
Development of a Global Network for Secure
Communication based on Quantum Cryptography
www.secoqc.net

# SECOQC White Paper on Quantum Key Distribution and Cryptography

**Reference: Secoqc-WP-v5**
**Document type:** White Paper
**Document Date:** January 22 2007
**Version: 5.1**

**Document history:** During the first year of the SECOQC project [1], Philippe Grangier initiated an internal debate regarding the "comparative advantages" of quantum key distribution (QKD). A first written contribution to this debate, by Philippe Grangier, Louis Salvail, Nicolas Gisin and Thierry Debuisschert [2], was then made available to all SECOQC partners. In their 3rd review report, issued on June 26 2006, SECOQC project reviewers and scientific officer pointed out at the need of a paper about the "added value of QKD to classical cryptography". Following this recommandation and extending on the arguments developped in [2], Romain Alléaume wrote a draft document, entitled *QKD and Cryptography: strong points, weaknesses and comparative advantages*. On October 12, at the London 10th SECOQC Core Group, project partners agreed to jointly contribute to the improvement of this draft document and make it evolve into the SECOQC cryptography white paper. Numerous comments, suggestions of corrections and new ideas were proposed through the SECOQC Wiki [3]. Based on those reactions, the first draft version of the paper has been modified and updated by Romain Alléaume, leading successively to the versions 2.0, 3.0, and 4.0. On November 21, version 4.0 of the white paper was presented at the Crypto networking session organized by the European Network of Excellence ECRYPT, at the Helsinki IST event. Preprints of the white paper have also been distributed. Final rounds of revisions, taking into account the comments received after the Helsinki event, have then lead to the current version, 5.1, of the white paper.

**Editing Author**: Romain Alléaume romain.alleaume@enst.fr

**Contributors :**

Romain Alléaume[1], Jan Bouda[2], Cyril Branciard[3], Thierry Debuisschert[4], Mehrdad Dianati[1], Nicolas Gisin[3], Mark Godfrey[5], Philippe Grangier[6], Thomas Länger[7], Anthony Leverrier[1], Norbert Lütkenhaus[8], Philippe Painchault[9], Momtchil Peev[6], Andreas Poppe[10], Thomas Pornin[11], John Rarity[5], Renato Renner[12], Grégoire Ribordy[13], Michel Riguidel[1], Louis Salvail[14], Andrew Shields[15], Harald Weinfurter[16], Anton Zeilinger[10].

**Affiliations :**

[1] Ecole Nationale Supérieure des Télécommunications, Paris, France.
[2] Masaryk University, Brno, Czech Republic .
[3] University of Geneva, Switzerland.
[4] Thales Research and Technology, Orsay, France.
[5] University of Bristol, United Kingdom.
[6] CNRS, Institut d'Optique, Orsay, France.
[7] Austrian Research Center, Vienna, Austria.
[8] University of Erlangen, Germany & Institute for Quantum Computing, Waterloo, Canada.
[9] Thales Communications, Colombes, France.
[10] University of Vienna, Austria.
[11] Cryptolog International, Paris, France.
[12] University of Cambridge, United Kingdom.
[13] Id Quantique SA, Geneva, Switzerland.
[14] University of Aarhus, Denmark.
[15] Toshiba Research Europe Ltd, Cambridge, United Kingdom.
[16] Ludwig-Maximilians-University Munich, Germany

**SECOQC Coordinator**: Christian Monyk christian.monyk@arcs.ac.at

# Contents

# 1 Introduction

During recent years quantum cryptography has been the object of a strong activity and rapid progress [4, 5], and it is now extending its activity into pre-competitive research [1] and into commercial products [7]. Nevertheless, the fact that Quantum Key Distribution (QKD) could be an interesting cryptographic primitive is often considered with scepticism by classical cryptographers [6]. Analysing the cryptographic implications of Quantum Key Distribution is indeed a complex task. It requires a combination of knowledge that usually belongs to separate academic communities, ranging from classical cryptography to the foundations of quantum mechanics and network security. Based on a thorough consultation and discussion among the participants of the European project SECOQC [1], this paper presents arguments showing that QKD can indeed be useful in cryptography, in addition to the scientifically well-established classical cryptographic primitives. We also believe that very fruitful research, involving the classical cryptography community and the QKD community, could emerge in the future years and try to sketch what may be the next challenges in this direction.

Here we argue that QKD is a cryptographic primitive that can be used for different purposes, of increasing complexity. We will distinguish three levels of complexity, reflecting the first three layers of the OSI network model.

- The first level is Key Establishment between two users (physical layer cryptographic primitive).
- The second level is two-user Secure Payload Transmission built on top of a Key Establishment scheme (link layer cryptographic primitive).
- The third level is Key Distribution over a global network composed of multiple users (network layer cryptographic primitive).

In each of these scenarios, we will give elements allowing to compare QKD with what is currently offered by classical cryptographic techniques. This paper is thus organized as follows: In Section 2, we provide a survey of Key Establishment techniques, and discuss some of their strengths, weaknesses, and relative advantages. In Section 3, we discuss the security and the performances of the different Secure Payload Transmission primitives that can be built on top of QKD, and that can be used to secure a point-to-point communication link. In Section 4, we expose the motivations for the development of QKD networks and provide a survey of the previous works on QKD networks. Some major design decisions of the SECOQC QKD network are presented in this context as well as elements of comparison between classical networks and quantum networks. Finally, in Section 5 we extend our perspectives and discuss some future research directions that could benefit from active collaboration between the QKD and the classical cryptography communities: the study of side-channels and of material security, the study of post-quantum-computing cryptography and the use of QKD networks as a new primitive in network security.

# 2 Key Establishment

Cryptography has for a long time conformed to the idea that the techniques used to protect sensitive data had themselves to be kept secret. Such principle, known as "cryptography by obscurity" has however become inadequate in our modern era. Cryptography, that has

developed as a science in the 1970s and 1980s [68] allowed to move away from this historical picture and most of the modern cryptographic systems are now based on publicly announced algorithms while their security lies in the use of secret keys.

Distributing keys among a set of legitimate users while guaranteeing the secrecy of these keys with respect to any potential opponent is thus a central issue in cryptography, known as the *Key Establishment Problem*.

There are currently five families of cryptographic methods that can be used to solve the Key Establishment Problem between distant users:

1. Classical Information-theoretic schemes
2. Classical public-key cryptography
3. Classical computationally secure symmetric-key cryptographic schemes
4. Quantum Key Distribution
5. Trusted couriers

We will present how each of those cryptographic families can provide solutions to the Key Establishment problem and discuss, in each case, the type of security that can be provided. We will also consider a sixth type of Key Establishment schemes: hybrid schemes built by combining some of the methods listed above.

## 2.1 Classical Information-Theoretic Key Establishment Schemes

A crypto-system is information-theoretically secure if its security derives purely from information theory. That is, it makes no unproven assumptions on the hardness of some mathematical problems, and is hence secure even when the adversary has unbounded computing power. The expression "unconditional security" is a synonym of "information-theoretical security" and is more widely used in the cryptographic literature. The One-Time Pad (OTP) is for example an unconditionally secure encryption scheme. As shown by Ueli Maurer [46], it is possible to establish an information-theoretically secure key between two parties using only public discussion over a classical channel, provided that these two parties have in their possession correlated strings of classical data that exhibit more correlation between them than with any string that could be in the possession of an eavesdropper. As we shall see in 2.4, the use of a quantum channel and of an appropriate protocol is a practical solution in order to obtain such correlated strings of classical data.

There are however also Key Establishment schemes that can exploit the ideas developed in [46] and that can be implemented within the framework of classical information theory. Such Classical Information-Theoretic Key Establishment schemes (CITKE schemes) however need to rely on some specific extra assumptions, limiting the power of the eavesdropper, to be unconditionally secure. Christian Cachin and Ueli Maurer [30] hence demonstrated that CITKE is possible in the bounded-storage model, in which the adversaries can only store a limited amount of data. CITKE is also possible in Wire-Tap channel model as established in the seminal work of Wyner [44]. The result of this work on CITKE has been extended to what is called the "noisy channel model" where the legitimate users are supposed to have access to a common source of randomness through classical channels that are less noisy than the channel the eavesdropper has access to [45]. Introducing the idea of advantage distillation, Maurer generalised the previous models and showed that CITKE is possible over a wide class of classical channels [46]

## 2.2 Classical Public-Key Cryptography and Key Establishment

Public-key cryptography foundations rest on the difficulty of solving some mathematical problems for which no polynomial algorithms are known. The computing resources needed to solve these problems become totally unreachable when long enough keys are used. Public-key cryptographic systems thus rely on what is called "provable computational security". Public-key cryptography is however not unconditionally secure; the problems on which it is based are not intractable; and in addition, their non-polynomial complexity has so far not been proven.

Public-key cryptography requires two keys, a public and a private key, which form a key pair and uses algorithms that are designed in such a way that anyone can encrypt a message using the public key, while only the legitimate recipient, in possession of the private key, can decrypt the message. Because of the asymmetry between the two users of a public-key crypto-system (one holding the private key, and keeping it secret, while the other user only need to know a public, non-secret key, and check for its authenticity), public-key cryptography is often referred to as asymmetric cryptography.

**Key Establishment based on public-key cryptography** As shown by Whitfield Diffie and Martin Hellman in 1976 [8], public-key cryptography can be used to establish a shared secret key over an unprotected classical communication channel, without using a prior shared secret. It thus provides a practical way to implement key distribution over open networks. Note however that, in order to ensure the authenticity of the key distribution scheme, the two users have to rely on a third trusted authority. This is the purpose of public-key infrastructure (PKI): a hierarchical infrastructure of trusted third parties that are issuing certificates for the users' public keys, provided that the users accept to rely on them (we basically don't really have the choice in current Internet, in absence of any other practical solution for key distribution).

**Security of public-key cryptography** Current asymmetric classical cryptographic schemes, such as RSA, are based on the difficulty to compute logarithms within a finite field. Today's implementations of RSA require to use private and public keys of at least $1024$ bits, in order to offer a reasonable security margin against the computational efforts of an eavesdropper [1], and asymmetric keys of $2048$ bits are preferable [9] . It is also important to note that most of the currently used public-key cryptographic schemes (for example RSA) could be cracked in polynomial time with a quantum computer: this results from Shor's algorithm for discrete log and factoring, that has a complexity of $O(n^3)$ [14]. Some alternative public-key cryptographic schemes, based on other problems than factoring, such as lattice shortest vector problem [16] or coding theory [15], could not be broken in a polynomial time on a quantum computer. Such schemes are however much less practical than RSA-like schemes.

**Performance of public-key cryptography** Making the computations relative to the asymmetric cryptographic protocols (over keys longer than $1024$ bits) is a rather computational intensive and time-consuming task. The performance of RSA-based key distribution implementations depend heavily on hardware : for RSA 2048 implemented on a recent PC (Pentium IV with a 2.1 GHz processor running under Windows XP), the computations

[1] Under the unverified assumption that there is no eavesdropper that possesses some unexpectedly strong computational power or knows better cryptanalysis techniques than the best published ones.

needed for one key exchange (essentially one RSA encryption and one decryption) take roughly 30 ms [27]. The same key exchange would be approximately 10 times faster (thus in the ms range) on dedicated coprocessors and 10 times slower (in the time range of a few tens of a second) on smart card coprocessors [28]. Because of those relatively low exchange rates, public-key cryptography is most commonly used solely for initial session key distribution (in network protocols like SSL for example), and classical symmetric-key cryptography is then generally used for symmetric encryption and/or authentication of data.

## 2.3 Classical Computationally Secure Symmetric-Key Cryptography and Key Establishment

Symmetric-key cryptography refers to cryptography methods in which both the sender and receiver share the same key. Symmetric-key encryption was the only kind of encryption publicly known until the discovery of public-key cryptography in 1976 [8].

Symmetric-key ciphers are used to guarantee the secrecy of the encrypted messages. The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and to their applications. AES is a block cipher that had been designed by a team of Belgium cryptographers (Joan Daemen et Vincent Rijmen) and has been adopted as an encryption standard by the US government (in replacement of DES). Block ciphers can be used to compute Message Authentication Codes (MACs) and can thus also be used to guarantee integrity and authenticity of messages. Stream ciphers, in contrast to the block ciphers, create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the One-Time-Pad. We will not consider stream ciphers in the remaining part of this sub-section, since, unlike block ciphers, they cannot be easily used to perform Key Establishment. Reference [11] provides a very complete survey of classical computationally secure symmetric-key schemes.

**Key Establishment based on Classical Computationally Secure Symmetric-Key Cryptography** Key Establishment can be realised by making use of only symmetric-key cryptographic primitives. Indeed, the combination of a symmetric-key encryption scheme with a symmetric-key authentication scheme allows one to build a Key Establishment primitive. Provided that a secret key is previously shared, symmetrically, by Alice and Bob, one can use a symmetric-key cipher to encrypt a message that will constitute the secret key for the key distribution protocol (this message can be random or not). Part of the previously shared symmetric key material can also be used to symmetrically compute (on Alice's side) and check (on Bob's side) a message authentication tag. Key Establishment based on symmetric-key cryptographic primitives are always based on a pre-established symmetric secret, needed for authentication. In this sense, they only allow *Key Expansion* more than *Key Establishment*.

**Security of classical computationally secure symmetric-key cryptography** The security of key distribution based on classical symmetric-key cryptography depends on the security of the cryptographic primitives that are used, and on the composability of those crypto primitives. Shannon has proven that there is no unconditionally secure encryption scheme which requires less key than a One-Time Pad, i.e., the number of key bits is at least as large as the length of the message [17]. Hence, if we consider the possibility of building

an unconditionally secure symmetric key expansion scheme, i.e., a method to symmetrically generate secret key out of a short initial symmetric shared secret key, the former results from Shannon tell us that such a scheme is impossible to achieve in the framework of classical cryptography. This is a fundamental limitation of any communication scheme relying solely on the exchange of classical messages since, in contrast to quantum messages, classical messages can be copied without errors.

It is however possible to use classical symmetric-key encryption and authentication schemes, that are not unconditionally secure, to build a Key Establishment scheme. AES can for example be used for symmetric-key encryption and can be also used to compute message authentication codes (using AES-MAC). Note that the security model that applies to such symmetric-key classical encryption schemes (symmetric-key block ciphers and stream ciphers) is not unconditional security (the entropy of the key is smaller than the entropy of the message) and not even "provable computational security" (based on some proven upper bounds or on some equivalence between the complexity of the cryptanalysis of a given cipher and another well-studied problem[2]). The security model that applies to classical symmetric-key cryptography can be called "practical computational security": a cryptographic scheme is considered "practically computationally secure" if the best-known attacks require too much resource (such as computation power, time, memory) by an acceptable margin [11]. The main problem with such a security model is that it is unable to guarantee anything about yet unknown attacks [23].

There are no publicly known efficient quantum attacks on classical symmetric-key cryptographic schemes (but no proof that efficient attacks cannot be found), and the cryptanalysis of symmetric-key classical cryptography on a quantum computer reduces to exhaustive search. Here a quantum computer would thus still give an advantage: the complexity of exhaustive search in a unsorted database of $N$ elements is of $O(N)$ on a classical computer but only of $O(\sqrt{N})$ on a quantum computer [29].

**Performances** In terms of performance, symmetric-key classical cryptography is much faster and less computational intensive than asymmetric cryptography[3]. In terms of speed, there are now 128-bit AES encryptors able to encrypt data at rates in the Gbit/s range [24, 25]. This is the reason why it is widely preferred to use symmetric-key schemes for encryption and/or authentication over currently deployed communication networks. AES is currently the chosen standard for symmetric-key classical block ciphers. Under the assumption that the best way to break a symmetric-key cryptographic scheme is exhaustive search within the key space[4], then, a symmetric key modulus of 77 bits is roughly comparable, in terms of computational requirements, to an asymmetric key modulus of $2048$ bits [9, 13]. Note that doubling the length of a symmetric key implies squaring the computational efforts needed for exhaustive search; on the other hand, the computational efforts scale not as fast with key length in the case of asymmetric cryptography (see [9] for details).

[2] on the other hand, provable computational security exists for classical asymmetric schemes.

[3] the difference is indeed of several orders of magnitude, see [12] for references and details.

[4] as we shall see in 3.2, the assumption that the best attack on AES is exhaustive search, somehow equivalent to say that there is no known successful attack on AES, is however seriously challenged by the fact that weaker versions of AES, with reduced number of rounds, can be attacked more efficiently. Note also that the possibility of powerful algebraic attacks on AES, although not regarded as a real threat by the majority of the classical cryptography community, still seems to be an open and controversial question[26].

## 2.4 Quantum Key Establishment - Quantum Key Distribution (QKD)

Quantum Key Distribution, invented in 1984 by Charles Bennett and Gilles Brassard [33], based on some earlier ideas of Stephen Wiesner [34], is an alternative solution to the Key Establishment problem. In contrast to public-key cryptography, it has been proven to be unconditionally secure, i.e., secure against any attack, even in the future, irrespective of the computing power or any other resources that may be used [35, 36]. QKD security relies on the laws of quantum mechanics, and more specifically on the fact that it is impossible to gain information about non-orthogonal quantum states without perturbing these states [37]. This property can be used to establish a random key between two users, commonly called Alice and Bob, and guarantee that the key is perfectly secret[5] to any third party eavesdropping on the line, commonly called Eve. In parallel to the "full quantum proofs" mentioned above, the security of real QKD systems has been put on a stable information-theoretic footing thanks to the work on secret key agreement done in the framework of information-theoretic cryptography [46] and to its extensions, triggered by the new possibilities offered by quantum information [47] and [53].

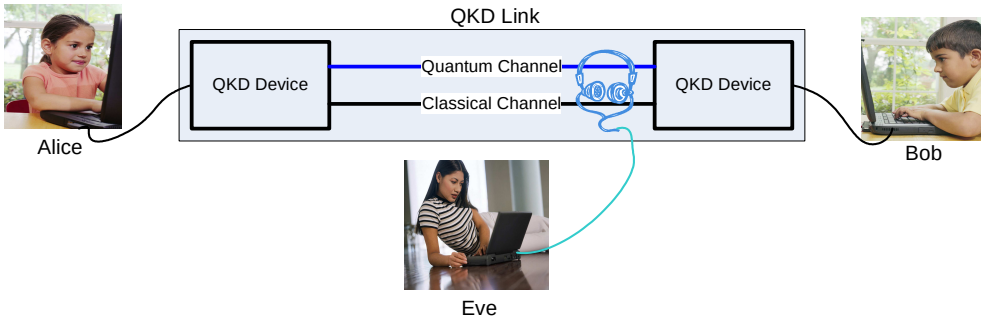


Figure 1: Structure of a QKD link as it is referred throughout this article

Without going into the details of the different implementations or protocols, we can describe the structure and the principle of operation of the basic practical QKD system: a QKD link. As depicted on Fig. 1, a QKD link is a point-to-point connection between two users, commonly called Alice and Bob, that want to share secret keys. The QKD link is constituted by the combination of a quantum channel and a classical channel. Alice generates a random stream of classical bits and encodes them into a sequence of non-orthogonal quantum states of light, sent over the quantum channel. Upon reception of those quantum states, Bob performs some appropriate measurements leading him to share some classical data correlated with Alice's bit stream. The classical channel is then used to test these correlations. If the correlations are high enough, this statistically implies that no significant eavesdropping has taken place on the quantum channel and thus that with very high probability, a perfectly secure symmetric key can be distilled from the correlated data shared by Alice and Bob. In the opposite case, the key generation process has to be aborted and started again.

QKD is a symmetric key distribution technique. QKD requires, for authentication purposes, that Alice and Bob share, in advance, a short secret key (whose length scales only logarithmically in the length of the secret key generated by a QKD session [18, 19, 20]).

[5] the perfect secrecy of the key has to be considered from an information-theoretic point of view: the information the eavesdropper may have about the key is, with an exponentially high probability, below a vanishingly small upper bound.

Hence, QKD is a symmetric unconditionally secure key expansion scheme. In contrast to what is achievable while relying solely on the exchange of classical messages, the key expansion factor provided by QKD is exponential, hence, after initialisation of the system (initial distribution of secret key), authentication is not a burden for the global performance (secret bit rate per second) of QKD schemes. QKD systems are being developed with an increasing reliability and with increasing performances, and the SECOQC project [1], gathering the most prominent experimental and theoretical European teams involved in QKD research, is actively contributing to the pursuit of this progression [39, 40, 41, 38]. One can currently expect to exchange between 1 and 10 kbits of secret key per second, over a point-to-point QKD link of 25 km (at 1550 nm, on dark fibres). The maximum span of QKD links is now roughly 100 km (depending on the systems) at 1550 nm on telecom dark fibres. Both secret bit rate and maximum reachable distance are expected to continue their progression during the next years due to combined theoretical and experimental advances. Note that in any case QKD performances are intrinsically upper bounded by the performance of classical optical communications[6]. It is important to notice that QKD systems can now basically be built with optimised, off-the-shelves telecom components (laser, phase modulators, beamsplitters, polarisation controllers, and etc.) at the notable exception of photodetectors. Photodetection is currently the bottleneck for the performance of QKD systems, but it is important to keep in mind that, even on that side, although there are many technical problems to overcome, there are very few fundamental limitations for rate and distance [49, 50, 51]. Another approach, known as "Continuous Variables QKD", and also implemented in SECOQC, uses only standard PIN photodiodes, but requires more sophisticated data processing in order to extract the secret key [48]. It is also very important to note that QKD would remain secure (unconditionally) even in the advent of a quantum computer. In addition, legitimate users (Alice and Bob) can perform unconditionally secure QKD even without possessing themselves a quantum computer, and QKD can thus be deployed today in order to secure communication networks. Studying how such QKD networks can be built and operated is the main focus of the SECOQC project and we will develop on this aspect in Section 4.

## 2.5 Trusted Couriers Key Distribution (TCKD)

The trusted courier method is known since the ancient times: a trusted courier travels between the different legitimate users to distribute the secret keys, hopefully without being intercepted or corrupted on his way by any potential opponent. Only practical security can be invoked in this case, which has to be backed by the enforcement of an appropriate set of security measures. Although trusted couriers become costly and unpractical when implemented on large systems, this technique has remained in use in some highly-sensitive environments such as government intelligence, or defence. The trusted courier method is also used by banks to solve the very common, but highly strategic problem of distributing their credit card PIN numbers to the bank customers[7].

The Trusted Couriers Key Distribution (TCKD) is probably the method used in the framework of network security for which the analogy with QKD is the closest:

- Like QKD, TCKD is a method relying on the physical security of the communication

[6] and it will always lag behind in terms of rate and distance. However, since current classical systems are now reaching rates of Terabit/s, there definitively remains some room - and thus reasons to hope - for improvements.

[7] The solution adopted today by the banks is to send the cards and the PIN numbers in different envelopes to minimize the possibility that someone could steal both.

line between Alice and Bob, it is thus also sensitive to distance and other characteristics (danger, perturbations ...) of the communication line between Alice and Bob.

- Like QKD, TCKD is a symmetric key distribution protocol.
- Like QKD, TCKD is a technique that finds its application when classical key distribution schemes are believed not to offer enough guarantee.

Despite the similarities listed above, there are important differences between QKD and TCKD:

- The first difference is really intrinsic to QKD and TCKD "physical realities". In the case of QKD, the "couriers" are quantum states of lights (flying qubits) travelling at the speed of light and on which eavesdropping can be detected with arbitrary high statistical certainty. On the other hand, TCKD cannot offer any of those guarantees and, whether one uses human beings or pigeons, trust or corruption of a classical courier cannot be proven nor tested.
- Reliability, automation and cost effectiveness will, very likely, be one of the major advances offered by the development of QKD networks. On the other hand, reliability and cost of TCKD infrastructures are critical problems and there is no hope that such systems can ever be automated.
- Unlike point-to-point QKD links, classical trusted couriers are not intrinsically limited in distance. They are also not very limited in rate since they can take advantage of the possibilities offered by today's portable and versatile classical memories, such as DVDs or USB keys, that can store Gigabytes of data. We will however see in section 4 that QKD networks could be used to go beyond QKD links distance limitations and that such networks could also be used to distribute key "on demand" to the end users, which is fundamentally different from relying on keys stored on the very same DVD, that can be duplicated at any time.

## 2.6 Hybrid Key Establishment schemes based on Dual Key agreement

**Cascaded ciphers** For all the cryptographic methods described in the previous subsections, and for which we have been discussing the applicability to solve the Key Establishment problem, there exists an encryption scheme that relies on the same principles and exhibits the same security properties: One-Time Pad for information-theoretically secure schemes, Public-key ciphers and symmetric-key ciphers respectively for asymmetric and for symmetric computationally-secure schemes.

The idea of *Cascade Cipher* is to compose several encryption primitives by applying them sequentially on the same cleartext. Note that the encryption primitives can be of different types as in AES-Twofish or the same one as in 3DES. The interest of cascading ciphers is to increase the amount of difficulty an adversary has to overcome in order to break the encryption and find the message. As pointed by Maurer and Massey, [52], the first encryption layer, i.e. the one directly applied to the message, is in all cases the most important one.

**Dual Key Agreement** This idea of Cascade Cipher can straightforwardly be applied to Key Establishment: two keys of the same length are established through two Key Establishment schemes (relying on either the same primitive or on different ones) and the

final key is obtained by XORing these two keys. We will talk, in this context, of *Dual Key Agreement*. Note that more than two Key Establishment schemes, of various types, can in principle be combined this way. We will restrict, in the following to a discussion of Dual Key Agreement involving QKD as one of the Key Establishment technique.

The approach of Dual Key Agreement could for example be beneficial when combining keys established through one CITKE scheme and keys established through QKD: breaking the entire Key Establishment schemes implies breaking the CITKE scheme *and* breaking QKD. If one has doubts about the security of QKD, the Dual Key Agreement procedure guarantees that the security will at least not be worst than that of the classical Key Establishment technique with which it is combined. The same is true if one has doubts about the security of Key Establishment schemes based on classical cryptography. Contrary to classical cryptography, where security standards exist (for example FIPS 140), there are not yet such standards for QKD. The approach of Dual Key Agreement could thus allow to certify a system according to already established criteria, without requiring to specify the quantum part of the Key Establishment.

# 3 Securing a point-to-point classical communication link

We consider here the problem of securely transmitting classical messages (payload) from Alice to Bob, while guaranteeing the secrecy, the integrity and the authenticity of those messages. This cryptographic task, that we can indeed simply refer to as "building a secure point-to-point link" can be obtained in two steps:

1. Establishment of a symmetric secret key $K_S = K_{encrypt} \cdot K_{auth}$ ($A \cdot B$ stands for the concatenation of string $A$ with string $B$).

2. Secure and authentic transmission of the message $M$ over the classical channel: $M$ is encrypted with encryption key $K_{encrypt}$ and authenticated with the authentication key $K_{auth}$.

We can now analyse several scenarios in which QKD is used as the Key Distribution primitive while different types of encryption and authentication schemes are used.

## 3.1 QKD composed with One-Time-Pad: Everlasting Secrecy

When keys established by QKD are used for One-Time Pad encryption and for information-theoretically secure authentication, then one can obtain unconditional security over the resulting point-to-point classical communication link.

This result can be proven because of the fact that the security of QKD can be expressed in the framework of Universal Composability [21]: unconditionally secure Key Establishment, realised by QKD, cannot be distinguished from an ideal Key Distribution protocol interacting with some environment. This implies that QKD can be composed with any other universally composable unconditionally secure cryptographic primitives, while still guaranteeing the unconditional security of the whole cryptographic scheme [53].

Concerning authentication, information-theoretically secure symmetric-key authentication primitives are based on universal hashing. Such authentication codes were first introduced by Wegman and Carter and further developed, especially by Stinson [18, 19, 20]. If One-Time Pad encryption and information-theoretically secure authentication scheme are used, one can show that both primitives are composable and thus that an unconditionally secure message transmission protocol can be built out of them [22].

Allowing to build an unconditionally secure classical communication link is one of the most important domains for the application of QKD to secure communications and to secure networks. This is the cryptographic framework in which we have chosen to work within the SECOQC project.

Since they benefit from the perfect secrecy offered by One-Time Pad and from the fact that the keys established by QKD are unconditionally secure, the messages exchanged over such unconditionally secure links enjoy one security property that can be called "everlasting secrecy": the messages are perfectly secret with respect to adversaries and there is provably absolutely no chance that future events could alter the secrecy of these messages. "Everlasting security" (which is achieved even if the authentication scheme is only computationally secure) is one of the big advantages of quantum cryptography compared to computational cryptography. It is important to note that an adversary could always store the ciphertext and wait with the decryption until better cryptoanalysis methods become available (which is very likely to happen at some point in the future, as it always occurred in the past [23]) [8].

## 3.2 QKD composed with a classical computationally secure encryption scheme: Key security and Key Ageing

Here we will consider one very frequent scenario: QKD is used for Key Establishment between two-users placed on each side of a point to point QKD link. Link encryption is then realised with encryption scheme (such as AES) in order to be able to encrypt large rates of classical data over the link layer. This solution is the one that is currently adopted by commercial QKD vendors: IdQuantique and MagiQ [7] and it was also the solution adopted within the BBN Darpa Quantum Network project [54]. Such a composition provides a practical solution to realise a point-to-point VPN encryptor, that can be deployed in layer 2 (link) in the OSI network layer model [7] or directly in the layer 3 (network), for example by interfacing QKD-based key exchange with IPSEC [55, 56]

It is clear that the final security of the exchanged data over such link cannot be stronger than the security of the encryption scheme. In the case of a symmetric-key block cipher, the security of the encrypted data depends on at least four factors:

1. the security of the key (can an opponent get even some partial information about the key ?);
2. the number of blocks that have been encrypted with the same key (key renewal rate);
3. the length of the key modulus (56 bits for DES, 128, 192 or 256 bits for AES);
4. the security of the symmetric-key encryption algorithm, for which only "practical computational security" can be claimed. For block ciphers, the practical security depends in particular on the number of rounds applied when encrypting one block (see [11] for details).

The last two factors are purely dependent on the encryption technique and not at all on the Key Establishment scheme. The first two factors, on the other hand, are influenced by the choice of the Key Establishment scheme: security of the key is intrinsically linked to the security of the Key Establishment while the key renewal rate strongly depends, on a practical level (hardware performance, security policy, implementation details, etc.),

[8] One should indeed note that securing today's highly sensitive data with computationally secure schemes is somehow very risky, unless one can assume that it is clear that the data will be irrelevant in 25 years or so.

on the Key Establishment scheme. Improvements on these two factors can lead to an improvement of the overall security of the encrypted communication link. We will explain why QKD-based schemes, used in replacement of traditional Key Establishment schemes, present an interest with respect to these two factors.

**Security of the key** The Key Establishment scheme, whether it is QKD or a public-key based method such as Diffie-Helman, has a direct impact on the security of the exchanged keys: QKD is the only Key Establishment scheme that can offer information-theoretic security and thus guarantee that the information that an opponent can get about the key is below a vanishingly small upper bound. We believe that strict requirements regarding the security of the key will be the the most important driving factors leading cryptography users, from high-security areas, to switch to QKD-based schemes.

**Key renewal rate** When we consider the global security level one can obtain on a communication link, there is also second factor that can as well indirectly depend on the Key Distribution scheme : the key renewal rate. As we shall see, the key renewal rate can indeed influence the security of the encrypted data. This is what we call the *Key Ageing* factor, that can be reformulated as a question: how often secret session keys should be changed and what is the impact on the global security of the classical message passing scheme ?

Let's first take the example of fast DES Xilinx encryption systems that are currently commercialised [24]. Data is encrypted at a rate of 1.5 Gbit/s, the number of packets (of 64 bits) encrypted per second (with a 56-bit key) is $10^{7.373} \simeq 2^{24.5}$ blocks/s. There exist known cryptographic problems with block ciphers, such as known plaintext attacks based on the birthday paradox, when the number of blocks encrypted with the same key reaches $2^{\text{keylength}/2}$ [11]. In the case of DES 56-bit keys, this would occur after $2^{3.5} \simeq 11$ seconds.
Let's now take the case of 128-bit AES for which Xilinx produces dedicated cipher modules that can support a data rate of $2.2$ Gbit/s [24] and for which "dedicated research hardware" has recently demonstrated a rate of $21.54$ Gbit/s [25]. In this case, the number of blocks (of 128 bits) encrypted per second (with a 128-bit key) is $10^{8.23} \simeq 2^{27}$ blocks/s. "Birthday paradox" collisions become very likely after $2^{64}$ blocks (of 128 bits) have been encrypted with the same key. This occurs in a time of about $2^{37}$ seconds, i.e. roughly $4000$ years ,which means in practice that this is not a problem. We must however not forget that the previous calculation is done under the assumption that exhaustive search is the best attack on AES. Indeed, even though the cryptanalysis of encryption schemes like AES is very difficult topic that is still subject to very active research, it seems that the ultimate difficulty of such cryptanalysis is currently not known. There moreover exists a variety of attacks, more subtle than exhaustive search, that can be used against AES. As explained in the security report of the IST FP5 program NESSIE (NESSIE Deliverable D20) [11], there exist cryptanalysis techniques that start to obtain better results than exhaustive search, on AES with a reduced number of rounds, as soon as $2^{32}$ blocks have been encrypted with the same key. If we come back to our example, such an event would occur in roughly $2^5$ seconds i.e. less than one minute.

As we can see from the previous examples, there exist arguments, based on some known cryptographic weaknesses of current block ciphers that would motivate to refresh the secret keys of symmetric-key ciphers over times shorter than a minute. Although this is possible in practice with current technology, relying on PKIs, such key renewal rate policies are very seldom enforced and the key renewal period of most currently deployed VPNs is more in the range of hours. As a matter of fact, since public-key cryptography

is rather slow and computational intensive and is using long key modulus (see details in 2.2), it could become an extremely high burden for end-users in terms of time and CPU consumption [9] if key renewal was to be done over times shorter than one minute.

On the other hand, despite the fact that QKD is very often portrayed as slow [6], QKD rates, as we have mentioned in the previous section, are currently in the range of 10 kbps over 25 km. They can typically allow one to refresh several 128-bits AES keys per second, over VPN links in a metropolitan network. This means that current QKD systems, when used to secure a communication link, compare rather favourably, at least from a pure "key renewal rate point of view" with respect to VPNs based on PKIs for the key establishment.

# 4 Key Distribution over a Network of QKD links : QKD Networks

There are several fundamental limits regarding what can be achieved with standalone QKD links. QKD links can by definition only operate over point-to-point connections between two users, which greatly restricts the domain of applicability of quantum key distribution within secure communication networks. Furthermore, since they rely on the transmission of quantum information in order to guarantee security against on-line eavesdropping, QKD links are limited in rate and distance, and cannot be deployed over any arbitrary network topology. To overcome those limitations, it seems important to study what can be achieved by networking QKD links in order to extend the extremely high security standard offered by QKD to the context of long distance communications between multiple users. The development of QKD network architectures appears from this perspective as a necessary step towards the effective integration of QKD into secure data networks. This is the main focus of the SECOQC project [1], that will culminate in the demonstration of information-theoretically secure key distribution over a fibre-based metropolitan area network in 2008.

We will begin this section by an overview on the previous work done on quantum Networks and on QKD networks. We will then present the specific QKD Network design adopted within the SECOQC project and will finally present some elements of comparison between QKD networks and classical network Key Distribution schemes.

## 4.1 Previous work on QKD Networks

What we call a "quantum network" is an infrastructure composed of quantum links connecting multiple distant nodes. A quantum network can be used for Key Distribution, relying for that on QKD. We call such infrastructures "QKD networks".

The essential functionality of the QKD network is to distribute unconditionally secure symmetric secret keys to any pair of legitimate users accessing the network. These first elements of definition are however fairly generic and can be refined. Indeed, even though we are at the infancy of the development of QKD networks, different models of QKD networks have already been proposed. The first QKD network demonstrator, the "DARPA Quantum network", has been deployed between Harvard University, Boston University and BBN in 2004 [54, 55].

It is convenient to characterise the different QKD network models by the functionality that is implemented within the nodes and thus by the different underlying quantum

[9] end-users support *all* the computational efforts linked to asymmetric cryptography in an open network

network models. We can, from this perspective, differentiate three main categories of network concepts, based on different "families" of node functionalities : 1) optical switching ; 2) quantum relaying ; and 3) classical trusted relaying.

**Optically switched quantum networks:** These are networks in which some classical optical function, like beam splitting, switching, multiplexing, demultiplexing, etc., can be applied at the network nodes on the *quantum* signals sent over the quantum channel. The interest of such optical networking capabilities in the context of QKD networks is that they allow to go beyond two-users QKD. One-to-many connectivity between QKD devices was demonstrated over a passively switched optical network, using the random splitting of single photons upon beam splitters [57]. Active optical switching can also be used to allow the selective connection of any two QKD nodes with a direct quantum channel. The BBN Darpa quantum network [54, 55] contains an active 2-by-2 optical switch in one node, that can be used to actively switch between two network topologies. Optical functions can thus be used to realise multi-user QKD and the corresponding nodes do not need to be trusted, since quantum signals are transmitted over a quantum channel with no interruption from one end-user QKD device to the other one. This QKD network model can however not be used to extend the distance over which keys can be distributed. Indeed, the extra amount of optical losses introduced in the nodes will in reality shorten the maximum span of quantum channels.

**"Full" quantum networks:** To be able to extend the distance on which quantum key distribution can be performed, it is necessary to fight against propagation losses that affect the "quality" of the quantum signals as they travel over the quantum channel. Quantum repeaters[59] can overcome the loss problem and can be used to form an effective perfect quantum channel [58]. A quantum network where nodes are constituted by quantum repeaters can thus be called a "full" quantum network. It is not necessary to trust the network nodes to have unconditional security when performing QKD over such full quantum networks.

Quantum repeaters however rely on elaborated quantum operations and on quantum memories that cannot be realised with current technologies. As discussed in [60], quantum nodes called quantum relays could also be used to extend the reach of QKD. Quantum relays are simpler to implement than quantum repeaters since they don't require quantum memories. Building quantum relays remains however technologically difficult and would not allow to extend QKD reach to arbitrary long distances.

**Trusted relays QKD network:** This technique can on the other hand be implemented with today's technologies since such nodes consist in classical memories placed within the nodes, that thus need to be trusted. QKD networks based on trusted key relays follow a simple principle: local keys are generated over QKD links and then stored in nodes that are placed on both ends of each link. Global key distribution is performed over a QKD path, i.e. a one-dimensional chain of trusted relays connected by QKD links, establishing a connection between two end nodes, as shown on Fig. 2. Secret keys are forwarded, in a hop-by-hop fashion, along QKD paths. To ensure their secrecy, One-Time Pad encryption and unconditionally secure authentication, both realised with a local QKD key, are performed. The link primitive of such network is indeed precisely the one discussed in 3.1, and the message sent is a random session key by one of the end-user (the sender). End-to-end information-theoretic security is thus obtained between the end nodes, provided

that the intermediate nodes can be trusted. Classical trusted relays can be used to build a long-distance QKD network. The advantage of such quantum networks is that they rely on QKD for link Key Establishment, which renders impossible to compromise the Key Establishment by direct attacks *on the links*[10].

This concept of trusted relay QKD network has been exploited by the BBN QKD network [54, 55] and will also be used within the SECOQC QKD network.

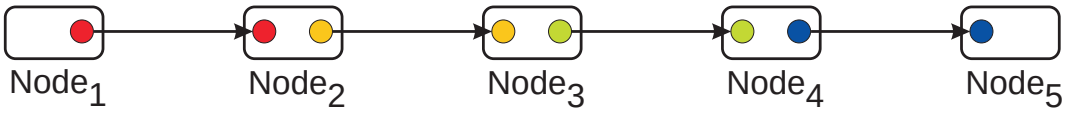


Figure 2: "Hop-by-hop" unconditionally secure message passing on a path made of trusted relay nodes connected by QKD links. Message decryption / re-encryption is done at each intermediate node, by using one-time-pad between the local key, distributed by QKD, $K_{local}$, and the secret message $M$ resulting in the ciphered message $M \bigoplus K_{local}$. Different key associations are symbolised by different colours.

## 4.2 The specific design of the SECOQC QKD network

The focus of the SECOQC project is on "long-range high security communications based on quantum key distribution". As explained above, this imposes to rely on trusted nodes used as key relays. We have adopted this network model within the SECOQC project. An important choice however relies in the network protocols and logical architecture allowing to use the QKD link-specific local keys in order to secure long-distance traffic.

We have adopted an original network architecture and a dedicated network management designed solely to address the problem of key distribution over a network of trusted nodes linked by QKD links. One can find details regarding this network architecture in [61] and in publications currently in preparation. The main originality of the SECOQC project, with respect to previous QKD networks, relies on the fact that we have opted for a *dedicated key distribution network infrastructure* that we have called "network of secrets" [64]. The functionality of the network of secrets is solely to store, forward, and manage the secret key materials generated by QKD. Such a key distribution network is characterised by dedicated link, network and transport layers and can be considered somehow independently from the quantum key establishment processes and from key requests arising from applications. Such an architectural design implies that our QKD network, contrary to previous works, clearly departs from a collection of QKD links: it implements distributed management and routing of the secret keys established on a link basis and can exploit the full advantages offered by the network characteristics: increased reliability and flexibility achieved through path redundancy, load balancing and traffic engineering of the network key exchanges performed through dedicated routing algorithms and appropriate signalings. We have moreover focused our attention on what we have called "Backbone QKD networks", i.e., QKD networks exhibiting a high connectivity and a meshed topology [63, 64]. As explained in [63, 65], a meshed topology ensures that there exist multiple disjoint paths between any pair of QKD nodes, a property that can be exploited to increase the security of final key distribution, by Dual Key Agreement over disjoint pathes [63].

[10] except for side-channel attacks on the QKD links (those attacks being only possible on "bad QKD implementations") and for denial-of-service attacks.

The central design issue behind our QKD network concept is that the keys are stored and managed within dedicated and well-specified key stores, placed in nodes, and not within QKD devices or within the machines running endpoint secure applications. This design choice will allow us to manage keys over a dedicated global network, *the network of secrets*, composed of key stores linked together with classical channels. The network of secrets is by essence a classical network, but, since it relies on QKD for Key Establishment and on unconditionally secure cryptographic primitives, it offers an unprecedented overall security. This last claim is of course only true if one can guarantee that the nodes are indeed trusted nodes. Even though such assumptions might not be unrealistic in today's high security infrastructures (government secure networks, bank secure networks, military headquarters and etc.) we will see in the next section that information-theoretical tools can be used to extend on this result and to guarantee unconditional security even when a fraction of the nodes are corrupted.

## 4.3 Classical Network Key Distribution Schemes and QKD Networks: Elements of comparison

## 4.4 Network Initialisation and Key Pre-distribution

**Key Pre-distribution over networks relying on symmetric-key cryptography** One of the central issues in network Key Distribution is the initialisation and the management of a potentially very large pool of secret keys: in a symmetric-key framework, where each member of a $n$-user network wants to be able to communicate securely with each of the other $n-1$ users, the Key Distribution scheme is required to provide any of the $n(n-1)/2$ pairs of users with a secret key before communication can start. Managing the security of those keys efficiently is thus very difficult task as $n$ grows. This is probably the reason why large-scale symmetric-key cryptography is seldom used in today's networks (however some network security schemes, like the Kerberos network authentication scheme [66] rely on classical symmetric-key cryptography and on a single trusted centre).

**Key Pre-Distribution over QKD networks:** As pointed out in [6], QKD networks need pre-distributed secret keys to perform the first rounds of authentication. The QKD-generated keys can then be stored and used for later authentication. Initialisation of a QKD network of $n$ nodes thus a priori requires the pre-distribution of $n(n-1)/2$ pairs of secret keys (one per pair of user). However, one can play with the QKD network connectivity and with the fact that keys can transitively be distributed between any two nodes along a connected QKD path, relying for that on hop-by-hop one-time-padding with local QKD keys. It is then easy to show that it is sufficient to distribute keys over a subset of those $n(n-1)/2$ pairs: what is needed is to distribute a pair of keys over QKD links so that the resulting graph of "initialised" QKD links is a covering graph of the QKD network. In this case, the complexity of Key Pre-distribution, that can typically only be done with trusted couriers, only scales linearly with the network size.

**PKI Initialisation and its application to QKD Network Initialisation:** PKI is the most commonly employed system for Key Distribution over open networks. PKI trust relations are materialised by certificates, i.e. signatures of public-keys and these trust relations can be organised hierarchically, which offers the advantage that one does not need to trust everybody in the network, but only to trust a third party which is called the certification authority. Moreover, Diffie-Hellman scheme allows to perform a key exchange between

two users that have never met before and do not share any common secret: the only condition is that they accept to trust the same certification authority (and accept its certificates). PKIs however also need to be initialised, and the only way to perform such an initialisation is also the use of secret couriers. In this sense, the initialisation of a QKD network and the initialisation of a PKI are two problems that share some similarities.

As pointed out in [6], QKD networks however present a security advantage over PKIs when we consider the initialisation phase: in order to threaten the security of a QKD network, the authentication of the messages sent over the classical channel of this network needs to be broken *before or during* the execution of the quantum key establishment protocol. In this sense, the authentication in QKD network exhibits a property called "forward security", which is of course not the case in public-key based secure networks. We could take advantage of this property in the case of QKD network initialisation and consider an hybrid scenario for Key Pre-distribution, in which the classical communications needed for the key distillation phase are authenticated, at least during the first QKD sessions, by a computationally secure message authentication scheme based on public-key cryptography (for which the PKI has been freshly initialised). If no active attack on authentication has been performed *before* the first -potentially vulnerable- QKD sessions, then the keys shared by Alice and Bob are identical and unconditionally secure. Note that the previous condition will always be verified if the computational power of the adversary is bounded *at the time of the QKD network initialisation*, with no restriction on how the adversary's capabilities may evolve in the future. Such keys could therefore be used to realise information-theoretically secure authentication of all future classical messages exchanged during the future key distillation phases. Hence, the flow of keys generated by QKD will remain future-proof unless an active attack on the authentication of the first QKD sessions can be mounted successfully.

There is a clear practical interest for such a scheme: it relaxes the requirement of distributing pre-established small keys in a QKD network for each network initialisation (which requires secret couriers and can be a difficult key management problem in the case of large networks).

## 4.5 Open networks versus trusted QKD networks

As pointed out in [68], "quantum cryptology is not a solution for open networks", i.e. a QKD network does not allow users that do not share any pre-established secret or trust relation to exchange a key and then communicate securely. In a sense QKD networks are tied by their "physical nature": they can only operate under trust conditions, are limited in distance because some physical, uncloneable quantum states are being exchanged over quantum channels and some physical interaction (trusted courier) is needed to initialise such networks. QKD networks, now at an early development stage, are intrinsically "physically-limited" networks. These physical limitations however bring a considerable security advantage: QKD networks can provide unconditional security to all the users that have access rights to the network and are thus inside the "circle of trust" of these closed networks.

The difference between quantum networks and classical networks thus appears to be almost philosophical : they do not offer the same services and exhibit a relation with space and distance that is extremely different: while classical open networks, and especially the Internet have been analysed as "small worlds", where physical signals can be regenerated, data can be copied and distances are almost abolished [69] , quantum networks are by essence closed networks where distance comes back into the game. We believe that

the topological design of the future quantum networks is indeed a very fertile research problem, and have started investigating this aspect within the SECOQC project [65].

# 5 Future directions

## 5.1 Resilience to side-channel attacks and historical security

Instead of trying to break the theoretical foundations of a given cryptographic system, another "attack philosophy" is to attack the physical implementation, i.e. the devices on which the cryptographic tasks are implemented. In fact, since a classical algorithm (for example of the RSA algorithm) says a priori nothing about how computations should be physically carried out over some physical devices, the theoretical security proof, even though it remains totally valid, does not provide any security guarantee against attacks made via physical side-channels such as electromagnetic radiation, heat dissipation, noise, observation of computation time, of power consumption and etc. Like for the attacks on the theoretical foundations of cryptographic systems, one distinguishes two types of side-channel attacks:

- Passive side-channel attacks, that are also well-known as "information leakage attacks". Such attacks do not require to actively manipulate the computation, but only to monitor the side-channel leakage during the computation.
- Active side-channel attacks, in which we assume that the attacker actively manipulates the execution of a cryptographic algorithm (trying for example to introduce faults in the computation).

Attacking the physical security of cryptographic systems has indeed proven to be an extremely successful way of breaking the security offered by those systems, and all classical cryptographic primitives (public-key-based and symmetric-key-based) that we have considered in this document are vulnerable to side-channel attacks [11]. There is indeed an intrinsic reason for the vulnerability of classical crypto-systems to side-channel attacks: classical crypto-systems are making use of classical physical channels to convey some secret information. Classical crypto-systems are thus exposed to a general vulnerability : it is not possible to guarantee the absence of eavesdropping on such systems, relying on classical channels and classical data to convey information, since classical data can be copied without introducing any perturbation.

There indeed seems to be an important potential advantage in a "quantum approach" of material security and of side-channels problems: quantum physics is a theory that is intrinsically adapted to precisely describe a physical system and its degrees of freedom: one can use the Hilbert space formalism to describe a quantum system in a vectorial space whose dimension and structure can be, at least in theory, explicitly given, and for which a precise mathematical description is possible. On the other hand, the security proofs for classical crypto-systems usually do not allow to model the physical implementations at all which makes the protection of current classical crypto-systems against side channel attacks a very challenging problem [68].

Despite their conceptual difference with classical crypto-systems, QKD hardware and quantum crypto-systems are nevertheless in a large part made of classical macroscopic objects and are indeed also vulnerable to side-channel attacks. We however believe that the theoretical foundations of quantum security proofs and the techniques developed to prove the security of QKD shed a new light on the problem of side-channel in cryptography. The

principle of QKD proofs indeed relies on the ability to describe mathematically the conditions (based on the Hilbert space dimension) under which the quantum channel becomes immune to side channel attacks. As a matter of fact, the "physical nature" of the quantum channel is embedded within the security proofs we have for QKD. In one sense, only "bad implementations of QKD" are vulnerable to side-channel attacks on the quantum channel. What we designate, in this context, as "bad implementations", are implementations that do not comply to the protocol and the assumptions for which their security proof has been derived. QKD security proofs are indeed based on explicit assumptions on the physical implementations, such as the mean number of photons per pulse sent on Alice's side, the detector noise, the attenuation of the quantum channel, etc. One crucial question is thus to know whether realistic QKD systems comply with the existing security proofs. This question has been widely tackled in the research literature on QKD: through the study of PNS attack [5], of its counter-measure (Decoy-State QKD) [42], of Trojan-horse attacks of various sorts [5], of QKD implementations based on imperfect devices [43], and etc. [4]; all these results are somehow reducing the gap between the conditions under which security proof fully applies and the reality of QKD implementations.

On the other hand, QKD security is *always* relying on an implicit assumption: *Alice and Bob, who are storing the final symmetric secret keys in classical memories must be located inside secure environments*. It is clear that if there exists a side-channel allowing to spy on the keys, once they are stored in a classical memory, then the security of the keys is compromised. In a more general sense, since QKD devices are for a large part made of classical objects, one crucial question will be relying on the way to *interface* the classical and quantum part of QKD crypto-systems. Such interfaces are potentially strategic choices for the opponents who want to eavesdrop on QKD crypto-systems side-channels, and should be designed with great care. We believe that a quantum description of the quantum / classical interfaces is necessary to correctly understand the related security challenges. Let us finally mention that, on the classical side of the interface only classical counter-measures, like the one implemented in smart-cards, can be proposed. It follows from this argument that the expertise of side-channels gathered on classical crypto-systems will remain crucial for the implementation of quantum crypto-systems.

There is one additional argument that illustrates another advantage of adopting a quantum description of crypto-systems in the perspective of side-channel attacks: by testing for some fundamental quantum statistical behaviour, like the non-local correlation properties involved in Bell Inequalities (BI) violations [4], one can [11] relate BI violations with the *absence of side-channels*, i.e. one can experimentally test and verify that the Hilbert space in which the quantum phenomena are controlled and observed is not leaking information towards another Hilbert space and thus to a potential eavesdropper [70]. This property is very fundamental and has absolutely no classical counterpart. It is indeed this property that is used in the derivations of the unconditional security proofs of QKD against arbitrary quantum attacks [35, 36]. The beauty of this property is that it can be, in principle, tested experimentally: one can experimentally prove that there exists no information leakage from a set of maximally entangled states, and thus no side-channel[12]. It is by essence impossible to have such a property on any classical cryptographic systems, because any classical message can be duplicated and cloned without any perturbation. It appears to us fascinating to notice that some very deep aspects of quantum information tools, like the loophole-free Bell Inequalities testing [71], that happen to be at the heart of

[11] under the assumption that such Bell Inequalities violations can be tested in what is called the loophole-free regime which remains currently an experimental challenge in quantum communications

[12] the appropriate set-up for such a "loophole-free" test is feasible in principle, but is not available presently.

quantum theory foundations, are seemingly bound to play an important role in the future development of secure cryptographic hardware.

Let us conclude this section with a very important precision: we do not claim that quantum crypto-systems are far superior to the classical ones with respect to side-channel vulnerability. Indeed, as pointed out by Michael Nielsen [72], quantum crypto-systems are currently lacking one essential element needed in modern cryptography, namely *historical security*: one can have confidence in a crypto-system only after this system has been intensively tested, and attacked and validated by a large number of experts and users. It is clear that QKD can for example still not claim any strong historical security, since very few teams have a QKD system at their disposal and even fewer teams have tried to attack the potential weaknesses of real QKD systems. We believe that it is now time for a more systematic and wide-spread testing of QKD systems , as well as for the establishment of security standards and certification procedures. This work has already started within the SECOQC project, within the Certification sub-project [73].

## 5.2 Post Quantum Computing Cryptography

As noted in [68], "If powerful quantum computers could be built, most asymmetric cryptographic protocols in use today would no longer be secure, which would present a serious challenge for open networks and cryptographers should be prepared for this situation".

Beyond the Classical Information-Theoretic Key Establishment (CITKE) schemes discussed in 2.1, the fast-growing knowledge accumulated on Quantum Computation can be used to design new public-key schemes and study their resilience to Quantum Computing attacks. One can indeed construct classical public-key schemes based on the lattice shortest-vector problem. Such a public-key scheme is extremely inefficient in terms of performance, however, since this problem is in Quantum NP [67], it is not threatened by any potential speed-up on a quantum computer.

We believe that post-quantum computing cryptography is an extremely rich and stimulating research field, on which close collaboration between computer scientists and physicists, both interested in quantum information, will continue to be extremely fertile, as it has already proven to be over the past years.

## 5.3 Classical Cryptographic Primitives built on top of QKD networks

QKD networks as the one developed within SECOQC can be considered, from the application point of view, as a "new security infrastructure"; we also believe that it can be interesting to consider such networks from a purely theoretical point of view, as "new cryptographic primitives", allowing the distribution of unconditionally secure keys, among a network of trusted centres connected by QKD links.

It seems indeed natural to examine what new classical cryptographic protocols could be built on top of such networks, beyond global pair-wise Key Distribution. As already proposed by Louis Salvail in [63], such QKD networks could be, in the bounded quantum-storage model [79], combined with Oblivious Transfer in order to allow unconditionally secure multi-party computations. One can also study the efficiency of secret sharing schemes over such new cryptographic infrastructure. An important work has already been lead on that topic (totally independently from QKD networks considerations) [74, 75, 76, 77, 78]

This work strikingly seems to fit with the unconditional security offered by QKD networks, and powerful information-theoretic tools have been developed to guarantee the

security of such networks even when some fraction of the network nodes are corrupted. We believe that this opens promising research perspectives in the domain of unconditionally secure networks.

## 6 Conclusion

Quantum cryptography and especially Quantum Key Distribution (QKD) has triggered intense and prolific research works during the past twenty years and now progresses to maturity. QKD enables Secret Key Establishment between two users, using a combination of a classical channel and a quantum channel, such as an optical fibre link or a free-space optical link. The essential interest of QKD, that is intrinsically linked to the "quantumness" of the signals exchanged on the quantum channel, is that any eavesdropping, on the line can be detected. This property leads to a cryptographic properties that cannot be obtained by classical techniques; this property allows to perform Key Establishment with an extremely high security standard which is known as unconditional or information-theoretic security. Highly security applications are thus the natural candidates for QKD-based security solutions.

There however remain important problems to be solved. Beside the existing challenges linked to the theoretical and experimental foundations of QKD, one new horizon is now to study and demonstrate the integration of QKD into real security infrastructures. From this perspective, it is important to develop a network architecture able to fully benefit from the possibilities offered by point-to-point, distance limited QKD links. This is one of the main objective of the SECOQC project; as we have explained in this paper, QKD networks, adapted to long-distance Key Distribution, would significantly mitigate the distance limitation problem.

QKD networks are however not ubiquitous networks; they are closed, secret-key-based and distance-limited infrastructures, and their characteristics are intrinsically linked to the quantum nature of their physical layer. As a consequence, such networks fundamentally differ from classical Key Distribution infrastructures and cannot be deployed to secure open networks. We however believe that QKD networks are likely to find promising applications in high-security environments that were, up to now, relying solely on trusted couriers for Key Establishment. QKD-based systems can also be considered as an alternative to public-key-based systems for session key exchange in the context of secure networks relying on symmetric-key encryption schemes. Let us finally mention that QKD networks constitute by themselves new security infrastructures allowing information-theoretic Key Distribution over a global network. We hope that their development can be successfully combined with "classical cryptography" ideas, which will open promising avenues for advances in cryptography and network security.

## Acknowledgment

We acknowledge financial support from the European Commission through the IST-SECOQC Integrated Project.

## References

[1] www.secoqc.net

[2] Documents available on the SECOQC repository server: `https://secoqc.arcs.ac.at/COMPADV/`

[3] SECOQC Wiki, `http://secoqcwiki.knallgrau.at/index.php/Main_Page`

[4] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, *Quantum Cryptography*, Reviews of Modern Physics 74(1): pp 145 - 195, `eprint arxiv :quant-ph/0101098`.

[5] M. Dusek, N. Lütkenhaus, M. Hendrych, *Quantum Cryptography*, In: Progress in Optics, vol. 49, Edt. E. Wolf (Elsevier, 2006). `eprint arxiv :quant-ph/0601207`.

[6] K. G. Paterson, F. Piper, R. Schack, *Why Quantum Cryptography?*, Cryptology ePrint Archive: Report 2004/156. `http://eprint.iacr.org/2004/156`.

[7] www.idquantique.com, www.magiqtech.com

[8] W. Diffie and M.E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory 22 , pp 644-654, 1976.

[9] S. Babbage, D. Catalano, C. Cid, L. Granboulan, T. Lange, A. Lenstra, P. Nguyen, C. Paar, J. Pelzl, T. Pornin, B. Preneel, M. Robshaw, A. Rupp, N. Smart, M. Ward, *ECRYPT Yearly Report on Algorithms and Keysizes (2005)*, available at `http://www.ecrypt.eu.org/documents/D.SPA.16-1.0.pdf`, 26. January 2006.

[10] B. Preneel, B. Van Rompay, L. Granboulan, G. Martinet, M. Dichtl, M. Schafheutle, P. Serf, A. Bibliovicz, E. Biham, O. Dunkelman, M. Ciet, J.-J. Quisquater, F. Sica, *Report on the Performance Evaluation of the NESSIE Candidates*, Deliverable 14 from the NESSIE IST FP5 project. November 20 2001. Available at `https://www.cosic.esat.kuleuven.be/nessie/deliverables/D14.pdf`

[11] B. Preneel, A. Biryukov, E. Oswald, B. V. Rompay, L. Granboulan, E. Dottax, S. Murphy, A. Dent, J. White, M. Dichtl, S. Pyka, M. Schafheutle, P. Serf, E. Biham, E. Barkan, O. Dunkelman, M. Ciet, F. Sica, L. Knudsen, H. Raddum, M. Parker, *NESSIE Security Report*, Deliverable 20 from the NESSIE IST FP5 project. February 19 2003. Available at `https://www.cosic.esat.kuleuven.be/nessie/deliverables/D20-v2.pdf`

[12] B. Preneel, B. Van Rompay, S. B. Örs, A. Biryukov, L. Granboulan, E. Dottax, M. Dichtl, M. Schafheutle, P. Serf, S. Pyka, E. Biham, E. Barkan, O. Dunkelman, J. Stolin, M. Ciet, J-J. Quisquater, F. Sica, H.Raddum, M. Parker, *Performance of Optimized Implementations of the NESSIE Primitives*, Deliverable 21 from the NESSIE IST FP5 project. February 20 2003. Available at `https://www.cosic.esat.kuleuven.be/nessie/deliverables/D21-v2.pdf`.

[13] Secrétariat Général de la Défense Nationale, Direction Centrale de la Sécurité des Systèmes d'Information. Report 2791/SGDN/DCSSI/SDS/Crypto. *Mécanismes cryptographiques - Regles et recommandation concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robusteóse* STANDARD. 19 Novembre 2004

[14] P.W. Shor, *Algorithms for quantum computation, discrete log and factoring*, FOCS'35, 124 (1994).

[15] R.J. McEliece, *A public key cryptosystem based on algebraic coding theory*, DSN progress report 42-44 (1978), 114-116.

[16] O. Regev, *New lattice based cryptographic constructions*, in STOC'03 [70], pp. 407-416.

[17] C. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal 28 (4): 656-715, 1949.

[18] M. N. Wegman and J. L. Carter, *Universal classes of hash functions*, Journal of Computer and System Sciences, 18, pp 143-154, 1979.

[19] M. N. Wegman and J. L. Carter, *New hash functions and their use in authentication and set equality*, Journal of Computer and System Sciences, 22, pp 265-279, 1981.

[20] D. R. Stinson, *Universal hashing and authentication codes* In Joan Feigenbaum, editor, Advances in Cryptology - Crypto '91, pages 74-85, Berlin, 1991. Springer-Verlag. Lecture Notes in Computer Science Volume 576.

[21] R. Canetti, *Universally Composable Security: A New Paradigm for Cryptographic Protocols*, FOCS 2001: 136-145.

[22] D. Raub, R. Steinwandt, J. Müller-Quade, *On the Security and Composability of the One Time Pad*, Lecture Notes in Computer Science, Springer, Volume 3381 2005. SOFSEM 2005: Theory and Practice of Computer Science, pp 288-297.

[23] See for example `http://en.wikipedia.org/wiki/Timeline_of_cryptography`

[24] http://www.xilinx.com/

[25] A. Hodjat, I. Verbauwhede, *A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA* Proceedings of the 12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'04).

[26] Nicolas T. Courtois maintains a webpage on the status of algebraic attacks: `http://www.cryptosystem.net/aes/#IsAesOk`.

[27] Crypto++, 5.2.1 benchmarks, `http://www.cryptopp.com/benchmarks.html`.

[28] RSA Laboratories, *RSAES-OAEP Encryption Scheme Algorithm specification and supporting documentation*. This document is referred to, on the RSA website (`http://www.rsasecurity.com/rsalabs/`) by the following sentence: "revised version of the algorithm specification submitted to the NESSIE project, containing the latest updates on the security of OAEP". 2000. `ftp://ftp.rsasecurity.com/pub/rsalabs/rsa_algorithm/rsa-oaep_spec.pdf`.

[29] L. K. Grover, *A fast quantum mechanical algorithm for database search*, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, p. 212, 1996.

[30] C. Cachin, U. M. Maurer, *Unconditional security against memory-bounded adversaries*, In Advances in. Cryptology - CRYPTO '97, pp 292-306.

[31] U. M. Maurer, S. Wolf, *Unconditionally secure key agreement and the intrinsic conditional information*, IEEE Transactions on Information Theory, 1999.

[32] N. Gisin, S. Wolf, *Linking Classical and Quantum Key Agreement: Is There "Bound Information"?*, Proceedings of CRYPTO 2000: 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 2000.

[33] C.H. Bennet, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", *in Proc. of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 1984, pp. 175-179.

[34] S. Wiesner, *Conjugate coding*, Sigact News, 15-1, pp 78-88 ,1983. The original paper, written around 1970, had been refused for publication and remained unpublished until 1983.

[35] D. Mayers, *Unconditionnal Security in Quantum Cryptography*, J. Assoc. Comput. Math. 48, 351, 1998, `Eprint quant-ph/9802025`.

[36] P. W. Shor et J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett., 85 2000, pp 441-444 ; `Eprint quant-ph/0003004`.

[37] A. Peres, *How to differentiate between non-orthogonal states*, Phys. Lett. A, vol. 128, pp. 19, Mar. 1988.

[38] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, A. Zeilinger, *Free-Space distribution of entanglement and single photons over 144 km*, 2006. *eprint quant-ph/0607182*.

[39] C. Gobby, Z. L. Yuan, and A. J. Shields, *Quantum key distribution over 122km standard telecom fiber*, Appl. Phys. Lett. 84, pp 3762-3764, 2004. Z. L. Yuan, A. W. Sharpe, A. J. Shields, *Unconditionally secure one-way quantum key distribution using decoy pulses*, 2006 `eprint quant-ph/0610015`.

[40] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, V. Scarani, *Towards practical and fast Quantum Cryptography*, `eprint quant-ph/0411022`

[41] R. T. Thew, S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, N. Gisin, *GHz QKD at telecom wavelengths using up-conversion detectors*, New J. Phys., Vol 8, 32, 2006 `eprint arxiv :quant-ph/0512054`.

[42] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, *Experimental Quantum Key Distribution with Decoy States*, Physical Review Letters 96, 070502, 2006, `eprint eprint arxiv :quant-ph/0503192`.

[43] D. Gottesman, H.-K. Lo, N. Lütkenhaus, J. Preskill, *Security of Quantum Key Distribution with Imperfect Devices*, Quantum Information and Computation 4, No. 5, 325-360, 2004, `eprint quant-ph/0212066`.

[44] A. D. Wyner, *The Wire-tap Channel*, Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, 1975. L. H. Ozarow, A. D. Wyner, *Wire-Tap Channel II*, Bell Syst. Tech. J., vol. 63, pp. 2135-2157, 1984.

[45] I. Csiszar, J. Korner, *Broadcast Channels with Confidential Messages*, IEEE Trans. Inform. Theory, vol. IT-24, pp. 339-348, 1978.

[46] U. M. Maurer, *Secret key agreement by public discussion from common information*, IEEE Transactions on Information Theory, vol 39, pp 733-742, 1993.

[47] C. H. Bennett, G. Brassard, C. Crépeau, U. M. Maurer, *Generalized privacy amplification*, IEEE Transactions on Information Theory, vol. 41, pp 1915-1923, 1993.

[48] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, P. Grangier, *Quantum key distribution using gaussian-modulated coherent states*, Nature 421 238 2003.

[49] P.A. Hiskett, D. Rosenberg, C.G. Peterson, R.J. Hughes, S. Nam, A.E. Lita, A.J. Miller and J.E. Nordholt. *Long-distance quantum key distribution in optical fibre*, New Journal of Physics, 2006. `eprint arxiv.org/quant-ph/0607177`

[50] On the progress on SPADs, the interested reader will learn valuable information on the following webpage `http://compoundsemiconductor.net/articles/magazine/12/3/7/1`.

[51] K. Gordon, V. Fernandez, G. Buller, I. Rech, S. Cova, and P. Townsend, *Quantum key distribution system clocked at 2 GHz*, Opt. Express 13, 3015-3020 2005. eprint `arxiv.org/quant-ph/0605076`.

[52] U. Maurer and J. L. Massey, *Cascade ciphers: The importance of being first*, Journal of Cryptology, vol. 6, no. 1, pp. 55-61, 1993.

[53] R. Renner, *Security of Quantum Key Distribution*, PhD thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2005. `eprint quant-ph/0512258`

[54] C. Elliott, *Building the quantum network*, New J. Phys. 4, 46, 2002.

[55] C. Elliott and al, *Current Status of The darpa Quantum Network*, `eprint arxiv:quant-ph/0503058`, 2005.

[56] M. A. Sfaxi, S. Ghernaouti Hélie, G. Ribordy, O. Gay, *Using Quantum Key Distribution within IPSEC to secure MAN communications*. IFIP-MAN 2005 Conference Proceeding.

[57] P. D. Townsend, S. J. D. Phoenix, K. J. Blow and S. M. Barnett, *Quantum cryptography for multi-user passive optical networks*, Electronics Letters, 30, pp. 1875-1877, 1994.

[58] E. Biham, B. Huttner, and T. Mor, *Quantum Cryptographic Network based on Quantum Memories*, Phys. Rev. A, 1996.

[59] J.Cirac, P.Zoller, and H.Briegel, *Quantum Repeaters based on Entaglement Purification*, eprint arxiv :quant-ph/9808065, 1998.

[60] D.Collins, N. Gisin and H. de Riedmatten, *Quantum Relays for Long Distance Quantum Cryptography*, eprint arxiv :quant-ph/0311101, 2003.

[61] M. Dianati and R. Alléaume, *Architecture of the SECOQC Quantum Key Distribution network*, `eprint http://arxiv.org/abs/quant-ph/0610202`. Oct 2006.

[62] H. Bechmann-Pasquinucci, N. Cerf, M. Dusek, N. Lütkenhaus, V. Scarani, M. Peev, *Report on a QIT-perspective comparison of the different platforms with respect to the evaluation criteria set in phase I of* SECOQC, SECOQC deliverable D-QIT-02, Sept. 2005.

[63] L. Salvail and C. Schaffner, *Requirements for security architectures (Rough network architecture for quantum communication applied to basic scenarios)*, SECOQC Deliverable D-SEC-17, Oct. 2004.

[64] O. Maurhart, P. Bellot, M. Riguidel and R. Alléaume, *Network Protocols for the QKD network*, SECOQC deliverable D-NET-03, Oct. 2005.

[65] R. Alléaume, F. Roueff, G. Cohen, G. Zémor and N. Lütkenhaus, *Topology and cost optimization of the QKD network*, SECOQC deliverable D-NET-04, May 2006. R. Alléaume, F. Roueff, E. Diamatin, N. Lütkenhaus, *Long-Distance Quantum Key Distribution networks: cost calculation and optimal working points of individual links*, in preparation.

[66] B. Clifford Neuman and T. Ts'o, *Kerberos: An Authentication Service for Computer Networks*, IEEE Communications, 32(9) pp33-38. September 1994.

[67] D. Aharonov, O. Regev, *A Lattice Problem in Quantum NP*, Proc. of FOCS 2003.

[68] C. Cachin, D. Catalano, I. Damgård, Dittmann, C. Kraetzer, A. Lang, T. Lange, M. Näslund, P. Nguyen, E. Oswald, C. Paar, G. Persiano, B. Preneel, M. Robshaw, A.-R. Sadeghi, *Challenges for Cryptology Research in Europe for 2007-2013 and beyond*, ECRYPT Deliverable, `http://www.ecrypt.eu.org/documents/D.SPA.22-1.0.pdf`, may 2006.

[69] L. A. Adamic, *The Small World Web*, Proceeding of the Third European Conference, ECDL'99, Paris, France, September 1999.

[70] A. Acín, N. Gisin, L. Masanes, *From Bell's theorem to secure quantum key distribution* Phys. Rev. Lett. 97, 120405, 2006. `eprint arxiv.org/quant-ph/0510094`

[71] P. Grangier, *Count them all*, Nature, 409, pp 774 - 775, 15 Feb 2001.

[72] M. Nielsen, *What's wrong with those cryptosystems* `http://www.qinfo.org/people/nielsen/blog/archive/000124.html`

[73] T. Länger, S. Rass, M. A. Sfaxi, *SECOQC QBB Link Security Environment: Assumption, Threats and Policies*, SECOQC Deliverable D-CCC-03, Feb. 2006.

[74] P. D'Arco, D. Stinson, *On Unconditionally Secure Robust Distributed Key Distribution Centers*, Advances in Cryptology, Proceedings of ASIACRYPT 2002, Lecture Notes in Computer Science, Vol. 2501, pp. 346-363, Springer-Verlag, 2002.

[75] C. Blundo, P. D'Arco V. Daza, C. Padrò, *Bounds and Constructions for Unconditionally Secure Distributed Key Distribution Schemes for General Access Structures*, Theoretical Computer Science, Vol. 320, pp. 269-291, 2004

[76] S. Cimato, A. Cresti, P. D'Arco, *A Unified Model for Unconditionally Secure Key Distribution*, Journal of Computer Security, Vol. 14, N. 1, pp. 45-64, 2006.

[77] I. Desmedt, Y. Wang, *Perfectly secure message transmission revisited*, in Advanced in Cryptology, Proceedings of Eurocrypt 20002, Lecture Notes Computer Science, 2332, L. Knudsen Ed., Springer-Verlag, pp 502-517, 2002.

[78] D. Dolev, C. Dwork, O. Waarts, M. Yung, *Perfectly secure message transmission*, Journal of the ACM, vol. 40, no. 1, pp 17-47, 1993.

[79] I. B. Damgard, S. Fehr, L. Salvail, C. Schaffner, *Cryptography In the Bounded Quantum-Storage Model*, Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science, pp 449 - 458, 2005.