

IMPROVING TLS SECURITY BY QUANTUM CRYPTOGRAPHY

Mohamed Elboukhari¹, Mostafa Azizi² and Abdelmalek Azizi^{1,3}

¹dept. Mathematics & Computer Science, FSO, University Mohamed Ist, Morocco

²dept. Applied Engineering, ESTO, University Mohamed Ist, Oujda, Morocco

elboukharimohamed@gmail.com , azizi.mos@gmail.com

³Academy Hassan II of Sciences & Technology, Rabat, Morocco

abdelmalekazizi@yahoo.fr

ABSTRACT

Quantum Cryptography or Quantum Key Distribution (QKD) solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of quantum physics. Extensive studies have been undertaken on QKD since it was noted that quantum computers could break public key cryptosystems based on number theory. Actually, the progress of research in this field allows the implementation of QKD outside of laboratories. Efforts are made to exploit this technology in the existing communication networks and to improve the performance and reliability of the implemented technologies. Some research is in progress for the integration of QKD with the protocols in different layers of OSI model. The examples of such research effort are the integration of QKD in point-to-point protocol (PPP) OSI layer 2 and the integration of QKD with IPSEC at OSI layer-3. All these works are moving towards the utilization of QKD technology for enhancing the security of modern computing applications on the internet. In this paper, we present a novel extension of the TLS protocol based on QKD. We introduce a scheme for integrating Quantum Cryptography in this protocol. Our approach improves the security of the process of authentication and data encryption. Also, we describe an example to illustrate the feasibility of our scheme's implementation.

KEYWORDS

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

1. INTRODUCTION

Since the 1910s, One time pad (OTP) cryptosystems have been in use. The crypto-key length of OTP is the same as the length of the plain text. If the key is never reused, truly random, and kept secret, the OTP can be proven to be unbreakable. But the difficulty of securing the sharing key has prevented it from becoming practical. Quantum Cryptography or Quantum key distribution (QKD) [1] is a new innovative technology that allows a more practical implementation of the classic OTP. This is because Quantum Cryptography enables two distant parties (say Alice and Bob) to generate a secret key that has guaranteed privacy due to the use of quantum physics. The secret key when it is used in a OTP cryptosystem provides perfect security.

So, QKD offers new methods of secure communication. Unlike classical cryptography, which relies on the computational difficulty of certain mathematical functions and employs various mathematical techniques to restrict eavesdroppers from learning the contents of encrypted messages, QKD is focused on the physics of information. The robustness of a given cryptosystem of conventional cryptography is based essentially on the secrecy of its private key and the difficulty with which the inverse of its one-way function(s) can be calculated. However, there is no mathematical proof that will establish whether it is not possible to find the inverse of a given one-way function. So, classical cryptography cannot provide guarantee of key security.

QKD, on the contrary, is a method for sharing secret keys, whose security can be formally demonstrated. Traditional cryptography also cannot provide any indication of eavesdropping. QKD has an important and unique property; it is the ability of the two communicating users (Alice and Bob) to detect the presence of any third party (say Eve) trying to gain knowledge of the key. What the eavesdropper can intercept and measure, and how, depends exclusively on the laws of quantum physics. Exploiting quantum phenomena, we can design and implement a communication system that can always detect eavesdropping.

Quantum Cryptography was proposed first by Stephen Wiesner in the early 1970s when he introduced the concept of quantum conjugate coding. His paper "Conjugate Coding" was rejected by IEEE Information Theory but was eventually published in 1983 in SIGACT News (15:1 pp. 78-88, 1983). In this paper he showed how to store or transmit two messages by encoding them in two "conjugate observables", such as circular and linear polarization of light, so that either, but not both, of which may be received and decoded. Building upon this work and after a decade, Charles H. Bennett, of the IBM Thomas J. Watson Research Center, and Gilles Brassard, of the University of Montreal, elaborated a method for secure communication based on Wiesner's "conjugate observables". Artur Ekert, in 1990, initially unaware of the earlier work, developed a different approach to QKD based on quantum correlations known as quantum entanglement.

The QKD's idea did not attract much attention at first. Research efforts have increased since the 1990s when it was proved that quantum computers could break the public-key cryptosystems commonly used in modern cryptography and when it is proved that QKD is secure against quantum computer attacks. A more interest also has been generated after the first practical demonstration over 30 cm of free space employing polarization coding [2]. Various different theoretical and experimental studies have been undertaken, and prototype products are now commercially available. Actually, several Quantum Cryptography protocols have been developed, and some that transmit keys through tens of kilometers in both optical fiber and free space have been experimentally demonstrated [3-7].

Actually, extensive research has been initiated for sophisticated implementation of QKD in practical communication networks. with funding from the US Defense Advanced Research Projects Agency (DARPA) and built by BBN Technologies, the DARPA Quantum Network was jointly developed by researchers at Harvard University, Boston University and BBN Technologies in 2004. The main goal of this point-to-point DARPA Quantum network is to exploit QKD technology for standard internet traffic. The European Union funded FP6 project SECOQC – Development of a Global Network for Secure Communication based on Quantum Cryptography. This project clearly shows the feasibility of constructing highly integrated QKD-networks and the SECOQC network prototype presents a splendid practical example for the development and operation of a point-to-point QKD network architecture with sophisticated protocols. Also, there are number of other approaches and models for the utilization of QKD in network fashion. Other research has also been initiated for the integration of QKD protocols into the existing classical protocols which are widely used on the internet for secure communication, like PPP, IPsec and TLS.

In this context, we treat in this paper the task of integrating QKD in the TLS protocol. Using the BB84 protocol, we defined an extended TLS protocol which enhances the security of the TLS protocol as it is described in RFC5246 [8]. There are several papers which discuss the integration of QKD in the TLS protocol [9-12]. Our work gives a new scheme illustrating our method to integrate QKD in the TLS protocol by providing more details. Also, we give a practical example to show the feasibility of our approach.

The organization of the remainder of the paper is as follows. We present related works in section 2. In section3, we describe in detail the TLS protocol. The BB84 protocol, which we use in the integration, will be presented in section 4. In section 5, we introduce our novel extension

of TLS protocol integrating the mechanism of QKD and we introduce an example to show the possible applicability of our TLS extension. Finally, we conclude the paper in section 6.

2. RELATED WORKS

Quantum cryptography is a point to point secure key generation technology which provides unconditional security. Now, a new innovative approach is studying by researchers with the main goal to exploit the security of QKD for a large scale practical communication. So, the practical realization of QKD opened new research in the area of secure QKD networking. There are number of approaches and models for the utilization of QKD to secure communications.

One approach is to use QKD in network fashion. SECOQC network of secrets and BBN DARPA quantum network are the examples of such networks.

The DARPA Quantum Network was jointly developed by researchers at Boston University, Harvard University, and BBN Technologies in 2004 [13]. The goal of this point-to-point DARPA Quantum network is to exploit QKD technology for standard internet traffic. The DARPA Quantum network is the first network that delivers end-to-end network security via high-speed Quantum Key Distribution, and testing that Network against sophisticated eavesdropping attacks. Since December 2002, the first network link has been up and steadily operational [8]. More detailed descriptions of DARPA Quantum network may be found in papers [13-15].

The European project SEcure COmmunication based on Quantum Cryptography (SECOQC) was a big research effort of 41 research and industrial organizations from the European Union, Switzerland and Russia, which was initiated in 2003 and carried out between April 2004 and October 2008. The SECOQC gives an approach to QKD networks with a focus on the trusted repeater prototype [16]. Description about SECOQC can be found in papers [17-19].

Other approaches and models in using QKD in network fashion are introduced in the literature as [20-23]. For example, in the paper [21], the authors describe how the ATM (Aeronautical Telecommunication Network) can be secured by QKD, either by optical fiber or free air.

A different approach is to exploit QKD in the existing protocols which widely used on the internet to enhance security with the main objective to achieve unconditional security. The papers [24-28] give some example of such approach. In these papers the researchers present a models and schemes to integrate QKD in classical security protocols as IPsec, PPP and TLS.

Related directly to our work, and in the same approach, several papers have treated the issue of integrating Quantum Cryptography in the TLS protocol as [9-12]. We argue that our work presents a new scheme to show how we integrate QKD in this protocol and we introduce several details to let our scheme to be practically operational.

3. THE TLS PROTOCOL

The TLS protocol has developed by Netscape [29], and standardized later by IETF [8]. It is a transaction security standard providing secure connections between two communicating entities, with integrity-protected security, mutual authentication, and key management. This protocol ensures two services: an encrypted point-to-point connection and the integrity of messages. It includes five sub-protocols: Record Protocol, Handshake Protocol, Change Spec Protocol, Alert Protocol and Application Data Protocol.

3.1 The TLS Record Protocol

Taking messages to be transmitted, the Record protocol, fragments the data into manageable blocks, compresses the data (optional), applies a MAC, encrypts, and transmits the result. To

allow a client and a server to agree upon security parameters, the TLS protocol uses the TLS handshake protocol.

3.2 The TLS Handshake Protocol

The client and the server in TLS handshake protocol authenticate each other using certificates or pre-shared keys (PSK) [30], instantiate the negotiation of security parameters and compute the session key that is used to encrypt exchanged data. This consists of three steps.

3.2.1 Step 1

The client and the server in the first step negotiate the parameters of the secure session. These parameters especially contain the session identifier (SessionID) and the cipher suite. This latter is formed by 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. In its ClientHello message, the client includes (Figure 1) a list of supported triplets in order of its preference. With its ServerHello, the server replies that especially conveys the selected cipher suite or, if no acceptable choices are presented, returns a handshake failure alert and closes the connection. The ServerHello and ClientHello establish the following attributes: Protocol Version, Session ID, Cipher Suite, and Compression Method. Two random values additionally are generated and exchanged: ServerHello.random and ClientHello.random.

3.2.2 Step 2

In a second step the client and the server authenticate each other. Two authentication modes have been defined in the TLS protocol: only server authentication and mutual authentication. The authentication is usually performed by using pre-shared keys [30] or public key certificates installed in both the client and the server and in such case a public key infrastructure (PKI) is required [8].

The server in based-certificate authentication sends a certificate request message (Figure 1), inviting the client to reply with a certificate. A certificate is hands by the client to the server by which the client proves that it is legitimately the owner of the certificate. The client by way of proof 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 Figure 1, (*) indicates that a ServerKeyExchange message may be sent, if it is required; for example if the certificate is for signing only [8].

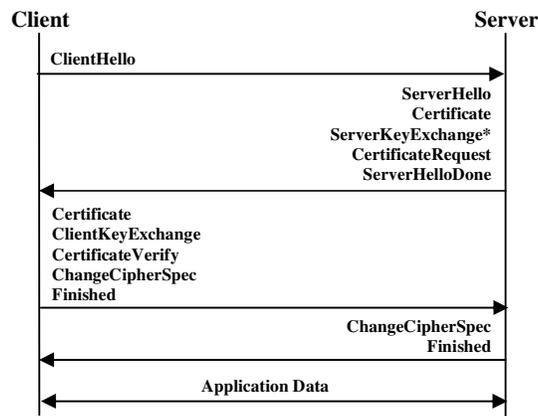


Figure 1. The TLS Handshake Protocol [8].

3.2.3 Step 3

In order to test the success of selected authentication mode and the key exchange processes, both the client and the server exchange the ChangeCipherSpec and the finished messages (Figure 1). The finished messages give proof to both the client and the server that they have the same key material because finished messages are the first messages processed and exchanged after applying the negotiated security parameters. The TLS finished messages is calculated by the following formula [8]:

$$PRF(\text{master_secret}, \text{finished_label}, \text{Hash}(\text{handshake_messages}))$$

Here, PRF is a pseudo-random function defined in [8]. To 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 indicates a Hash of the handshake messages. The handshake_messages includes all handshake messages starting at ClientHello up to, but not including, this TLS finished message. So, 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 value of master_secret is presented by the formula [8]:

$$\text{master_secret} = PRF(\text{pre_master_secret}, \text{“master secret”}, \text{ClientHello.random} + \text{ServerHello.random})$$

The pre_master_secret is derived from the mechanism of key distribution (such as an RSA or Diffie-Hellman). Therefore, 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. To decrypt the pre_master_secret, the server uses its private key. If conventional Diffie-Hellman computation is performed, the negotiated key is used as the pre_master_secret [8]. In the previous formula, the symbol “+” represents the operator of concatenation (for more detail please refer to [8]).

4. THE BB84 PROTOCOL

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

The quantum key distribution protocol BB84 was the first studied and practical implemented QKD physical layer protocol. Charles Bennett and Gilles Brassard elaborated this protocol in 1984 in their article [31]. This protocol is surely the most famous and most realized quantum cryptography protocol. Its scheme uses the transmission of single polarized photons (as the quantum states). The photons' polarizations are four, and are grouped together in two different non orthogonal basis.

The two non-orthogonal basis are Generally described as follows:

- The horizontal (0°) and vertical polarization ($+90^\circ$) shape the base \oplus , and we denote the base states with the intuitive notation: $|0\rangle$ and $|1\rangle$. We note $\oplus = \{|0\rangle, |1\rangle\}$.

- The diagonal polarizations ($+45^\circ$) and ($+135^\circ$) form the base \otimes . 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 state $\otimes = \{|+\rangle, |-\rangle\}$.

The information bit, taken from a random number generator, are associated with the basis as shown in Table 1.

Table 1. Association between information bit and the basis in the BB84 protocol.

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

An in [32-33], The BB84 protocol can be described as follows:

1) Quantum Transmissions (First Phase)

- a) Alice possesses a random string of bits $d \in \{0,1\}^n$, and a random string of bases $b \in \{\oplus, \otimes\}^n$, with $n > N$. N is the length of the final key.
- b) A photon in quantum state a_{ij} is prepared by Alice for each b_i in b and d_j in d as in Table 1, and sends it to Bob over the quantum channel.
- c) According 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) Over the classical channel, Alice sends the value of b_i to Bob.
 - ii) In reply to Alice, Bob states whether he used the same basis for the measurement. The values of d_i and d'_i are discarded if $b_i \neq b'_i$.
- b) Alice forms 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 (Eve) is detected and communication is aborted.
- c) The common secret key $K = \{0,1\}^N$ is the string of bits remaining in d once the bits disclosed in step 2b) are deleted.

In order to understand BB84 protocol it very important to introduce how we measure a qubit in the field of quantum physics; if we have a qubit as $|qubit\rangle = a|b\rangle + c|d\rangle$ so the measure of this state in the basis $\{|b\rangle, |d\rangle\}$ produces the state $|b\rangle$ with the probability of $|a|^2$ and the state of $|d\rangle$ with the probability of $|c|^2$ and of course $|a|^2 + |c|^2 = 1$ ($|a|^2$ is the absolute square of the amplitude of a). So, measuring with the incorrect basis yields a random result, as predicted by quantum theory. so, 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 test for eavesdropping in step 2b). Wherever Alice and Bob's bases are identical (i.e. $b_i = b'_i$), the idea is that, 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. All disturbances are supposed to be caused by Eve.

5. INTEGRATION OF QUANTUM CRYPTOGRAPHY IN THE TLS PROTOCOL: QKD-TLS

5.1 Processes of key distribution in TLS protocol

The TLS Record Protocol uses the TLS Handshake Protocol to generate security parameters. This task is achieved by using key distribution process. In description of TLS Handshake [8] the key distribution is limited to the only both Diffie Hellman (DH) and RSA exchange protocol. The problem is that both DH and RSA are not unconditional secure; their security is computational and so their security depends of the computation power or the time (or the execution time). For example the article [34] presents a simulation which shows that RSA can be broken with time.

By using QKD, we tend to achieve unconditional security because QKD is proven scientifically to be unconditional secure. This means that the security in this case is independently of the power of the eavesdropper and so security will not be menaced by the technological advancement. We propose for this reason to integrate QKD in the TLS Protocol instead of DH or RSA key exchange.

5.2 The requirements needed to QKD-TLS

Some requirements must be satisfied to integrate QKD in TLS Protocol:

- a) An optical channel: QKD uses photons to encode information to exploit the laws of quantum physics. Now, there are two mediums to transport photons: the optical fiber or free space [35]. But some recent research works experiment the use of atoms and electrons as quantum particle [36-37] and perhaps a novel kind of quantum channel will appear in the future. For our work, we choose the optical fiber because it is the most used in quantum systems. This is due to the fact that optical fiber reduces the noises than the free air.
- b) Optical modem: the modem can play the role of detector and emitter of photons. The purpose of the optical modem is to detect and to send photons. The modem has to include a photon detector and a photon emitter and also polarizer to encode data using different values of polarization as quantum states. It is employed to provide quantum key but also can be used to exchange data depending on the method of encoding information. The modem is very important because it can include the both roles of quantum and classical channel. There are many techniques used to elaborate such modem [38-39].
- c) Protocol of QKD: to generate a key, it is necessary to implement a protocol of QKD between the two optical modems. The key once generated, it is stored in a flash memory in order to be used in the phase of enciphering data. We have chosen in our work the BB84 protocol; firstly it is proved to be unconditionally secure and secondly it is simple to implement.

5.3 An additional component of TLS protocol: QKD Configuration Protocol

To facilitate the implementation of our novel scheme of TLS (including the service of QKD) we add to the TLS Protocol a new component which plays the role of configuration of QKD sub-network. The additional component brings the name of QKD Configuration Protocol. So in our solution, the TLS Protocol has five components: Handshake Protocol, Change Spec Protocol, Alert Protocol, Application Data Protocol and QKD Configuration Protocol.

We have proposed a message format to the QKD Configuration Protocol. The format contains an important field of the length of the key which will be generated by the mechanism of QKD. Others fields are shown in the Figure 2.

Type	Protocol	Version
Length		
Key-Length		
TTL	T	Authentication
Encoding		
Content		

Figure 2. The message format of QKD Configuration Protocol

The description of fields of the message format is as follows:

Type (1 byte): denotes the type of quantum cryptography protocol used. For example protocols based on the Heisenberg's Uncertainty Principle as BB84 or protocols based on the Bell's Inequality as E91 [40].

Protocol (1 byte): shows the quantum key protocol used (e.g. BB84, B92 [41], or E91).

Version (1 byte): allows the use of more than one version of the same protocol.

Length (4 byte): indicates the length of the message in byte.

Key-length (4byte): this field provides the length of the key provided by the execution of the quantum key protocol. Its length is between 1 and 4 bytes. The length is so huge in order to use the One Time Pad to achieve unconditional security. The length of the key in this case must be equal to data which will be encrypted [42].

TTL field (2 byte minus one bit): shows an amount of time (in seconds) or the number of messages when a key could be used in encryption process. If the time is expired or the max of messages is reached, the mechanism of QKD started to generate a new key.

T field (one bit): this field indicates if we use the number of messages or the amount of time. When its value is "1", the TTL filed shows an amount of time and when its 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 shows data associated with this message.

5.4 The modified TLS handshake Protocol: Quantum TLS Handshake Protocol

In QKD-TLS Protocol, we have added certain changes in the TLS Handshake Protocol. Our main goal is to generate security parameters by the mechanism of QKD and to remove all structure based on PKI (Public Key Infrastructure).

Firstly, we suppose the client and the server share a secret noted S. Secondly, 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.

We give the modified TLS Handshake Protocol the new name of Quantum TLS Handshake Protocol. Figure 3 summarizes how different messages are exchanged between the client and the server during the Quantum TLS Handshake Protocol.

As BB84 is vulnerable to "man in the middle" attack [31], we verify if an eavesdropper is detected once the execution of BB84 protocol is finished, by calculating the TLS finished in both sides of the client and the server. This is done by using the shared secret S and the key K derived from the BB84 Protocol.

During the Quantum TLS Handshake Protocol and when the server receives the ClientHello, it sends to the client a series of polarized photons. The number of photons to be transmitted

depends on the length of the desired key, the error correction algorithm and the privacy amplification algorithm used. For each photon to be sent, the server randomly chooses a state a_{ij} . The remaining steps (phase of public discussion) are exactly the same as it has described in section 4.

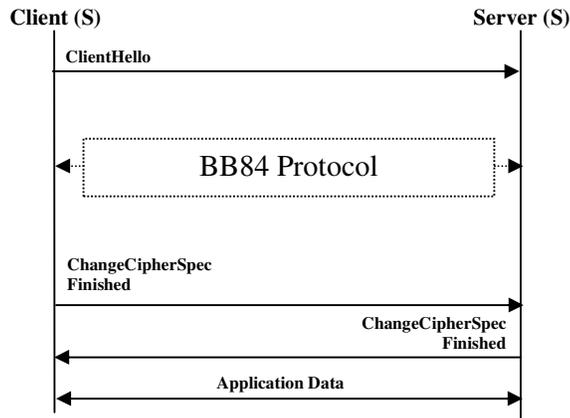


Figure 3. Messages exchanged in the Quantum TLS Handshake Protocol.

5.5 QKD-TLS in Operation Mode

Our objective is to use the mechanism of QKD in the process of authentication and in the data encryption. First, we use the key generated by BB84 protocol with the secret S in the expression of pre_master_key presented in formula of calculation of $master_secret$ which used in calculation of the TLS finished and so we check the mutual authentication of the client and the server. Secondly, we exploit the key provided by BB84 protocol 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 Figure 4 gives our scheme of QKD-TLS protocol.

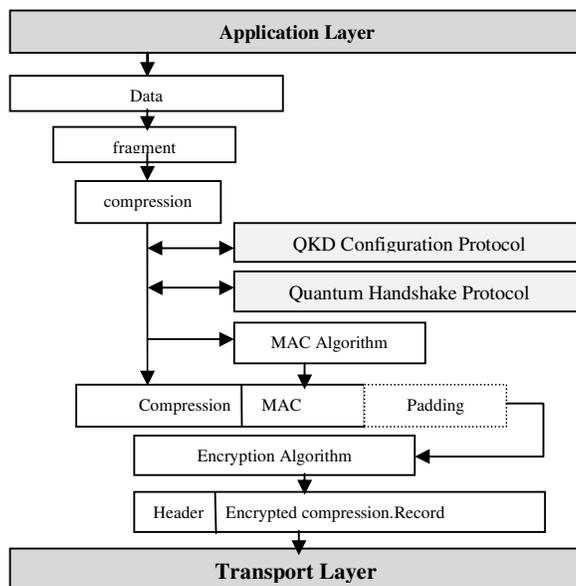


Figure 4. QKD-TLS protocol in operation mode.

In our scheme, the TLS Protocol occurs two changes. We integrate a new component named QKD Configuration Protocol and we have done some changes in the original TLS Handshake Protocol (Quantum TLS Handshake Protocol) to include the service of QKD.

In operating mode, when TLS Record receives from the Application Layer the data, 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 Figure 2. Once QKD Configuration Protocol is executed, a session of Quantum TLS Handshake begins (Figure 3). Then the client and the server start the BB84 protocol to derive a key K which the security is guaranteed by the laws of quantum physics.

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

$$pre_master_secret = K + S$$

The TLS finished is computed as described in section 3 by the expression:

$$PRF(master_secret, finished_label, hash(handshake_messages))$$

We note that the calculation of TLS finished uses the key generated by QKD because we have for our QKD-TLS protocol:

$$master_secret = PRF(pre_master_secret, "master_secret", ClientHello.random)$$

It is very important to mention that in the all public messages exchanging during the executions of BB84 protocol are part of the value of the handshake_messages

Once the server receives the TLS finished message from the client, it calculates its own TLS finished 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 done by the client when it receives the TLS finished of the server. We conclude then that the mechanism of QKD is exploited in checking the mutual authentication between the client and the server.

The Record Protocol needs an algorithm to generate keys required by the current connection state from the security parameters provided by the Handshake Protocol. The key K (instead of pre_master_key as in the original TLS Protocol) is divided 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 [8]. We conclude thus that the mechanism of QKD is used in the data encryption in QKD-TLS protocol.

In the next connection between the client and the server we change the secret shared S by K: $S=K$. and so any key generated by the BB84 protocol will play the role of S in the next connection. This improves the security by varying S at any connection because this makes the task of discovering S by an eavesdropper very hard.

5.6 Example of using QKD-TLS Protocol

In this section, we present an example of implementing QKD-TLS. We consider two LAN networks connected via two optical modems as illustrated in Figure 5.

To improve the security of a TLS connection between A and B using Quantum Cryptography, six phases must be done:

Phase 1: when TLS Record Protocol in the point A gets the data from the Application Layer, it calls its Application Data Protocol. The data then is fragmented and for each fragment a compression could be done.

Phase 2: the TLS Record Protocol uses the QKD Configuration Protocol in order to let the points A and B agree on the parameters illustrated in QKD Configuration Protocol format (Figure 2). The most interesting fields are: the protocol, the key-length, the TTL and the T fields. We choose the protocol BB84 for this example. We suppose that version=1. We assume that there is no mechanism of authentication and encryption. We propose these choices: Key-length= 40 bytes, TTL = 400 messages, T=0. We must choose TTL =1 if we plan to use One Time Pad to attain unconditional security.

Phase 3: the Quantum Handshake Protocol is used by the TLS Record Protocol to obtain the security parameters. The Quantum Handshake Protocol begins and during the QKD process, the BB84 protocol is implemented between the two modems. The key generated K 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 K 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 Figure 4. Also, in this phase A and B check each other the authentication using TLS finished with the two secret S and K.

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.

Phase 6: We change the value of S by K ($S=K$) and the new shared secret between the client and the server is K.

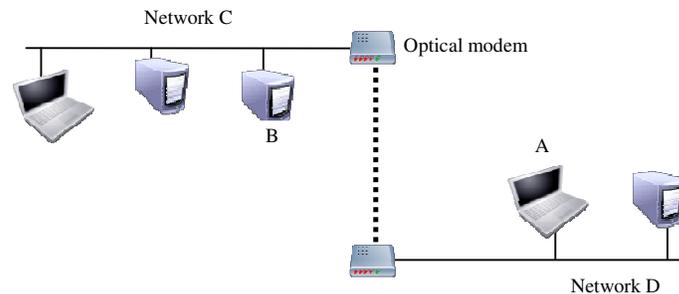


Figure 5. An example of QKD-TLS implementation

6. CONCLUSION

A novel scheme of TLS Protocol based on QKD is presented in this paper. We have introduced a Quantum TLS Handshake which enhances the security of the TLS Handshake; the mechanism of key distribution is established by QKD instead of the classical key distribution as RSA or Diffie-Hellman. We have added also a new component to the TLS Protocol in order to render our scheme applicable. Our new scheme of QKD-TLS Protocol includes the following advantages:

- During the Quantum Handshake Protocol, the messages exchanged become simpler. We needn't certificates and the infrastructure of PKI is removed.
- The secret shared S is modified at each new connection. This improves hugely the security.

-Our scheme does not need to invent or to build new quantum devices. The optical modem is composed of standard already existing components as the single photon source and photon detector.

-In our scheme, the unconditional security could be reached with a very low price. Many companies and organization are already using the optical fiber. Therefore, companies can use the existing infrastructure to generate keys by the service of Quantum Cryptography.

REFERENCES

- [1] Gisin, N., et al.: 'Quantum cryptography', *Rev. Mod. Phys.*, 2002, 74, pp. 145–195.
- [2] Bennett, C.H., et al.: 'Experimental quantum cryptography', *J. Cryptol.*, 1992, 5, pp. 3–28
- [3] 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.
- [4] 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.
- [5] 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.
- [6] arXiv: Quant-ph/0403104, 2004.
- [7] 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.
- [8] Tim Dierks , Eric Rescorla, " The Transport Layer Security (TLS) Protocol, Version 1.2" , RFC 5246 , August 2008.
- [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] M. Elboukhari, M. Azizi, A. Azizi "Integration of Quantum Key Distribution in the TLS Protocol", *IJCSNS*, Vol. 9 No. 12 pp. 21-28, 2009. http://paper.ijcsns.org/07_book/200912/20091204.pdf
- [13] Elliott, C., "The DARPA Quantum Network", *Quantum Communications and Cryptography*, 2006.
- [14] C. Elliott, D. Pearson, G. Troxel, "Quantum Cryptography in Practice," *Proc. ACM SIGCOMM* 2003.
- [15] C. Elliott, "Building the quantum network," *New J. Phys.* 4 (July 2002) 46.
- [16] M Peev and al, " The SECOQC quantum key distribution network in Vienna", *New Journal of Physics* 11 (2009) 075001.
- [17] Mehrdad Dianati, R.A., Maurice Gagnaire, Xuemin (Sherman) Shen, *Architecture and protocols of the future European quantum key distribution network. Security and Communication Networks*, 2008. 1(1): p. 57 - 74.

- [18] Poppe, A., M. Peev, and O. Maurhart, Outline of the SECOQC quantum-keydistribution network in Vienna. *International Journal of Quantum Information*, 2008. 6(2): p. 209-218.
- [19] Alleaume, R., et al., SECOQC White Paper on Quantum Key Distribution and Cryptography. Arxiv preprint quantph/ 0701168, 2007.
- [20] Khan, M.M., et al., A Quantum Key Distribution Network through Single Mode Optical Fiber. *Proceedings of the International Symposium on Collaborative Technologies and Systems*, 2006: p. 386- 391.
- [21] Le, Q.C. and P. Bellot, Enhancement of AGT Telecommunication Security using Quantum Cryptography. *Research, Innovation and Vision for the Future*, 2006 International Conference on, 2006: p. 7-16.
- [22] Kimble, H.J., The quantum internet. *Nature*, 2008. 453(7198): p. 1023.
- [23] Gisin, N. and R. Thew, Quantum communication. *NATURE PHOTONICS*, 2007. 1(3): p. 165.
- [24] Nguyen, T.M.T., M.A. Sfaxi, and S. Ghernaouti-Hélie, 802.11 i Encryption Key Distribution Using Quantum Cryptography. *JOURNAL OF NETWORKS*, 2006. 1(5): p. 9.
- [25] Ghernaouti-Helie, S. and M. Sfaxi, Upgrading PPP security by quantum key distribution. *NetCon 2005 conference*, 2005.
- [26] Ghernaouti-Helie, S., et al., Using quantum key distribution within IPSEC to secure MAN communications. *MAN 2005 conference*, 2005.
- [27] Ghernaout-Helie, S. and M.A. Sfaxi, Applying QKD to reach unconditional security in communications.
- [28] Rass, S., et al., Secure Message Relay over Networks with QKD-Links. *Quantum, Nano and Micro Technologies*, 2008 Second International Conference on, 2008: p. 10-15.
- [29] A. Frier, P. Karlton, P. Kocher, "The SSL 3.0 Protocol", Netscape Communications Corp., November 1996.
- [30] P. Eronen, et. al., "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", RFC 4279, December 2005.
- [31] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing*, New York, Bangalore, India, 1984, pp. 175–179.
- [32] M. Elboukhari, M. Azizi, A. Azizi, "Analysis of the Security of BB84 by Model Checking", *IJNSA*, Vol 2, Number 2, pp. 87-98, April 2010. <http://airccse.org/journal/nsa/0410ijnsa7.pdf>
- [33] M. Elboukhari, M. Azizi, A. Azizi, "Analysis of Quantum Cryptography Protocols by Model Checking", *IJUCS*, Vol 1, pp. 34-40, 2010. <http://www.hypersciences.org/IJUCS/Iss.1-2010/IJUCS-4-1-2010.pdf>
- [34] 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.
- [35] 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/>
- [36] Knight, P (2005). "Manipulating cold atoms for quantum information processing". *QUPON conference Vienna 2005*.
- [37] Tonomura, A (2005). "Quantum phenomena observed using electrons". *QUPON conference Vienna 2005*.
- [38] Idquantique : www.idquantique.com
- [39] magiQ www.magiqttech.com

- [40] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991)
- [41] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., vol. 68, pp. 3121–3124, 1992.
- [42] 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>

Authors:



Mohamed Elboukhari received the DESA (diploma of high study) degree in numerical analysis, computer science and treatment of signal 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 his diploma of State engineer in Automation and Industrial Computing in 1993 from the Mohammadia's School of engineers at Rabat (Morocco) and obtained his PH.D in Computer Science in 2001 from the Université de Montréal (DIRO-FAS) at Montreal (Canada). He is currently professor at the University of Oujda (Morocco). He teaches several courses in the domain of computer science such as OOP, IA, RT-systems, Distributed Systems, TCP/IP, WEB, and Computers Security. He also supervises a number of Master/PH.D students. His research interests include: Verification/Coverification of real-time and embedded systems, Data communication and security, and Computer-aided management of industrial processes.



Abdelmalek Azizi obtained his first Doctorate in Number Theory in 1985 from the Mohammed Vth University at Rabat (Morocco). He then obtained a Ph.D. in the same domain in 1993 from the Laval University at Quebec (Canada). Since this date, he supervises the organization of the Doctoral studies in the research area of class field Theory and its Cryptography applications at the Mohammed First University at Oujda (Morocco). Currently, he is the head of the ACSA Research Laboratory (Arithmetic, Scientific Computation and Applications) at the Mohammed First University at Oujda (Morocco). His research interests are in several fields such as History of Mathematics and Cryptography in Morocco, Class Field Theory and its Applications to Cryptography and the Mathematical Didactics...