Quantum key distribution and cryptography: a survey[☆]

R.Alléaume[a,b,**], N. Lütkenhaus[c], R. Renner[d], P. Grangier[e], T. Debuisschert[f], G. Ribordy[g], N. Gisin[h], P. Painchault[i], T. Pornin[j], L. Salvail[k], M. Riguidel[a], A. Shields[l], T. Länger[m], M. Peev[m], M. Dianati[n], A. Leverrier[a], A. Poppe[m], J. Bouda[o], C. Branciard[h], M. Godfrey[p], J. Rarity[p], H. Weinfurter[q], A. Zeilinger[r], C. Monyk[m,*]

[a] *Telecom ParisTech & CNRS LTCI, Paris, France*
[b] *SeQureNet SARL, Paris, France*
[c] *Institute for Quantum Computing, Waterloo, Canada*
[d] *Eidgenössische Technische Hochschule Zürich, Switzerland*
[e] *CNRS, Institut d'Optique, Palaiseau, France*
[f] *Thales Research and Technology, Orsay, France*
[g] *Id Quantique SA, Geneva, Switzerland*
[h] *University of Geneva, Switzerland*
[i] *Thales Communications, Colombes, France*
[j] *Cryptolog International, Paris, France*
[k] *Université de Montréal, Canada*
[l] *Toshiba Research Europe Ltd, Cambridge, United Kingdom*
[m] *Austrian Research Center, Vienna, Austria*
[n] *University of Surrey, Guildford, UK*
[o] *Masaryk University, Brno, Czech Republic*
[p] *University of Bristol, United Kingdom*
[q] *Ludwig-Maximilians-University Munich, Germany*
[r] *University of Vienna, Austria*

Abstract

mfdsfdqfdsqdsqsqfdsq fdsq fdq fdqfdq

Contents

[☆] This document is the fruit of a collaborative effort initiated within the FP6 Trust and Security European integrated project SECOQC (IST-2002-506813). It is based for a large part on the SECOQC Crypto White Paper [1] that had been released in 2007.

[*] Project coordinator: christian.monyk@arcs.ac.at
[**] Editing author and corresponding author: romain.alleaume@telecom-paristech.fr

Dagstuhl Seminar Proceedings 09311
Classical and Quantum Information Assurance Foundations and Practice
http://drops.dagstuhl.de/opus/volltexte/2010/2361

1. Introduction

During recent years quantum cryptography has been the object of a strong activity and rapid progress [3, 4, 5], and it is now extending its activity into pre-competitive research [6] 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 [8, 9, 10, 11]. 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. Very little work has so far been published on this global issue, even though [2] should be considered as a pioneering contribution on that matter. Based on a thorough consultation and discussion among the participants of the European project SECOQC [6], this review article discusses how 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 quantum cryptography community, could emerge in the future years and try to sketch what may be the next challenges in this direction.

The logical construction of the paper is based on the idea 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 Secret Key Agreement between two users sharing an initial small secret symmetric key[1] and having access to a quantum channel (that can supposed fully accessible to eavesdroppers). QKD, that could indeed be preferably called QKA (Quantum Key Agreement), falls in the category of physical layer security cryptographic primitives.
- The second level is two-user Secure Payload Transmission built on top of a Key Agreement scheme (secure link layer cryptographic primitive).
- The third level is Secure Key Distribution over a global network composed of multiple users (network layer cryptographic primitive).

For each of these three cryptographic primitives, of increasing complexity level, we will give elements allowing to compare QKD-based solutions with the alternative solutions that are currently available, in the framework of classical cryptography. This paper is thus organized as follows: In

[1] a stronger requirement is to rely on an authenticated, but public classical channel, channel than can be obtained as soon as the two users share a small secret symmetric key [24, 25].

Section 2, we provide a survey of Secret Key Agreement 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 as well as a discussion of the possible interest of Secret Key Distribution schemes based on QKD networks. Some major design decisions of the SECOQC QKD network are then presented in section 5. Finally, in Section 6 we try to widen the scope of this review paper by discussing some future research directions that could benefit from active collaboration between the quantum and the classical cryptography communities: the study of side-channels and of material security, the study of post-quantum-computing cryptography, the use of QKD networks as a strong building block for new network security protocols and the development of unified cryptographic standards and evaluation methods for quantum and classical cryptography.

2. Secret Key Agreement

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 [94] 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 *Secret Key Agreement Problem*.

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

1. Classical Information-theoretic schemes
2. Classical computationally secure 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 Agreement problem and discuss, in each case, the type of security that can be provided. We will also consider a sixth type of Secret Key Agreement schemes: hybrid schemes built by combining some of the methods listed above.

2.1. Classical Information-Theoretic Secret Key Agreement 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.

Studying the question of Classical Information-Theoretic Secret Key Agreement (CITSKA) requires us to go back to the foundations of information-theoretic security, which builds on Shannon's notion of perfect secrecy [23]. In seminal papers, Wyner [64] and later Csiszàr and Körner [65] prove that there exist channel codes guaranteeing both robustness to transmission errors and an arbitrarily small degree of information leakage towards non-authorized parties eavesdropping on the communications performed on the channel. CITSKA is thus possible in the wire-tap configuration, as long as the legitimate users have access to a common source of randomness through classical channels that are less noisy than the channel the eavesdropper has access to [65]. The results obtained by Csiszàr and Körner generalize the framework in which CITSKA is possible: they show that whenever 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, then information-theoretic secret key agreement is possible. 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 Secret Key Agreement schemes that can exploit the ideas developed in [65] and that can be implemented within the framework of classical information theory. Such CITSKA schemes however need to rely on some specific extra assumptions, limiting the power of the eavesdropper in order to be information-theoretically secure. Christian Cachin and Ueli Maurer [36] hence demonstrated that CITSKA is possible in the bounded-storage model, in which the adversaries can only store a limited amount of data. Introducing the idea of advantage distillation, Maurer later generalized the previous models and showed that CITSKA is possible over a wide class of classical channels [66].

2.2. Classical Public-Key Cryptography and Secret Key Agreement

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 algorithms for encryption require two keys: a public and a private key, which form a key pair. Algorithms 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 needs to know a public, non-secret key, and worry about its authenticity), public-key cryptography is often referred to as asymmetric cryptography.

Secret Key Agreement based on public-key cryptography. As shown by Whitfield Diffie and Martin Hellman in 1976 [12], 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 secret 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 secret key distribution).

Security of public-key cryptography . Current asymmetric classical encryption 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 [2], and asymmetric keys of 2048 bits are preferable [13, 14]. 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 $O(n^3)$ [19]. It however seems possible to build alternative public-key cryptographic schemes on problems that are known to resist polynomial cryptanalysis on a quantum computer, such as lattice shortest vector problem [21, 93]. Such schemes are nevertheless much less practical than RSA-like schemes. This topic is at the moment actively studied, in the framework of what is called Post-Quantum Computing Cryptography [22], and we will discuss some implications of what researchers already know in subsection 6.3.

[2] 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.

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 depends 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 needed for one key exchange (essentially one RSA encryption and one decryption) take roughly 13 ms [33]. 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 [34]. Because of those relatively low exchange rates, public-key cryptography is most commonly used solely for initial secret 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 Secret Key Agreement

Symmetric-key cryptography refers to cryptography methods in which both the sender and receiver share the same secret key. Symmetric-key encryption was the only kind of encryption publicly known until the discovery of public-key cryptography in 1976 [12].

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 Secret Key Agreement. Reference [16] provides a very complete survey of classical computationally secure symmetric-key schemes.

Secret Key Agreement based on Classical Computationally Secure Symmetric-Key Cryptography . Secret Key Agreement can be realised by making use of solely symmetric-key cryptographic primitives. Indeed, the combination of a symmetric-key encryption scheme with a symmetric-key authentication scheme allows one to build a Secret Key Agreement primitive. Provided that an initial small secret key is previously shared, symmetrically, by Alice and Bob, they can use a symmetric cipher to encrypt messages. These messages (that can consist of random bit strings or not) will constitute the next keys that can thus be shared securely between Alice and Bob. The initially shared symmetric key material can be used to symmetrically compute (on Alice's side) and check (on Bob's side) a message authentication tag, and thus guarantee the authenticity of the newly distributed secret keys. As we shall see, only $\log n$ bits of secret keys are necessary to authenticate n bits of messages in this context, therefore, only small initial secret keys are needed. Since Secret Key Agreement based on symmetric-key cryptographic primitives always relies on pre-established (small) symmetric secrets, needed for authentication one has to call such Secret Key Agreement schemes *Secret Key Expansion* schemes more than *Secret Key Establishment* schemes.

Security of Classical Computationally Secure Symmetric-Key-based Secret Key Agreement . The security of Secret Key Agreement based on classical symmetric-key cryptography depends on the security of the cryptographic primitives that are used, and on the composability of those cryptographic primitives. Shannon has proven that there is no unconditionally secure encryption scheme which requires less encryption key bits than the One-Time Pad [23]. This has a fundamental implication: the number of bits of the encryption key needs to be at least as large as the entropy (in bits) of the message to be encrypted if one wants to build an unconditionally secure scheme. Hence, if we consider the possibility of building an unconditionally secure symmetric key expansion scheme, i.e., a method to symmetrically generate secret keys out of a short initial symmetric shared secret key, the former results from Shannon imply that such a scheme is impossible to achieve in the framework of classical cryptography. However, as we shall see in subsection 2.4, such a cryptographic primitive is possible in a quantum cryptographic context.

It is however possible to use classical symmetric-key encryption and authentication schemes, that are not unconditionally secure, to build a Secret Key Agreement 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 "provably computationally security" (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[3]). 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 [16, 14].

There are no publicly known efficient quantum attacks on classical symmetric-key cryptographic schemes 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 [35]. The complexity reduction offered by Grover algorithm is only polynomial (as opposed to the super-polynomial complexity reduction offered by Shor algorithm), and this implies that doubling the key size of would be enough to maintain (against quantum computers) the level of algorithmic complexity one currently has today (against classical computers) for symmetric-key primitives.

Performances. In terms of performance, symmetric-key classical cryptography is much faster and less computational intensive than asymmetric cryptography[4]. In terms of speed, there are now 128-bit AES encryptors able to encrypt data at rates in the Gbit/s range [30, 31]. 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 there exists no better way to break a symmetric-key cryptographic scheme is exhaustive search within the key space (assumption that will be discussed in more details in subsection 3.3) then, a symmetric key of 103 bits is roughly comparable, in terms of computational requirements, to a RSA key modulus of 2048 bits [14]. 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 [13, 14] for details).

2.4. Quantum Key Agreement - Quantum Key Distribution (QKD)

Quantum Key Distribution, invented in 1984 by Charles Bennett and Gilles Brassard [39], based on some earlier ideas of Stephen Wiesner [40], is an quantum cryptographic alternative solution to the Secret Key Agreement 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, irrespectively of the computing power or any other resources that may be used, including quantum computers [41, 42, 69]. 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 [43]. 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 [66] and to its extensions, triggered by the new possibilities offered by the advances in quantum information science [67] and [69].

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

[4] the difference is indeed of several orders of magnitude, see [17] for references and details.

[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.

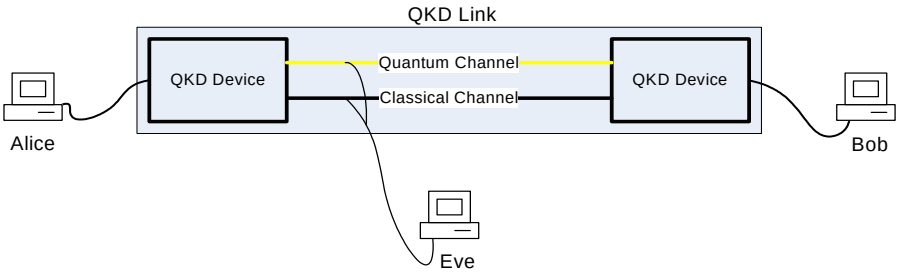

Figure 1: Structure of a QKD link as it is referred throughout this article

Without going into the details of the different implementations or protocols (one can consult Refs [3, 4, 5] for an extensive overview on that point) 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[6]. 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 Secret Key Agreement technique that requires, as initial resources, a public quantum channel and an authenticated public classical channel. As discussed in [2, 119] and also in sections 3 and 4 , there are different ways to obtain an authenticated public channel. If one wants to stay in the paradigm of information-theoretic security even for the authentication, then Alice and Bob need to share, in advance, a short secret key (whose length scales only logarithmically in the length of the secret key generated by a QKD session [24, 25, 26, 27]). Hence, QKD, operated in this regime, is a symmetric unconditionally secure Secret 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 initialization of the system (initial distribution of small secret authentication keys), authentication is not a burden for the global performance (secret bit rate per second) of QKD schemes. 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 has been 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 intelli-

[6]Note that a quantum channel can always been used as a classical channel, when restricted to convey orthogonal quantum states, so without loss of generality, only a quantum channel is "materially speaking" needed

gence, or defense. 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 one of the methods 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 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 can be used as a Secret Key Agreement protocol.
- Like QKD, TCKD needs some initial trust in the relative identities of Alice and Bob. Moreover, like for QKD, this necessary initial trusted authentication can be handled via different techniques, such as the pre-distribution of a secret key (such as a password), or the use of an unforgeable (or at least reputed to be such) public identity certificate issued by a trusted third party (such as as the seal that was used by emperors and kings or the signed certificates we now use for public keys).
- Like QKD, TCKD is a technique that currently finds its application when classical Secret Key Agreement schemes are believed not to offer enough security guarantees.

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) traveling 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, that can moreover efficiently handle key management issues. On the other hand, reliability and cost of TCKD infrastructures are critical problems and there is no real hope that such systems can ever be automated, leading to serious key management issues and very high operational costs.
- 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 secret keys "on demand" to the end users, which is fundamentally different from relying on keys stored on the very same DVD, that could be duplicated at any later point in time if some adversary manages to break the protections around the storage device.

2.6. Cascaded schemes and 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 Secret Key Agreement 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 *Cascaded 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 out by Maurer and Massey, [68], the first encryption layer, i.e. the one directly applied to the message, is in all cases the most important one.

[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.

Dual Secret Key Agreement. This idea of Cascaded Cipher can straightforwardly be applied to Secret Key Agreement: two keys of the same length are established through two Secret Key Agreement 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 Secret Key Agreement*. Note that more than two Secret Key Agreement schemes, of various types, can in principle be combined this way. We will restrict, in the following to a discussion of Dual Secret Key Agreement involving QKD as one of the Secret Key Agreement technique.

The approach of Dual Secret Key Agreement could for example be beneficial when combining keys established through one CITSKA scheme and keys established through QKD: breaking the entire Secret Key Agreement scheme implies breaking the CITSKA scheme *and* breaking QKD. If one has doubts about the security of QKD, the Dual Secret Key Agreement procedure guarantees that the security will at least not be worse than that of the classical Secret Key Agreement technique with which it is combined. The same is true if one has doubts about the security of Secret Key Agreement scheme based on classical cryptography. However, while there already exist security standards in classical cryptography (for example FIPS 140 [72], or Common Criteria [73]), there are not yet such standards for QKD. The approach of Dual Secret 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. However, as we shall see in subsection 6.2, the certification of quantum crypto-systems is a topic on which work is already being initiated [70, 71] and we can hope to have FIPS-140 or Common Criteria certified QKD systems within a few years.

3. Securing a point-to-point classical communication link by combining QKD with symmetric encryption

QKD is a Secret Key Agreement primitive that can be realized solely at the physical layer level. In the previous section, we have compared QKD to the other existing solutions for Secret Key Agreement. We will now analyze how the secret keys established by QKD can be used to perform a link layer cryptographic task: securing the data sent on a classical communication link, by relying solely on the keys generated by QKD (plus some initially shared small secret authentication keys) and on symmetric-key cryptographic primitives.

More formally, we consider here the problem of securely transmitting classical messages (payload) from Alice to Bob via the following generic protocol:

1. Establishment of a symmetric secret key $K_S = K_{encrypt} \cdot K_{auth}$ between Alice and Bob ($X \cdot Y$ stands for the concatenation of string X with string Y).
2. Secure and authentic transmission of the message M over the classical channel, with symmetric-key cryptographic primitives: M is encrypted with encryption key $K_{encrypt}$ and authenticated with the authentication key K_{auth}.

After a brief subsection about the performances of QKD devices we will analyze several declinations of the generic scenario described above, in which QKD is used as the Secret Key Agreement primitive over a point-to-point link, while different types of encryption and authentication schemes are used.

3.1. Performance of QKD link devices: recent progresses

QKD systems are being developed with an increasing reliability and with increasing performances, and the SECOQC project [6], gathering many of the most prominent experimental and theoretical European teams involved in QKD research, has actively contributing to the pursuit of this progression that is indeed carried out also on an international level [45, 47, 44, 51, 48, 50, 49, 52, 54, 59, 53, 55]. One can currently expect to exchange up to 1 Mbits of secret key per second, over a point-to-point QKD link of 20 km [51]. The maximum span of QKD links is now roughly around 100 km or even 140 km [51, 48] (depending on the type of single photon detector that is used) at 1550 nm on a telecom dark fiber[8]. Both secret bit rate and maximum reachable distance

[8] somehow surprisingly, a comparable maximum span has also been reached in the context of ground-to-ground free space QKD [44]. This experiment was successfully realized with a quantum channel whose losses were one order of mag-

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[9]. It is important to notice that QKD systems can now basically be built with optimized, 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, as detection methods are making significant progresses [57, 58, 59, 51, 48, 55]. Another approach, known as "Continuous Variables QKD" (CVQKD), and also implemented in SECOQC, uses only standard PIN photodiodes, but requires more sophisticated data processing in order to extract the secret keys [56]. Within the duration of the SECOQC project, significant progresses, on the theoretical [60] as well on the implementation side [50] have been achieved for CVQKD. Moreover, further advances on the protocol side may allow CVQKD systems, that were known to be able to deliver high bit-rate but only for small or medium losses on the quantum channel, to become suitable for long-distance, high-bit rate QKD [49].

3.2. 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 formally proven thanks to the fact that the security of QKD can be expressed in the framework of Universal Composability [28]: unconditionally secure Secret Key Agreement, realized by QKD, cannot be distinguished from an ideal Secret Key Agreement protocol interacting with some environment. This implies that QKD can be composed with any other universally composable unconditionally secure cryptographic primitive, while still guaranteeing the unconditional security of the whole cryptographic scheme [69].

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 [24, 25, 26]. 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 [29].

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 the SECOQC project has chosen to work, as described in subsection 5.

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.

As pointed out in [119], long-term security is needed in many specific application scenarios, such as the protection of medical records, industrial secrets and military or governmental classified informations. However, offering long-term security for highly sensitive data is not something that can be guaranteed by today's computationally secure schemes. Indeed, as written in [14], "beyond approximately 10 years into the future, the general feeling among ECRYPT partners is that recommendations made today should be assigned a rather small confidence level, perhaps in

nitude larger than what we expect them to be in the framework of space-to-ground communications. It thus has paved the way towards QKD between a satellite and a ground station [54]

[9] and it will always lag behind in terms of rate and distance. However, since current optical networks are now reaching capacity in the Petabit/s range, there definitively remains some room - and thus reasons to hope - for improvements.

particular for asymmetric primitives". As a matter of fact, it is important to note that when one deals with the transmission of encrypted information, an adversary can always store the ciphertext and wait for the decryption until better cryptanalysis methods become available (for example more efficient algorithms for factoring or the discovery of an efficient way to attack AES) or better cryptanalysis hardware (indeed large quantum computers would be very efficient for breaking most of the asymmetric encryption primitives in use today). The recommendation of ECRYPT is indeed to consider using One-Time-Pad encryption for high-security levels, "provided the key management can be solved" [14]. In this perspective, the combination of QKD with One-Time-Pad, which provides a practical solution for unconditionnally-secure data transmission over a point-to-point link (solution that can indeed be extended in the context of networks, see section 4) seems to be a natural response to meet some of the most stringent requirements within high-security communication infrastructures: long-term security.

3.3. QKD composed with a classical computationally secure symmetric encryption scheme: Key security and Key Ageing

Here we will consider one very frequent use case: QKD is used for Secret Key Agreement between two users placed on each side of a point to point QKD link. Link encryption is then realised with a computationally secure symmetric encryption scheme (such as AES) in order to be able to encrypt large rates of classical data over the link layer. This solution is indeed the one that is currently adopted by all the commercial QKD vendors: IdQuantique, MagiQ and SmartQuantum [7] and it was also the solution adopted within the BBN Darpa Quantum Network project [80]. 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 [81, 82]

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.

The last two factors are purely dependent on the encryption technique and not at all on the Key Agreement scheme. The security implications (and the security level) associated with the choice of a given symmetric cipher, with a given key modulus length is discussed in detail in [16, 13, 14]. In the ECRYPT Yearly Report on Algorithms and Keysizes published in july 2008 [14], a symmetric key modulus of 128 bits is recommended for long-term security (while 256 bits is recommended for a good protection of symmetric ciphers against a quantum computer).

The first two factors, on the other hand, are influenced by the choice of the Secret Key Agreement scheme: the security of the key is intrinsically linked to the security of the Secret Key Agreement scheme while the key renewal rate also strongly depends, on a practical level (hardware performance, security policy, implementation details, etc.), on the Key Establishment scheme. We will discuss in the following whether QKD-based schemes, used in replacement of traditional Key Agreement schemes, present an interest with respect to these two factors, and thus where QKD-based key renewal can lead to an improvement of the overall security of a computationally-secure, symmetric-key, encrypted communication link.

3.3.1. Security of the key

As explained in section 2, the Secret Key Agreement scheme can be of different types, but QKD is the only existing and practically implementable 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. All the other alternative Secret Key Agreement schemes, based on computationally secure symmetric-key or public-key primitives, cannot offer the same security guarantee regarding the security of the keys that will be used for encryption and authentication.

Of course, as previously discussed, QKD has to rely on some initial trusted material in order to allow the initial authentication of the classical communications that is needed to perform Secret Key Expansion with unconditional security (see subsection 2.3 for more details). The security of the keys will inherently be derived from this trust that can consist in previously shared small secret keys (distributed by an initial "rendez-vous" between Alice and Bob, or by a Trusted Courier) or in a trusted third party and the use of public-key cryptography. In this section, we consider a link layer scenario, based on symmetric-key cryptography and thus assume that authentication is guaranteed by the pre-distribution of a small symmetric key between Alice and Bob. We will discuss in the next section, how the constraints attached to this requirement can be mitigated in a network context and indeed even married with public-key cryptography. A recent article [119] also discusses the issue of authentication and QKD with great clarity, answering some of the claims expressed earlier in [8]. The book of Gilles Van Assche [2] also contains an extremely valuable discussion about the question of authentication in QKD.

3.3.2. Key renewal rate

When one considers the global security level one can obtain on a communication link, there is also a second factor that can as well indirectly depend on the Secret Key Agreement 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 ? To give elements of answer to this question, we will consider the practical example that corresponds to what current QKD vendors are selling: combining QKD-based Secret Key Agreement with AES, in order to make a link encryptor.

- A practical example: key renewal for AES encryption

Let's first take the example of fast DES Xilinx encryption systems that are currently commercialised [30]. 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 some block ciphers (including AES operated in Cipher Block Chaining mode or in Accumulated Block Chaining mode or DES) such as known plaintext attacks based on the birthday paradox, when the number of blocks encrypted with the same key reaches $2^{\mathrm{blocklength}/2}$ [16] [10]. In the case of DES 56-bit keys, this would occur after $2^{7.5} \simeq 3$ minutes.
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 [30] and for which "dedicated research hardware" has recently demonstrated a rate of 21.54 Gbit/s [31]. 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. It seems thus important to question this assumption and study what can be said about the influence of the encryption key renewal rate on the security of AES. As we shall see in the next paragraph, this complex question is indeed intrinsically linked to the security assumptions one can make on AES itself.

- Security of AES: confronting the different assumptions to what we currently know

The cryptanalysis of encryption schemes like AES is a difficult topic that is still subject to very active research and it seems realistic to think that the ultimate difficulty of such cryptanalysis is currently not known.

The actual status is however that there exist no known breaks of AES. More precisely, if one considers the problem of finding the secret key used in AES, and has access to a large number N

[10] This is because one only require $2^{\mathrm{blocklength}/2}$ ciphertext to obtain a matching pair of ciphertexts with probability $> 1/2$.

of couples of blocks of known cleartext / ciphertext, there is no published attacks known to be more efficient than attacks based on exhaustive search on the key space (for AES, such exhaustive search starts to have a non-negligible chance of success only if the number of trials is comparable or greater than 2^{64}.

For block ciphers, the practical security depends in particular on the number of rounds applied when encrypting one block (see [16] for details). Even though AES is thus believed to be secure (and is currently a standard whose use is recommended even for institutions dealing with high-security: for example AES128 is considered sufficient up to the SECRET level, while AES192 or AES256 is required for TOP SECRET [79]) it is already known that weaker versions of AES, with reduced numbers of rounds, can be attacked successfully by strategies that require less computational efforts than exhaustive search. As explained in the security report of the IST FP5 program NESSIE (NESSIE Deliverable D20) [16], 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.

Some cryptographers also claim that powerful algebraic attacks could break AES based only on a very small number of known cleartext / ciphertext [32]. However, algebraic attacks have never been successfully demonstrated on AES and are not regarded as a real threat by the majority of the classical cryptography community. We indeed quote the ECRYPT 2008 report [14] on the question of algebraic attacks: "While issues remain somewhat opaque, the AES cannot currently be considered vulnerable to such analysis".

Finally, as also noted in [14], security aspects of implementation(s) of the AES are probably the most pressing issues. Indeed as first established thanks to the pioneering work of P. Kocher at the end of the 1990's [77, 78], one can exploit physical properties of crypto-systems (and in particular the so-called "physical side-channels", through which information about secret keys is leaking while cryptographic computations are being conducted) to mount extremely powerful on those crypto-systems. The first efficient attacks to be studied were passive attacks based on monitoring the execution time and then the power consumption of classical cryptographic devices (whose implementations ultimately rely on the use semiconductor logic gates and thus of transistors) [77, 78]. The variety of side-channel attacks and of counter-measures has gradually expanded since then and one can for example consult the Side Channel Cryptanalysis Lounge ECRYPT for a good overview of what is already known[76].

Such attacks are of course only possible as long as the opponent can observe the signals associated with the side-channels, it thus implies that the opponent has a certain degree of physical access to the crypto-systems he wants to attack. This last remark is of particular interest when we consider the combination of QKD with AES to perform link encryption: since current QKD devices need to be installed in trusted environments, on both end of the quantum and classical channels (that are allowed to be fully untrusted), then it is logical to assume that the AES encryptors are also placed inside the same trusted environments and thus protected against side-channel cryptanalysis. However, in the general case (and especially considering the large variety of application scenarios that can be imagined, based on a QKD network such as the one demonstrated at the end of the SECOQC project, cf. 4), the environment in which Secret Key Agreement is performed does not need to be the environment in which the AES encryption can take place (indeed, AES encryption on a smartphone connected to the SECOQC QKD network has been demonstrated as one potential use case of QKD networks [70]).

- Combining QKD with AES encryption: what can we say about the influence of the key renewal rate ?

If AES is considered perfectly sure, then the limit of $2^{\text{blocklength}/2}$ blocks after which the keys have to be renewed in order to avoid collision-related problems is in practice not a problem, and one cannot justify the need to renew the AES keys as often as a QKD can allow to do it [11].

However, as we have seen in the previous paragraphs, there exist arguments, based on some known algorithmic cryptographic weaknesses of reduced versions of AES, that indicate that it

[11] with 13 kbit/s of secret bit rate, one could renew more than 100 AES128 secret keys per second

could be beneficial for the global security of AES encryption to refresh the secret keys after a number of blocks that is significantly smaller than $2^{\mathrm{blocklength}/2}$, which could indeed lead to a need to renew keys with a periodicity of the order of a few minutes.

Indeed, if we consider in addition the existing vulnerabilities of AES implementation to side-channel attacks, then the requirements on key renewal rate become even more stringent: state-of-the-art DPA attacks (Differential Power Analysis attacks, that do not disrupt at all the encryption process) can successfully break unprotected AES implementations after the acquisition of 100 power traces, while roughly 50000 power traces are needed to break protected implementations of AES. Even dedicated and protected hardware implementations of AES can thus be broken in a few minutes with DPA (see [75] for details). Moreover, if one allows attacks based on fault injection in the circuit, then a full break of AES128 has been obtained in a few seconds, with only 2 pairs of correct and faulty ciphertext [74]. This result indicates that, in the context of embedded systems where trust in the environment cannot be guaranteed, very fast key renewal can become a necessity when one wants to guarantee the security of AES and thus of the entire scheme[12].

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 [6], that has culminated by the demonstration of information-theoretically secure key distribution over a fiber-based telecom metropolitan area network in Vienna, Austria, in october 2008 [116].

We will begin this section by an overview on the different generic QKD network architectures that have already been proposed. We will then present some elements of comparison between QKD networks and classical network, for the purpose of network-wide Key Distribution.

4.1. QKD network architectures

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.

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 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.

[12]This necessity is likely to be justified operationally when one wants to guarantee a relatively high security level even on embedded systems, however there are alternative ways (already actively explored) to tackle this issues, such as the development of algorithmic and hardware counter-measures to make systems more to side-channels attacks [76]. Our point is that QKD-based key renewal could also be an option worth considering, in combination with the other efforts already in order to strengthen the security of systems that use AES encryption in non-trusted environments

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 [83]. 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 [80, 81] 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[85] can overcome the loss problem and can be used to form an effective perfect quantum channel [84]. 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 [86], 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 repeater 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 repeater nodes 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 repeaters 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 a network is indeed precisely the one discussed in 3.2, and the message sent is a random session key by one of the end-users (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 repeaters 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*[13].

4.2. Classical Network Key Distribution Schemes and QKD Networks: Elements of comparison

4.2.1. Key Establishment Rate

As we have seen in 3.3.2, some security requirements related to current block ciphers such as AES could motivate the need to refresh secret keys of such ciphers over times shorter than a minute. Although this is possible in practice with current technology, relying on Diffie-Hellman and PKIs, such key renewal rate policies are very seldom (if not never) enforced and the key renewal period

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

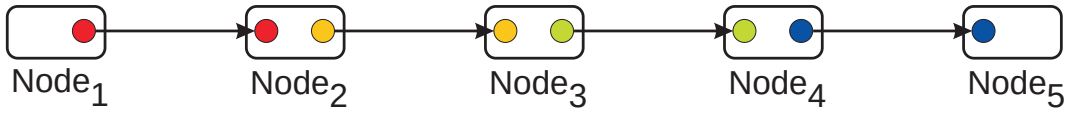

Figure 2: "Hop-by-hop" unconditionally secure message passing on a path made of trusted relay nodes connected by QKD links. Message decryption / re-encryption is done at each intermediate node, by using one-time-pad between the local key, distributed by QKD, K_{local}, and the secret message M resulting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

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 [14] 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 [8], QKD rates, as we have mentioned earlier, are currently reaching several hundreds kbit/s for metropolitan distances. This implies that QKD networks could typically allow to refresh thousands of 128-bits AES keys per second, over VPN links in a metropolitan network. This means that QKD networks, when used as a security enabler of other network applications, could compare rather favourably, at least from a pure "Key Establishment rate point of view" with respect to asymmetric cryptography and PKIs.

4.2.2. Network Initialization and Key Pre-distribution

Secure networks always rely on some initial trust in order to be able to provide some security guarantee. As discussed in 2.4, a pair of initial small secrets or an authenticated classical channel is necessary to initialize a QKD link. We now consider the question of network initialization and key pre-distribution for symmetric-key-based and asymmetric-key-based secure networks and compare it with the requirements of QKD networks. Indeed, as noted in [119], we also argue that the combination of asymmetric-key (for key pre-distribution) and QKD presents some specific interests.

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 [92] rely on classical symmetric-key cryptography and on a single trusted center).

Key Pre-Distribution over QKD networks:. As pointed out in [8], 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. Initialization 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 "initialized" 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.

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

PKI Initialization. PKI is the most commonly employed system for Key Distribution over open networks. PKI trust relations are materialized by certificates, i.e. signatures of public-keys and these trust relations can be organized 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 initialized, and the only way to perform such an initialization is indeed the use of another PKI (of higher hierarchy) or the use of secret couriers. In this sense, the initialization of a QKD network and the initialization of a PKI are two problems that share some similarities.

Interest of PKIs for QKD Network Initialization. As pointed out in [8], QKD networks however present a security advantage over PKIs when we consider the initialization 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 initialized). If no active attack on authentication has been performed *before* the first -potentially vulnerable[15]- 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 initialization*, with no restriction on how the adversary's capabilities may evolve in the future. Such keys could therefore be used to realize 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 initialization (which requires secret couriers and can be a difficult key management problem in the case of large networks).

4.3. Open networks versus trusted QKD networks

As pointed out in [94], "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 initialize 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. Indeed, as we shall discuss in 6.3, the practicality of asymmetric cryptography and its suitability for open networks may have as a counterpart the existence of stronger vulnerabilities to cryptanalysis (vulnerabilities that moreover are not restricted to quantum-computer-based cryptanalysis). This situation implies that the use of asymmetric cryptography is somehow more risky that the use of symmetric primitives when one wants to guarantee long-term security.

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 described as "small worlds", where physical signals can be regenerated, data can be copied and

[15] the vulnerability we consider here would stem from weaknesses of asymmetric cryptography

distances are almost abolished [95] , 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 [91, 112].

5. Demonstrated QKD Networks, with a focus on the SECOQC QKD network design

The first QKD network demonstrator, the "DARPA Quantum network", has been deployed between Harvard University, Boston University and BBN in 2004 [80, 81]. It relied on the concept of trusted repeater QKD network described in 4.1, and also demonstrated optical switching on the quantum channel to allow one to two connectivity.

The concept of truster repeater QKD network has also been used within the SECOQC QKD network [87, 114, 116].The focus of the SECOQC project was to contribute to scientific and technical achievements leading to "long-range high security communications based on quantum key distribution". As explained above, combining this objective with the constraints of today's technology imposes to rely on an architecture based on classical trusted repeater nodes. An important choice however lies in the network protocols and logical architecture allowing to use the QKD link-specific local keys in order to secure long-distance traffic. The SECOQC consortium has 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 [87] and in [114, 115, 116]. The main originality of the SECOQC project, with respect to previous QKD networks, relies on the fact that it has opted for a *dedicated key distribution network infrastructure* called "network of secrets" [90]. 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 layer protocols and can be considered somehow independently from the quantum key establishment processes and from the key requests that arise from applications running on top of the network of secrets. This architectural design implies that the SECOQC 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. These functionality have indeed been demonstrated, as describedd in [116]. The focus of SECOQC has moreover been put on what has been called "Backbone QKD networks", i.e., QKD networks exhibiting a high connectivity and a meshed topology [89, 90]. As explained in [89, 91], 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 Secret Key Agreement over disjoint pathes [89, 113, 117, 116].

The central design issue behind the SECOQC 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 local Secret Key Agreement and on unconditionally secure cryptographic primitives to allow network-wide key distribution, it offers an unprecedented overall security even for long-distance communications. 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 have also shown that this assumption can be partially relaxed to the case of Trusted Repeaters QKD networks where some nodes may be corrupted [113, 117].

6. Future directions

6.1. 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. We indeed discussed in 3.3.2 the fact that passive attacks have proven to be extremely efficient to break even protected implementation of AES [75]. Indeed all classical cryptographic primitives (public-key-based and symmetric-key-based) that we have considered in this document are vulnerable to side-channel attacks [16]. There is 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 [94].

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 [4], of its counter-measure (Decoy-State QKD) [61, 62], of Trojan-horse attacks of various sorts [4], of QKD

implementations based on imperfect devices [63], and etc. [5]; 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 ones 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 [3], one can [16] 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 [96]. 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 [41, 42]. 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. Based on this idea, it has been recently shown [118] that one can propose and prove the security of some so-called "device-independent quantum cryptography" schemes, where the influence of *all* the possible side-channels of QKD hardware is taken care of within the security proof. The derivation made within Ref. [118] indeed demonstrates that side-channel-resistant positive secret key rate could be obtained in practical QKD systems, provided one is able to violate Bell Inequalities in the loophole-free regime[17]

It is by essence impossible to extend such side-channel-resistance properties to 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 [97], that happen to be at the heart of quantum theory foundations, are seemingly bound to play an important role in the future development of secure cryptographic hardware.

6.2. Cryptographic certification of quantum crypto-systems

Even though we have argued that a quantum perspective on physical side-channels can be promising, we however do not claim that current quantum crypto-systems are superior to the classical ones with respect to side-channel vulnerability. Indeed, as pointed out by Michael Nielsen [98], 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 current QKD implementation cannot claim any kind of 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. Some pioneering work has however been initiated in

[16] 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

[17] the appropriate set-up for such a "loophole-free" test and thus of device-independent QKD is feasible in principle, but is not available presently.

the direction of testing implementation vulnerabilities of quantum crypto-systems already some years ago [106] and this line of research is currently gaining momentum [107, 108].

We indeed 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 [99]. Moreover, an industry standardization group on QKD based on the outcome of the SECOQC project has been launched in October 2008. It is hosted by the European Telecommunications Standards Institute (ETSI), and shall bring together the important actors from science and industry in order to converge towards industry standards for QKD, including standards concerning the cryptographic certification of QKD hardware implementations.

6.3. Post Quantum Computing Cryptography

As noted in [94], "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[21]. Building a public-key scheme on such a problem would be extremely inefficient in terms of performance, however, since one can find lattice problems in Quantum NP [93], public-key crypto-systems that would derive from it would not be threatened by any potential speed-up on a quantum computer.

There also exist other classical public-key crypto-systems, that are conjectured to resist quantum computers such as the NTRU encryption system [18], or the McEliece encryption system, based on coding theory [20]. Note however that even though there exist no known quantum algorithm able to attack efficiently these last two problems, neither NTRU or McEliece public-key are proven to be difficult problems (of super-polynomial complexity) on a quantum computer. Indeed, as noted in [110] the question of whether the complexity classes related to mathematical problems are ultimately different on a quantum computer than what they are classically remains essentially an open question. There are even some indications leading to partially answer negatively to this question: as demonstrated in [109] oracle methods can be used to give evidence that the complexity class NP is not included in BQP (which contains the problems that can be considered as efficiently solvable on a quantum computer). This last result, even though it does not constitute a definitive proof, nevertheless indicates that the classical problems of asymmetric cryptography that are currently known to be efficiently solvable on a quantum computer (RSA, discrete logarithm, elliptic curve cryptography, etc.) could indeed also be relatively easy on a classical computer, and thus could already be seriously at stake *today* (and not only when large quantum computers would be developed).

Post-quantum computing cryptography is thus an extremely important and stimulating research field, not only for the cryptography of tomorrow, but also for the cryptography of today. We believe moreover that this field is an ideal opportunity for close collaboration between computer scientists and physicists, both interested in quantum information, and that such research will continue to be extremely fertile, as it has already proven to be over the past years [22].

6.4. 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

[18] algorithm presented as an alternative to RSA and whose security is claimed to be related to solving shortest vector problem in a high-dimensional lattice [111]. However, the security of NTRU is still not considered as well established

Salvail in [89], such QKD networks could be, in the bounded quantum-storage model [105], 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) [100, 101, 102, 103, 104]

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.

7. Conclusion

QKD is currently the only known cryptographic technique that has lead to secret key agreement protocols for which the unconditional security can be formally established. Since the first QKD protocol, BB84, proposed 25 years ago [39] , prolific theoretical and experimental research work has been conducted. Quantum cryptography has rapidly become an established academic topic within quantum information science, while QKD technologies have continuously moved forward in terms of performance and reliability.

The significant progresses achieved through the coordinated collective efforts of the consortium of partners in the European project SECOQC and materialized by the final live demonstration of the real QKD network deployed in the city of Vienna [116] have set an important milestone on the road towards the industrialization of QKD. Indeed, one of the main collective achievements of SECOQC has consisted in developing protocols, dedicated hardware and software, all compliant with an original architecture based on the "network of secrets" concept, and to demonstrate that it allows the integration of QKD into real security infrastructures.

The QKD community is nevertheless aware that the acknowledgement of these advances by security experts and by leading classical cryptographers is likely to play a key role in the development dynamics of a QKD industry and cannot be taken for granted. We therefore hope that the skepticism expressed by some of the opinion leaders of the security industry[8, 9, 10, 11] can gradually evolve into a more positive attitude, based on scientific discussions and confrontation of ideas.

The main objective of this article was thus to discuss the applicability of QKD to some network security scenarios and to present use cases where we believe that QKD can present advantages with respect to the current existing solutions based on classical cryptography. We thus explained that it could be interesting to use QKD in many different scenarios, ranging from data encryption over a point-to-point link to security applications running over large networks with many users. For all of these scenarios, we believe that the search of long-term security, that cannot really be guaranteed by today's cryptographic techniques, will be the driving reason to develop QKD-based alternatives.

Acknowledgment

We would like to thank collegially all the partners of the SECOQC project for the numerous stimulating discussions about many of topics that are tackled in this article. R. A. wants to thank Gilles Van Assche for his extremely valuable and important help on improving the article, and in particular subsection 3.3. R. A also thanks Sylvain Guilley, Philippe Hoogsvorst and Jean-Luc Danger from enlightning discussions about side-channel attacks on cryptographic hardware and about what is possible in terms of countermeasures. We acknowledge support from the European Union under project SECOQC (IST-2002-506813). R. A. and A. L. acknowledge support from Agence Nationale de la Recherche under projects PROSPIQ (ANR-06-NANO-041-05), SEQURE (ANR-07-SESU-011-01) and COQC (ANR-08-EMER-003).

References

[1] R. Alléaume (editing author), J.Bouda, C. Branciard, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, A. Leverrier,N. Lütkenhaus, P. Painchault, M. Peev, A. Poppe,

T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, A. Zeilinger and C. Monyk, *SECOQC white paper on quantum key distribution and cryptography*, January 2007. `eprint arxiv: quant-ph/0701168`

[2] G. Van Assche, *Quantum Cryptography and Secret-Key Distillation*, Cambridge University Press 2006.

[3] 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`.

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

[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, M. Peev, *The Security of Practical Quantum Key Distribution*. `eprint arxiv: quant-ph/0802.4155`

[6] www.secoqc.net

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

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

[9] B. Schneier, Crypto-Gram: Quantum cryptography, December 2003.
URL `http://www.schneier.com/crypto-gram-0312.html#6`

[10] B. Schneier, Schneier on Security: Switzerland protects its vote with quantum cryptography, October 2007.
URL `http://www.schneier.com/blog/archives/2007/10/switzerland_pro.html`

[11] B. Schneier, *Quantum cryptography: As awesome as it is pointless.*, Wired, October 2008.
URL `http://www.wired.com/politics/security/commentary/securitymatters/2008/10/securitymatters_1016`

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

[13] 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.

[14] S. Babbage, D. Catalano, C. Cid, O. Dunkelman, C. Gehrmann, L. Granboulan, T. Lange, A. Lenstra, P. Nguyen, C. Paar, J. Pelzl, T. Pornin, B. Preneel, C. Rechberger, V. Rijmen, M. Robshaw, A. Rupp, N. Smart, M. Ward, *ECRYPT Yearly Report on Algorithms and Keysizes (2007-2008)*, July 2008.
URL `www.ecrypt.eu.org/ecrypt1/documents/D.SPA.28-1.1.pdf`

[15] 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`

[16] 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`

[17] 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`.

[18] 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

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

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

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

[22] D. J. Bernstein, J. Buchmann, E. Dahmen, editors. *Post Quantum Cryptography*, Springer, 2009.

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

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

[25] 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.

[26] 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.

[27] M. Peev, M. Nölle, O. Mauhardt, T. Loruenser, M. Suda, A. Poppe, R. Ursin, A. Fedrizzi, A. Zeilinger, *A novel protocol-authentication algorithm ruling out a man-in-the middle attack in quantum cryptography*, International Journal of Quantum Information 3, 225 (2005). `eprint: quant-ph/0407131`.

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

[29] 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.

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

[31] 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).

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

[33] Crypto++, 5.5 benchmarks, `http://www.cryptopp.com/benchmarks-p4.html`, May 2007.

[34] 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`.

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

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

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

[38] 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.

[39] 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.

[40] 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.

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

[42] 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`.

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

[44] 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*.

[45] 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`.

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

[47] 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`.

[48] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel and H. Zbinden, *High speed coherent one-way quantum key distribution prototype*, `eprint arxiv: quant-ph/0809.5264`, September 2008.

[49] A. Leverrier and P. Grangier *Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation* `eprint arxiv:0812.4246`, December 2008.

[50] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, P. Grangier, *Field test of a continuous-variable quantum key distribution prototype*, eprint arxiv:0812.3292, December 2008.

[51] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, *Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate*, Opt. Express 16, 18790-18979, eprint arxiv:0810.1069, October 2008.

[52] A. Treiber, A. Poppe, M. Hentschel, D. Ferrini, T. Lorünser, E. Querasser, T. Matyus, H. Hübel, A. Zeilinger, *Fully automated entanglement-based quantum cryptography system for telecom fiber networks*, eprint arxiv:0901.2725, January 2009.

[53] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, Ch. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, *Experimental demonstration of free-space decoy-state quantum key distribution over 144 km*, Phys. Rev. Lett. 98, 010504 (2007). eprint arxiv: quant-ph/0607182

[54] J. M. Perdigues Armengol, B. Furch, C. Jacinto de Matos, O. Minstera, L. Cacciapuoti, M. Pfennigbauer, M. Aspelmeyer, T. Jennewein, Rupert Ursin, T. Schmitt-Manderbach, G. Baister, J. Rarity, W. Leeb, C. Barbieri, H. Weinfurter, A. Zeilinger, *Quantum communications at ESA: Towards a space experiment on the ISS*, Acta Astronautica, Volume 63, Issues 1-4, July-August 2008, Pages 165-178. Electronic version available at http://dx.doi:10.1016/j.actaastro.2007.12.039

[55] A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, *Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization*, Opt. Express 16, 11354-11360 (2008). eprint arxiv: quant-ph/0805.2193

[56] 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.

[57] 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

[58] 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.

[59] L. Ma, T. Chang, A. Mink, O. Slattery, B. Hershman, X. Tang, *Experimental demonstration of an active quantum key distribution network with over Gbps clock synchronization*, IEEE Communications Letters, Vol. 11, No. 12, P.1019, December 2007.

[60] R. Renner, J. I. Cirac, *A de Finetti representation theorem for infinite dimensional quantum systems and applications to quantum cryptography*, September 2008, eprint arxiv.org/quant-ph/0809.2243.

[61] W.-Y. Hwang, *Quantum key distribution with high loss: toward global secure communication*, Phys. Rev. Lett. 91, 057901-1-4 (2003).

[62] 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.

[63] 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.

[64] 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.

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

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

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

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

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

[70] `http://www.sequrenet.fr`

[71] `http://www.quantumworks.ca/section/view/?fnode=49`

[72] see `http://csrc.nist.gov/groups/STM/cmvp/standards.html#02` for the FIPS 140 official documents.

[73] see `http://www.commoncriteriaportal.org/`

[74] C. H. Kim, J.-J. Quisquater, *New Differential Fault Analysis on AES Key Schedule: Two Faults Are Enough*, CARDIS 2008.

[75] S. Tillich, C. Herb, *Attacking State-of-the-Art Software CountermeasuresÑA Case Study for AES*, CHES 2008.

[76] ECRYPT, The Side Channel Cryptanalysis Lounge, available at `http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html`

[77] P. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, pp 104Ð113, CRYPTO 1996.

[78] P. Kocher, J. Jaffe and B. Jun, *Differential Power Analysis*, Lecture Notes in Computer Science, Vol. 1666, Pages 388 to 397, Springer-Verlag, Berlin, Heidelberg, 1999.

[79] Lynn Hathaway, *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information* available at `http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf`, (June 2003).

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

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

[82] 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.

[83] 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.

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

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

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

[87] M. Dianati and R. Alléaume, *Architecture of the SECOQC Quantum Key Distribution network*, The First International Workshop on Quantum Security, Guadeloupe, Jan 2007. `eprint: quant-ph/0610202`.

[88] 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.

[89] 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.

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

[91] 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.

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

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

[94] 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.

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

[96] 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`

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

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

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

[100] 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.

[101] 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

[102] 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.

[103] 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.

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

[105] 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.

[106] A. Vakhitov, V. Makarov, and D. R. Hjelme, *Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography*, J. Mod. Opt. 48, 2023 (2001).

[107] V. Makarov and J. Skaar, *Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols*, Quant. Inf. Comp. 8, 0622 (2008).

[108] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, H.-K. Lo, *Experimental demonstration of time-shift attack against practical quantum key distribution systems*, Physical Review A, 78, 042333 (2008). `eprint arxiv.org/quant-ph/0704.3253`

[109] C.H. Bennett, E. Bernstein, G. Brassard and U. Vazirani, *Strengths and Weaknesses of Quantum Computing*, SIAM Journal on Computing, 26, pp 1510-1523, (1997).

[110] D. Simon, *On the Power of Quantum Computation*, SIAM Journal on Computing, 26, pp 1474-1483 (1997).

[111] `http://www.ntru.com/`

[112] R. Alléaume, F. Roueff, E. Diamanti, N. Lütkenhaus, Topological optimization of QKD networks, `eprint arxiv: quant-ph/0903.0839`, 2009.

[113] L. Salvail, M. Peev, E.Diamanti, R. Alléaume, N. Lütkenhaus, T. Länger, *Security of Trusted Repeater Quantum Key Distribution Networks*, J. Computer Security 2009 (to be published).

[114] M. Dianati, R. Alléaume, M. Gagnaire, X. Shen, *Architecture and Protocols of the Future European Quantum Key Distribution Network*, Security and Communication Networks, 1, 57, 2008.

[115] M. Dianati, R. Alléaume, *A Transport Layer Protocol for the SECOQC QKD Quantum Key Distribution Networks*, The Third IEEE LCN Workshop on Network Security (WNS 2007), Dublin, Ireland, Oct. 2007.

[116] M. Peev et al. (40 authors or so.), *The SECOQC quantum key distribution network in Vienna — In preparation*, 2009.

[117] T. R. Beals, B. C. Sanders, *Distributed Relay Protocol for Probabilistic Information-Theoretic Security in a Randomly-Compromised Network*, In the proceedings of the Third International Conference on Information Theoretic Security (ICITS) 2008, Reihaneh Safavi-Naini editor, Lecture Notes in Computer Science 5155 Springer 2008. `eprint arxiv: quant-ph/0803.2919`.

[118] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, *Device-independent security of quantum cryptography against collective attacks*, Phys. Rev. Lett. 98 2305001 (2007). `eprint arxiv: quant-ph/0702152`

[119] D. Stebila, M. Mosca, N. Lütkenhaus, *The Case for Quantum Key Distribution*, `eprint arxiv: quant-ph/0902.2839`