Upgrading PPP security by Quantum Key Distribution*

Solange Ghernaout-Helie and Mohamed Ali Sfaxi

Inforge-HEC
university of Lausanne, Switzerland
{sgh@unil.ch, MohamedAli.Sfaxi@unil.ch}

Abstract. Quantum cryptography could be integrated in various existing concepts and protocols to secure communications that require very high level of security. The aim of this paper is to analyse the use of quantum cryptography within PPP. We introduce basic concepts of the Point to Point Protocol; we propose a solution that integrates quantum key distribution into PPP. An example is given to demonstrate the operational feasibility of this solution

Keywords. PPP, Quantum Key Distribution (QKD) within PPP, unconditional security transmission, data-link layer security, enhance PPP security, feasibility study, application domain

1 Introduction

Cryptography is largely used to increase security level of ICT infrastructures. However the enciphering mechanisms currently deployed are based on mathematical concepts whose robustness is not proven. Nowadays, with the sight of new discoveries in cryptanalysis, technology empowerment, new generations of computers and architectures (GRID computing...), trust, security dependability and resilience cannot be satisfied any more by a classical approach of cryptography. Since few years ago, the progress of quantum physics allowed mastering photons which can be used for informational ends (information coding, transport...). These technological progresses can also be applied to cryptography (quantum cryptography). Quantum cryptography could be integrated in already existing algorithms and protocols to secure networks. For instance, IP Security protocol (IPSEC) [RFC2401] can support the use of quantum cryptography [11]. Another kind of protocols could take benefits of the quantum cryptography concepts to optimise and to enhance security in link layer (OSI layer 2 protocols) such as the Point to Point Protocol (PPP) [RFC1661].

* This work has been done within the framework of the European research project : SECOQC - www.secoqc.net

2 The importance of OSI layer 2 security

Securing layer 2 transactions is fundamental because this layer is common to all kinds of nodes' connections. The security processing is made transparently to the users and to the other protocols. Securing this layer is more optimised than securing the above OSI layer since neither additional encapsulation nor header is required.
The Point to Point Protocol [RFC1661] is a layer 2 protocol. It is widely used to connect two sets of nodes. This protocol was published in 1994 and natively the only security is done by additional authentication protocols. The confidentiality is not implemented in the original protocol but it was introduced by the Encryption Control Protocol [RFC1968]. This protocol uses the classical cryptography (algorithms such as DES or 3DES). Since, traditional cryptography is not based on "unconditional" evidence of security in term of information theory, but on not proven mathematical conjectures. It rests thus on what one calls the "computational" assumptions, i.e. on the idea that certain problems are difficult to solve and that one can control the lower limit of time necessary to the resolution of these problems [1]. In this context, security cannot be guaranteed. It is a crucial problem for an effective protection of sensible data, critical infrastructures and services. Using quantum cryptography concepts, the sender and the receiver could exchange secret keys. This exchange is proved to be unconditionally secure. Quantum key distribution with the One Time Pad [27] brings an unconditional security aspect to the communication upon the layer 2.

3 Brief presentation of PPP [RFC1661]

This section describes the PPP concept to point out the operating mode and the security issues in this protocol. The point to point protocol is a data-layer protocol ensuring a reliable data exchange over a point to point link. When the connection is established and configured, the PPP allows the data transfer of many protocols (IP, IPX, AppleTalk). That's why; PPP is widely used in Internet environment.

3.1 PPP components

The PPP protocol consists of three elements:

- a link control protocol (LCP): this element carry on the establishment, the configuration, the test of data link connection;
- a set of network control protocols (NCP) to communicate (and configure if needed) with network layer protocols (NP);
- An encapsulation protocol: The packets or datagram are encapsulated in PPP frame. The protocols encapsulated in the frame are identified by protocol field.

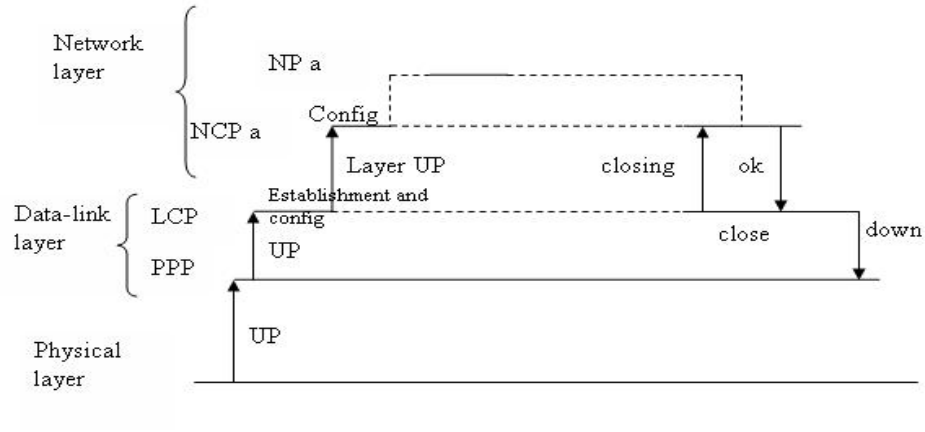

Fig. 1. PPP components connections (adapted from Labouret96)

The data-link layer is informed that the physical layer is "UP" and ready to be used (Figure 1). The LCP establishes and configure the PPP connection. After that, the network protocols could be encapsulated in PPP frame. In the figure 1, "NP a" is a network protocol related to the network control protocol "NCP a".

3.2 PPP connection

To establish a PPP connection, many steps have to be done before sending user's data. Following these steps, a reliable communication is possible between two linked nodes. These steps are presented in figure 2.

Dead status:
This status means that the link is not ready to receive any data. Every connection starts with this status. By receiving an "Up" event (carrier detection for instance), PPP goes to the "establishment" phase.

Establishment phase:
During the establishment phase, the Link Control Protocol (LCP) is used to establish and configure the connection.

Authentication phase:
The authentication phase is optional. If the use of an authentication protocol (PAP [RFC1334], CHAP [RFC1994], EAP [RFC2284],) has been required during the LCP negotiation, the authentication protocol is applied to authenticate

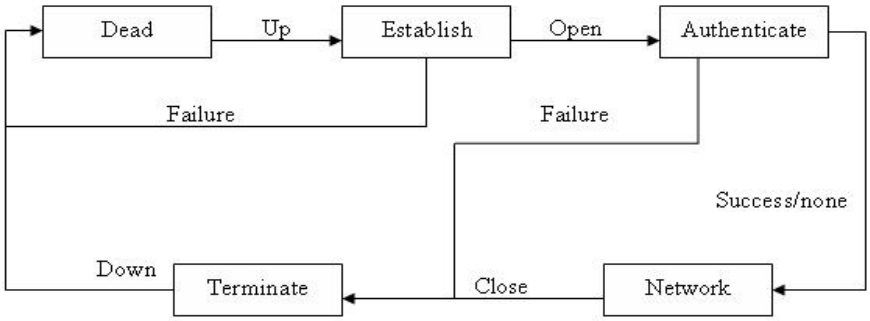

Fig. 2. PPP connection steps (RFC1661)

users. If the authentication fails, a "Down" event occurs.

Network phase:
After the establishment of the link connection by LCP, one or many NCPs have to be configured to let the corresponding network protocols to send their data by encapsulating it into PPP frame. As early as a NCP reaches the open status, the corresponding network protocol can transfer data until the closing of its NCP.

Terminate phase:
To close the connection, an LCP "Terminate frames" is sent. The LCP informs the network protocols that the connection will be closed.

3.3 The Link Control Protocol

The LCP transmits data using PPP; a LCP packet is encapsulated in PPP frame, in the PPP information field (Figure 3). The Link Control Protocol number is 0xC021. A LCP packet consists of 4 fields (Figure 4): The code field indicates the type of the LCP packet. There are 3 types of LCP packets:

- The configuration packets (Configure-Request, Configure-Ack, Configure-Nak, Configure-Reject). If a machine wants to establish a connection, it must start by transmitting a configuration packet (configure-request). The data field of this packet contains the desired configuration or modification.
- Termination packets (Terminate-Request and Terminate-Ack). These packets are sent if a machine wants to close a connection or if the identification fails.
- Maintenance packets (Code-Reject, Protocol-reject, Echo-Request, Echo-Reply, Discard-Request). These packets are used to test and to determine the performance of the link.

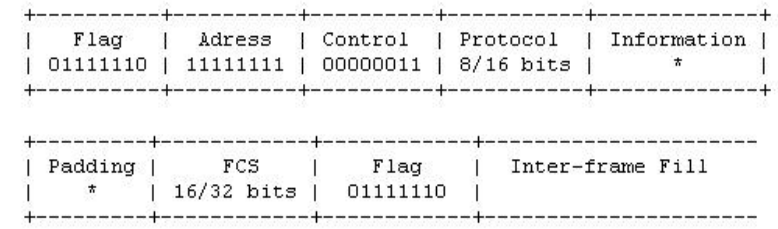

Fig. 3. PPP frame

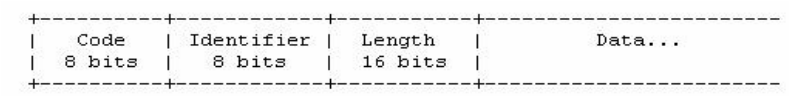

Fig. 4. a LCP packet

3.4 The security level in PPP

The unique security of PPP [RFC1661] is limited in the authentication phase. The two nodes use an authentication protocol such as Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). In 1996, Meyer published an additional security protocol for PPP called ECP (Encryption Control Protocol) [RFC1968]. This protocol allows the use of the encryption in PPP frame. The ECP gives the possibility to select the encryption algorithm and its parameters. This ensures the confidentiality and the integrity of the PPP frame. The weakness of this use resides in the way of generating and exchanging the encryption key. In fact, for all the encryption algorithms the secret key is assumed to be already shared between the communicating parties.

4 Enhancing PPP security by Quantum Key Distribution (QKD)

4.1 The use of (QKD) to secure PPP (Q3P)

As we have seen previously, the key exchange is not considered in the common use of the encryption algorithms. This fact leads to a misuse of cryptography in PPP. A possible key exchange method is Diffie-Hellman key agreement protocol [26]. This protocol allows two users to exchange a secret key over an insecure medium without any prior secrets. However, the Diffie-Hellman key agreement protocol can be compared to the discrete logarithm problem for its security. This

is not unconditional secure (i.e. secure independently of the computation power or the time) and can be broken. The Quantum Key Distribution is scientifically proven to be unconditional secure. That's why we propose to use the QKD to exchange the secret key between two nodes.

4.2 Key distribution using quantum concepts

Quantum cryptography is the only method allowing the distribution of a secret key between two distant parties, the emitter and the receiver with provable absolute security [2, 10]. Both parties encode the key on elementary quantum systems, such as photons, which they exchange over a quantum channel, such as an optical fiber. The security of this method comes from the well-known fact that the measurement of an unknown quantum state modifies the state itself: a spy eavesdropping on the quantum channel cannot get information on the key without introducing errors in the key exchanged between the emitter and the receiver. In equivalent terms, quantum cryptography is secure because of the no-cloning theorem of quantum mechanics: a spy cannot duplicate the transmitted quantum system and forward a perfect copy to the receiver [29].

4.3 Encryption Control Protocol (ECP) for Quantum Key Distribution (QKD)

The Encryption Control Protocol (ECP) defines the negotiation of the encryption over PPP links. After using LCP to establish and configure the data link, the encryption options and mechanisms could be negotiated. The ECP packets exchange mechanism is nearly the same as the LCP mechanism. The ECP packets are encapsulating into PPP frame (a packet per frame). The type is 0x8053 to indicate the Encryption Control Protocol. Two additional messages are added to the code field: the Reset-Request and Reset-Ack message. These two messages are used to restart the encryption negotiation. An encrypted packet is encapsulated in the PPP information field where the PPP protocol field indicates type 0x0053 (encrypted datagram). The ECP packet is presented in figure 5. In the

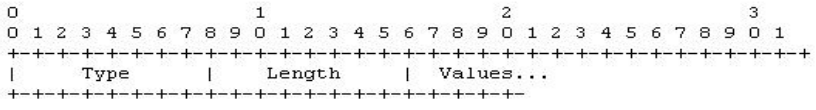

Fig. 5. an ECP packet

ECP packet, the type represents the encryption protocol option to be negotiated (for instance type 1 is DES encryption). The number of octets in the packet is

contained in the length field. The values field gives additional data or option needed for the encryption protocol. Up to now, there are only 4 encryption algorithms (type 0 = OUI, type 1 = DES, type 2 = 3DES, type 3 = DES modified) that could be used [16].

5 Integrating QKD in PPP: QKD-PPP (Q3P)

In order to exchange the encryption key, a key exchange protocol is necessary. In this section, we present how to integrate QKD in PPP

5.1 Q3P requirements

Some requirements must satisfied to integrate quantum cryptography within PPP.

a- An optical channel: the optical channel is the physical link between two adjacent nodes. Nowadays, there are two means able to carry a quantum cryptography transmission: the optical fibber or the free space (the air) [14]. As the quantum cryptography uses photons to encode the information no other channel could be used up to now. However, as the quantum physics are experimenting the use of atoms and electrons as a quantum particle [28, 17] maybe other kind of channel could be used in the future.

b- A Q3P modem: this modem has to polarize, send and detect photons; it has to include a photon detector and a laser with a single photon emitter and photon polariser. The source and the detector are widely commercialised and many techniques are employed[1]. However, these devices are used to exchange the quantum key but could also used to send and receive simple data depending on how encoding the information. The modem in this case is a simple optical fiber modem.

c- QKD protocol: in order to establish an unconditional secure key, a quantum key distribution protocol is needed. This protocol must be implemented in the Q3P modem. The protocol will deliver a secure key after distilling the key and error correction [10]. The key is stored in a flash buffer memory and used when enciphering the data. The QKD protocols BB84 and B92 [2, 3] are nowadays the quantum cryptographic protocols widely used. These protocols are securely proven and largely experimented [13].

5.2 ECP-QKD format

To establish and configure the quantum key distribution between the two nodes, it is necessary to exchange some data between them. We propose a specific ECP packet format to carry QKD parameters (Figure 6):
Type field:

[1] Idquantique : www.idquantique.com
magiQ www.magiqtech.com
CNRS France : http://www2.cnrs.fr/presse/journal/1979.htm

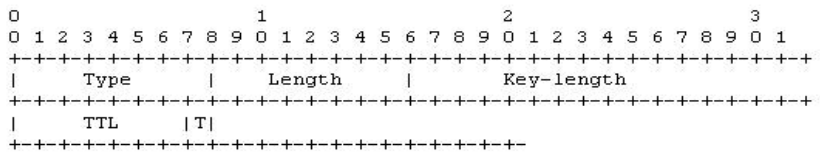

Fig. 6. ECP packet carrying a QKD protocol

As in the ECP standard packet the type field gives information about the option of encryption protocol negotiated. For this case, we will use an unassigned number for the QKD protocol. The selected QKD protocol is BB84 and the request to obtain an assigned number for this protocol is on going in IANA organisation [16].

Length field:
The length is number of octets in the packet and it is more than "5" octets (1 octet for the type, 1 octet for the packet length, 2 octets for the key length and one octet for the TTL and the T field).

Key-length field:
This field indicates the length of the encryption key. It is encoded on 16 bits and represents the size of the key in octet. The key size is comprised between 1 to 65535 octets. The size can be viewed as huge but we consider the possibility to use the One Time Pad function as the encryption algorithm. In this case, the key size must be equal to the PPP-data size [27].

TTL field:
This field can represent either the number of messages or the amount of time (in second) where a key could be used in the encryption mechanism. When the max number of messages is reached or the deadline expires, the QKD starts.

T field:
The T field specifies if the TTL field concerns the number of messages or the amount of time. If the value is "1", the TTL field corresponds to the amount of time in second. If it is "0", the TTL is the number of messages per key.

5.3 The Q3P operating mode

We adapt PPP connection steps [RFC1661] to integrate QKD process as shown Figure 7. The three first steps of Q3P are identical with PPP (phase 1 to 3). After authenticating the two nodes, the negotiation of the encryption parameters starts. In this phase, the encryption algorithm with its parameters is negotiated. If the two nodes do not need to use encryption, then the network phase starts. Else, if an encryption key is required, a QKD phase begins.

For Encryption negotiation (4) the nodes negotiate the key length and the TTL by sending an adequate ECP packet. After that (in 5), a quantum cryptography

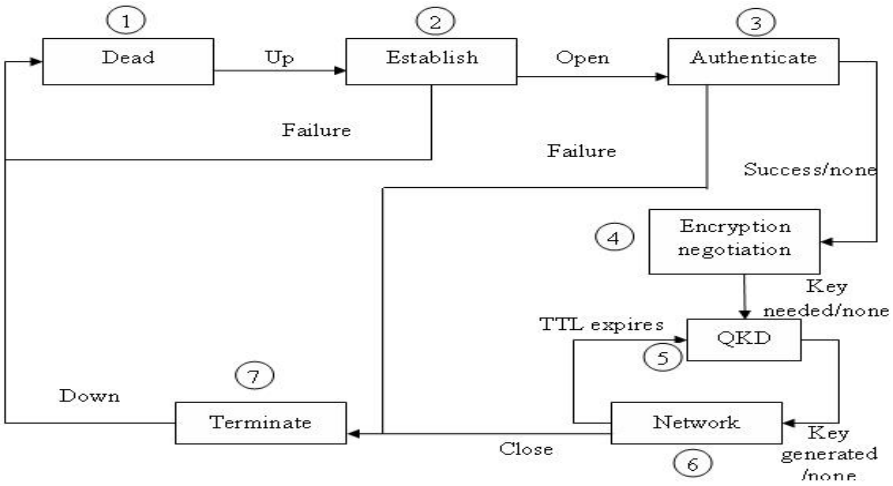

Fig. 7. Proposed Q3P steps and operating mode

exchange starts. At the end of the quantum key distribution phase, both nodes share a secret key, the encryption algorithm and the TTL of the key. This key is used in the network phase (6) while sending data. The data is enciphered thanks to the encryption key and the algorithm. When the TTL is expired, a new QKD phase starts. The end of the communication is the same as the PPP. The Figure 8 gives more details about Q3P operating mode. The modification (in bold in the figure 8) are little so that the adaptation of the PPP operating mode is easy to realise.

6 Advantages of Q3P solution

There many solutions dealing with the use of the quantum cryptography. Some of them are implementing on the layer 3 of the OSI model (network layer) [11]. Many issues rose when using the quantum key distribution in the network layer, such as the distance, the trust points, etc. Applying quantum cryptography in the layer two of the OSI model solves many issues and offers many advantages:

1. By using the link layer to carry on the quantum cryptography, the routing problem is avoided. In fact, as the network packets are encapsulated in a secure PPP frame and then transmitted, the routing issue is resolved as in a standard network. The encryption is transparent not only to the user but also to the whole network.
2. Implementing this solution do not need to built or invent any new quantum equipments. The only new device is the Q3P modem which is composed of

```
1- Initial state (Dead):
      a. When detecting an Up event then go the Establish
         phase
2- Establish phase:
      a. Configuration packets are exchanged (LCP)
      b. When finishing configuring the link connection go to
         the Authentication phase
3- Authentication phase:
      a. If required, the peer has to authenticate himself.
      b. If the authentication succeed or it is not required
         then go to Encryption negotiation phase else go to
         terminate phase
4- Encryption Negotiation phase:
      a. If required, the two nodes negotiate the encryption
         protocol parameters and the quantum key exchange
         parameters (such as TTL, Key length).   If not
         required, go the Network phase
      b. After the end of the negotiation, go to QKD phase
5- QKD phase:
      a. The source and the detector share a secret key
         exchanged using quantum cryptography
      b. When the secret key is ready go to Network phase
6- Network phase:
      a. The two node exchange data
      b. When the encryption TTL expires go to QKD phase
      c. If the communication is finished, go to terminate
         phase (a close event is generated)
7- Terminate phase:
      a. Terminate messages are exchange, when finish go to
         Dead state
```

Fig. 8. The Q3P algorithm

standard and already existing components such as the photon detector, the single photon source, etc.

3. Finally, the unconditional security could be reached with a very low price. In fact, many organisations and companies are already using optical fiber. So, organisations can use the existing infrastructure to exchange quantum key distribution. The Q3P modems are the most expensive equipments in these scenarios (approximately 100KEuros per pair[2]) however, according to specialist; it will become cheaper in the future.

7 Example of Q3P application - feasibility study

This section presents an example of using QKD-PPP to prove the functional feasibility. We assume that we have two LAN network connected via Q3P modems with optical fiber (Figure 9). We only apply protocols available nowadays with the QKD assigned number. We focus on the specific point of communication

[2] Source IdQuantique. www.idquantique.com

between the two modems (Figure 9).
Phase 1: The two modems are in the initial state. When the Q3P modems are on and connected via the optical fiber, an Up event is generated and the establishment phase starts.
Phase 2: The PPP configuration begins with the exchange of the LCP configura-

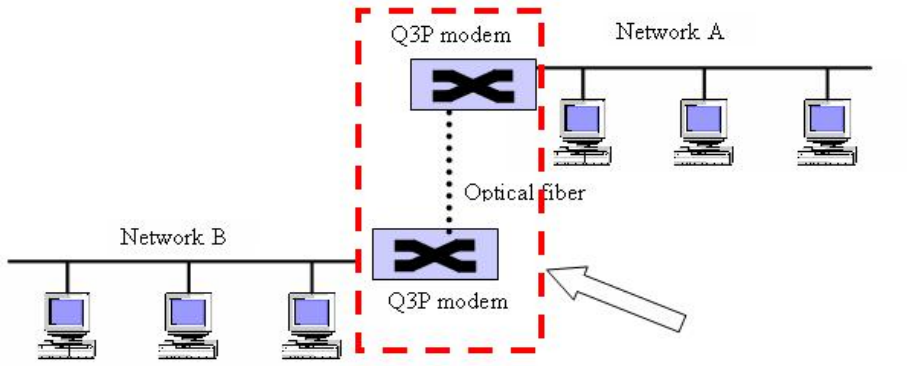

Fig. 9. An example of using Q3P

tion packets. In this example, we will select the authentication protocol CHAP from the list of the PPP authentication protocols. The identification of CHAP is 0xC223. So, the modem sends a LCP packet type3[3] for the authentication negotiation and the identification of authentication protocol is in the data field of the LCP packet (Figure 10). The Figure 11 shows the whole PPP frame for this exchange.
Phase 3: The modem sends a LCP packet type 4 to negotiate the quality proto-

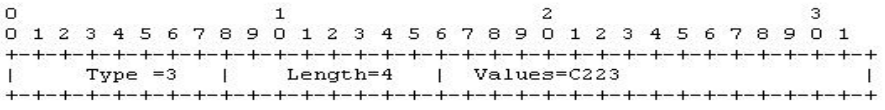

Fig. 10. the data of the LCP authentication packet

[3] The most common LCP types are: type 1 for the maximum receive unit, type 2 for asynchronous control character map, type 3 for the authentication protocol, type 4 for the quality protocol, type 5 for magic number see RFCs 1661, 1570.

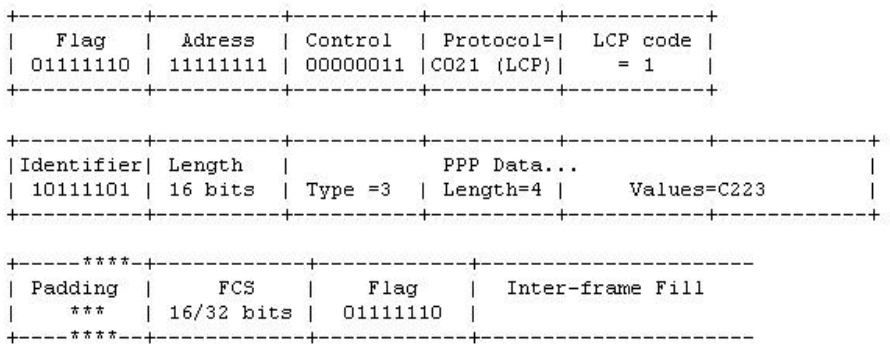

Fig. 11. the whole PPP frame

col. We choose the link quality protocol (LQP - 0xC025) as the quality protocol. In fact, the LQP is the quality protocol mostly used in PPP.
Phase 4: Then, the authentication phase starts. The CHAP packets are encapsulated in PPP frame.
Phase 5: When the authentication succeeds, the encryption negotiation begins. In our example, we use the triple DES encryption algorithm (ECP type 2)[4]. In fact, triple DES is the most secure algorithm usable in PPP. So the two nodes exchange ECP packets to negotiate the parameters of this protocol. The secret key shared by QKD protocol (we assumed that the IANA associates it to type 5), the length of the packet is 5 octets, the key length is 21 octets (168 bits), and we choose the TTL randomly say 100 messages so the T field is zero (Figure 12).
When, the network phase could start. For instance, we use Internet protocol as

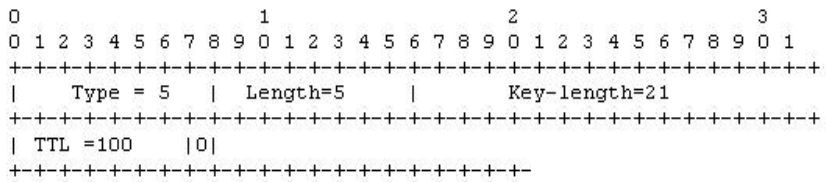

Fig. 12. ECP packet with QKD protocol negotiation

[4] The ECP types available nowadays are: 0 for OUI, 1 for DES, 2 for 3DES, 3 for DES modified. See [16] for more details.

the network protocol so we need to use the IPCP as a NCP in the Point to Point Protocol (Figure 13). After sending 100 messages, an ECP reset-request packet is sent to the peer node. Then, when receiving the reset-ack, a QKD phase starts. If one of the two nodes wants to close to communication, a terminate packet is sent.

Hypothesis:

- The authentication protocol : CHAP
- the encryption algorithm : 3DES
- the quality protocol : LQP
- the encryption Key length : 168 bits
- the TTL : 100 messages
- the network protocol : IP

Fig. 13. Q3P application hypothesis

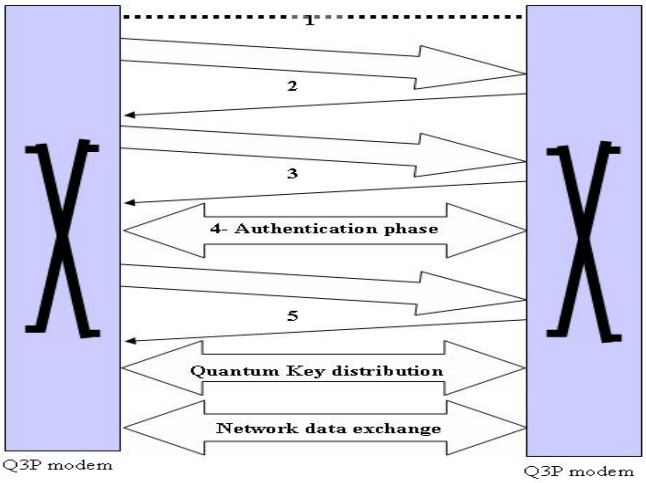

Fig. 14. type of messages exchanged between two quantum modems

8 Conclusion

Classical cryptography algorithms are based on mathematical functions. The robustness of a given cryptosystem 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. Unfortunately, there is no mathematical proof that will establish whether it is not possible to find the inverse of a given one-way function. On the contrary, quantum cryptography is a method for sharing secret keys, whose security can be formally demonstrated. The use of quantum cryptography will enforce safety, dependability and security of ICT infrastructures and critical infrastructures. The enciphering mechanisms rely on classical cryptography which we know the limits. To enhance the security level of protocols, we studied the possibility to integrate quantum key distribution into already existing protocols. It is important to have the option to secure efficiently the data transmission between two adjacent nodes. Using quantum cryptography in conjunction with PPP offer a better level of security in transmission. Our study points out the adaptation of the PPP protocol to integrate quantum key exchange (Q3P). The modifications to PPP are identified (packet format and operating mode). A data exchange example illustrates the operational feasibility of the proposed solution. Applying quantum key exchange and one-time-pad function at the layer 2, communication is not only possible but will upgrade considerably, with a low cost and less effort (modification, performances,), the security level of a communication between 2 adjacent nodes. The unconditional security could be effective for transmission. We recommend the use of quantum key distribution to share enciphering keys and the one-time-pad function to exchange confidential data. By using jointly the two mechanisms at the data-link layer, confidentiality and integrity of sensible information transmission is maximised.

References

1. Alléaume R (2004). "Réalisation expérimentale de sources de photons uniques, caractérisation et application à la cryptographie quantique" (Secoqc partner)
2. Bennet, C; Brassard, G (1984). IEEE International Conference on Computers, Systems, and Signal Processing. IEEE Press, LOS ALAMITOS
3. Bennet, (1992). *C Quantum Cryptography: Uncertainty in the Service of Privacy.* Science 257.
4. Donald S.Bethune and William P.Risk (2002). "*AutoCompensating quantum cryptography*". New journal of physics 4 (2002)42.1-42.15 URL: http://www.iop.org/EJ/article/1367-2630/4/1/342/nj2142.html
5. Clark, C. W; Bienfang, J. C; Gross, A. J; Mink, A; Hershman, B. J; Nakassis, A; Tang, X; Lu, R; Su, D. H; Williams, C. J; Hagley E. W; Wen, J (2000). "*Quantum key distribution with 1.25 Gbps clock synchronization*", Optics Express.
6. Crypto-Gram (March 2005). "SHA-1 Broken".Schneier, B. March 15th 2005.
7. Artur Ekert (1991). "*Quantum Cryptography based on Bell's Theorem*". Physical Review Letters. URL: http://prola.aps.org/abstract/PRL/v67/i6/p661_1
8. Elliott, C (2002). "*Building the quantum network*". New Journal of Physics 4 (46.1-46.12)

9. Elliott, C; Pearson, D; Troxel, G (2003). "*Quantum Cryptography in Practice*".
10. Gisin, N; Ribordy, G; Tittel, W; Zbinden, H. (2002). "*Quantum Cryptography*". Reviews of Modern Physics 74 (2002): http://arxiv.org/PS_cache/quant-ph/pdf/0101/0101098.pdf
11. Ghernaouti Hélie, S; Sfaxi, M.A; Ribordy, G; Gay, O (2005). "Using Quantum Key Distribution within IPSEC to secure MAN communications". MAN 2005 conference.
12. Grosshans,Van Assche, Wenger,Brouri,Cerf,Grangier (2003). "*Quantum key distribution using gaussian-modulated coherent states*" Letter to nature. URL: http://www.mpq.mpg.de/Theorygroup/CIRAC-/people/grosshans/papers/Nat421_238.pdf
13. Guenther, C (2003) "The Relevance of Quantum Cryptography in Modern Cryptographic Systems". GSEC Partical Requirements (v1.4b). http://www.giac.org/practical/GSEC/Christoph_Guenther_GSEC.pdf
14. 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/
15. IdQuantique (2004) "A Quantum Leap for Cryptography". http://www.idquantique.com/files/introduction.pdf
16. Internet Assigned Numbers Authority - IANA (2005). http://www.iana.org/numbers.html
17. Knight, P (2005). "Manipulating cold atoms for quantum information processing". QUPON conference Vienna 2005.
18. Labouret, G (2000). "IPSEC: présentation technique". Hervé Schauer Consultants (HSC). URL : www.hsc.fr
19. Le journal Le monde (march 2005). "Menace sur la signature lcronique". march the 5th 2005.
20. Lo, H.K; Chau, H.F. (1999). "*Unconditional security of quantum key distribution over arbitrarily long distances*". Science 283: http://arxiv.org/PS_cache/quant-ph/9803/9803006.pdf
21. Magic Technologies (2004). "Quantum Information Solutions for real world". http://www.magiqtech.com/products/index.php
22. Mayers, D (1998). "*Unconditionnal Security in Quantum Cryptography*". J. Assoc. Comput. Math. 48, 351
23. Paterson, K.G; Piper, f; Schack, R (2004). "*Why Quantum Cryptography?*". http://eprint.iacr.org/2004/156.pdf
24. Riguidel, M; Dang-Minh, D; Le-Quoc, C; Nguyen-Toan, L; Nguyen-Thanh, M (2004). "Quantum crypt- Work Package I". ENST/EEC/QC.04.06.WP1B. (Secoqc partner)
25. Rivest, R.L; Shamir, A; Adleman, L.M (1978). "*A Method of Obtaining Digital Signature and Public-Key Cryptosystems*". Communication of the ACM 21 no. 2 1978.
26. Schneier, B (1996). "Applied Cryptography" Second Edition. New York: John Wiley & Sons, 1996
27. 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
28. Tonomura, A (2005). "Quantum phenomena observed using electrons". QUPON conference Vienna 2005.
29. Wootters, W.K; Zurek, W.H (1982). "*A single quantum cannot be cloned*". Nature, 299, 802
30. Zemor, G (2001) "Cours de cryptographie", Editeur: Cassini