Secured Scheme for Encryption Key Distribution in WLAN Using Quatum Cryptography

R.DJELLAB
Computer Science Department, University of Batna
Batna, Algeria
rima.djellab@gmail.com

M.BENMOHAMMED
Computer Science Department, University of Constantine
Constantine, Algeria
ben_moh123@yahoo.com

***Abstract*—WLANs are deployed almost everywhere and relevant information, as passwords, cards number, etc, are transmitted over wirelesses channels. Such information must be secure in such way that only legitimist communicants can read it. Cryptography is the main solution that allows participants A and B, to exchange data without risk of eavesdropping. Nevertheless, the classical cryptography is front of pertinent problematic, how to share a secured key to encrypt information? Shannon theory stipules that an encryption key is secured and can resist to all attacks even the one using quantum computation, if and only if it's randomly generated and used only once time.**

The Quantum Key Distribution, based on physical lows, offers the opportunity to generate completely random bit string that can be use for deriving encryption key. It seems also, to be the only technique that does not present vulnerability against the quantum calculating power.

In this paper, we present an enhanced scheme for deriving a secured encryption key for WLAN using the quantum key distribution principals.

Keywords-802.11i stadard, BB84, cryptography, key distribution, network security, QKD, quantum cryptography, security, wireless network.

I. INTRODUCTION

The main way to protect transmission of data from point A to point B is cryptography. Cryptography is defined to be "the science of secret" [1], the main role of cryptography is to transform a clear text message M, into ciphered one M', within a function E such as:

$$M'=E(M).$$

To retrieve the message M from M' a function D is used, such as:

$$M=D(M').$$

Transforming the message M to unreadable one M' for all illegitimates participants, to avoid any risks of eavesdropping is very important, to preserve the security of the communication especially in a network.

The taxonomy of the actual cryptography (classical cryptography) divides it into two types, the symmetric and the asymmetric cryptosystem. Nevertheless, the security of those techniques suffers from several vulnerabilities that will be discussed afterwards.

In the other hand, the miniaturisation in processor industry –Moor's Law- can cause serious interferences that can disturb the data integrity; this later is one of the main pillars of data security that must be preserved. More again, the calculating power is increasing –Quantum calculating power- and this really threat the security of cryptosystem, especially those based on mathematical concept.

That is why, basing on the lows of quantum mechanics new cryptographic paradigm, that can resolve most of the classical cryptographic problems, appear, the 'Quantum Cryptography'.

Because it is based on Heisenberg principal of uncertainty, as it will be presented, it is more correct to call it a quantum key distribution rather than quantum cryptography.

It was thought that the application of the quantum key distribution was only a point-to-point one, but it is proved nowadays that it can be applied to wireless mobile network, by allowing participants to share a secure encryption key. Thus, offer a high security level for the wireless mobile network.

In this paper, we present a stat of the art of classical and the quantum cryptography in first time, then how this later can contribute in securing a wireless network by exchanging a totally secured encryption key.

The rest of the paper is organized as follow: in section two, we present the state of the art of the classical techniques of cryptography. In section three, we study and analyse the main key exchange techniques .In section four we introduce the principals of quantum cryptography. The fifth section will discuss some failures of the WLAN and the contribution of integrating the QKD (Quantum Key Distribution) in the 802.11i, then we present a scheme of using the QKD to derive secured

encryption key for wireless transmission in WLAN. The scheme is reinforcement of the work we presented in [17].

II. CLASSICAL CRYPTOSYSTEM: TAXONOMY

A. *Symmetric cryptosystem*

In such a cryptosystem, described in "Fig. 1", the sender and the receiver used the same and unique key to encrypt and decrypt a message M. In this case, every two participants of the communication need to

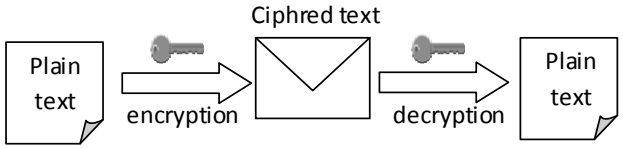

Figure 1. In symmetric cryptosystem the same key is used to encrypt and decrypt the message; the key must be exchanged before starting transmission.

have the same encryption key that they have to share in such secured way before starting any transmission, thing that brings us to the point zero. In the other hand, for N participants, N(N-1)/2 keys are need. So if N grows, it becomes quickly impracticable to manage the

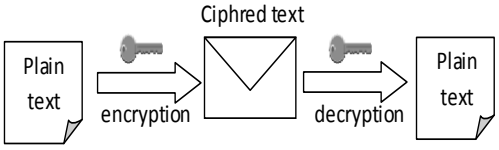

Figure 1. In symmetric cryptosystem the same key is used to encrypt and decrypt the message; the key must be exchanged before starting transmission.

key number.

B. *Asymmetric key*

Using an asymmetric cryptosystem, shown in "Fig. 2", the participants, Alice and Bob, used a pair of key (private, public), where, generally, the public key is used to encrypt and the private key to decrypt the message. So, if Alice wants to send a message to Bob, she encrypts the message using Bob's public key then sends it to Bob. Any other participant can perform the same operation. Arriving to Bob, he is the only one who can decrypt the message via the private key; this later is never revealed so Bob is the only one who can read the message.

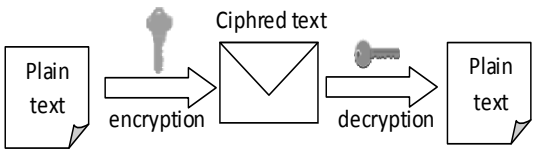

Figure 2. In asymmetric cryptosystem two different keys are, the public key is use to encrypt and the secret key is used to decrypt the message.

The drawback of this cryptosystem is that it is based on the one-way function, like factoring a large number into its two prime numbers. A one-way function is a function that can easily be performed in one way but difficult to perform in the other way using the actual calculating power.

This cryptosystem rely on the fact that it is difficult to deduce the private key, which is used to decrypt the message, from the public key, which is used to encrypt it. Nevertheless, if an adversary has the necessary power to factorize a big number in a realistic time, all security of the cryptosystem based on will entirely fall-down.

In practice, it is a combination of symmetric and asymmetric technique, which is used; an asymmetric procedure is use to share the symmetric key between participants before starting transmission.

Nevertheless, only one cryptosystem is proved to by secure by the Shannon theory, that stipules that a cryptosystem is secure if and only if the encryption key is generated absolutely randomly and used only once, this is the case of the OTP (One Time Pad). With the OTP, the key is generated randomly then it is X-Ored with the clear text message to get the ciphered one.

III. KEY EXCHANGE

Bruce Schneier in [1], explains how key exchange can be carry out using classical cryptography techniques.

A. *Key exchange using secret key*

Alice asked the KEC (Key Exchange Center) for a session key to communicate with Bob.

KEC generates randomly a session key, and then sends it to Alice. A copy of the same key is send to Bob. Each copy of the key is encrypted with the secret key that the KEC shares with respectively Alice and Bob.

The KEC sends also the identity information of Alice to Bob encrypted with the secret key of this later.

Alice sends identity information to Bob, and this later will check if the information is true.

Alice and Bob, got each one the same key and can use it to communicate.

B. *Key exchange using public key*

Alice generates here pair of (secret/public) key, and forwards the public one.

Bob generates a session key, and encrypts it with the public key of Alice then sends it to here.

Alice is the only one who can decrypt the message and restore the session key using here secret key.

C. Key exchange using Data Base

In this case, Alice brings back the public key of Bob from a central DB.

Alice generates a session key, and then sends it to Bob after encrypting it using his public key.

Bob is the only one who can decrypt the message and restore the session key.

Other mechanisms for exchanging key can be found in [1].

D. Analyses and critics

In the first case, Alice and Bob must share in a secret way a key to use it in key exchange; the deal is how they can exchange the first key to use it after that.

Obviously, the physical exchange is the most secured way to exchange a key but unfortunately, not the most practical one.

In the second case, the technique is time consumer, because based on the one way functions. In the other hand, it is vulnerable against quantum computer.

In the third case, the deal is in the vulnerability of the DB, if this later is corrupted, an eavesdropper can personify Alice to Bob and vice-vers-ca.

IV. PRINCIPALS OF QUANTUM CRYPTOGRAPHY

The risk of interferences that can alter the validity of data grows with the miniaturization technology. MOOR's low stipules that processor double their speed every 18 months, so that in 2020 just one atom will be need to represent data. So, we need a new information support to face up this challenging. The Qubit is that required information support.

In a physical point of view, the Qubit can be represented by an elementary physical entity like photon; the main characteristic that will be used to represent the value hold by the Qubit is its polarization of the photon.

In the other hand, as introduced in section two, the actual cryptosystem suffers from some vulnerability that makes them on the risk of eavesdropping. Especially, if the adversary has the calculating power that a quantum computer can provide. It is known that, a classical computer with N bits will perform the same operation 2^N times, while quantum computer will perform the same operation on 2^N stats on the same time, because of the superposition principle.

A. Superposition

In quantum world, the Qubit is used to represent the data, like the bit in classical data. However, it is important to note that one Qubit, can hold two information at the same time.

In DIRAC notation the Qubit is note as follow:

$$|\psi>=\alpha|0>+\beta|1> \quad (1)$$

Where:

$$0> = \begin{pmatrix}1\\0\end{pmatrix} \quad \text{and } |1> = \begin{pmatrix}0\\1\end{pmatrix} \quad (2)$$

And α, β are a complex numbers where $|\alpha|^2+|\beta|^2 = 1$; α represents the probability to have 0 and β the probability to have 1 after the measurement.

B. Non cloning theorem

According to the superposition principals the Qubit holds two values at a time. Only the measurement of the Qubit will, randomly, discard one value and give as a result the other one.

That is why in fact, it is impossible to copy a quantum stat. Any measurement of the stat will alter it and discriminates the value hold by the Qubit, and thus change it. The non-cloning theorem is one of the important one on which the quantum cryptography is based as it will be explained later.

C. Heisenberg principal

A quantum stat is a combination of numerous parameters, e.g position and speed of the photon. The uncertainty principal of Heisenberg stipules that it is impossible to measure one of those parameters simultaneously without disturbing the others.

These reinforce the idea of the non-cloning theorem, because to copy a quantum stat it is imperative to get all information about it, so measure it. But measuring it will inevitably disturb some parameters. Thus, without having the complete description of the quantum stat, no way to reproduce it.

Based on those principals, sender and receiver, traditionally called Alice and Bob, can share a secured message without any risk of eavesdropping. The eavesdropper, trying to intercept the message will change its value and, Alice and Bob will discover the eavesdropping just by measuring the error rate in the message after transmission.

Nevertheless, because the message formed between Alice and Bob is *randomly* generated, the quantum cryptography cannot be used to exchange predefined message.

D. BB84 Protocol

Charles BENETT and Gilles BRASSARD in 1984 proposed (based on Wisner's works) the first quantum cryptography protocol using the photon's polarisation. Actually, the protocol presents a solution to deal with the key distribution problem. Therefore, it is correct to define it as quantum key distribution rather than quantum cryptography.

To perform a key distribution, Alice generates random string, and sends it to Bob throw a quantum channel. Bob will try to receive the photons in the right polarization; otherwise, the photon will be discarded from the string key. Once the key generated it could be used to encrypt data.

Actually, we can find two cases:

1) Without eavesdropper:

In the ideal case, where there is no eavesdropper as shown in "Fig. 3", Alice will generate a random string that represents the polarisation's bases of the photons, then sends the photon throw a filter that polarise the photon according to the bases' string and sends it to Bob throw the quantum channel.

Suppose the use of rectilinear base noted + and the diagonal base noted ×. The rectilinear base contains two polarizations axes: – that represents 0º traduced as the value 0, and | that represents the axe 90º so the value 1. The second base, the diagonal one, contains also two polarisation axes / and \ to represent respectively 45° et 135° to traduce as 0 and 1.

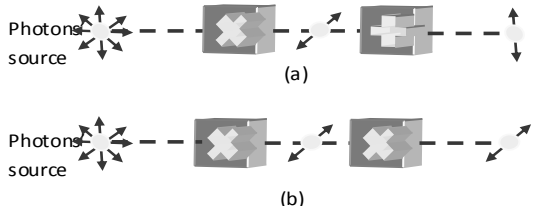

Figure 3. BB84 Protocol case without eavesdropper: in (a) Alice and Bob already choose two different bases, in (b) Alice and Bob chose the same bases.

Once the message arrived to Bob, he performs reverse operation. He randomly chooses filter to measure the value hold by the photon. If Alice and Bob choose the same bases they will have the same value, but if they choose different bases, that happened half a time, they will certainly have different values for the same photon.

2) With eavesdropper:

If an eavesdropper, attempts to intercept the string exchanged between Alice and Bob, he/she will automatically perform the same process as Bob. So, if Bob and the eavesdropper use the same base as Alice, he will have the same value sent by Alice and the eavesdropping will not be detected. However, if the eavesdropper use different base to intercept the photon sent by Alice, he/she will certainly change its polarisation, so if Bob use the same base as Alice; there will be the case where the two legitimates protagonists choose the same bases but got different value of the same photon which is contradiction. Otherwise, if Alice and Bob used different bases the Qubit will be discarded automatically from the string key.

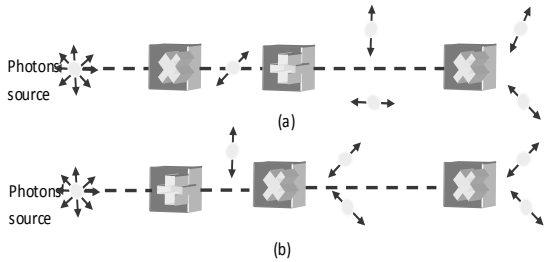

Figure. 4. BB84 Protocol case with eavesdropper; in the first case (a) Alice and Bob choose the same bases but got different value; the bit will be discarded. In the second case (b) Alice and Bob used already different bases so the bit will be discarded however is the value.

In the two cases and after photon exchanging Alice and Bob will share a string that is not identical. They have to go throw other steps to eliminate the differences and get an identical string.

First, Alice and Bob announce, throw public channel, the bases, but not the values, used for photon's polarization, the different bases for the same photon will be discarded.

The next step is error correction using error correction algorithm. The most efficient one is the CASCADE algorithm, based on dichotomy research of the error that could occurred during the BB84 and could not be detected neither by Alice nor by Bob. At the end of the CASCADE algorithm, Alice and Bob will share an identical string.

The last step is privacy amplification, in which the length of the string shared between Alice and Bob will be reduced again, by discarding some Qubits. This will decrease the number of the Qubits that an eventual eavesdropper could possess and by that augmenting the entropy of the key.

V. INTEGRATING QKD IN 802.11

A. Failures in 802.11security mechanism

WEP was the first security mechanism defined for the wireless network but it suffers from some failures:

1) The WEP used the same key for authentication and encryption, and this is not a good strategy.
2) WEP is based on the RC4 stream cipher, in which the encryption key is a concatenation of an IV (Initialization Vector) of 24 bits send in clear and WEP key of 40 bits length.
3) The IV should be used once with each key, but in the WEP, there is no mechanism to avoid using the same IV with many WEP key.

The failures of the WEP lead to a new mechanism the 802.11i.

Originally, the 802.11i passes throw 3 steps to authenticate a new supplicant S (mobile client) who would like to connect to a network via an access point AP as shown in "Fig. 5".

Once the PMK (Pair wise Master Key) derived and shared between the AP and S, the other keys are derived from it according to the following hierarchy.

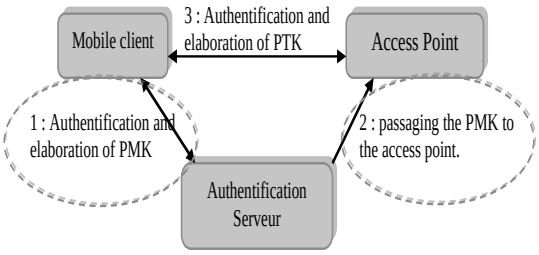

Figure. 5. Summary of IEEE 802.11i authentication and key exchange [17].

Two ways can be used to derive the PMK, for small network the PMK can be the PSK (Pre Shared Key) and it's equal to the MK (Master Key) derived at the first time between the Supplicant and the authentication server, in a large network. The PTK (Pair wise Transient Key) is derived from the PMK using PRF (Pseudo Random Function). The PTK is then split into four keys, KCK (Key Confirmation Key), KEK (Key Encryption Key), TK (Temporal Key) and TMK (**T**emporary **M**IC **K**ey).The "Fig.6" represents the key hierarchy

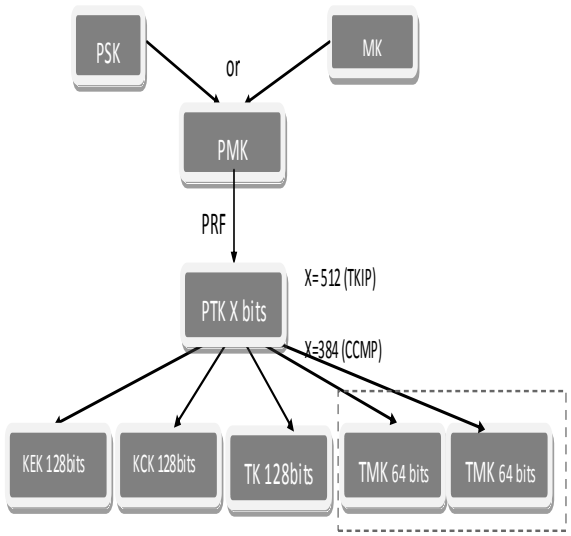

Figure. 6. Key hierarchy in 802.11i.

B. Integrating QKD in 802.11i

Choosing the application of the QKD to the 802.11i is not deliberated:

1) The user mobility is not so much high so there would not be a problem of maintaining the line of sight between the Access point and the Supplicant to send photons.
2) The devices used in WLAN have high battery autonomy. The energy is consumed in performing the large calculating operations of the BB84.
3) A 802.11i network is used to exchange relevant data like password, e-banking card number… This kind of data must be efficiently secured.
4) Bluetooth is used to replace the wired links of devices such keyboard, mouse… so it would be too much integrating QKD at this plan.
5) GSM is used in high level mobility environment, integrating the QKD will encounter a technical problem, which is how to maintain line of sight when sending of the photons. In the other hand the mobility that offers the GSM network can be a drawback and source of noise.

In [8] the main proposed idea is to introduce the QKD in the 4 Way-Handshake. The proposed scheme allows mobile client and the Access Point to establish a fresh and random PTK (Pair wise Transient key) once the BB84 was finished. Detailed description of this integration can be found in [8].

Once the PTK is derived, the other keys could be derived as in the classical 4 Way-Handshake.

The drawback of this scheme is that it always needs a classical authentication. Hence, a secret may be shared before starting any photons' transmission, in such a way that the participants can use the shared secret key to authenticate themselves before starting the BB84. This brings us to point zero.

In the other hand, the PMK, after being established between Supplicant and Authentication Server still need to be distributed to the Access Point, to derive the KCK (Key Encryption Key)

C. New Proposed scheme

Let us use the notations below:

$A \rightarrow B:\{X\}_y$ means A sends message X to B encrypted via the key y.

$X=x_1||x_2$ means X is the concatenation of x_1 and x_2.

The proposed scheme to integrate the quantum key distribution in the 802.11i is an improvement of our presented work in [17], were the integration still need an authentication using a pre-shared key. The new scheme of integrating the QKD to derive a secured encryption key in wireless network follows the steps below:

1- When Supplicant S sends request to the Authentication Server AS, this later considered as third trusted part, will execute two BB84 protocols, one on each side, one with the Access Point AP and another one with the Supplicant. Thus, the Authentication server got two different keys, respectively K_{SA} and K_{SB}. AS splits each key into two parts so to get K_{SA1}, K_{SA2}, K_{SB1}, and K_{SB2}.
AS generates two Nonces (Number used only once) S_1 and S_2 to be used respectively with AP and S.

2- $AS \rightarrow AP:\{\{K_{SB2}\}_{KSA2}, \{S_1\}_{KSB2}\}$, AP decrypts the message and get K_{SB2}, the AP get the ticket $\{S_1\}_{KSB2}$. Only AS and AP could decrypt the ticket and find the original S_1. If the AP is a legitimate one and used the same key as AS, which is KSA_2, so it could recover S_1; otherwise (if an eavesdropper

intercepts the message) it will use a random string different from KSB_2, and so get a different S_1.

In the other hand:

AS→S:{ $\{K_{SA1}\}_{KSB1}$, $\{S_2\}_{KSA1}$ }S decrypts and got K_{SA1} and a ticket $\{S_2\}_{KSA1}$. Idem, but in this case only the AS and the supplicant S could decrypt the ticket $\{S_2\}_{KSA1}$.

3- When the AP recovers the KSB_2 and S_1 using this later, then:

AP→AS:$\{S_1\text{-}1\}_{KSB2}$.

AS→AP:OK

Thus, AS and AP are authenticated.

Once S recovers KSB_1, and S_2 via KSB1 then:

S→AS:$\{S_2\text{-}1\}_{KSA1}$.

AS→S:OK

So the AS and S are authenticated too.

4- Now S and AP can concatenate the exchanged sub-keys K_{SA1} and K_{SB2} to shape the final key K.

5- $K= K_{SA1}||K_{SB2}$.

6- To verify that the AP and S share now the same key K.

S→AP:$\{S'\}_K$

AP → S:$\{S'\text{-}1\}_K$

The "Fig. 7" illustrates the proposed scheme.

D. Security analyse:

Because its implementation is expensive in two terms, physical and financial, such integration needs to be analyzed via simulation tools to get numerical results to explore.

However, until now there is no quantum network simulator, so we use speech scenario to analyze and prove the correctness of the scheme.

We assume also that the proposed scheme is not based on the EPR photon pairs, but on the unique photon pulse. The unique photon pulse sends only one photon by pulse [18][19]. With a unique photon pulse, it is impossible to an eavesdropper to execute a beam splitting attack without being detected. Measuring the photon polarisation will inevitably change it. Whereas with attenuated laser pulse, a pulse can contain more than one photon, thus the eavesdropper can measure one of it without disturbing the other one and he/she will not be detected.

In addition, the proposed scheme offers the opportunity to get a fresh derived key, avoiding the problem of reusing the same key, or even the use of IV (Initialisation Vector) with the PRF (Pseudo Random Function).

The scheme is secure against MIMA (Man In the Middle Attack). That is possible because in step 2 only the Authentication Server AS, which is a third trusted part, and one of the two parties know the -correspondent- part of the initial keys that would be exchanged. If the other party is a *legitimate* one, then it could correctly decrypt the message and then recover a half part of the final key K. Otherwise, it will get a completely random string.

The new scheme is enhanced with an authentication process by using the Nonce (Number Only used Once) at the second step. Again, if the party is a legitimate one, then surely it recover the part of the key send to it by the AS, so it could then use it to decrypt the Nonce, decrease it, then sends it again to the AS. The AS compares the send and the received Nonce, and verifies that the right party correctly received it. Otherwise, the process is aborted, and a new process is started again.

Once AP and S are authenticated by the AS, a mutual authentication process is run between them. The AP sends to the S a new Nonce S' encrypted via the newly created key K, which results from the concatenation of K_{SA1} and K_{SB2}. See step 6 in "Fig. 7".

Let us assume that Eve, the eavesdropper, cannot perform a collaborative attack (attack at each side of the Authentication server). We also assume that Eve will perform a Man in the Middle Attack. She personates the Access point to Supplicant.

Using the same notation, Eve will get two keys K_{ES} and K_{EB} to use respectively with the Supplicant and the Access Point. Keys will be split, as in the ideal case, to get K_{ES1} K_{ES2} K_{EB1} and K_{EB2}.

Then: AS→AP :{ $K_{SB2}\}$ K_{ES2}, $\{S_1\}$ K_{SB2}

The Supplicant decrypts $\{K_{SB2}\}$ K_{ES2} but using K_{EB1}, which is half of the key K_{EB} that it gets from the eavesdropper Eve.

Thus, the supplicant gets a random key completely different from K_{SB2} that it should get. Let us note X the string that it gets. The supplicant will use X to decrypt S_1 that was encrypted via K_{SB2}. Let us note S' the string that the supplicant gets, it's clear that S' will be completely different from S_1. The Access Point will detect the difference between S_1 and S', and the process will be aborted. New process is run.

VI. CONCLUSION

In this paper, we give, at first section, a description of classical cryptography techniques. We present the main principals of the quantum cryptography, which is correct to call quantum key distribution, in section three. Section four, was about the failure of the security mechanism of wireless network, and how the quantum key distribution can be used to enhance the security of WLAN. It was proved that the quantum key distribution offer the opportunity to generate unconditionally secured key.

The main idea of the paper was to present a scheme of integrating the QKD in 802.11i to profit of this security avoiding the use of the PRF (Pseudo Random Function) and IV (Initialization Vector). Once a BB84 protocol run on each side of the AS, intermediate keys are generated. The final key, K, is the concatenation of half of each intermediate key.

Mutual authentication is run between Supplicant and Access Point after establishment of valid final key.

The integration of the QKD in the wireless mobile network is steel a new open field, and all new ideas are accepts, we hope that this one would be one of them, and that the presented work could bring some contribution to this field.

REFERENCES

[1] D. Bowmeester, A. Ekert, and A. Zeilinger, The physics of quantum information. Edition Springer, 2000.

G. Dubertret, Initiation à la cryptographie. Vuibert informatique,

International Journal of Computer Science and Network Security, vol 6, no.5B, pp 138-156, May 2006.

[12] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography in practice", in Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '03, pp. 227 - 238 ,August 2003, ACM Press.

[13] G. Ribordy, and O. Guinnard , N. Gisin and H. Zbinden, "Un saut quantique en cryptographie", version 02, idQuantique, 2004.

[14] A. Ahmed, Wireless and mobile data networks, Wiley-interscience Piblication, 2005.

A. M. Al Naamany , A. Al Shidhani, and H. Bourdoucen; "IEEE 802.11 Wireless LAN security overview", IJCSNS International Journal of Computer Science and Network Security, vol 6, no.5B, pp 138-156, May 2006.

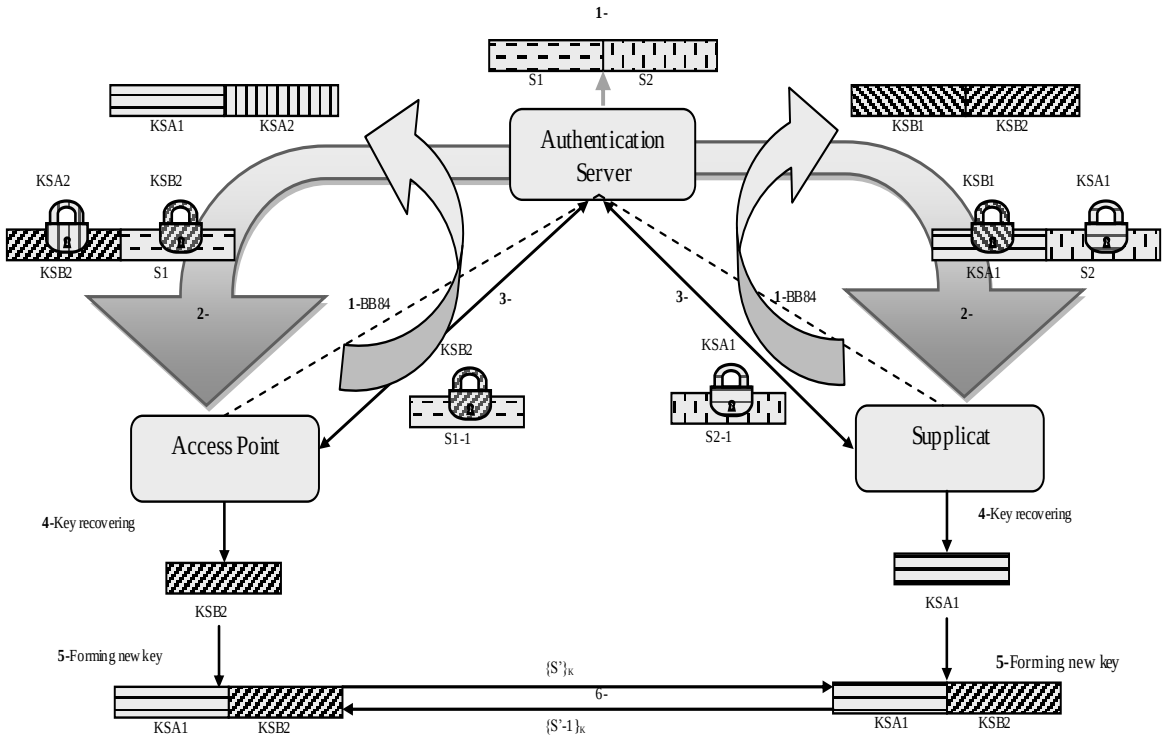

Figure 7. Key derivation in Quantum Handshake, the BB84 allows the establishment of the PTK that will be use d to extract KEK and TK but KCK is derived from PMK.

[2] Avril 2000.

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", Review of modern physics, 8 March 2002.

[4] Avril 2000.

[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", Review of modern physics, 8 March 2002.

[6] S. Loepp, W.K. Wootters, Protecting Information From Classical Error Correction to Quantum Cryptography, Cambridge University Press, 2006.

[7] S. Loepp, W.K. Wootters, Protecting Information From Classical Error Correction to Quantum Cryptography, Cambridge University Press, 2006.

[8] A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, Handbook of applied cryptography. CRC press, 1997

[9] idQuantique, 2004.

[10] A. Ahmed, Wireless and mobile data networks, Wiley-interscience Piblication, 2005.

[11] A. M. Al Naamany , A. Al Shidhani, and H. Bourdoucen; "IEEE 802.11 Wireless LAN security overview", IJCSNS International Journal of Computer Science and Network Security, vol 6, no.5B, pp 138-156, May 2006.

[15] A. M. Al Naamany , A. Al Shidhani, and H. Bourdoucen; "IEEE 802.11 Wireless LAN security overview", IJCSNS International Journal of Computer Science and Network Security, vol 6, no.5B, pp 138-156, May 2006.

[16] M. Riguidel, P. Bellot, T. Nguyen, M. Dang, Q. Le, and T. Nguyen, "QUANTUM CRYPT, Enhancement of AGT communications security using quantum cryptography", Rapport of stage, Ecole nationale supérieure des telecommunications, Network and Computer Science department, Juin 2006.

[17] R. Djellab, "New scheme of integrating quantum key distribution in 802.11i", In IEEE International Conference on Multimedia Computing and Systems 2009, Ouarzazat, Morocco.

[18] G. Messin, François Treussart, "Photon Unique et cryptographie quantique", Quanta et Photon, page118.

[19] A. Pasquinucci, "Authentication and routing in simple Quantum Key Distribution networks", 02 Juillet 200,

available on: http://arxiv.org/abs/cs/0506003.

[20] R.Djellab, M.Benmohammed, ", Secured Key Distribution in 802.11 via Quantum Cryptography ", JGED, Annaba, Algeria, 2009.
[21] R.Djellab, M.Benmohammed, " Multi-participants key generation in WLAN using QKD ",ICAI, Bourdj Bou Ariridj, Algeria, 2009.