol (EAP)", RFC 3748, June 2004.

[12] B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999.

[13] R. Rivest, "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[14] IEEE Standard 802.1X, Port-based Network Access Control, December 2004.

[15] C. H. Bennett, "Quantum Cryptography using any two nonorthogonal states", *Physical Review Letter*, Vol. 68, pp. 3121-3124, May 1992.

[16] B. Schneier, *Applied Cryptography*, John Wiley & Son, 1996.

[17] National Institute of Standards and Technology, FIPS Pub 197: Advanced Encryption Standard (AES), November 2001.

[18] W.K. Wootters, and W.H. Zurek, "A single quantum cannot be cloned", *Nature*, Vol. 299, 1982, pp. 802-803.

[19] C. Bennet, and G. Brassard, G. "Quantum cryptography: Public key distribution and coin tossing", *IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE Press, LOS ALAMITOS, 1984.

[20] D. Mayers, "Unconditional Security in Quantum Cryptography", *Journal of the ACM*, Vol. 48, 1998, pp. 351.

[21] H.K. Lo, and H.F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances", *Science*, Vol. 283, 1999.

[22] D.S. Bethune and W.P. Risk, "AutoCompensating quantum cryptography", *New Journal of Physics*, Vol. 4, 2002, pp. 42.1-42.15.

[23] Artur Ekert, "Quantum Cryptography based on Bell's Theorem", *Physical Review Letters*, 1991.

[24] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states", *Nature.com*, 2003.

[25] R. Hughes, J. Nordholt, D. Derkacs, and C. Peterson, "Practical free-space quantum key distribution over 10km in daylight and at night", *New Journal of Physics*, Vol. 4, 2002, pp. 43.1-43.14.

[26] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997.

[27] U.S. DoC/NIST, Federal Information Processing Standards (FIPS) Publication 180-1, Secure Hash Standard (SHS), April 1995.

[28] G. Brassard, and L. Salvail, "Secret-key reconciliation by public discussion", *Proceedings of Eurocrypt'93*, Springer-Verlag, 1994, pp. 410-423.

[29] T.M.T. Nguyen, M. A. Sfaxi, and S. Ghernaoui-Hélie, "Integration of Quantum Cryptography in 802.11 Networks", *Proceedings of the First International Conference on Availability, Reliability and Security (ARES)*, pp. 116-123, Vienna, April 2006.

[30] C.H. Bennett, G. Brassard, and J.M. Robert, "Privacy amplification by public discussion", *SIAM journal on Computing*, Vol. 17, No. 2, April 1988.

[31] M.N. Wegman, and J.L. Carter, "New hash function and their use in authentication and set equality", *Journal of Computer and System Sciences*, Vol. 22, pp. 265-279, 1981.

[32] H. Weier, "Experimental Quantum Cryptography", *Diploma thesis, LMU Munich*, December 2003.

[33] W.T. Buttler, R.J. Hughes, P.G. Kwiat, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C. M. Simmons, "Free-space quantum key distribution", *arXiv:quant-ph/9801006 v1*, January 1998.

[34] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", *arXiv:quant-ph/0101098 v2*, September 2001.

[35] <http://xqp.physik.uni-muenchen.de/exp/qc2/index.html>

[36] K.J. Resch, M. Lindenthal, B. Blauensteiner, H.R. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger, "Distributing entanglement and single photons through an intra-city, free-space quantum channel", *Optics Express*, Vol. 13, No. 1, January 2005.

Thi Mai Trang Nguyen received her Engineer degree in telecommunications from HoChiMinh city University of Technology, Vietnam, in 1999, M.S. degree in computer science and networking from University of Versailles, France, in 2000, and Ph.D degree in computer science from University of Paris 6, France, in 2003.

She involved in many national and European projects related to the development of the next generation of the Internet. She was research scientist at France Telecom in 2004 and has been postdoctoral researcher at University of Lausanne since 2005. She published in several international journals and has one French patent on mobile networking. Her research interests include quality of service, mobility management, and security in fixed and mobile networks.

Dr. Nguyen is an IEEE member.

Mohamed Ali Sfaxi, Computer Science Engineer, is a PhD student in Information Systems at the Business School of the University of Lausanne, Switzerland. Mr. Sfaxi obtained his engineering diploma in Computer Science from the Computer science school of Tunis, Tunisia.

He participated in various projects such as the European project SECOQC and now is working as a professor assistant at the University of Lausanne, Switzerland. His research interests are in IT security, communication protocols, cryptography and network administration.

Mr. Sfaxi is a member of IEEE. He won the best paper award in ICETE 2005 conference.

Solange Ghernaouti-Hélie is Professor at the University of Lausanne, Switzerland. She received her Ph.D degree in computer science from University of Paris 6, France, in 1986.

She was network architect, expert in standardisation (AFNOR, SPAG, ISO), and marketing product manager of IT international companies. Since 1987, she has been full professor at the University of Lausanne. At present, she is Vice-Dean of the School of Economics and Management and Business School of the University of Lausanne and also Director of the Information System Institute (Inforge). Specialized in information technology security and computer related crime, she is an international expert and a senior consultant in network and information system security. Her research interests include Information, computer and network security; Informational and technological risks; Data-processing criminality, Trust and proof in digital environments; Social, legal, and economic dimensions of IT security; Personal data protection and privacy; Security certification and assurance.

Prof. Ghernouti-Hélie is member of the Scientific Advisory Board of GMD (German National Research Center for IT) and Editorial advisor and editor of series for several publishers (since 1993, Masson, Dunod (F), Springer Verlag London (UK)). She is also member of United Nations - Economic Commission for Europe (UNECE) Steering group on Knowledge Economy Development.