Integration of Quantum Key Distribution in the TLS Protocol*

Mohamed Elboukhari[1], Mostafa Azizi[2], and Abdelmalek Azizi[1,3]

[1]dept. Mathematics & Computer Science FSO, University Mohamed I[st], Oujda, Morocco
[2]dept. Applied Engineering, ESTO, University Mohamed I[st], Oujda, Morocco
[3]Academy Hassan II of Sciences & Technology, Rabat, Morocco

Summary
Quantum Key Distribution (QKD) or quantum cryptography has been developed within the last decade; it is proved that QKD is secure against computer attacks and it is considered as a promising solution towards absolute security within long-term cryptosystems. Currently, research efforts are required to make strongly secure the existing communication protocols; we suggest as an issue to improve their security levels by integrating QKD. In this paper, we explore the possibility of using QKD for local area networks (LAN); we propose thus a scheme for integrating quantum cryptography in the TLS protocol. This will much contribute to enhance the process of authentication and data encryption. We present also an example to illustrate the feasibility of our scheme's implementation.

Key words:
BB84 Protocol, Cryptography, Quantum Key Distribution, TLS Protocol

1. Introduction

Security has become a big concern in wired and wireless networks. The network characteristics present both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non repudiation. Cryptographic techniques are widely used for secure communications. Most cryptographic mechanisms, such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. However, all cryptographic techniques will be ineffective if the key distribution mechanism is weak. The purpose of key distribution mechanism is to provide secure procedures for handling cryptographic keying materials. The security of most modern cryptographic systems with key distribution mechanism is based on the computational complexity and the extraordinary time needed to break the code. This means that current cryptographic systems will become more vulnerable as the speeds and powers of computers continue to increase.

Quantum key distribution (QKD) [1]-[2] is attracting much attention as a potent candidate. This is because QKD enables two distant parties to generate a secret key that has guaranteed privacy due to the use of quantum physics. So, quantum cryptography (or QKD) solves the secure random key distribution problem. The concept of quantum cryptography was introduced by Bennett and Brassard in the early 1980s [1] from an idea of Wiesner [3]. The BB84 protocol's unconditional security can be easily proved using the no-cloning theorem and the nonorthogonality of states used to encode the information.

Various theoretical and experimental studies have been undertaken on quantum cryptography, and also prototypes of products are now commercially available. Up to date, several QKD protocols have been developed, and some of them allow managing the transmission of keys through tens of kilometers in both fiber and free space [4]–[8]. So, the LAN networks present a big interest for using QKD due to the limited coverage area.

In the literature, there are some papers treating the task of integrating QKD in the TLS Protocol [9]-[10]-[11]. In our paper we propose a different approach. We give more details to let our method becomes applicable, we also added a new component to the TLS Protocol with specific attributes to facilitate the elaboration of our solution.

So, we discuss in this paper how to integrate QKD in the LAN networks. we propose a method for integrating QKD in the TLS protocol for LAN environments. Using the BB84 protocol, we have defined a Quantum TLS Handshake Protocol which enhances the security of TLS Handshake Protocol as described in [12]. Also, we have added a new component to the TLS protocol to make our method operational.

The paper is organized as follows: In the second section, we describe the TLS Protocol. The BB84 Protocol is presented in the third section. In section 4, we introduce the Quantum TLS Handshake Protocol, a scheme that integrates QKD in TLS Handshake Protocol. We give also in this section a full description to the new component added to the TLS Protocol.

2. TLS Protocol

Due to its native integration in Web browsers, TLS Protocol [12] is the most widely used protocol to protect

(*) This work is partially supported by the Academy Hassan II of Sciences and Technology (Morocco).
Manuscript received December 5, 2009
Manuscript revised December 20, 2009

and authenticate communications across the Internet. It has developed by Netscape [13], and standardized later by IETF [12]. This protocol is a transaction security standard providing secure connections between two communicating entities, with integrity-protected security, mutual authentication, and key management.
The TLS Protocol ensures two services: an encrypted point-to-point connection and the integrity of messages. This protocol includes five sub-protocols: Record Protocol, Handshake Protocol, Change Spec Protocol, Alert Protocol and Application Data Protocol.

2.1 TLS Record Protocol

The Record protocol takes messages to be transmitted, fragments the data into manageable blocks, compresses the data (optional), applies a MAC, encrypts, and transmits the result. The TLS handshake protocol allows a client and a server to agree upon security parameters.

2.2 TLS Handshake Protocol

In TLS handshake protocol, the client and the server authenticate each other using certificates or pre-shared keys (PSK) [14], instantiate the negotiation of security parameters and compute the session key that is used to encrypt exchanged data. This consists of three steps.

1) Step 1

Both entities in the first step negotiate the parameters of the secure session. These parameters especially include the session identifier (SessionID) and the cipher suite. This latter is a triplet conveying the method of the key exchange that is used to exchange the session key, the cipher algorithm that is deployed to encrypt/decrypt the application data, and a hash function to ensure data integrity. The client includes in its ClientHello message (Fig. 1) a list of supported triplets in order of its preference. The server replies with its ServerHello that especially conveys the selected cipher suite or, if no acceptable choices are presented, returns a handshake failure alert and closes the connection. The ClientHello and ServerHello establish the following attributes: Protocol Version, Session ID, Cipher Suite, and Compression Method. Additionally, two random values are generated and exchanged: ClientHello.random and ServerHello.random.

2) Step 2

The client and the server authenticate each other in a second step. TLS protocol has defined two authentication modes: mutual authentication and only server authentication. This authentication is usually performed by using pre-shared keys [14] or public key certificates installed in both the client and the server, in a such case a public key infrastructure [12] is required. We are interested in this paper in TLS mutual authentication and in Public key based-certificate authentication.
In based-certificate authentication, the server sends a certificate request message (Fig. 1), inviting the client to reply with a certificate. The client hands a certificate to the server and proves that it is legitimately the owner of the certificate. By way of proof, the client sends the CertificateVerify message, which handles the hash of all messages exchanged between the client and the server starting at ClientHello up to, but not including, the CertificateVerify message. The server verifies that the client is in possession of the private key corresponding to the certified public key. In case that the validation fails, the server stops the handshake. In Fig. 1, (*) indicates that a ServerKeyExchange message may be sent, if it is required; for example if the certificate is for signing only [12].

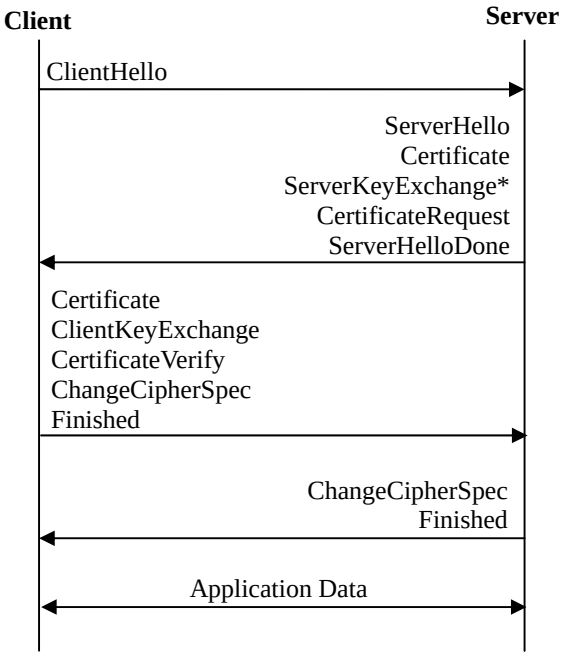

Fig. 1 Message flow for the full TLS Handshake Protocol [12].

3) Step 3

To verify the success of selected authentication mode and the key exchange processes, both the client and the server exchange the ChangeCipherSpec and the finished messages (Fig. 1). The finished messages prove to both the client and the server that they have the same key material

since finished messages are the first messages processed and exchanged after applying the negotiated security parameters.We calculate the TLS finished messages by the formula [12]:

PRF(master_secret, finished_label, Hash(handshake_messages))

Where PRF is a pseudo-random function defined in [12]. For finished_label, we use the string "client finished" for the message sent by the client and "server finished" for that sent by the server. Hash denotes a Hash of the handshake messages. The value handshake_messages includes all handshake messages starting at ClientHello up to, but not including, this TLS finished message. Therefore, the handshake_messages for the finished message sent by the client will be different from that for the finished message sent by the server, because the one that is sent second will include the prior one. The master_secret is defined by the following formula [12]:

master_secret = PRF(pre_master_secret, "master secret", ClientHello.random + ServerHello.random)

The pre_master_secret is generated by the mechanism of key exchange (such as an RSA or Diffie-Hellman). So, when RSA is used for key exchange, a pre_master_secret is generated by the client, encrypted under the server's public key, and sent to the server. The server uses its private key to decrypt the pre_master_secret. If conventional Diffie-Hellman computation is performed, the negotiated key is used as the pre_master_secret [12]. The symbol "+" in the previous formula represents the operator of concatenation (for more detail please refer to [12]).

3. The BB84 Protocol

Quantum cryptography is only used to produce and distribute a key $K = \{0,1\}^N$, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel (classical channel).

The security of quantum cryptography relies on the foundations of quantum mechanics, in contrast to traditional public key cryptography which relies on the computational difficulty of certain mathematical functions. Also traditional public key cryptography cannot provide any indication of eavesdropping or guarantee of key security. QKD has an important and unique property; it is the ability of the two communicating users (usually named Alice and Bob) to detect the presence of any third party (named Eve) trying to gain knowledge of the key. This third party trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum superpositions or quantum entanglement and transmitting information in quantum states over a quantum channel (such as an optical fiber or free air), a communication system that detects eavesdropping can be implemented.

BB84 was the first studied and practically implemented QKD physical layer protocol. It was elaborated by Charles Bennet and Gilles Brassard in 1984 in the article [1]. It is surely the most famous and most realized quantum cryptography protocol. This scheme uses the transmission of single polarized photons (as the quantum states). The number of polarizations of the photons is four, and is grouped together in two different non orthogonal basis. Generally the two non orthogonal basis are:

-base $\oplus$ of the horizontal (0°) and vertical polarization (+90°), and we represent the base states with the intuitive notation: $|0\rangle$ and $|1\rangle$. We have $\oplus = \{|0\rangle, |1\rangle\}$.

-base $\otimes$ of the diagonal polarizations (+45°) and (+135°). The two different base states are $|+\rangle$ and $|-\rangle$ with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. We have $\otimes = \{|+\rangle, |-\rangle\}$.

In this protocol, the association between the information bit (taken from a random number generator) and the basis are described in Table 1.

Table 1: Coding scheme for the BB84 protocol.

Bit	$\oplus$	$\otimes$
0	$\|0\rangle = a_{00}$	$\|+\rangle = a_{10}$
1	$\|1\rangle = a_{01}$	$\|-\rangle = a_{11}$

The BB84 can be described as follows [15]:

1) Quantum Transmissions (First Phase)

a) Alice chooses a random string of bits $d \in \{0,1\}^n$, and a random string of bases $b \in \{\oplus,\otimes\}^n$, where $n > N$.

b) Alice prepares a photon in quantum state a_{ij} for each bit d_i in d and b_j in b as in Table 1, and sends it to Bob over the quantum channel.

c) With respect to either $\oplus$ or $\otimes$, chosen at random, Bob measures each a_{ij} received. Bob's measurements produce a string $d' \in \{0,1\}^n$, while his choices of bases form $b' \in \{0,1\}^n$.

2) Public Discussion (Second Phase)

a) For each bit d_i in d:

i) Alice over the classical channel sends the value of b_i to Bob.

ii) Bob responds to Alice by stating whether he used the same basis for measurement. Bot d_i and d_i' are discarded if $b_i \neq b_i'$.

b) Alice chooses a random subset of the remaining bits in d and discloses their values to Bob over the classical channel (over internet for example). If the result of Bob's measurements for any of these bits does not match the

values disclosed, eavesdropping is detected and communication is aborted.
c) the string of bits remaining in d once the bits disclosed in step 2b) are removed is the common secret key, $K = \{0,1\}^N$.

To understand BB84 protocol it is very important to describe how we measure a qubit in the field of quantum physics; if we have a qubit as $|qubit\rangle = e|c\rangle + f|g\rangle$ so the measure of this state in the basis $\{|c\rangle, |g\rangle\}$ produces the state $|c\rangle$ with the probability of $|e|^2$ and the state of $|g\rangle$ with the probability of $|f|^2$ and of course $|e|^2 + |f|^2 = 1$ ($|e|^2$ is the absolute square of the amplitude of c). So, measuring with the incorrect basis yields a random result, as predicted by the quantum theory. Thus, if Bob chooses the $\otimes$ basis to measure a photon in state $|1\rangle$, the classical outcome will be either 0 or 1 with equal probability because $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$; if the $\oplus$ basis was chosen instead, the classical outcome would be 1 with certainty because $|1\rangle = 1|1\rangle + 0|0\rangle$.
To detect Eve, Alice and Bob perform a test for eavesdropping in step 2b) of the protocol. The idea is that, wherever Alice and Bob's bases are identical (i.e. $b_i = b_i'$), the corresponding bits should match (i.e. $d_i = d_i'$). If not, an external disturbance is produced or there is noise in the quantum channel, we suppose all that is caused by Eve.

4. Integration of QKD in TLS Protocol: QKD-TLS

4.1 Why integration of QKD in TLS Protocol?

To secure inter-host communication, TLS Handshake Protocol is responsible of providing security parameters to the TLS Record Protocol. This is done by using key management process. In TLS Handshake the key management is limited to the only both Diffie Hellman (DH) and RSA exchange protocol. Neither DH nor RSA is unconditionally secure and cannot be broken; their security depends of the computation power or the time (or the execution time). QKD is proven scientifically to be unconditional secure and in this case security is achieved independently of the power of the eavesdropper. For this raison we propose to integrate QKD in the TLS Protocol instead of DH or RSA key exchange.

4.2 QKD-TLS requirements

To integrate QKD in TLS Protocol some requirements must be satisfied.
a) An optical channel: quantum cryptography uses photons to encode information. Actually, there are two mediums to transport photons: the optical fiber or free space [16]. Recent research works experiment the use of atoms and electrons as quantum particle [17]-[18] and perhaps a novel kind of quantum channel will appear.
b) Optical modem: the purpose of the optical modem is to send and detect photons. The modem has to include a photon detector and a single photon emitter and polarizer to encode data. It is used to provide quantum key but also can be used to exchange data depending on the method of encoding information. To elaborate such modem there is many techniques employed [19]-[20]. To achieve unconditional security, a quantum key protocol is needed and it must be implemented between two optical modems. The quantum key protocol will provide a secure key which will be stored in a flash memory in order to be used when enciphering data.

4.3 A novel component of TLS Record Protocol: QKD Configuration Protocol

In the objective to guarantee that our novel scheme of TLS (including the service of QKD) will work well, we propose to add to the TLS Protocol an additional component which plays the role of configuration of QKD sub-network. We give the new component the name of QKD Configuration Protocol. So the TLS Protocol in our solution has five components: Handshake Protocol, Change Spec Protocol, Alert Protocol, Application Data Protocol and QKD Configuration Protocol.
The message format of QKD Configuration Protocol contains a field of the length of the key which will be generated by the mechanism of QKD. All filed of the message format of QKD Configuration Protocol is shown in Fig. 2.

<table>
<tr><td colspan="2">Type</td><td>Protocol</td><td>Version</td></tr>
<tr><td colspan="4">Length</td></tr>
<tr><td colspan="4">Key-Length</td></tr>
<tr><td>TTL</td><td>T</td><td>Authentication</td><td>Encoding</td></tr>
<tr><td colspan="4">Content</td></tr>
<tr><td colspan="4">Tag</td></tr>
</table>

Fig. .2 Message format of the QKD Configuration Protocol.

The description of this message format is as follows:

Type (1 byte): shows the type of quantum key protocol used. For example protocols based on the Heisenberg's Uncertainty Principle as BB84 or the Bell's Inequality as E91[21].

Protocol (1 byte) indicated the quantum key protocol used (e.g. BB84, B92[2], or E91).
Version (1 byte): permits the use of more than one version of the same protocol.
Length (4 byte): provides the length of message in byte.
Key-length (4byte): this field shows the length of the key provided by the execution of the quantum key protocol. Its length varies between 1 and 4 bytes. We choose the length to be huge in order to use the One Time Pad to attain unconditional security. In this case, the length of the key must be equal to data which will be encrypted [22].
TTL field (2 byte minus one bit): enables to show an amount of time (in seconds) or the number of messages where a key could be used in encryption process. Once the time is expired or the max of messages is reached, the mechanism of QKD started to provide a new key.
T field (one bit): this field specifies if we use the number of messages or the amount of time. When the value is "1", the TTL filed shows an amount of time and when the value is "0", the TTL filed corresponds to the number of messages.
Authentication (1byte): shows if the message is authenticated or not.
Encoding (1byte): this field specifies certain encoding technique if it is used to encrypt the content filed of the message.
Content (its length is not fixed): this field provides data associated with this message.
Tag: when the message is authenticate, this field would show the authentication tag and its size is related to the used authentication code.

4.4 Novel TLS Handshake Protocol: Quantum TLS Handshake Protocol

In our scheme of TLS Protocol, we have introduced also certain changes in the TLS Handshake Protocol. Our purpose is to generate security parameters by the service of QKD.
We have replaced in TLS Handshake Protocol the procedure of classical process of key exchange (such RSA or Diffie-Hellman) by the mechanism of QKD using the BB84 protocol. Because we integrate BB84 protocol in TLS Handshake, we call it Quantum TLS Handshake.
Fig. 3 summarizes how different messages are exchanged between the client and the server during the Quantum TLS handshake messages.

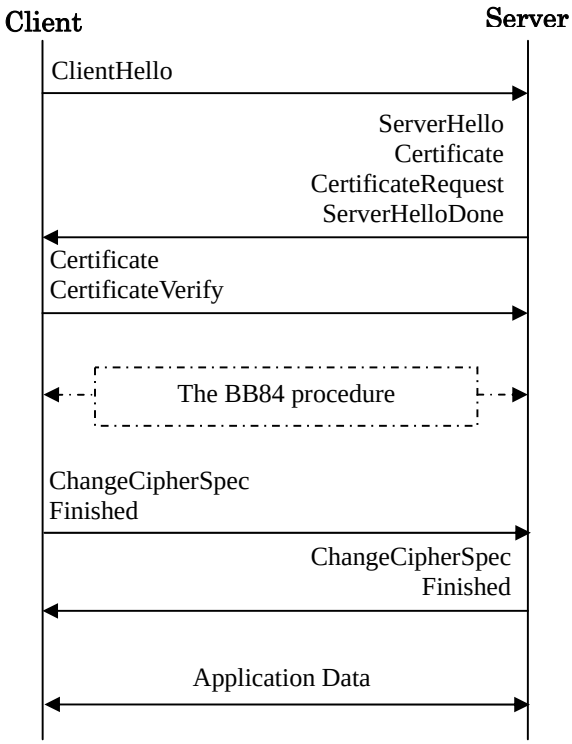

Fig. 3 Message flow for the Quantum TLS handshake

The BB84 procedure integrated in TLS handshake is shown in Fig. 4. As BB84 is vulnerable to "man in the middle" attack [1], we check if the authentication is successful once the execution of BB84 protocol is finished, by calculating the TLS finished message in both sides of the client and the server.

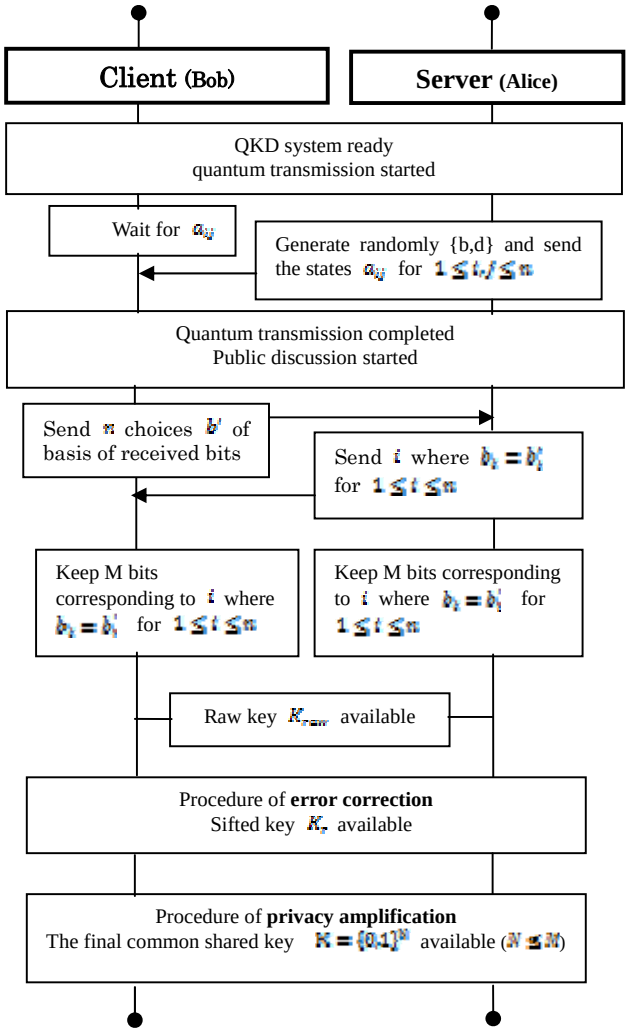

Fig. 4 The BB84 procedure integrated in TLS handshake

At the beginning of the quantum transmission phase, the server sends to the client a serie of polarized photons. The number of photons to be sent depends on the length of the desired key, the error correction algorithm and the privacy amplification algorithm used. For each photon, the server randomly chooses a state a_{ij} and sends it to the client. The remaining steps in public discussion phase (phase of error correction and privacy amplification) are exactly the same as it has described in section 3.

4.5. TLS Protocol in Operation Mode

Our main objective is using QKD to establish the pre_master_secret presented in formula of calculation of master_secret which used in calculation of the TLS finished messages and to generate the key material for data encryption in the TLS protocol. So, QKD is exploited in procedure of authentication and data encryption between the client and the server.

The TLS Protocol in our scheme occurs two changes as in Fig. 5. Firstly, we have integrated a new component named QKD Configuration Protocol and we have modified the original TLS Handshake Protocol (Quantum TLS Handshake Protocol) to include the service of QKD.

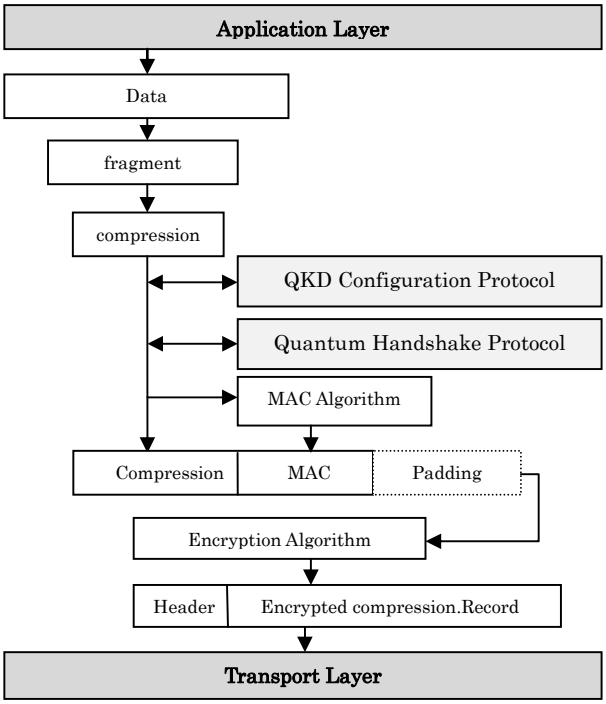

Fig. 5 The functionality of the Novel TLS Protocol.

In operating mode, when TLS Record receives data from the Application Layer, the QKD Configuration Protocol is exchanged between the client and the server to agree on the length of the key desired and the TTL and T fields and other fields as in Fig. 2. When QKD Configuration Protocol is executed, a session of Quantum TLS Handshake begins (Fig. 3).

Once the mutual authentication finished by exchanging the certificates, the client and the server start the BB84 protocol for the establishment of pre_master_secret. The server corresponds to Alice and the client corresponds to Bob because the mutual authentication (before BB84 procedure) must be successful, by verifying the both certificates of the client and the server, and the last certificate verified is that of the client.

As mentioned before, the BB84 protocol is vulnerable to “man in the middle” attack, so to check that the process of authentication was established correctly, the client and the server must calculate the TLS finished message using the shared secret which is the key generated by the mechanism of QKD, $K = \{0,1\}^N$. We propose:

pre_master_secret = K

The TLS finished messages are calculated as described in section 2 by the expression:

PRF(master_secret, finished_label, hash(handshake_messages))

We deduce that the calculation of TLS finished messages use the key generated by QKD because we have:

master_secret = PRF(pre_master_secret, "master secret", ClientHello.random + ServerHello.random)

It is very important to note that in the all public messages exchanging during the executions of BB84 procedure are part of the value of the handshake_messages.
When the server receives the TLS finished message from the client, it calculates its own TLS finished message and verifies whether it is the same as that of the client or not; if yes, then the client is successfully authenticated. The same operation is used by the client when it receives the TLS finished message of the server. So we conclude that the mechanism of QKD is helpful in checking the authentication of the peer and the server.
Also, the Record Protocol requires an algorithm to generate keys required by the current connection state from the security parameters provided by the Handshake Protocol. The master secret is expanded into a sequence of secure bytes, which is then split to a client write MAC key, a server write MAC key, a client write encryption key, and a server write encryption key [12]. Thus, we conclude also that the mechanism of QKD enhances the security of data encryption in TLS protocol.

5.6. Feasibility Study: Example of QKD-TLS application

To demonstrate the functional feasibility, we present in this section an example of implementing QKD-TLS. Let us consider two LAN networks connected via two optical modems which play the two role of quantum and classical channels in the same time.
Our discussion is focused on the specific points of communication between the two modems: C and D as shown in Fig. 6.
To enhance the security of a TLS connection between C and D using the mechanism of QKD, five phases must be executed:
Phase 1: when TLS Record Protocol in the point C for example gets the data from the Application Layer, it calls its Application Data Protocol. So, the data is fragmented and for each fragment a compression could be done.
Phase 2: the TLS Record Protocol calls the QKD Configuration Protocol in order to let the points C and D agree on the parameters illustrated in QKD Configuration Protocol format (Fig. 2). The most important fields are: the protocol, the key-length, the TTL and the T fields. In our example we choose the protocol BB84 because is the first protocol experimented and it is proven to be unconditional secure. Also we suppose that version=1 . We assume that there is no mechanism of authentication and encryption. We propose these choices: Key-length= 20 byes, TTL = 200 messages, T=0. If we plan to use One Time Pad to attain unconditional security we must choose TTL =1 message.
Phase 3: The TLS Record Protocol uses the Quantum Handshake Protocol to obtain the security parameters. So, the Quantum Handshake Protocol begins and during the BB84 procedure, the BB84 protocol is implemented in the two modems. The key generated is stored in a flash memory to be used later in encryption by the Record Protocol.
Phase 4: The TLS Record Protocol receives the key provided by the QKD service and builds its security parameters. These parameters are used to generate keys to encrypt data and to assure integrity (MAC) as illustrated in Fig. 5.
Phase 5: Once the whole record (compressed fragment, MAC and optionally padding) is encrypted, a header is added to the encrypted block and the whole packet is passed to the Transport Layer.

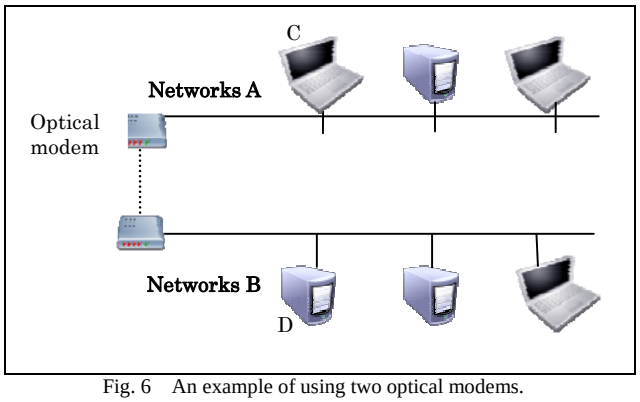

Fig. 6 An example of using two optical modems.

5. Conclusion

In this paper, we have presented a Quantum TLS Handshake which enhances the security of the TLS Handshake; the mechanism of key exchange is established by QKD instead of the classical key exchange as RSA or Diffie-Hellman. Also, we have added a new component to the TLS Protocol in order to render our scheme applicable.
Our new scheme of TLS Protocol includes the following advantages:
1) The messages exchanged during the Quantum Handshake Protocol become simpler: the certificate of server doesn't contain the public parameters of key exchange and we don't need to transmit and receive the messages of classical key exchange.
2) Implementing our scheme does not need to build or to

invent new quantum devices. The optical modem is composed of standard already existing components as photon detector, the single photon source.

3) The unconditional security could be reached with a very low price. Many organization and companies are already using the optical fiber. Therefore, organizations can use the existing infrastructure to generate keys by the service of QKD.

Finally, since in the Quantum Handshake Protocol the authentication is assured by the exchange of the certificates, the authentication is not unconditional secure. For this raison we are planning to render TLS unconditional secure by using some unconditional secure authentication as the Wegman-Carter authentication [23].

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. Int. Conf. Comput. Syst. Signal Process., Bangalore, India, 1984, pp. 175–179.

[2] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., vol. 68, pp. 3121–3124, 1992.

[3] S. Wiesner, "Conjugate coding," SIGACT News, vol. 15, no. 1, pp. 78–88, 1983.

[4] C.-Z. Peng et al., "Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication," Phys. Rev. Lett., vol. 94, no. 15, pp. 150501-1–150501-4, Apr. 2005.

[5] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system," New J. Phys., vol. 4, pp. 41.1–41.8, Mar. 2002.

[6] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, "Entangled state quantum cryptography: Eavesdropping on the Ekert protocol," Phys. Rev. Lett., vol. 84, no. 20, pp. 4733–4736, May 2000.

[7] arXiv: Quant-ph/0403104, 2004.

[8] R.J. Hughes, J.E. Nordholt, D. Derkacs, and C.G. Peterson, "Practical free space quantum key distribution over 10 km in daylight and at night," New JPhys. , vol. 4, pp. 43.1–43.14, May 2002.

[9] Mario Pivk, Christian Kollmitzer, Stefan Rass, "SSL/TLS with Quantum Cryptography," Proceeding of the Third International Conference on Quantum, Nano and Micro Technologies icqnm, pp.96-101, 2009.

[10] S. Faraj, "A novel extension of SSL/TLS based on quantum key distribution" Proceeding of International Conference on Computer and Communication Engineering ICCCE10, pages 919-922, Kuala Lumpur, 2008.

[11] Alan Mink, Sheila Frankel and Ray Perlner, "Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration"J. International Journal of Network Security & Its Applications (IJNSA), vol Volume 1. Number 2, July 2009. http://airccse.org/journal/nsa/0709s9.pdf

[12] Tim Dierks , Eric Rescorla, " The Transport Layer Security (TLS) Protocol, Version 1.2" , RFC 5246 , August 2008.

[13] A. Frier, P. Karlton, P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., November 1996.

[14] P. Eronen, et. al., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, December 2005.

[15] M. Elboukhari, M. Azizi, A. Azizi, "Implementation of secure key distribution based on quantum cryptography", in Proc. IEEE Int. Conf Multimedia Computing and Systems (ICMCS'09), pages 361 - 365, 2009.

[16] R.Hughes,J.Nordholt,D.Derkacs,C.Peterson, (2002). "Practical free-space quantum key distribution over 10km in daylight and at night". New journal of physics 4 (2002)43.1-43.14.URL: http://www.iop.org/EJ/abstract/1367-2630/4/1/343/

[17] Knight, P (2005). "Manipulating cold atoms for quantum information processing". QUPON conference Vienna 2005.

[18] Tonomura, A (2005). "Quantum phenomena observed using electrons". QUPON conference Vienna 2005.

[19] Idquantique : www.idquantique.com

[20] magiQ www.magiqtech.com

[21] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).

[22] Shannon, C.E (1949). "Communication theory of secrecy systems". Bell System Technical Journal 28-4. URL: http://www.cs.ucla.edu/jkong/research/security/shannon.html

[23] 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.

Mohamed elboukhari received the DESA (diploma of high study) degree in numerical analysis, computer science and treatment of signal in 2005 from the University of Science, Oujda, Morocco. He is currently a PhD student in the University of Oujda in the field of computer science. His research interests include cryptography, quantum cryptography and wireless network security.

Mostafa azizi received the diploma of engineer in automatic and computer industry in 1993 from school Mohammadia of engineers, Rabat, Morocco and he received the PH. D in computer science in 2001 from the university Montreal, Canada. He is currently professor at university of Mohamed first, Oujda, Morocco. His main interests include aspect of real time, embedded system, security and communication and management of the computer systems in relation with process industry.

Abdelmalek azizi received the Ph. D in theory of numbers in 1993 from university Laval, Canada. He is professor at department of mathematics in university Mohamed first, Oujda, morocco. He is interesting in history of mathematics in morocco and in the application of the theory of number in cryptography.