Intl. Conf. in Computer Science – RIVF'05
February 21–24, 2005, Can Tho, Vietnam

Usages of Secure Networks built using Quantum Technology

Patrick Bellot [(1)], Toan-Linh-Tam Nguyen [(1,2)]
Minh-Dung Dang, Quoc-Cuong Le, Thanh-Mai Nguyen [(1,2)]
{bellot, dang, tnguyen, qle, mai}@infres.enst.fr

Abstract— **Quantum networks are based on Quantum Key Distribution (QKD). QKD allows to distribute an encryption key on a physical link with confidentiality certified by the quantum properties of the physical world provided that quantum mechanics is complete. Such a key can be used with a symmetric encryption scheme such as 3-DES or AES to establish a secure communication between two endpoints. The main drawback is that, nowadays, QKD can be done using optic fiber over 120 km but no more. With current and forseeable technology, QKD cannot be used to build and secure a general-purpose network copied from Internet. Our point is that using QKD requires the design of dedicated networks for specific usages.**

Résumé – **Les réseaux quantiques sont basés sur la distribution quantique de clé (QKD). La QKD permet de distribuer une clé de codage sur un lien physique avec une confidentialité démontrée par les propriétés quantiques du monde physique si l'on admet la complétude de la physique quantique. Une telle clé, utilisée avec un mécanisme classique de codage comme 3-DES ou AES, permet d'établir une communication sécurisée entre deux extrémités. L'inconvénient principal est que la QKD peut être réalisée sur une distance de 120km au plus. Avec les technologies actuelles, il est donc impossible de construire un réseau aussi général que l'Internet sécurisé par la QKD. Nous montrons donc que l'utilisation de la QKD requiert des réseaux dédiés à des usages spécifiques.**

Index Terms— **quantum network, nework security, quantum cryptography, quantum key distribution**

I. Introduction

The expression *Quantum Networks* is widely used to name the future networks that will be secured using *Quantum Key Distribution (QKD)*. QKD allows to share an encryption key, also called a session key, between two endpoints usually named Bob and Alice. QKD uses a quantum channel, usually an optic fiber but it may be a free-space laser beam. The confidentiality of the key is certified by the law of quantum physics. That is to say that any *eavesdropper*, usually named Eve, who tries to get information about the key will be detected andthe current tentative to establish a secure communication may be aborted without disclosing information. The main point is that the confidentiality of QKD is ensured by the physical properties of the quantum world instead of the assumed intractability of some mathematical problems.

Then, the session key can be used to establish a secure communication using classical resources such as Internet and symmetric encryption schemes. Symmetric encryption is claimed to be secure as far as the key distribution mechanism is secure. The most secure encryption scheme is *Vernam cypher*. It has been used for the communications between Kremlin and Washington. But it uses encryption keys as long as the encrypted messages. Thus, it is better to use more common encryption scheme such as *Advanced Encryption Standard* (AES) which cannot be broken if a reasonable key length is used (118 bits for AES) and if keys are oftenly renewed.

QKD allows to build a secure communication link between two endpoints. However, the best current and usable technology [13] limits the length of the quantum channel to at most 120 km if an optic fiber is used. See table I from www.idquantique.com.

TABLE I
Current key transmission rates of QKD.

Distance	*Available rate*
10 km	4,0 Kb/s
20 km	1,5 Kb/s
50 km	0,1 Kb/s

One may expect length and rate improvements [13] in the following decade because developments are sustained by institutional projects such as SECOQC or future US projects already in preparation. But no one expects, now, several hundreds of kilometers.

Another point is that quantum physics *Heisenberg principle of uncertainty* forbids cloning quantum objects and, thus, *quantum repeaters* which would extend the quantum channel seem impossible to design. That means that Quantum Networks architectures cannot be copied from Internet architecture and we have to design *specific architectures* dedicated to *specific usages*.

Section II briefly describes the most classical scheme for QKD and how a secure communication can be established and mentions the problem of authentication in Quantum Communication. Section III describes a published proposal for a Quantum Network [10]. Section IV describes some of our proposals

[1] GET-ENST, 46 rue Barrault, 75634 Paris Cedex 13, France.
[2] AUF-IFI, 42 pho Ta Quang Buu, Hanoi, Vietnam.

for using QKD. Then in section V, some alternatives are mentionned. Finally, section VI describes specific networks usages.

II. Quantum Key Distribution

Very efficient encryption algorithms exist and some are proved to be unbreakable by Shannon's theory of information. For instance, Vernam cypher, also called the *one-time pad*, assumes that the two endpoints share a key as long as the message to be encrypted. Vernam encryption is just doing an XOR between the key and the clear message and decryption is just doing an XOR between the key and the encrypted message. Reading the encrypted message does not give any information about the clear message. However the required length of the key, and the fact that the key must be changed after each use, rule out Vernam cypher for an everyday usage.

A. State of the art: PKI

Modern Data Encryption Algorithms (DEA) such as DES, 3-DES, AES, elliptic curves cryptosystems allow secure encryption using a fixed-length key. They are reasonnably considered as unbreakable. However, all these algorithms assume that a key is shared between the two endpoints. Thus, security is a problem of key distribution.

Nowadays, key distribution can be done using *Public Key Infrastructure* (PKI). A PKI is a security system for the management of keys using asymmetric encryption algorithms. But asymmetric encryption is subject to serious attacks with brute force, with progress in mathematics or with the possible creation of quantum computers. An encrypted message now currently unbreakable may be broken in ten years, or tomorrow, delivering a posteriori secrets.

Moreover, in the general case, PKI assumes many trustable third parties. All this is good enough for most of applications where there is no big business or industrial stake, no far future concerns, and when national security is not involved. For instance, one may admit the PKI system when it distributes certificates and keys for software download or for restricted electronic payment. But recent affairs, cf. *http://news.bbc.co.uk/1/hi/world/europe/820758.stm*, involving the Echelon electronic communications surveillance systems have proved that governments do not hesitate using military power to serve their own private companies. In recent UNO dispute on Irak, one has learned that the same technics have been used by governments against UNO and opposite diplomacy. Perfect classical digital confidentiality needs huge organisation and means. Quantum Cryptography may provide a solution.

The questions are: do we trust encryption algorithms which are potentially breakable ? Which PKI can we trust ? Even trustable, your PKI may not be secure enough since a single break in such a complex system opens a large breach in the security.

Quantum Key Distribution allows two endpoints to share a key with total confidentiality and to use symmetric encryption algorithms. S. Wiesner described the idea in the 70s. He officially published in 1983 [19]. It has been fully developped and finalised by Gilles Brassard and Charles H. Bennett in 1984 and it is known as the *BB84 protocol* [2].

B. BB84 Basics

The quantum law underlying QKD is *Heisenberg principle of uncertainty*: two non-commuting observables of a quantum system cannot be both accurately measured. It ensures that it is not possible to clone a quantum system (*no-cloning theorem*). Otherwise, it would be possible to measure one observable on the original and the other observable on the clone.

The BB84 protocol is simple enough to be understood by a non-specialist of quantum physics. Photons can have a rectangular or a circular polarisation, two non-commutable observables. A physical device can observe *rectangular* or *circular polarisation* but not both. Rectangular polarisation can be *horizontal* noted "↔" or *vertical* noted "↕". Circular polarisation can be *left* noted "↻" or *right* noted "↺". Moreover, if a physical device tries to measure circular polarisation on a photon that is rectangularly polarised, then it gets a random results: either left or right, each with a probability of 50%. And the act of measurement changes the state of the photon. The situation is symmetric if a physical device measures rectangular polarisation of a photon that is circularly polarised.

Session keys are made of bits, 0 or 1. We agree that: bit 0 can be encoded either by an horizontal (↔) or a left (↻) polarisation of a photon and bit 1 can be encoded either by a vertical (↕) or a right (↺) polarisation of a photon. Such an encoded bit is called a *quantum bit* or *qubit*. Transmitting a key becomes transmitting a sequence of polarised photons.

C. BB84 Key exchange scheme

Alice and Bob are connected using two channels. The first is the *quantum channel*, typically an optic fiber. The second is the *classical channel*, typically an Internet link.

(i) First, Alice generates a *random* sequence of bits called the *raw key*. Randomness is crucial. For each bit, Alice chooses to encode its value using either the rectangular basis or the circular basis for the polarisation of a photon. The choice of the basis must be *random* too. And she sends the photons, one after the other, to Bob using the quantum channel.

(ii) For each received photon, Bob chooses *randomly* to measure it using either the rectangular basis or the circular basis. Because Alice and Bob choices of bases are random, the probability that they use the same basis for a given photon is 50%. If they use the same basis for a given photon, then Bob gets the right encoded bit with a high probability. If they do not use the same basis, then Bob gets a random result as explained in 2.b.

(iii) Then Bob uses the classical channel to tell Alice which bases he used for the measurements. And Alice, also using the classical channel, answers which bases are correct according to her own encoding choice, i.e. when they used the same basis. Note that these communications are public. There is no need to encrypt the classical channel at this stage.

(iv) When they used the same basis, the bit encoded by Alice is identical to bit decoded by Bob. They get a shared sequence of bits which is called a *sifted key* and which will be used to build a *session key*. The length of the sifted key is about half the length of the raw key.

Example: In the figure 1 below, rectangular and circular bases are represented respectively by symbol "$\oplus$" and "$\otimes$". The first line contains Alice's randomly chosen sequence of bits. Second line contains the encoding bases randomly chosen by Alice for each bit and the third line contains the qubits, i.e. the photons with the appropriate polarisation. Fourth line contains Bob's randomly chosen measurement bases and fifth line contains the results of the measurements. We have put a symbol "?" to mention that Bob's measurement has a random result which will be discarded anyway. The last line contains the bits for which Alice and Bob have chosen the same basis, this is the sifted key which value is **"00100100111"** in our example.

D. Eavesdroppers and security

The eavesdropper, usually named Eve, has access to both the quantum and the classical channels. If Eve accesses a photon, she has no way to know the basis used by Alice to encode the bit. Thus, she has to guess a basis for measuring the photon. And then she resends the photon to Bob. This is the *intercept-resend* strategy [12]. If she chooses the same basis as Alice for measurement, then she gets theright value and the resent photon is in an appropriate quantum state. If she chooses the wrong basis, then she destroys the quantum state of the photon and, in the cases where Bob chooses the right basis, he gets an incorrect result in 50% of the cases. On the average, Eve chooses the wrong basis in 50% of the cases. Thus, Eve's action introduces a supplementary error rate, about 25%. In this case, Alice and Bob can detect the intrusion and know that the sifted key cannot be trusted.

Another strategy for Eve is the *man-in-the-middle* attack [1]. In this attack, Eve gets control over the two channel and lets Alice think she is communicating with Bob and conversely. Eve plays the role of Bob w.r.t. Alice and plays the role of Alice w.r.t. Bob. In this case, Quantum Cryptography provides no riposte and one must rely on classical *authentication* algorithms stemmed from classical cryptography.

[3], [4], [12], for instance, give a rather complete description of the "non-impossible" quantum attack strategies, for instance beam splitting scheme or entanglement scheme or quantum copying sheme or collective attacks, in various configuration and for various QKD technologies, and why they are unlikely to succeed. Formal proofs of security rely on protocols such as the following BB84. They uses Shannon's Information Theory [17] and, most important, the laws of Quantum Physics.

E. Other QKD

Because this article is not devoted to QKD but to the usage of QKD, we do not describe many other quantum technologies and protocols. For instance: B92 two-state protocol [5] using two non orthogonal states instead of four, six-state protocol which reduces the error rate [1], EPR protocol [9], continuous variables, autocompensating weak laser pulse, etc.

F. BB84 Protocol

The BB84 protocol is used over the physical devices handling the key distribution. Rationales for this protocol are multiple. First, the quantum devices, for producing quantum states, for transporting and measuring them, are not totally perfect. For instance, one must consider the *dark count* which is the probability of detection of an unsent photon, a low probability about 10^5 which cannot be neglected according to communication standards. One must consider the probability of measure errors due to apparatus defects which is far more important. Thus, if the sifted key length becomes a few percents of the initial bits string length, it can be considered as a performance[11]. The protocol is there to take into account the error rates due to technical imperfections and to the eavesdropper's action. The error rate in the sifted key is called the QBER for Quantum Bit Error Rate. The aim of the protocol is to reduce the QBER to standard communication Bit Error Rate (BER), about 10^9, and to reduce as much as wanted EveÕs knowledge about the key. The steps of the protocol are the following:

(1) *Sifting*. Alice sends a random string of bits, the raw key, as described above, cf. II-C. Alice and Bob must be synchronized to detect photons that Alice did not send but Bob received and, conversely, photons that Alice sent but Bob did not receive. The result is the sifted key. The length of the sifted key is about a few percents of the length of the raw key. At this step, Alice and Bob may detect Eve's intrusion because a significant intrusion must raise the usual error rate.

(2) *Reconciliation*. The sifted key is made of qubits on which Alice and Bob agree because they have used the same encoding basis. However, some bits may differ because the quantum apparatus is not reliable or because there has been a light intrusion of Eve which has not been recognised as so. The error elimination algorithm uses the public classical channel. Several algorithms have been proposed. For instance, [4] proposes that Alice and Bob use the same random permutation of bits to randomize the locations of errors. Then, the key is divided into small enough equal-size blocks such that one block is unlikely to contain more than one error. Alice and Bob compare the parities of their respective blocks and discard blocks for which parities differ. After reconciliation, the sifted key may have been shortened but it is almost certainly shared between them.

(3) *Privacy amplification*. It may be that Eve knows some bits of the key resulting from the previous operations. Privacy amplification is a technique to reduce Eve's information. The price is once again shortening of the key. Again, several algorithms are possible. For instance, in [12], Alice randomly chooses two bits and tells Bob the position of

Fig. 1. A QKD Session

Random bits of the raw key	0	0	1	0	1	1	1	0	0	1	0	0	1	1	1	1	0	1
Alice's random bases choice	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\oplus$
Sent qubit	$\leftrightarrow$	$\leftrightarrow$	$\circlearrowright$	$\leftrightarrow$	$\circlearrowright$	$\updownarrow$	$\circlearrowright$	$\circlearrowleft$	$\circlearrowleft$	$\updownarrow$	$\circlearrowleft$	$\circlearrowleft$	$\updownarrow$	$\circlearrowright$	$\updownarrow$	$\updownarrow$	$\leftrightarrow$	$\updownarrow$
Bob's random bases choice	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
Bob's result	$\leftrightarrow$	?	?	$\leftrightarrow$	?	?	$\circlearrowright$	$\circlearrowleft$	$\circlearrowleft$	$\updownarrow$	$\circlearrowleft$	$\circlearrowleft$	$\updownarrow$	?	$\updownarrow$	?	?	$\updownarrow$
Sifted key	0			0			1	0	0	1	0	0	1		1			1

these bits. Alice and Bob replaces the two bits by the result of their XOR. If Eve has only partial information on these two bits, i.e. if she knows zero or one bit, then she has no information on the XOR result. Therefore, Eve's information is less than before. This operation may be repeated by Alice and Bob to reduce Eve's knowledge.

(4) *Authentication*. The two parties identify themselves. This relies on classical algorithms not especially related to Quantum Cryptography. These algorithms assume that a piece of data, an *authentication key*, is shared by Alice and Bob before all. In fact, they may share a stack of authentication keys. They are subject to keys exhaustion, and then *denial of service* (DoS), if an eavesdropper simulates a lot of connections. [8] proposes a new algorithm which protects itself against keys exhaustion. At the difference of usual approach, his algorithm is dedicated to Quantum Cryptography.

Then Alice and Bob share a key with a very high probability and Eve's information about the key is as samm as wished.

III. BBN NETWORK ARCHITECTURE

Let us name BBN network architecture the attempt to build a quantum network with sponsorship of the US DARPA as described in [10] and [11]. Basically, the BBN network is an Internet *Virtual Private Network* (VPN) in which the key distribution and renewing is done using QKD devices instead of more classical technologies such as Diffie-Hellman key exchange [7]. As the authors wrote, the distance limitation of QKD only allows circumscribed networks.

A. A Single QKD Link

The most simple network consists of a QKD link between two enclaves, see Figure 2, which marries QKD with classical Internet security protocol IPSec [7]. QKD is used for key sharing between two enclaves gateways. The enclave is a *Local Area Network* (LAN) which is assumed to be secured. An IPSec secured Internet link connects the two gateways. IPSec is a well-established Internet technology which allows traffic between two endpoints to be confidential provided the endpoints share an encryption key. The two gateways ensure the routing of IP communication. The only non-classical feature is that the keys necessary to IPSec are distributed using quantum technology. The authors have extended NetBSD, a BSD operating system, with a modified version of *Internet Key Exchange protocol* (IKE) to accept quantum keys for encryption of the traffic using *Advanced Encryption System* (AES) but it could be any other encryption system. The two QKD devices produce continuous streams of bits which can be used for regular *key renewing*.

B. A Long Distance QKD Link

Simple QKD links as above are limited to several tens of kilometers length. In order to extend the length, one may use QKD data relay. One must note that a QKD data relay is not a quantum repeater. A QKD data relay is a network apparatus able to establish a single QKD link with the previous element of the chain and another QKD link with the following element of the chain.

It is a data relay with the following characteristics:

- Relay k establishes an encrypted communication (a QKD link) with relay $k-1$.
- Relay k receices encrypted data from relay $k-1$.
- *Data are decrypted and stored in the memory* of relay k.
- Relay k establishes an encrypted communication (a QKD link) with relay $k+1$.
- Data in memory are encoded and sent to relay $k+1$.

We can see that QKD data relays present a serious weakness: data appear unencrypted inside the relay memory. QKD data relays establish pairwise secure communications using QKD in order to securely transport a randomly generated encryption key, hop-by-hop from one endpoint to the other as in Figure 3. The QKD relays network at the bottom of the figure is used to exchange an encryption key that used to encrypt the communication on the top Internet link.

The communication between QKD relays is done as the communication between LAN enclaves of section III-A above. The encryption key which is exchanged using the QKD Relays Network appears unencrypted inside the relays. Thus, the relays must be seriously protected against eavesdropper. In Europe, due to the concentration of cities, such a scheme could be used by many institutions. This may not be applicable to larger countries such as USA, Canada or Russia where extended non-urban areas exist. This scheme could also be used by European armies which have many bases covering the whole territory.

C. A Quantum Network

In section III-B, it was chosen to use QKD Relays Network to transmit keys between two endpoints of an ordinary Internet

Fig. 2. A simple QKD link between two enclaves.

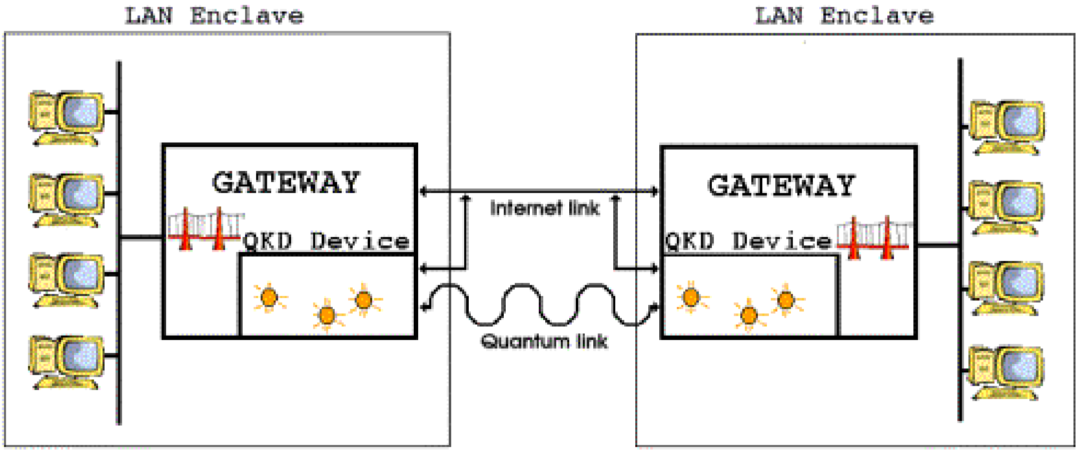
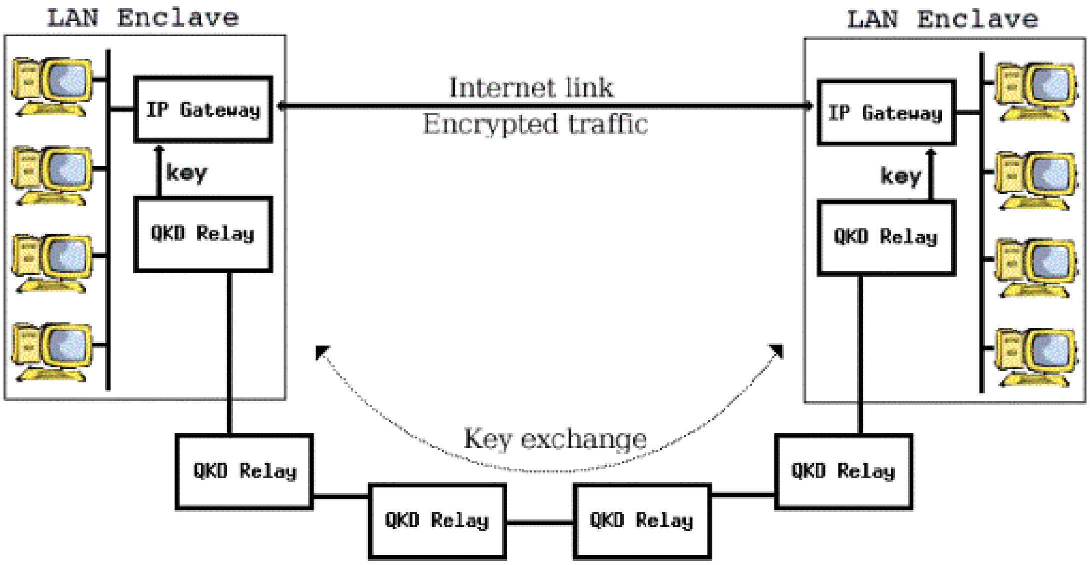


Fig. 3. QKD relays used to transport keys.



network. But the QKD relays may be used to transmit the plain traffic. Then, we obtain a true Quantum Network. In this network, we have a set of enclaves. Some of these enclaves are pairwise connected by a Single QKD Link as in section III-A. It is not obvious that such a network would be more interesting. Security level is the same. And it would be a little more complex to build and to administrate without the gain of a wider usage.

D. Conclusions

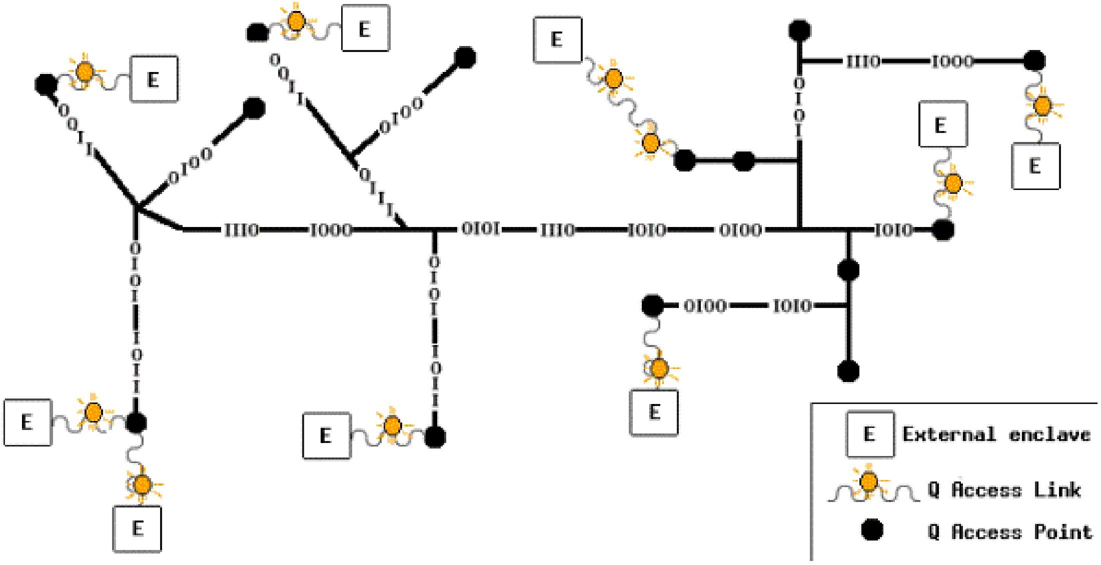
The building of a network totally secured by QKD would require one-to-one QKD link between each pairwise endpoints of the network. This is clearly not realistic. Therefore, some nodes of the network must be relays as described above. QKD networks built this way have drawbacks. The main one is that all points, QKD relays or LAN enclaves, must be totally secured. One failure at one of these points and the security of the whole network is seriously threatened. In the same vein, network security operators must be trusted. Only a Single QKD Link between two parties is totally secure. Other schemes have weakness.

IV. The QBONE

Because the total security of QKD networks surely relies on the operators, we propose to imagine a trustable operator owning a classical Virtual Private Network (VPN) over Internet with an *Access Network* secured with QKD. In this scheme, the VPN is under the responsibility of a security operator.

For instance, it may be owned by one company which main sites are distributed over a country. The VPN is assumed to be highly secured using classical means in terms of encryption and physical protection against eavesdropper. LetÕs name it the QBONE.

Fig. 4. The QBONE.



The QBONE connects *Quantum Access Points* (QAP) together, see Figure 4. The QAP is just a endpoint of a Single QKD Link as described in III-A. It is assumed that QAP are physically secured as the QBONE is. The Single QKD Link is named a *Quantum Access Link* (QAL). The other extremity is an enclave which may consist of only one computer.

With this scheme, we assume a secure classical Internet network, the QBONE, and QKD simply allows to secure the access to the QBONE from an outside and unprotected point. The interest of this approach is that the operator only needs to implement a single access point in a given area. Such a network may be incrementally developped. The QAP acts as a gateway to the QBONE. It could be a simple *Network Address Translator* (NAT).

If the QBONE is trusted, then the whole network can be trusted, even the enclaves that are outside the QBONE. Such a network could be used by a bank, a big company or by a government. Each main city should provide QAP. All agencies distributed around the city could be connected using QALs.

Q Access Point have two network interfaces: one facing the QBONE and one facing the Q Access Link, see Figure 5. The most simple view is considering that the Q Access Link allows to build a local network secured by QKD and that Q Access Point is a gateway to the QBONE.

This approach is good if we assume that the QBONE is totally secured by its operator by classical means and physical means. Then it allows to extend the QBONE outside the secured area of the QBONE. Again, a bank could be able to protect a QBONE in its agencies spread over the country and to propose outside QKD secured access point to its network.

V. World-wide Satellite QKD

A growing number of research papers mention the possibility of distributing keys using quantum technology with satellites [14][16]. The feasability evaluations are just standing.

The satellite must be a low earth orbit (LEO) satellite, between 800 km and 1600 km. With current state of the art, the satellite must carry a small, 10 to 30 cm diameter, telescope meanwhile terrestrial material a bigger, 50 to 100 cm diameter, telescope. One may expect smaller apparatus sizes in the future. See [16] for a complete description about required and proposed characteristics.

Three possibilities exists:

- The ground station transmits a key to the satellite.
- The satellite transmits a key to the ground station.
- The ground station transmits a key to another ground station using the satellite as a mirror.

Such a system would be hardly eavesdropped since it would require the eavesdropper to be in position to intercept the laser beam either in space or on earth.

A. Quantum Satellites Network

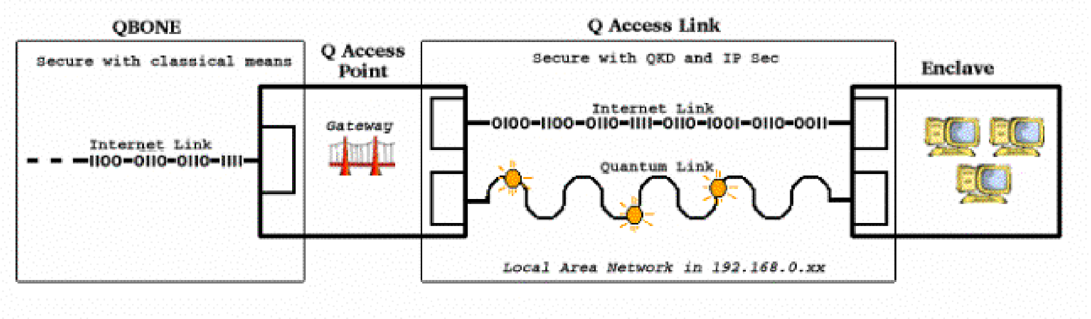
One may expect such a technology to be operationnal in a near future. Thus, one may imagine a Quantum Satellites Network covering the earth in a way similar to US GPS satellites network or future European Galileo satellites network.

Because there is few turbulence in outer space, satellites may secure pairwise radio communications using QKD if they are visible one to each other. And hop by hop, one may assume that satellite to satellite communications is secure.Thus, one may assume that radio communications hop by hop between any two given satellites is totally secured.

This Quantum Satellites Network may allow two ground stations GS1 and GS2 to share en encryption key in the following way:

(i) GS1 receives a particular encryption key from the satellite SAT1 currently covering its area. Using this key, GS1 and SAT1 establishes a secure radio communication link.

Fig. 5. The Q Access Point.



(ii) GS2 receives a particular encryption key from the satellite SAT2 currently covering its area. Using this key, GS2 and SAT2 establishes a secure radio communication link.

(iii) GS1 and GS2 authenticate themselves with classical means. Note that ground station authentication may be done by physical locations.

(iv) GS1 and GS2 exchange an encryption key using the satellites network.

(v) GS1 and GS2 create a secure communication on a classical link using the shared key and symmetric encryption.

With the current assumed performances, the sharing of a key for symmetric encryption between GS1 and GS2 may be established in a few seconds.

Point (v) suggests using a classical link instead of using satellites for the main traffic because satellites do not provide enough bandwidth and long delay (0.5 sec) for signal propagation. But a classical link secured with symmetric encryption can be considered as totally confidential.

B. *Free Space QKD*

Free Space QKD is the possibility of sharing a key using laser beam in free space. Satellite QKD uses free space technology [14][15].

Free Space QKD has been realised up to 23.4 km in the atmosphere. The main problems are air turbulence, positionning and orienting the apparatus. As there is no physical link between the two endpoints, endpoints are free to move provided they remain visible one to each other.

VI. Usages of Quantum Networks

Quantum Networks projects exist. Among them, the European project SECOQC, covering every aspects, from the physical layer to the network morphology, protocols and security certification, will provide the means to design a quantum network. ENST is in charge of the NET subproject which is responsible of the network architecture. The BBN Technologies project, see section III, funded by US DARPA, has similar objectives. The QUANTUM CRYPT project funded by Eurocontrol studies the possibility to secure the future *Aeronautical Telecommunications Network* (ATN), an IPv6 network covering *Ground Earth Stations* (GES) and flying aircraft, using QKD instead of PKI. And people already mention a huge US project similar to SECOQC.

As we have seen, it is not obvious that QKD can be applied to general purpose networks. In our view and for a long time, Quantum Networks will be dedicated networks with specific usages where security is crucial. Thus, we have to think about the usages corresponding to the near future characteristics of the Quantum Networks.

A. *Enterprise private network*

Enterprise means a large entity able to host a network and which may require total secrecy. Such enterprises can be:

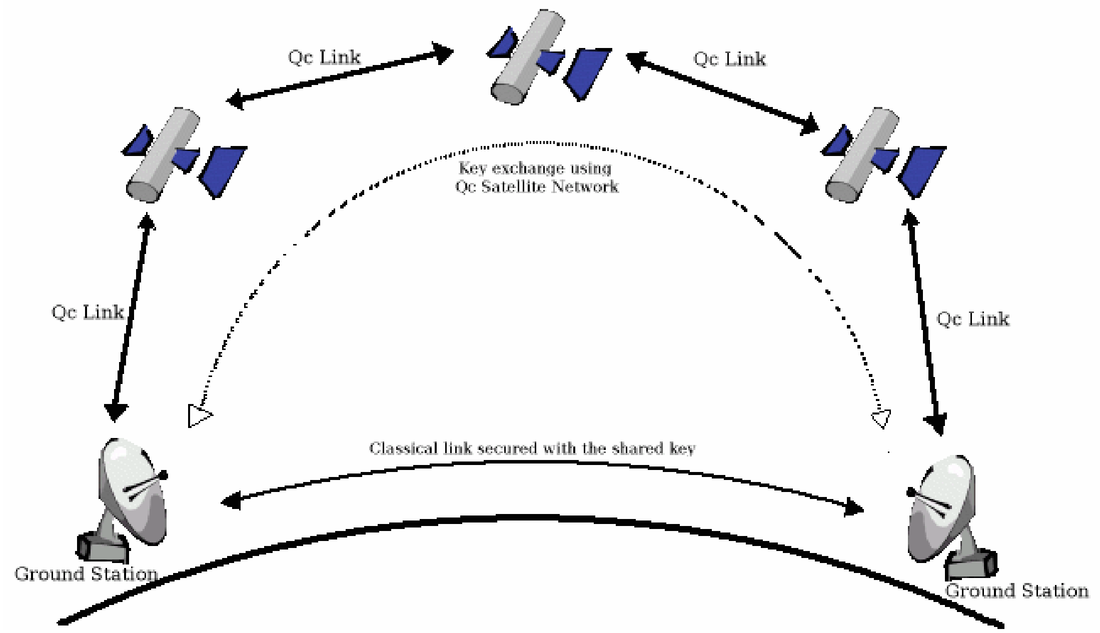
- Governemental institutions such as Foreign Affairs which require secrecy in the context of diplomacy disputes, police and secret services in the context of international terrorism.
- Big companies, such as worldwide companies, which require total confidentiality about their products, future announcements, investments and so on.
- Banking institutions, Stock Exchange institutions which require total secrecy on their heavy transactions.
- Defense agencies which require secrecy meanwhile most of their elements are mobile: boats, planes, submarines, ground units, etc.
- International institutions such as UNO, IMF, OCDE, OIF, etc. may require confidentiality of their internal communications.

These entities are able to hold a QBONE. For instance, a bank may hold the QBONE and its Quantum Access points in its main highly secured agency widely spread around the country while providing Quantum Access Link to its secondary agencies.

Some of these worldwide entities such as multinationales or Foreign Affairs departments, may use satellites based QKD for covering the world. Some multinationale companies already use private satellites networks for their private communications. In such a use, authentication may be done by location. For instance, Embassies have precise locations and satellites may be programmed to allow quantum links with these locations.

Defense agencies may take advantage of Free Space QKD and Satellite Networks to distribute keys to its mobile elements.

Fig. 6.   Quantum Satellite Network.



For instance, nuclear bombers waits at the extremities of their take-off strip. Nuclear lauching secret codes are planned to be sent using physical means, for instance a courrier officer, since radio communications can be eavesdropped. Free Space QKD could do the job, and enhance reactivity, since its range exceeds the size of a military airport.

B. *Distributing ephemeral secrets*

It is well known in security industry that most secrets must be ephemeral. For instance, the ATN *Standards and Recommanded Practices* (SARP) states that encryption key, cf. VI-C, must be renewed every 28 days.

A usage of QBONE that can be applied in several domains is the distribution of ephemeral or one-time secrets. Again, the QBONE is considered as secured either by conventional technologies or even Quantum technologies. The QBONE is able to distribute secrets outside its area using Q Access Link which may securely join external endpoints similar to *Automated Teller Machines* (ATM). Here are a few examples of secrets that could be distributed :

- Credit cards hold secrets which allow cards identification in conjunction with the PIN codes of cards owners. Secrets are held in the card memory. Newspapers relate many stories where credit cards have been copied by unscrupulous crooks. Once a user if afraid of being hacked, he could go to the ATM to renew its secret without invalidating and renewing his card.
- Mobile phone communications are not secured. We could imagine secured endpoints where a mobile phone could get a secret to encrypt its communication either with the operator or with another mobile phone. This secret could be renewed according to security level needs. Similarly for mobile laptop computers.

The main drawback of these distributions of secrets is that secrecy relies on the trustability of the QBONE security operator whatever technology is used for securing the QBONE.

C. *Aeronautical Telecommunications Network*

The Aeronautical Telecommunications Network (ATN) is the next generation communication network for aircraft and ground stations supporting *Air Traffic Management*. It is encouraged by *International Civil Aviation Organisation* (ICAO), see www.icao.org. In the current state of elaboration, it will be an IPv6 Internet classically secured and using PKI for encryption keys distribution. As ATN PKI will be managed by ATN authorities, there will be only a few concerns about security.

Nevertheless, one can imagine key distribution to aircraft to be done on the ground when standing at the airport. This will be secure only if the airport country is a member of the ATN organisation and if it is trustable. If Europe wants to secure its own sky, it will not be reasonable to trust a key distribution done outside Europe. Free Space Quantum technology offers new possibilities which do not rely on the trustability of external operators.

Key distribution to aircraft could be done *en route* using a Quantum Satellites Network at any location around the world. It could also be done using Free Space technology from the ground at the frontiers of Europe or at some mandatory rendezvous locations for aircraft entering the European sky. Because long distance aircraft usually flights at altitude of 11 km (33000 feets), free space technology have to be enhanced in order to be applied this way.

VII. Conclusions

The main challenge of Quantum Cryptology is the elaboration of efficient quantum apparatus. It is also a goal of the European SECOQC project. With the current technology, Quantum Cryptography is restricted to specific usages. There is no doubt that the entire world would buy a more usable technology. This is a work for quantum physicists.

Network morphology and protocols for Quantum Cryptography depend on the technology. But even if we imagine a few hundreds kilometers quantum link, we cannot plan every two endpoints to be connected by a quantum link. Thus, quantum relays will be mandatory to build a network.

The great victory would be *quantum repeater-router* able to take a quantum state as input and to regenerate it because signals debilitate, to re-route it to another point according to routing tables as Internet does, without observing it nor disclosing informations. It could destroy the input while recreating it for retransmission without violating Heisenberg's principle of uncertainty. This would allow to have a totally secured and trustable network for two endpoint parties. Without such an apparatus, Quantum Networks will likely sound like the BBN Network, cf. Section III, or the QBONE, cf. Section IV.

We think that the most up-to-date usage of Quantum Cryptography is to connect a secured area, a QBONE for instance, to outside unsecured endpoints. Of course, this is not unconditionnal security because security relies on the network security operator but it could be applied to several situations, cf. section VI-A, where the security operator and the secrecy demander are the same entity.

VIII. Future works

As we are in the SECOQC European project, we will work on network morphology, protocols and certification. Our first view very similar to the BBN Network may evolve, especially if we consider specific usages: government, defense, bank, mobile communications, etc. We are going to implement a Java emulator of a BB84 Quantum Link and a Java emulator for Quantum Key Distribution and usage. As we are in the QUANTUM CRYPT Eurocontrol project, we will work on the possible use of Quantum Cryptography to secure Air/Ground Telecommunications (AGT) in the future IPv6 Aeronautical Communications Network. If this study terminates successfully, then we may be able to conduct a development project in which we will search for Free Space quantum physicist as project associates.

We think that Authentication is another important area of study in Quantum Cryptography. Most of classical cryptography specialists criticize Quantum Cryptography because it lacks of authentication mechanism. We are currently exploring two ways. The first one is software based. It assumes that a common piece of data, the authentication key, is shared by the two parties because the communication link is set. Every authentication procedure must assume this kind of data. However, classical authentication is subject to key exhaustion: a hacker may try to communicate with one of the parties and run the authentication process; each time he or she tries, one of the shared key is consummed. After several tries, the bag of authentication keys may be exhausted resulting in a denial of service. We have designed an authentication algorithm which uses quantum properties so that no key exhaustion attack is possible. Therefore, one key only is necessary.

The second strategy is time-location authentication. It may be applied to Quantum Satellites Network, to mobile communication (mobile phones, mobile computers, defense network, etc.) and to Aeronautical Telecommunications Network (ATN). For example, a Quantum Satellites Network may deliver keys to some well-predefined locations. Authentication of these locations may be done by position and authentication of the satellite may be done the same way. In the case of ATN, aircraft may authenticate the satellite by its position in space and reciprocally. This may be completed by usual authentication of aircraft as done by classical means already in use by Air Traffic Controllers.

In a much more speculative domain, one point that may be studied in the case of terrestrial networks is the possibility to develop a quantum technology that allows the use of several simultaneous paths. The point is that using one-by-one photons to transmit a key is mimicing ordinary classical Shannon bit-by-bit communications. Even if Quantum Cryptography can claim to be totally secure, the risk, then, would be that conventionnal encryption technology would always be in advance in the same way that ordinary Intel-based PC have always been in advance compared to specialised computers, for instance language-oriented or algorithm-oriented computers. Would it be possible to send plain traffic, not key exchange traffic, photon pulses around an optic fibers network that would use several path simulteanously in such a way that the eavesdroppers would have to catch all the network to understand the messages ? Such a technology would use stochastic protocols such as protocols already in use in Network Intrusion Detection System (IDS).

References

[1] H. BECHMANN-PASQUINUCCI and N. GISIN, “Incoherent and Coherent Eavesdropping in the 6-state Protocol of Quantum Cryptography”, in *Physical Review A*, vol. 59, issue 6, pp. 4238-4248, june 1999. Web : http://prola.aps.org/abstract/PRA/v59/i6/p4238_1.

[2] C. H. BENNETT and G. BRASSARD, “Quantum Cryptography: Public Key Distribution and Coin Tossing”, in proceedings of the *IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175-179, Bangalore (India), 1984.

[3] C. H. BENNETT, G. BRASSARD and G. CREPEAU, “Practical Oblivious Transfer”, in proceedings of *Advances in Cryptology, CRYPTO'91*, J. FeigenBaum, Springer Verlag, LNCS no. 576, pp. 351-366, Santa Barbara (CA,USA), 1991.

[4] C. H. BENNETT, F. BESSETTE, G. BRASSARD, L. SALVAIL and J. SMOLIN, “Experimental Quantum Cryptography”, *EUROCRYPT'90*, Ahrus (Denmark), published in *Journal of Cryptology*, vol. 5, issue 1, pp. 3-28, 1992.

[5] C. H. BENNETT, “Quantum Cryptography using two Non orthogonal States”, in *Physical Review Letter*, vol. 68, issue 21, pp. 3121-3124, may 1992. Web: http://prola.aps.org/abstract/PRL/v68/i21/p3121_1.

[6] D. BRUB and N. LUTKENHAUS, “Quantum Key Distribution: from Principles to Practicalities”, in *Applicable Algebra in Engineering, Communication and Computing (AAECC)*, vol. 10, pp. 383-399, 2000. Web: http://babbage.sissa.it/abs/quant-ph/9901061

[7] D. COMER, *Internet Working with TCP/IP*, Prentice-Hall, 2000.

[8] MINH-DUNG DANG, “A New Authentication Protocol Dedicated to Quantum Cryptography”, personnal communication to appear in proceedings of *RIVF'05*, M. Bui ed., Hanoi(Vietnam), february 2005.

[9] A. K. EKERT, “Quantum Cryptography based on Bell's Theorem”, in *Physical Review Letter*, vol. 67, issue 6, pp. 661-663, august 1991. Web: http://prola.aps.org/abstract/PRL/v67/i6/p661_1.

[10] C. ELLIOT, “Bulding the Quantum Network”, in *New Journal of Physics*, vol 4, pp. 46.1-46.12, 2002. Web: http://www.njp.org.

[11] C. ELLIOT, D. PEARSON and G. TROXEL, “Quantum Cryptography in Practice”, in proceedings of the conference on *Application, Technologies, Architectures and Protocols for Computer Communications,* Karlsruhe (Germany), 2003. Web: http://doi.acm.org/10.1145/863955.863982.

[12] N. GISIN, G. RIBORDY, W. TITTEL and H. ZBINDEN, “Quantum Cryptography”, in *Review of Modern Physics*, vol. 74, pp. 145-195, march 2002. Web : http://www.gap-optique.unige.ch/Publications/Pdf/QC.pdf.

[13] C. GOBBY, Z. L. YUAN, and A. J. SHIELD, “Quantum key distribution over 122 km of standard telecom fiber”, *Applied Physics Letters*, vol 84, no. 19, pp. 3762-3764, may 2004.

[14] 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”, in *New Journal of Physics*, vol 4, pp. 43.1-43.14, 2002. Web: http://www.njp.org.

[15] C. KURTSIEFER, P. ZARDA, M. HALDER, P.M. GORMAN, P.R. TAPSTER, J.G. RARITY and H. WEINFURTER, “Long Distance Free Space Quantum Cryptography”, in proceedings of *Quantum Optics in Computing and Communications*, SPIE 4917, S. Liu, G. Guo, H.-K. Lo, N. Imoto eds., 2002. Web: http://scotty.quantum.physik.uni-muenchen.de/publ/42106762.pdf

[16] J.G. RARITY, P.R. TAPSTER, P.M. GORMAN and P. KNIGHT, “Ground to Satellite Secure Key exchange using Quantum Cryptography”, in *New Journal Physics*, vol. 4 , pp. 82.1-82.21, 2002. Web: http://www.njp.org.

[17] C. E. SHANNON, “Communication Theory of Secrecy Systems”, in *Bell Systems Technology Journal*, vol. 28, pp. 656-715, 1949.

[18] D. STUCKI, N. GISIN, O. GUINNARD, G. RIBORDY and H. ZBINDEN, “Quantum key distribution over 67 km with a plug&play system”, in *New Journal Physics*, vol. 4 , pp. 41.1-41.8, 2002. Web: http://www.njp.org.

[19] S. WIESNER, “Conjugate Coding”, in *SIGACT News*, vol. 15, no. 1, pp. 78-88, 1983.