How QKD can improve the security level of future e-commerce transactions

M.A Sfaxi I. Tashi
S. Ghernaouti Hélie
ISI - University of Lausanne
CH-1015 Switzerland
{mohamedali.sfaxi,igli.tashi,sgh}@unil.ch

Abstract

To achieve an efficient use of cryptographic mechanisms to secure ICT infrastructures, we propose to integrate quantum key distribution into main communication protocols. This article gives some benefits and contributions of the use of quantum Key Distribution to enforce ICT security level. Several feasibility ways to implement solutions based on quantum key distribution are proposed.

1 Introduction

The enciphering mechanisms currently deployed are based on mathematical concepts whose robustness is not proven. 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 cryptography approach. In this context, security cannot be guaranteed.

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 aims at exploiting the laws of quantum physics in order to carry out a cryptographic task. Its legitimate users can detect eavesdropping, regardless of the technology which the spy may have [1].

Quantum Key Distribution (QKD) could be integrated in already existing algorithms and protocols to secure communication networks. The Point-to-Point Protocol, IP Security protocol (IPSEC) and Transport Layer Security (TLS) can support the use of quantum Key Distribution. These protocol are widely used. Integrating QKD into these protocols will highly affect the security level of the telecommunications.

This article identifies shortly the weaknesses of classical cryptography and analyses the advantages, benefits and contributions of the use of quantum Key Distribution to enforce ICT security level. The two ways of integrating Quantum Key Distribution (QKD) already proposed are: within the Point-to-Point Protocol, and within the

Internet Security Protocol (IPSEC. This paper focuses on the way to integrate Quantum Key Distribution in The Transport Layer Security (TLS) protocol to enhance the security level of Internet transactions.

2 Quantum cryptography as a substitute for the classical cryptography

2.1 Weaknesses of classical cryptography

The security of a given cryptosystem is based on the secrecy of its (private) key and the difficulty of computing the inverse of its one-way function(s) [14]. It is considered difficult to inverse a function if the time it takes to calculate the inverse depends exponentially on the size of the input. Unfortunately, there is no mathematical proof that will establish whether it is impossible to find the inverse of a given one-way function [10, 26]. The fact that an efficient algorithm has not yet been found (or rather published) does not mean that such an algorithm does not exist.
For instance, consider RSA and the Diffie-Hellman key exchange. The security of these two cryptosystems is based on the factorization into prime numbers of large integers and the calculation of the discrete logarithm in a predetermined field respectively. Both functions are believed to be mathematically difficult to calculate. However, it has never been proven that factorization and the computation of the discrete logarithm are not feasible. In addition, it has not been proven to be impossible that a private key (regardless of the length) can not be deduced from a public key. Informed observers believe it to be currently impossible (and perhaps forever impossible) for the 'good' asymmetric algorithms; no key deduction techniques have been publicly shown for any of them. In fact, some of the well respected, and widely used, public key / private key algorithms can be broken by any of cryptanalytic attacks. Indeed, all can be broken if the key length used is short to permit practical brute force key search; this is inherently true for all encryption algorithms using keys, including both symmetric and asymmetric algorithms.
Latter, the famous signature algorithm SHA-1 was broken by the team of Xiaoyun Wang in China [18, 5]. This only an example of how fragile is the classical cryptography.

2.2 Upgrading the security level by using quantum key distribution

Quantum Key Distribution (QKD) experimental systems and their performances progressed to reach these last years a stage sufficiently advanced to justify investments and the birth of start-ups seeking the market systems of quantum cryptography [20, 16].

In practice, QKD is able to propose a method of unconditional distribution of secret key. This key can then be used in various manners, by taking for that the methods and the techniques established by the classical cryptographers.

C SHANNON [27] in particular showed that there is a coding method which makes it possible to guarantee unconditional security of the communications between two protagonists sharing a secure key: it is the Code of VERMAN, also called “One Time Pad”which imposes to have a random key as long as the message and to use this key only once.

Quantum key distribution is capable to provide random keys which the security is unconditional, and which, combined with the Code of VERNAM, allows to obtain an unconditional cryptography technique. However, such encryption method is very “greedy”since it requires keys as long as the messages to be protected. We can, in practice, obtain an excellent security by exchanging the keys using quantum cryptography in order to use symmetric cryptography techniques, for example AES algorithm [31]. This method is the most adopted solution for the “commercial”quantum cryptography applications [20, 16]. It allows enciphering flows of several hundreds of Mbits/s. We can moreover show that security obtained exceeds largely the security implemented by traditional cryptographic methods.

3 Other work related to integrating QKD in other protocols

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

The Point to Point Protocol [RFC1661] is a layer 2 protocol. It is widely used to connect two sets of nodes. The encryption functionality in PPP is called ECP (Encryption Control Protocol) [RFC1968]. This protocol allows the use of the encryption in PPP frame but limits the key exchange. In fact, it is assumed that the two points have already shared the secret key. However, in order to exchange the encryption key, a key exchange protocol is necessary[29]. In the following, we present how to integrate QKD in PPP in order to share a secret key.

3.1.1 Q3P requirements

Some requirements must be satisfied to integrate quantum Key Distribution 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: optical fiber or free space (the air) [15].

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 (Idquantique : www.idquantique.com, magiQ www.magiqtech.com, CNRS France : http://www2.cnrs.fr/presse/journal/1979.htm).

c- QKD protocol: in order to establish an unconditionally 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 [10].

3.1.2 The Q3P operating mode

We adapt the PPP connection steps [RFC1661] to integrate the QKD process as shown in Figure 1.

The three first steps of Q3P are identical to PPP (phases 1 through 3). After authenticating the two nodes, the negotiation of the encryption parameters starts. In this phase, the encryption algorithm and its parameters are negotiated. If the two nodes do not need to use encryption, then the network phase starts. Otherwise, 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 a proper ECP packet. After that (in 5), a quantum cryptography 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 using the encryption key and the algorithm. When the TTL expires, a new QKD phase starts. The end of the communication is the same as in PPP.

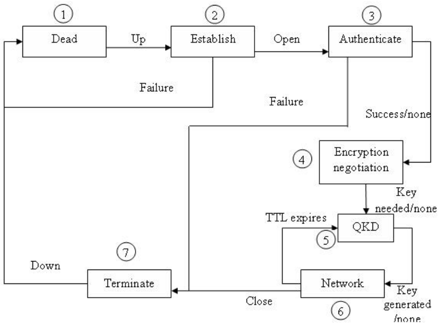


Figure 1: Proposed Q3P steps and operating mode

3.2 Integrating QKD within IPSEC (SEQKEIP)

Using QKD in IPSEC has already been proposed and implemented by Elliot of BBN technologies [7]. He proposes the idea of using QKD in IPSEC as a key generator for AES. In 2003, BBN technologies described the possibility of integrating QKD within the standard IKE [8] and announces some concerns linked to the compatibility of QKD with IKE [RFC 2409]. In our paper, we propose a QKD solution for IPSEC called SEQKEIP that is not based on IKE but on ISAKMP [RFC 2408]. Using this method, we avoid the problem of compatibility between IKE and QKD.

The idea is to stick to traditional IPSEC and the Internet Security Association and Key Management Protocol (ISAKMP). In fact, ISAKMP does not impose any condition on the negotiation mechanisms or on the SA's parameters. To use Quantum Key Distribution with IPSEC we simply have to define the two phases of IKE. We create a Secure Quantum Key Exchange Internet Protocol (SeQKEIP). SeQKEIP, like IKE, uses ISAKMP mechanisms, and takes advantage of Quantum Key Distribution in order to build a practical protocol [11].

SeQKEIP runs similary to the IKE. It includes 3 phases: phase 1 for the negotiation of the ISAKMP SA, phase 2 for the negotiation of SA, and we add a phase called "phase 0", in which Alice and Bob will share the first secret key. There are only three modes in SeQKEIP: Quantum Mode, Main Mode and Quick mode. Quantum mode is the quantum cryptography key exchange in phase 0. Main Mode is used during phase 1, and Quick Mode is an exchange in phase 2. Both the Main Mode and the Quick Mode are nearly the same of those in IKE.

In the beginning (Figure 2), phase 0 and phase 1 start (1&2). After these two phases the parameters of the protocol are fixed. In (3), we will use key exchanged thanks to Quantum Key Distribution. This key will be used either as a session key (4) or in the one-time-pad function (4').

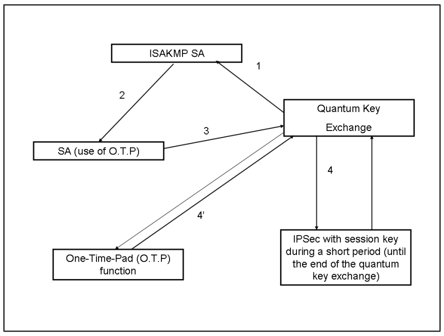

ISAKMP SA
1
2
Quantum Key Exchange
3
SA (use of O.T.P)
4
4'
One-Time-Pad (O.T.P) function
IPSec with session key during a short period (until the end of the quantum key exchange)

Figure 2: Functioning of IPsec with Quantum Cryptography

In (4), we use traditional symmetric cryptography algorithms to exchange data. The IPSEC packets are the same as without the use of quantum cryptography. The session key, therefore, is exchanged using quantum key distribution. The lifetime of the session key is very short, equal to the time needed to exchange the secret key using quantum cryptography. This solution is a transition solution to (4')

In (4'), we use quantum cryptography concepts totally. The idea is to shift completely to unconditionally secure functions, i.e. quantum key distribution and the one-time-pad function. We call this kind of cryptosystem, "the quantum cryptography". After fixing the SA parameters, the "session"key's length will be the size the data of in the IPSEC packet. Then, it is possible to use one-time-pad function (simply perform an XOR of the message with the key and then send the result). We need to exchange a key for every packet. The weakness of this solution resides in the time needed to exchange the key. The total bit rate is negatively affected due to this problem, but as the quantum cryptography technology progresses, this issue will soon be solved.

4 E-commerce and TLS/SSL

Transactions between buyers and sellers in E-commerce can include requests for information, quotation of prices, placement of orders and payment, and after sales services. This implies a high degree of confidence concerning the authenticity, confidentiality and timely delivery of such transactions. The problem is raised by the fact that these transactions are executed in a public network such as the Internet.

The interception of transactions, and in particular credit card details, during transmission over the Internet has often been cited as a major obstacle to public confidence in E-commerce.

The principle means of countering the threats to transactions in the Internet environment is the use of cryptography. Cryptography essentially provides three distinct capabilities:

- the content of electronic transactions can be hidden;
- any changes to electronic transactions can be detected;
- the source of electronic transactions can be confirmed.

Encryption and decryption allow secure transfer of information between an Internet browser and server

These capabilities are achieved through a combination of encryption and cryptographic digital signatures. Early E-commerce systems used server-based solutions to authenticate the users and terminate the TLS/SSL session. It very quickly became apparent that the server performance was a bottleneck to mass market E-commerce. To authenticate the users, the server would associate a particular session with an individual and go through an authentication sequence.

This mechanism is widely used by on-line merchants to ensure that credit card numbers and other sensitive information are protected during transmission across the Internet. TLS/SSL also allows verification of merchant identity via the SSL server certificate Generally SSL allows transacting business with the confidence that critical data will be safeguarded.

As with encryption, basic digital signature capability is built into standard web servers and browsers through TLS/SSL, which then allows users to:

- prove their identity in a way that is much more reliable than user-name/password mechanisms;
- confirm the identity of the web server with which they are communicating (e.g. to ensure they do not provide sensitive information to the wrong web site).

The use of TLS/SSL for encrypting payment card details is currently the dominant approach adopted by Internet merchants as it is cheap to implement and appears to be gaining consumer acceptance. Many Web sites use TLS/SSL to encrypt the personal and financial information sent over the Internet.

5 An example Q-Transaction

This section shows how QKD can be used in TLS/SSL to secure the transaction of sending credit card data in E-commerce.

E-commerce transactions are carried on by HTTP. The Web allows customers to select merchandises and finally pay by providing a credit card data. The credit card data is very critical information. There are (n) cases of thieving credit card data over the Internet every year.

The credit card data is sent from the Web browser to the Web server via parameters in a HTTP request. Before the Web browser sends the HTTP request with these parameters, it (the Web client is also the TLS/SSL client) initiates an TLS/SSL session to establish a quantum key between the Web browser and the Web server. The OtherParty parameter of the *getNewKey* API is the IP address of the Web server. The *KeyLength* parameter is set to the size of the HTTP request:

KeyLength = TLScipherText.length

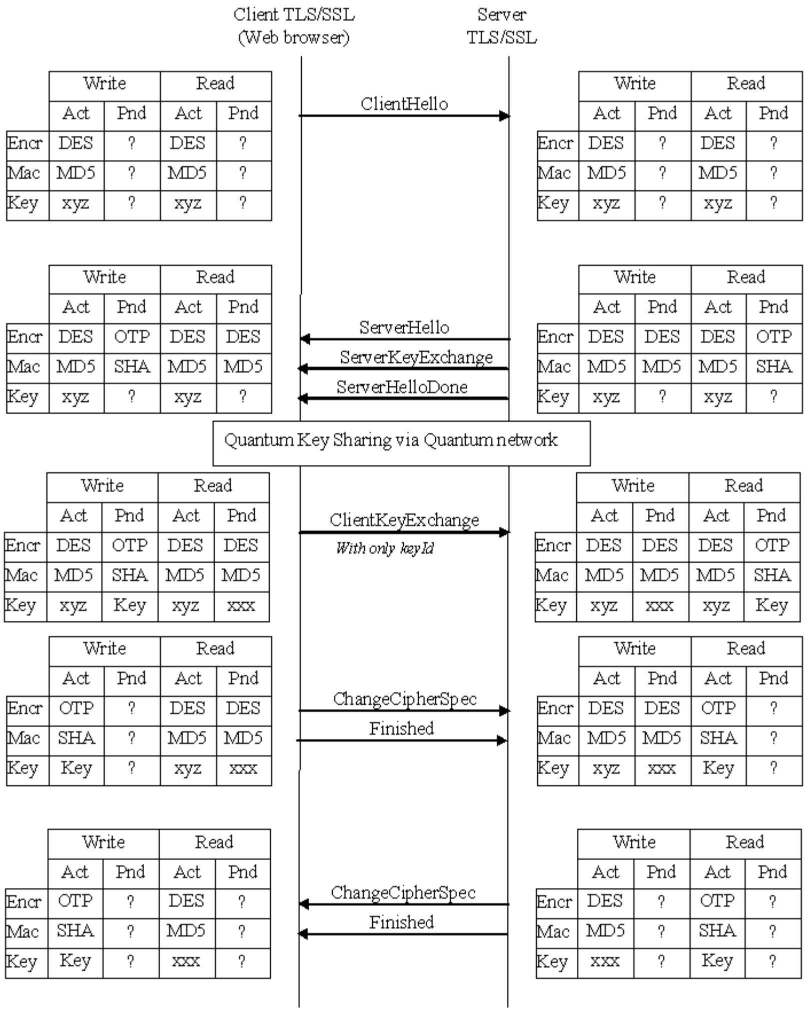
During E-commerce transaction ones has to identify the sensitive data being liable to be intercepted. To identify these in formations we analysed the main public materials of the three most important Credit Card companies VISA, MASTERCARD and AMERICAN EXPRESS.

The credit card's sensitive details which forward during a credit card transaction are as follows:

- Card number composed to the maximum of 16 digits.
- Expiry date composed of 4 digits
- The security code composed of 4 digits
- The Card Holder's name and first name composed to the maximum of 24 characters, including spaces.

We have the total of 48 characters. So if we consider that every character will be encoded on 1 byte, the total of 384 bits is required for a credit card transaction.

The TLS/SSL session is negotiated to use the One-time-pad encryption algorithm and SHA or MD5 algorithm for the MAC calculation. Once the security information is negotiated and the quantum key is established, the ChangeCipherSpec protocol activates the TLS/SSL session for the encryption of the HTTP request (Figure 3). After sending the HTTP request, the previous TLS/SSL session can be resumed and the quantum-based TLS/SSL session is no longer necessary. As the One-time-pad needs different random key for each encryption, the quantum-based TLS/SSL session cannot be reused. A new TLS/SSL session is established every time the Web client needs to encrypt an HTTP request containing credit card number.



	Write		Read	
	Act	Pnd	Act	Pnd
Encr	DES	?	DES	?
Mac	MD5	?	MD5	?
Key	xyz	?	xyz	?

	Write		Read	
	Act	Pnd	Act	Pnd
Encr	DES	?	DES	?
Mac	MD5	?	MD5	?
Key	xyz	?	xyz	?

	Write		Read	
	Act	Pnd	Act	Pnd
Encr	DES	OTP	DES	DES
Mac	MD5	SHA	MD5	MD5
Key	xyz	?	xyz	?

	Write		Read	
	Act	Pnd	Act	Pnd
Encr	DES	DES	DES	OTP
Mac	MD5	MD5	MD5	SHA
Key	xyz	?	xyz	?

	Write		Read	
	Act	Pnd	Act	Pnd
Encr	DES	OTP	DES	DES
Mac	MD5	SHA	MD5	MD5
Key	xyz	Key	xyz	xxx

	Write		Read	
	Act	Pnd	Act	Pnd
Encr	DES	DES	DES	OTP
Mac	MD5	MD5	MD5	SHA
Key	xyz	xxx	xyz	Key

	Write		Read	
	Act	Pnd	Act	Pnd
Encr	OTP	?	DES	DES
Mac	SHA	?	MD5	MD5
Key	Key	?	xyz	xxx

	Write		Read	
	Act	Pnd	Act	Pnd
Encr	DES	DES	OTP	?
Mac	MD5	MD5	SHA	?
Key	xyz	xxx	Key	?

	Write		Read	
	Act	Pnd	Act	Pnd
Encr	OTP	?	DES	?
Mac	SHA	?	MD5	?
Key	Key	?	xxx	?

	Write		Read	
	Act	Pnd	Act	Pnd
Encr	DES	?	OTP	?
Mac	MD5	?	SHA	?
Key	xxx	?	Key	?

Figure 3: QKD-TLS exchange

The client and the server establish a secure HTTPS connection using the traditional TLS/SSL mode. When a critical data is to be sent (either by the client or the server) a TLS handshake is engaged. The Hello messages allow to select the encryption algorithm which is one-time-pad (OTP), the algorithm to check the integrity. When this phase is over and the party sends a getNewKey, a quantum key sharing phase begins. Then, this party send using *"KeyExchange"* message the id of the key to other party in order to get the encryption key. At the end, to send sensitive data, a *changeCipherSpec* message is sent and the data will be sent using the one-time-pad associated to the quantum key (Figure 3).

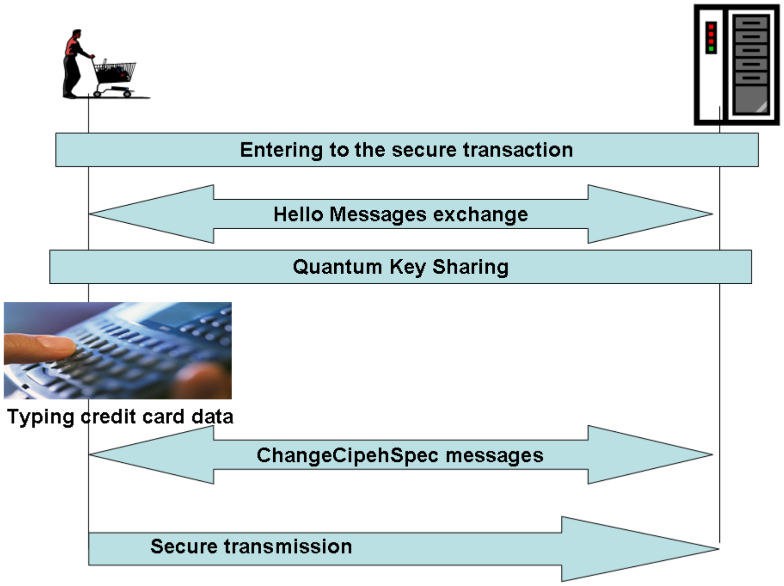


Figure 4: Example of QKD/TLS use to secure the transmisson of credit card data

For our example the client uses a secure connection with the E-commerce server (Figure 4). When arriving to a sensitive transmission, the client starts a TLS Handshake and puts the OTP, Hash hash function as pending parameters. The client also estimates the size of the data. In our case, it is credit card data, the size is assumed to be known. When this phase ends, the client asks for a quantum key. At the end of the quantum key sharing, the client put the secret Key in the key field of the pending and sends the id of this key to the server. The server gets the secret Key and puts it in the pending. When the client finishes entering sensitive data and presses the button to send it to the server, a *"changeCipherSpec"* is sent by the client. At the end this step (transmission of the finished messages), the data is encrypted using the quantum key and the one-time-pad.

6 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 key distribution is a method for sharing secret keys, whose security can be formally demonstrated.

As we have seen, it is possible to integrate the QKD concept into existing and widely used protocols. In our work, we call "quantum cryptography", the use of QKD with the One-time-Pad. Using these two methods we get an unconditional secure cryptosystem. Applying the QKD concept is possible at OSI-layer 4, OSI-layer 3, and layer 2 protocols. However, using QKD concept at OSI layer 2 is more suitable and more easier to integrate than applying it at layer 3 or 4(which need to have a quantum routing process). Nowadays, two commercial companies sell quantum cryptography devices and both of them chose to use the QKD concept at layer 2.

Acknowledgement

This work has been done within the framework of the European research project : SECOQC - www.secoqc.net. We would like to thank IDQuantique S.A (www.idquantique.com) and specially Gregoire Ribordy and Olivier Gay for their help and useful information. We would like to thank Dr. Thi Mai Trang Nguyen for the proposition of figure 3 of this paper.

References

[1] Bennet, C; Brassard, G (1984). IEEE International Conference on Computers, Systems, and Signal Processing. IEEE Press, LOS ALAMITOS

[2] Bennet, (1992). *C Quantum Cryptography: Uncertainty in the Service of Privacy.* Science 257.

[3] 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

[4] 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.

[5] Crypto-Gram (March 2005). "SHA-1 Broken".Schneier, B. March 15th 2005.

[6] Artur Ekert (1991). "*Quantum Cryptography based on Bell's Theorem*". Physical Review Letters. URL: http://prola.aps.org/abstract/PRL/v67/i6/p661_1

[7] Elliott, C (2002). "*Building the quantum network*". New Journal of Physics 4 (46.1-46.12)

[8] Elliott, C; Pearson, D; Troxel, G (2003). "*Quantum Cryptography in Practice*".

[9] Freebsd people. "IPSEC outline". URL: http://people.freebsd.org/~julian/IPSEC_4_Dummies.html Freesoft2004freesoft (2004). "IPSEC Overview". URL: http://www.freesoft.org/CIE/Topics/141.htm

[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] Alléaume et Al. (2007) “*SECOQC White Paper on Quantum Key Distribution and Cryptography*”. ArXiv.org. URL : http://arxiv.org/pdf/quant-ph/0701168

[14] 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

[15] 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/

[16] IdQuantique (2004) ”A Quantum Leap for Cryptography”. http://www.idquantique.com/files/introduction.pdf

[17] Labouret, G (2000). ”IPSEC: présentation technique”. Hervé Schauer Consultants (HSC). URL : www.hsc.fr

[18] Le journal Le monde (march 2005). “Menace sur la signature lcronique”. march the 5th 2005.

[19] 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

[20] Magic Technologies (2004). ”Quantum Information Solutions for real world”. http://www.magiqtech.com/products/index.php

[21] Mason A, (2002). ”IPSec Overview Part Five: Security Associations”. Cisco Press. URL: http://www.ciscopress.com/articles/printerfriendly.asp?p=25443

[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] Ghernaouti Hélie, S (2006). “Sécurité Informatique et Réseaux”. 1st Edition, Dunod 2006.

[29] Ghernaouti Hélie, S; Sfaxi (2005) : “Upgrading PPP security by Quantum Key Distribution”. Network Control and Engineering for QoS, Security and Mobility (NetCon 2005). Lanion, France - November 2005.

[30] Wootters, W.K; Zurek, W.H (1982). ”*A single quantum cannot be cloned*”. Nature, 299, 802

[31] Zemor, G (2001) ”Cours de cryptographie”, Editeur: Cassini

[32] Knight, P (2005). “Manipulating cold atoms for quantum information processing”. QUPON conference Vienna 2005.

[33] Tonomura, A (2005). “Quantum phenomena observed using electrons”. QUPON conference Vienna 2005.

[34] M. T. Nguyen Thi , M. A. Sfaxi, S. Ghernaouti - Hélie (2006): “Integration of quantum cryptography in 802.11 networks”. ARES 2006. Vienna, Austria, April 2006.