Using Quantum Key Distribution within IPSEC to secure MAN communications[1]

M.A. SFAXI* — **S. GHERNAOUTI-HÉLIE*** — **G. RIBORDY**** — **O. GAY****

(*)HEC - University of Lausanne
1015 Switzerland

{mohamedali.sfaxi,sgh}@unil.ch

(**) IdQuantique - Geneva
Switzerland

{Gregoire.Ribordy, Olivier.Gay}@idquantique.com

ABSTRACT. *Quantum cryptography could be integrated in various existing concepts and protocols to secure Metropolitan Area Networks communications. One of the possible use of quantum cryptography is within IPSEC. The applications of quantum cryptography are linked to telecommunication services that require very high level of security in Metropolitan Area Networks.*
The aim of this paper is to analyse the use of quantum cryptography within IPSEC to secure MAN communications and to present the estimated performances of this solution.
We analyse classical IPSEC advantage and limits to point out how quantum cryptography could enhance the security level of IPSEC. After having introduced basic concepts in quantum cryptography, we propose a solution that integrate quantum key distribution into IPSEC. A performance analysis is done to demonstrate the operational feasibility of this solution.

KEYWORDS: *MAN, Quantum cryptography, IPSEC, Security, performances.*

1. Introduction

Quantum cryptography aims exploiting the laws of quantum physics in order to carry out a cryptographic task. The uncertainty relations of Heisenberg can in particular be exploited to implement communication channels that cannot be passively - i.e. without disturbance of the transmission - eavesdropped. Its legitimate users can detect eavesdropping, no matter what technology is available to the spy [Bennet1983].

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

The power of quantum cryptography lies primarily in the fact that the keys distributed on the quantum channel are invulnerable to eavesdropping and can be guaranteed without assumptions on the computing power of an eavesdropper.

Quatum cryptography could be integrated in already existing algorithms and protocols to secure Metropolitan Area Networks (MAN) as the distance afforded by quantum cryptography is more than 100 Km. IP Security protocol (IPSEC) can support the use of quantum cryptography [RFC 2401]. This protocol is a collection of standards that was designed specifically to create secure end-to-end secure connections. The standard was developed by the Internet Engineering Task Force (IETF) to secure communications over both public and private networks.

The next section presents the IP Security Protocol (IPSEC). The third section gives a brief description of the principles of quantum cryptography scheme. Finally, we prove the feasibility of the use of quantum cryptography within the framework of IPSEC.

2. The classical IPSEC

2.1. *IPSEC Presentation*

IPSec is a collection of protocols and algorithms and is a flexible framework that allows vendors who use IPSec into their products to select the algorithms, keys, and authentication methods they want to use.

IPSec provides two basic services Authentication and Confidentiality

[Freebsd2004]:

– Authentication is achieved by the addition of an Authentication Header (AH) which comes after the basic IP header and contains cryptographically secured Hashes of the data and Identification information [RFC2402].

– Confidentiality is achieved through the addition of an Encapsulating Security Payload (ESP) header, and the possible rewriting of the payload in encrypted form [RFC2406]. ESP applies cryptographic concepts that provide authentication, integrity, and confidentiality of messages.

IPSEC defines a "Security Association" (SA) as its primitive means of protecting IP packets [Freesoft2004]. An SA is defined by the packet's destination IP address and a 32-bit Security Parameter Index (SPI), that functions somewhat like a TCP or UDP port number allow multiple SAs to a single destination address.

2.2. *IPsec Key management*

IKE (Internet Key Exchange) is a system developed specially for IPsec to give authentication mechanisms and exchanging keys within the possible situations over the Internet. It is composed of many elements: ISAKMP and a part of Oakley [RFC 2412] and SKEME [Labouret2000].

2.2.1. *ISAKMP*

As we have seen previously, security services are given by the use of security associations. These SAs defines parameters necessary to secure a data flow. ISKAMP (Internet Security Association and Key management Protocol) has as functionality the negotiation, the establishment, the modification and the suppression of security associations and their attributes.

ISAKMP is a generic framework independent from the negotiation mechanisms. It does not impose any condition to the SAs parameters [RFC 2407]. ISAKMP comprises two phases, which allow a clear separation of the negotiation of SA for a given protocol and protection of the traffic specific to ISAKMP:

During the first phase, a whole of attributes relating to security is negotiated; the identities are authenticated and the keys are generated. These elements constitute a first "security association", known as SA ISAKMP.

The second phase allows to negotiate the security parameters relative to SA for the account of a given security mechanism (for example AH or ESP). The exchanges in this phase are protected (confidentiality, authenticity...) thanks to SA ISAKMP.

ISAKMP is also independent of the keys generation method and the authentication and encryption algorithms used. It is thus independent of any key exchange protocol, which makes possible to clearly separate the details of the management of security associations from the details of key exchange. Various protocols of key exchange, presenting different properties are thus usable with ISAKMP.

2.2.2. *IKE*

IKE uses ISAKMP to build a practical protocol. IKE includes four modes: the Main Mode, the Aggressive Mode, the Quick Mode and the New Group Mode. Main Mode and Aggressive Mode are used during phase 1; Quick Mode is an exchange of phase 2. New Group Mode is neither an exchange of phase 1, nor an exchange of phase 2, but it can take place only if SA ISAKMP is established; it is used to agree on a new group for future exchanges DIFFIE-HELLMAN.

Phase 1: Main mode and Aggressive Mode

The following attributes are used by IKE and are negotiated during phase 1: an encryption algorithm, a hash function, and a method of authentication and a group for DIFFIE-HELLMAN.

Three keys are generated at the end of phase 1: one for enciphering, one for the authentication and one for creating other keys. These keys depend on the cookies, the exchanged number and public values DIFFIE-HELLMAN or the preliminary shared secrecy. Their calculation utilizes the chosen hash function for SA ISAKMP and depends on the selected authentication mode [RFC 2409]. The number of messages in the main mode is six while there are only three exchanged messages in the aggressive mode

In these two cases, the selected method for the authentication affects the contents of the messages and the method of the generation of session key [RFC 2409].

Phase 2: Quick mode

The messages exchanged during phase 2 are protected in authenticity and confidentiality thanks to the elements negotiated during phase 1. The authenticity of the messages is ensured by the addition of a HASH block after ISAKMP header, and the confidentiality is ensured by enciphering the whole blocks of the message.

Quick Mode is used for the negotiation of SA for given security protocols like IPsec. Each negotiation leads in fact to two SA, one in each direction of the communication.

2.3. *Limits of IPSEC and the benefits of using Quantum cryptography*

IPsec is one of the classical cryptography protocols. 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, in order to make in practice impossible "to break" these methods of encryption in a reasonable computing time with current data processing means [Alleaume2004].

The vulnerability with Internet Key Exchange (IKE) of IPSEC is the risk of compromising the first key exchange. It fact, the point is only secured either by a preshared secret or by Diffie-Hellman cryptography concepts. The classical cryptography is not an unconditional secure. That is why a substitution with quantum cryptography can provide an efficient and unconditional secure way.

Using quantum cryptography concepts, the sender and the receiver exchange secret keys. This exchange is proved to be unconditionally secure [Paterson2004].

3. The principles of quantum cryptography

This section briefly presents the principles of quantum cryptography, as well as state of the art realizations of quantum cryptography systems and their performance.

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 [Bennet1983, Gisin2002]. Both parties encode the key on elementary quantum systems, such as photons, which they exchange over a quantum channel, such as an optical fibber. 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, QC 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 [Wootter1982].

Several QC protocols exist. These protocols describe how the bit values are encoded on quantum states and how the emitter and the receiver cooperate to produce a secret key. The most commonly used of these protocols, which was also the first one to be invented, is known as the Bennett - Brassard 84 protocol (BB84) [Bennet1983]. The emitter encodes each bit on a two-level quantum system either as an eigenstate of x (coding for "0" and coding for "1") or as an eigenstate of y (or , with the same convention). The quantum system is sent to the receiver, who measures either x or y. After the exchange of a large number of quantum systems, the emitter and the receiver perform a procedure called basis reconciliation. The emitter announces to the receiver, over a conventional and public communication channel the basis x or y (eigenstate of x or y) in which each quantum system was prepared. When the receiver has used the same basis as the emitter for his measurement, he knows that the bit value he has measured must be the one, which was sent over by the emitter. He indicates publicly for which quantum systems this condition is fulfilled. Measurements for which the wrong basis was used are simply discarded. In the absence of a spy, the sequence of bits shared is error free. Although a spy who wants to get some information about the sequence of bits that is being exchanged can choose between several attacks, the laws of quantum physics guarantee that he will not be able to do so without introducing a noticeable perturbation in the key. Other protocols - like for example the B92 protocol [Bennet1992] - have been proposed.

In practice, the apparatuses are imperfect and also introduce some errors in the bit sequence. In order to still allow the production of a secret key, the basis reconciliation part of the protocol is complemented by other steps. This whole procedure is called key distillation. The emitter and the receiver check the perturbation level, also know as quantum bit error rate (QBER), on a sample of the bit sequence in order to assess the secrecy of the transmission. In principle, errors should be encountered only in the presence of an eavesdropper. In practice however, because of the imperfections of the apparatus, a non-zero error probability is always observed. Provided this probability is not too large, it does not prevent the distillation of a secure key. These errors can indeed be corrected, before the two parties apply a so called privacy amplification algorithm that will reduce the information quantity of the spy to an arbitrarily small level.

After the first demonstration of quantum cryptography by Bennett and his coworkers [Bennett...], several groups started developing experimental systems. The 90's saw rapid progresses in terms of key creation rate, key distribution range and practicality. Several approaches have been implemented in or out of the laboratory (see [Gisin2002] for a presentation of these different approaches. Refer also to [Grosshans2003] for a more recent approach.). All these implementations have in common the fact they allow the exchange of a cryptographic key whose security is based on the laws of quantum physics. They require two stations - an emitter and a receiver - connected by two channels, a quantum channel and a classical channel. The quantum channel must be a direct point-to-point optical link. It usually consists of a dark optical fibber, although some experiments have been performed in free space. The classical channel is a conventional communication channel and can take several forms: Internet, LAN, phone line, etc. It is used to exchange protocol information between the two stations. A key exchange using quantum cryptography basically consists of two phases. First, the raw key exchange, using photons over the quantum channel and second, the key distillation, where the two stations collaborate by exchanging information over the classical channel to establish the secrecy of the raw key.Current systems can distribute securely keys over distances up to 100 - 120 kilometers. The raw key creation rate ranges from 100 bits per second to 100'000 bits per second, depending on the system and the distance. After distillation, the key rate is smaller or equal to 50% of the raw key rate and usually around 10% - 20%. The actual percentage depends on the system, the distance and the amount of eavesdropping. It is reasonable to expect that within the next three years, systems achieving key distribution rates of more than 1M bits per second over distances of several dozens of kilometers will be developed.

4. SEQKEIP operating mode

As IPsec uses classical cryptography to secure communication, in this paragraph, we propose to use quantum cryptography to replace the classical cryptographic protocols used for symmetric distribution.

Using QKD in IPSEC has already been proposed and implemented by Elliot of BBN technologies [Elliott2002]. It proposes the idea of using QKD in IPSEC as Key generator for AES. In 2003, BBN technologies describes the possibility of integrating QKD within the standard IKE [Elliott2003] and announces some concerns linked to the compatibility of QKD with IKE. In our paper, we propose a QKD solution for IPSEC called SEQKEIP that is not based on IKE but on ISAKMP. Using this method, we avoid the problem of compatibility between IKE and QKD.

The idea is to stick to the traditional IPsec and the Internet Security Association and Key management Protocol (ISAKMP). In fact, ISAKMP does not impose any condition to is the negotiation mechanisms or to the SAs parameters. To use quantum cryptography with IPsec we have simply to define the two phases described above. We create a Secure Quantum Key Exchange Internet Protocol (SeQKEIP). The SeQKEIP

like IKE uses ISAKMP mechanisms and takes advantage of quantum cryptography in order to build a practical protocol.

SeQKEIP runs nearly like the IKE. It includes 3 phases: the 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 the phase 0. Main Mode is used during the 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.

Phase 0: Key exchange - Quantum Mode

This phase is the beginning of the secure exchange using quantum cryptography. After, these exchange both the sender and the receiver share a secret key. This key constitutes the pre-shared secret in IKE mechanism.

Phase 1: Negotiation of ISAKMP SA - Main Mode

During this phase, the cryptographic algorithm and the hash function are negotiated. Only the two parameters discussed in the phase 1 constitute the SeQKEIP attribute. The method to authenticate is the pre-shared secret (the secret key exchanged with Quantum Key Exchange method). Contrarily to IKE, SeQKEIP do not define DH groups and do not need to use digital signature nor digital certificates (Figure **??**). No cryptographic key are generated in this phase. The first exchanged key is used to encipher packets and to authenticate users.

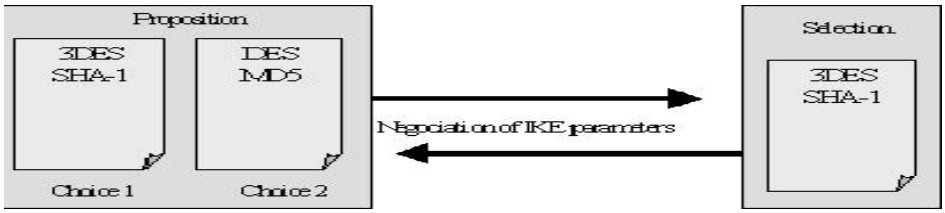

Figure 1. *Message exchanged during the first phase*

After the phase 0 and the phase 1, both sender and receiver will have the following information:

Shared secret key	This key is generated during the phase 0 with Quantum Key exchange mechanism. The secret key is used to authenticate users and to encrypt packet.
Encryption algorithm	The encryption algorithm is applied to the phase 2 (negotiation of SA parameters). The algorithm could be 3DES, DES, AES. But, if we want to have the maximum security, we have to use One-Time-Pad function (OTP).
Hash function	The hash function will give the opportunity to the sender and the receiver to check the integrity of the message and the authentication of the correspondents.

Note that the phase 0 and the phase 1 are totally independent and could be done at the same time. We need the secret key only from the phase 2.

Phase 2: Negotiation of SA - Quick Mode

As in IKE, the exchanged messages in phase 2 are protected in authentication and confidentiality by the negotiated parameters of the phase 1 and phase 0. The authentication is guaranteed by the addition of the HASH block after the ISAKMP header and the confidentiality is ensured by the encryption of the whole message blocks. The aim of this phase is to negotiate the SA. i.e. to negotiate the "IPsec" parameters. The SA parameters are [Mason2002]: Destination address, Security Parameter Index (SPI), the security mechanism (AH or ESP) and encryption & Hash function, the session key and additional attribute like the lifetime of SA.

For SeQKEIP, to extend security, we can use One-Time-Pad encryption function. The first exchanged key, in this case, will have the length of the message. We do not need thus any encryption algorithm for SA. We still need a Hash function to verify the integrity of the data. The run of IPSec could be modified in order to use one-time-pad function.

In the beginning (Figure 2), the phase 0 and the 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 cryptography. This key will be used either as a session key (4) or in the one-time-pad function (4').

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 exchange. The lifetime duration of the session key is very short and it is equal to the time needed to exchange the secret key using quantum cryptography. This solution is a transition solution to the (4')

In (4'), we use quantum cryptography concepts totally. The idea is to shift completely to the unconditional secure functions .i.e. quantum key exchange and one-time-pad function. After fixing the SA parameters, the "session" keys length will be of the size the data in the IPsec packet. Then, it is possible to use one-time-pad function (simply perform an XOR of the message and the key and then send the result).

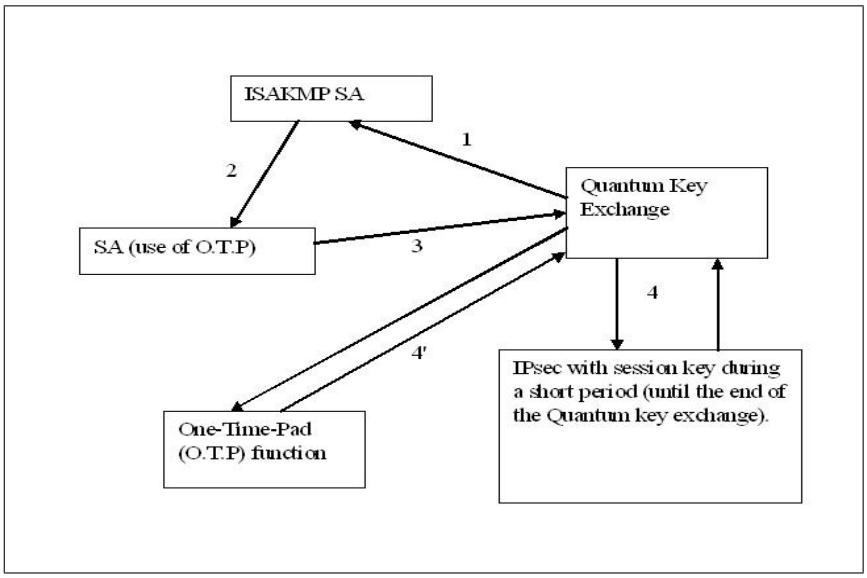

Figure 2. *Functioning of IPsec with Quantum Cryptography*

We need to exchange key for every packet. The weakness of this solution resides in the time needed to exchange the key. The total bit rate is highly affected due to this problem but as the quantum cryptography technology is progressing, this issue will soon be solved.

There are two possibilities. The first case is to exchange the key and distillation using the quantum channel (Time division multiplexing). The other is to exchange only the key over the quantum channel and all the other data over the public channel (Figure 3).

K: the duration to exchange the quantum key

D: the duration of key distillation

T: the duration of transmitting the message

1-first solution:

In this case, we propose to use the quantum channel to exchange the key and for distillation. There are two possibilities: K+D is greater than T (K+D$>$T) and K+D is less or equal to T (K+D$\leq$T).

The effectiveness (θ) of this solution is given by (θ represents the difference between the use of quantum cryptography and the use of unenciphered transmission):

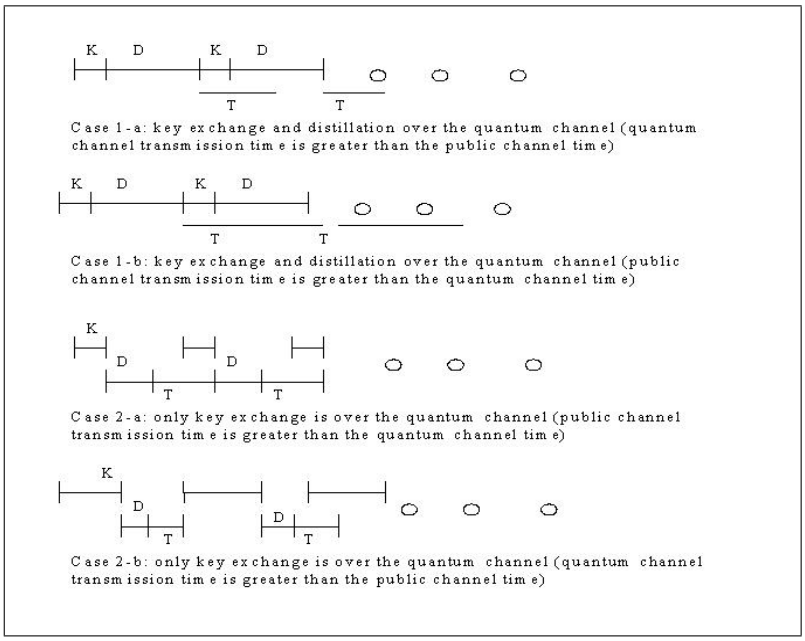

Figure 3. *the two cases of using totally quantum cryptography in IPsec*

a- K+D > T

If K+D>T then

$$\theta = \frac{T \times N}{(K+D) + T \times N + (N-1) \times ((K+D) - T)} \tag{1}$$

Where N is the number of packet.

$$\theta = \frac{T \times N}{(K+D) + T \times N - (N-1) \times T + (K+D) \times (N-1)} \tag{2}$$

Finally, after simplification:

$$\theta = \frac{T \times N}{T + (K+D) \times N} \tag{3}$$

If N is very large (infinite), θ is equal to:

$$\lim_{N\to\infty} \theta = \frac{T}{K+D} \tag{4}$$

Example 1 *Traditionally, the size of MTU (Maximum Transmission Unit) is 1500 bytes (i.e. 12 Kbits); we suppose that the unprotected header size is 250 bytes, so we have to secure 1250 bytes i.e. 10 Kbits. Therefore, the key length will be 10Kbits if we want to use One-Time-Pad function. The flow rate to exchange the key is 1 MBit/s and about 100 MBit/s to exchange normal data on optical fibber. We suppose that we have an Internet connection of 1 Mbit/s. As the error rate for exchanging quantum key is normally 50%, we need to exchange 20 Kbits in order to get 10Kbits of key length. We estimate the distillation data to be 40 Kbits. The time to XOR data with the key is neglected.*

Having the previous assumption:

K = 20/1000 = 0.02 s

D = 40/100000 = 0.0004 s

And T = 12/1000 = 0.012 s

In this case, K+D (20.4 ms) is greater than T (12 ms). The effectiveness θ when the number of packet N is infinite (4) is equal to 120/204 ~60 % of the total performance.

NB: if we have a faster Internet connection, say 10Mbit/s, the effectiveness θ given by (4) will be equal to 6 % of the total performance. In this case, the use of SeQKEIP is useless if we see only the performance. But, as the rate of quantum key exchange is progressing the effectiveness will increase.

b- K+D≤T

If K+D≤T then

$$\theta = \frac{T \times N}{(K+D) + T \times N} \tag{5}$$

if N is very large (infinite), θ is equal to:

$$\lim_{N\to\infty} \theta = \frac{T}{T} = 1 \tag{6}$$

So, in this case, there is no difference in the performance between using SeQKEIP and IP. The additional time cost induced by the use of quantum cryptography is negligible.

2-second solution

The quantum channel is used only to exchange the key. The distillation is done over the public channel. There are also two possibilities depending on the time needed to exchange the key and, on the other hand, the time to validate and send the message.

We take the same notation as previous:

K: the duration to exchange the quantum key

D: the duration of the key distillation

T: the duration of transmitting the message

So, we distinguish two scenarios: when K $>$ D+T and K $\leq$T+D.

a- K $>$ D+T

If K$>$T+D then

$$\theta = \frac{T \times N}{K + (T + D) \times N + (N - 1) \times (K - (D + T))} \tag{7}$$

And, after simplification:

$$\theta = \frac{T \times N}{(T + D) + K \times N} \tag{8}$$

if N is very large (infinite), θ is equal to:

$$\lim_{N \to \infty} \theta = \frac{T}{K} \tag{9}$$

Example 2 *We take the same parameters as in the "NB" the previous example (10 Mbit/s for the Internet connection, 1Mbit/s to exchange the quantum key). Having the previous assumption:*

K = 20/1000 = 0.02 s

D = 40/10000 = 0.004 s

And T = 12/10000 = 0.0012 s

In this case, K (20 ms) is greater than T +V (42 ms). The effectiveness θ if the number of packet N is infinite (9) is equal to 12/200 = 6 % of the total performance.

The flow rate configuration is the both solutions gives the same performance rate (6 %) of the whole performance. To upgrade this rate, the only solution is to have the K $\leq$T+D in this case and K+D $\leq$T in the previous solution.

b- If K$\leq$T+D

If K$\leq$T+D then

$$\theta = \frac{T \times N}{K + (T + D) \times N} \tag{10}$$

if N is very large (infinite), θ is equal to:

$$\lim_{N \to \infty} \theta = \frac{T}{T + D} \tag{11}$$

If we take the following configuration: the rate of quantum key exchange is 1Mbit/s and the Internet connection is 1Mbit/s, then T= 0.012 s and D = 0.04s. T+V is greater than K (0.02 s). So, the effectiveness θ if the number of packet N is infinite (11) is equal to 12/52 = 23 % of the total performance.

5. 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.

As we have seen, using quantum cryptography in conjonction with Ipsec to offer a better level of security in a Metropolitan Area Network is possible. If, we apply the quantum key exchange and one-time-pad function, we reach the unconditional security in communication. The distillation of the quantum key could be done in two different ways: over the optical channel or over the public channel. The performance obtained when distilling the key over the optical channel is higher than when using public channel (up to 100% when using optical channel versus 23% when using public channel). Actually, we can reach 100Kbit/s when exchanging the quantum key and hope to reach 1Mbit/s next few years. The possible flow rate over an optical fibber is 100Mb/s. If, we use an Internet connection of 1Mbit/s, we get 60% of the total performance (solution1, a) i.e. a flow rate of 600Kbit/s if the distillation of the key is done over the optical channel and we get only 23% of the total performance if we validate the key over the public channel (solution 2, b) i.e. a flow rate of 230Kbit/s. If we could reach the rate of 10Mbit/s in quantum key exchange and we use the first solution, we will get a performance of 100% in the flow rate i.e. 1Mbit/s.

6. References

[Alleaume2004] Alléaume R (2004). “Réalisation expérimentale de sources de photons uniques, caractérisation et application à la cryptographie quantique” (Secoqc partner)

[Bennet1983] Bennet, C; Brassard, G (1983). IEEE International Conference on Computers, Systems, and Signal Processing. IEEE Press, LOS ALAMITOS

[Bennet1992] Bennet, (1992). *C Quantum Cryptography: Uncertainty in the Service of Privacy.* Science 257.

[Bethune2002] 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

[Clark2000] 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.

[Ekert1991] Artur Ekert (1991). “*Quantum Cryptography based on Bell’s Theorem*”. Physical Review Letters. URL: http://prola.aps.org/abstract/PRL/v67/i6/p661_1

[Elliott2002] Elliott, C (2002). "*Building the quantum network*". New Journal of Physics 4 (46.1-46.12)

[Elliott2003] Elliott, C; Pearson, D; Troxel, G (2003). "*Quantum Cryptography in Practice*".

[Freebsd2004] Freebsd people. "IPSEC outline". URL: http://people.freebsd.org/~julian/IPSEC_4_Dummies.html

[Freesoft2004] freesoft (2004). "IPSEC Overview". URL: http://www.freesoft.org/CIE/Topics/141.htm

[Gisin2002] 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

[Grosshans2003] 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

[Hughes2002] 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/

[Labouret2000] Labouret, G (2000). "IPSEC: présentation technique". Hervé Schauer Consultants (HSC). URL : www.hsc.fr

[Lo1999] 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

[Mason2002] Mason A, (2002). "IPSec Overview Part Five: Security Associations". Cisco Press. URL: http://www.ciscopress.com/articles/printerfriendly.asp?p=25443

[Mayers1998] Mayers, D (1998). “*Unconditionnal Security in Quantum Cryptography*”. J. Assoc. Comput. Math. 48, 351

[Paterson2004] Paterson, K.G; Piper, f; Schack, R (2004). "*Why Quantum Cryptography?*". http://eprint.iacr.org/2004/156.pdf

[Riguidel2004] 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)

[Rivest1978] 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.

[Wootter1982] Wootters, W.K; Zurek, W.H (1982). "*A single quantum cannot be cloned*". Nature, 299, 802