Introduction to Quantum Key Distribution

Vicente Martin*[1], Jesus Martinez-Mateo†[1], and Momtchil Peev‡[2]

[1]Center for Computational Simulation, Universidad Politécnica de Madrid, 28660 Boadilla del Monte, Madrid, Spain
[2]Quantum Communication & Computation Lab, German Research Center, Huawei Technologies Duesseldorf GmbH, Munich, Germany

August 15, 2016

Abstract

Quantum Key Distribution is a cryptographic primitive that allows for exponential growing of an initial key, shared among the end-points of a quantum channel: a communications channel over which quantum signals can be transmitted. Its security can be derived from the laws of quantum mechanics, which allow to prove the Information Theoretic Security of QKD . In this entry the process and specific characteristics of QKD are discussed. This includes the meaning of the "absolute security" character that is usually ascribed to QKD, its limitations and practical implementation.

keywords: security, cryptography, cyphering, symmetric key, quantum key distribution, quantum safe cryptography.

1 Introduction

Quantum key distribution (QKD) is a part of *quantum cryptography*. It describes a set of protocols that allow the growing of an initial secret key, known only to the two parties taking part in the communication, into a larger one. Under reasonable assumptions, the information leakage to the outside world of the newly created bits can be bounded as tightly as desired, thus providing a mechanism to securely create symmetric keys. Beyond the correct execution of the protocol, the assumptions are limited to the physics of the implementation: (i) the parties devices do not leak information to the outside world (i.e., there is a security perimeter), a common requirement on any cryptosystem,

*vicente@fi.upm.es
†jmartinez@fi.upm.es
‡momtchil.peev@Huawei.com

(ii) both parties have access to a source of true randomness, e.g., an adequately implemented quantum random number generator (QRNG), and (iii) the laws of quantum mechanics as we know them are universally valid, and thus pose a restriction on any potential adversaries [1]. In this sense, QKD security is based on the laws of physics. QKD protocols are then absolutely secure in a mathematically provable way, something that we will address more precisely below. No conceivable attack, classical or quantum, could ever break the system, whatever the resources used. This is in contrast to other modern protocols dedicated to key distribution which base their security on mathematically unproven assumptions. A prime example is the widely used Diffie-Hellman protocol which derives its security from the computational difficulty of solving the discrete logarithm problem. If, however, the computational complexity turns out to be lower than assumed, then the algorithm would become useless and any Diffie-Hellman transaction could be deciphered, including those recorded in the past. In fact, the standard computational complexity assumption on this problem does not hold in the quantum world. A quantum computer would be able to break Diffie-Hellman and other widely used protocols such as RSA and elliptic curve cryptography by using Shor's algorithm [2, 3]. The algorithms that can be performed using a quantum computer with an advantage over their classical counterparts are the subject of *quantum computing*. Classical algorithms that are developed to be resistant to Shor's algorithm, or in general to quantum computing, are the subject of *post-quantum cryptography*.

QKD protocols require the ability to create, manipulate, transmit and detect signals at the quantum level. This makes for an extremely demanding technology, although the wait was not very long for a real world realization. It was first implemented in the lab as a proof of concept in 1989 [4] and, as early as 2002, it was already a commercial product [5]. Since then it has been implemented in real settings many times, including in classical communication networks, and there are several companies that sell QKD devices in the security market.

The main differences of QKD with the equivalent (i.e., symmetric key) algorithms in conventional cryptography is the fact that it solves in an unconditionally secure way (under the above mentioned assumptions) the problem of secret key agreement. QKD does this, however, at the expense of using a quantum channel —a communication channel able to transport quantum correlations— connecting the two parties, that has to be physically implemented. It also requires an authenticated and integrity preserving classical channel, but this can be easily provided in today's communication infrastructures. In contrast, the conventional way of distributing secret keys requires just an algorithm (e.g., Diffie-Hellmann) running on a computer and a readily available classical communications channel. From a cryptographic point of view, a pair of QKD systems can be regarded as a seeded, distributed and correlated source of randomness with the added guarantee that only a bounded amount of information, that can be made as small as desired, is leaked outside the security perimeters of the two legitimate parties. Another way to see this is as an extension of the security perimeter of the two parties' devices to the communications line connecting both.

From an information theoretic security (ITS) perspective QKD is an enabling build-

ing block (subroutine) needed to transmit secrets with absolute security, serving as an input to the one time pad (OTP), an algorithm that encrypts data with the same level of security by encoding one bit of information with one bit of fresh random key. For this reason QKD is customarily denoted to be an absolutely secure or ITS primitive.

Note that in both cases, quantum and conventional, the requirement of having a security perimeter surrounding the apparatus must be met. This implies that in practice, some assessment on how realistic this assumptions is must be provided. The security perimeter restricts the ability of an attacker to gain information and this must be understood not only as his ability to, for example, breach a physical enclosure, but also to not have access to side channels that can reveal information, like electromagnetic emission from the device or the existence of correlations among several quantum degrees of freedom such that measuring one can give information about the other. Side channels and incorrect implementations, apart from misuse, have been the most usual source of security leaks in cryptosystems [6, 7]. Since they can depend on very specific details, newer implementations are not necessarily better and the resiliency of a given system, demonstrated by its continuous use without security breaches, is often sought when deciding on a security system. To assess the security of a system in practice, there are third party certification organization that test the systems under well defined specifications looking for implementation weaknesses. QKD systems have the ability to factor out complete subsystems (e.g., detectors [8–10]) from being a part of a side channel by testing them to check if there are still enough hidden quantum correlations allowing an adversary to gain information on the secret key. Side channels have also been found in QKD systems, similar to the case of conventional crypto devices. Whereas for the latter there are specifications and testing procedures defined for third party testers to check whether a given implementation meet certain security criteria [11], in the quantum case these are still in development [12].

Finally, with current technology, there is a maximum tolerable absorption beyond which no secret key can be extracted. The propagation medium, be it free space (air or vacuum), optical fiber or passive optical components in a network, absorbs or modifies the quantum signals and this is indistinguishable from the action of an eavesdropper. Thus, after some distance or after crossing a few network components, the signals are either lost or tainted with too much errors to allow for the extraction of any secret key. In spite of a very remarkable progress in this respect, this limit is very unlikely to be raised beyond a few hundreds kilometers or, equivalently a few tens of dB [13]. The only way to overcome distance limitations is through quantum repeaters [14], devices that allow the distillation of quantum correlations over unlimited distances. Much work on these devices has been done, but the production of practical and efficient quantum repeaters, although less complex than quantum computers, is likely many years away. They would allow for a fully quantum internet, able to provide services beyond the capabilities of stand-alone QKD. Digital quantum signatures, not unlike RSA does today, will be among these services. It is to be noted that, since QKD is a symmetric key protocol, implying that exactly the same information is known to both parties, it is not possible to sign a document without the intervention of a trusted third party. Note, it has been proven that

ITS asymmetric quantum cryptography that does not rely on the trust in third parties is impossible [15]. However, asymmetric quantum primitives have been developed that ensure security against an adversary who has bounded or noisy quantum memory [16].

The rest of the entry is organized starting with a historical perspective of QKD, that precedes the description of the physical part of a QKD protocol, including its security and physical limits. The prepare and measure protocols will be the ones primarily considered. In these protocols, quantum signals are prepared by the emitter, one per time slot, and then sent for measurement to the receiver end. The original BB84 protocol will be described in detail and then, to exemplify the disparate implementations of QKD, an entanglement based protocol and a Continuous Variables protocol will be also discussed. To give a general idea of how this is implemented in real devices, a sample physical implementation will be described followed by a description of QKD operation in networks. Finally, we will describe the last part of every QKD protocol. This is the post-processing step that distills a secure key out of the already measured quantum signals. It is a very important part that is often disregarded, although it is critical to attain good performance in practice. Here we will describe Cascade, the best known algorithm for error correction in QKD, and also new algorithms derived from information theory ideas. The contribution finish with a description of the privacy amplification part. This is the last post-processing step. Its purpose is to bound the information that an eavesdropper might have due to the non-zero error rate that a real world implementation always has.

2 History

Inspired by the early 1970's ideas of Stephen J. Wiesner about quantum money, later published in 1983 [17], quantum key distribution emerged from the seminal work by Charles H. Bennett and Gilles Brassard, who first coined the term quantum cryptography in a contribution to the Crypto 82 conference [18]. In 1984 they published the first QKD protocol [19]. Presented the year before during their talk at the 1983 IEEE Symposium on Information Theory, where the term quantum key distribution was first used, this protocol came to be the well known Bennett-Brassard 1984 (BB84) protocol. The original work did not receive much attention, until it was implemented in practice five years later [4]. Although a crude proof of principle lab implementation over a distance of merely 32.5 cm, it kick started the broad interest in the field. The work of Bennett and Brassard, however, went well beyond. Of particular relevance to QKD was their work on secret key post-processing: the set of necessary classical procedures that transform the raw measurements of the quantum signals into a usable secret key through information reconciliation and privacy amplification [20–22].

Shortly after, many experiments were carried out and the field advanced steadily. The distance increased from a few kilometers to a few hundreds out of the lab in field installations using optical fiber. The secret key throughput grew from a few bits to a few Mbps. Network demonstrators showed the feasibility of the technology in networks as early as 2005 in the DARPA network in Boston [23]. In 2008 a breakthrough network was demonstrated in Vienna [24], using many different kinds of QKD links. Similar

networks where shown in Tokyo in 2010 and 2015 [25, 26]. Specialized networks showing the long term robustness of the technology [27] and the compatibility with commercial, passive network equipment and shared classical/quantum optical fiber links in a metro area was demonstrated in 2009 [28]. As of 2016 there are very ambitious networks being deployed. The Battelle network in USA [29] plans to deploy links of up to 700 km. The China network [30], from Hefei to Beijing will link five metropolitan area networks in a backbone of 2000 km of length. The UK Quantum Communications hub [31], will be deployed from Bristol to London and Cambridge.

In experiments based on transmission of light over the air (the so called "free space" QKD), the length of the link has gone from the few centimeters of the Bennett and Brassard 1989 experiment to the 148 km of the link between two of the Canary islands in 2007 [32] that demonstrates the feasibility of a ground to space link. The distance was doubled in the same place just a couple of years later [33] using a double link between the islands. Currently China has unveiled plans to set up a space link [34].

This spectacular progress has been mirrored by some commercial success, and there are currently several vendors of QKD equipment (ID Quantique, Quintessence, Qaskey) and many of the major companies and laboratories worldwide have demonstrated equipment or are actively developing the technology (NEC, Toshiba, Huawei, ...).

After the initial 1989 implementation, important theoretical advances contributed to establishing the QKD field. Notably, the publication by Arthur Ekert of a QKD protocol based on entanglement in 1991 [35], that came to be called E91, and the unconditional security proofs [36]. Entanglement designates the non-classical correlations that arise in quantum theory when two (or more) physically distinct entities (e.g., photons) are described by a non-separable function (i.e., that cannot be written as a direct product of functions describing each physical entity). According to the measurement postulate in quantum theory, this leads to correlated outcomes when the relevant properties of the entities are measured, although they could be physically separated to the extent that the two measurement events might be separated by a space-like interval (using the relativistic term meaning that these events cannot causally influence each other as a signal must travel quicker than the speed of light to "inform" one measurement event of the outcome of the other). This strange phenomenon, that shows the non local nature of quantum mechanics, was highlighted by Einstein, Podolski and Rosen in their famous 1935 paper [37], in which they presented objections to the then new quantum theory. It raised a controversy that has only recently been settled in favor of the quantum mechanical view. The E91 protocol, although equivalent in the end to the BB84, makes direct use of entanglement. The introduction of entanglement in QKD protocols provided new insights that led to concepts like the quantum repeater [14], a device subject of intense research that would eventually allow for an unlimited range quantum network, as was pointed out above.

3 Overview of a QKD protocol

A QKD protocol requires (see Fig. 1) a quantum channel, capable of transmitting the quantum signals —typically embodied in qubits: physical systems that can be described by a complex Hilbert space of dimension two— and a classical channel to transmit classical information "bits" connecting the two legitimate parties participating in the protocol. Both channels are public and it is assumed that they can be manipulated by any attacker at will. The only requirement is that the classical channel is authentic and integrity preserving, i.e., any legitimate party can identify with certainty if a (classical) message originates from the other legitimate party and that it has not been changed. This can be achieved using classical algorithms known to be information theoretically secure [38, 39], thus this requirement does not reduce the security of the protocol. Information theoretically secure authentication and integrity, however, requires utilization of fresh key at each communication round. To this end, initial key must be shared between the legitimate parties. This is usually done at installation time. Once the first set of new key material is generated, part of it is reserved for the next round of authentication without reducing the security of the protocol.

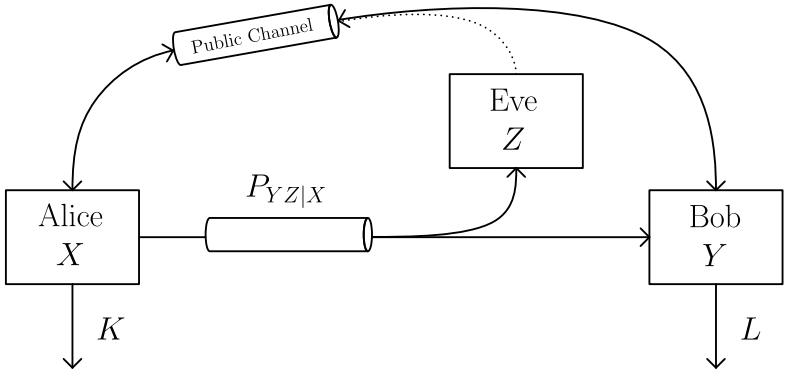

Figure 1: The process of growing a key between the two end points of a quantum channel, here labeled Alice and Bob, requires not only the quantum channel, depicted in the figure as a probability distribution $P_{YZ|X}$ (i.e., the probability that the outcome of a measurement by Bob is Y and that of the spy (Eve) Z if the emitter, Alice, sent X.) but also a public and authenticated and integrity preserving classical channel. This is required so that in the postprocessing steps (see Section 5) the secret key K can be extracted from the string L having the certainty that both are the same and the original signals come from the real Alice and not from a faked one. Eve can extract information from both, classical and quantum channel. The (ITS) classical authentication and integrity of the messages in the public channel forbids Eve to modify it, whereas there is no restriction on the manipulations that Eve can do in the Quantum one.

QKD protocols come in equivalent pairs that either use entanglement or not. In the latter case, the emitter (that typically goes by the name of Alice) encodes the information in a quantum state embodied in a single physical object (e.g., a photon). The object is then sent to a receiver (named Bob). This mode of operation is known as a prepare and measure protocol. In this kind of protocols, the presence of an attacker is detected by

monitoring the unavoidable perturbation introduced as a consequence of the properties of the measurement process in quantum mechanics. If entanglement is used, then the information emerges in the correlations of the measurement results of the two legitimate parties. The entangled quantum state itself is distributed to the two (or in some cases more) participants. This entangled state can be prepared by a source external to either Alice or Bob and could even be a device produced by an attacker, who, however, cannot get any extra information from this fact. In this case, the attacker is detected as his activity would lead to a deterioration of the mentioned measurement correlations (a check can be carried out by, e.g., testing the Bell inequalities).

4 The physical part of a QKD protocol

For simplicity in what follows we will consider prepare and measure protocols. A QKD device produces quantum signals in a known and precisely defined state belonging (in most protocols) to a finite dimensional Hilbert space. Here we will concentrate mainly on the case in which individual quanta are used to code the information, the so called discrete variables case, in which most implementations work. The typical dimension of the Hilbert space in this case is two, hence we speak about qubits. The qubits will encode the information that allows the creation of the secret key. The creation and manipulation of the qubits must be such that no extra correlations among them or any additional degrees of freedom of the signal emitted by the QKD device are introduced. In this way, no information gain on one qubit can be obtained by measuring the signal by some non-perturbative measurements.

4.1 The security of a QKD Protocol

The security of a QKD protocol is entrenched in the fundamental laws of quantum physics. Any adversary action is in itself a measurement process applied to the quantum system of the signal and it inescapably disturbs the system itself. Alternatively, the Heisenberg uncertainty principle states that variables that do not commute (conjugate variables) cannot be measured simultaneously: An information gain on one of the variables implies information loss on the other. The no-cloning theorem [40] establishes the unusual property —from a classical point of view— that an unknown quantum state cannot be perfectly copied and therefore an attacker cannot simply save a copy of a by-flying quantum state and get later the same input as the legitimate receiver [41].

Using these principles, it is possible to build a protocol that, by encoding the information at the quantum level, is able to detect any modification on the information of quantum carriers, thus factoring out any attempt to extract information by a third party. Thus, at least ideally, QKD can be proven to be *unconditionally secure* meaning that any adversary is powerless to break it irrespectively of his resources. It is of utmost importance to note that the fundamentals come from the properties of the physical world, not from computational complexity assumptions, thus guaranteeing security no matter the computational capabilities of the attacker.

The unconditional security of the protocols based on these intuitive ideas has been first formally proven by Mayers in 1996 for the BB84 protocol [42]. Other proofs followed, notably the one due to Shor and Preskill [43] is well known for its connections to quantum error correction. Below we give a rough overview of QKD security, following [36].

The starting point of any (quantum) adversary is to get some quantum state in the process of her eavesdropping, generically bringing some auxiliary state of her choosing —an ancilla— to interact with the quantum signal during the transmission of the latter.

Historically, the notion of security originally revolved around the assumption that the adversary measures this state after the protocol has finished. She gets some knowledge on the key, and the legitimate parties should be able to reduce at will the measure of this information —the accessible information— to an arbitrarily small number, denoted traditionally by ϵ. To do so, they utilize the quantum mechanical fact that by increasing her information, the attacker also increases the transmission error on the quantum channel. So they observe the transmission channel error, assuming "paranoically" that any disturbance is due to an adversarial activity, and correspondingly reduce the key generation rate, factoring out the eavesdropper's information and limiting it to a desired bound ϵ. The reduction factor monotonously increases with error, yielding no secure output above some error threshold. The reduction process employs classical ITS primitives, discussed below (see subsection 5.2 on Privacy Amplification). The key of Alice and Bob is thus ITS, "unconditionally secure" or ϵ-secure.

Meanwhile cryptographers had realized that a sound security is "composable" security. Generically a cryptographic primitive (algorithm) is composably secure if it is completely independent on the context of its application and not interdependent with the specific set of algorithms it is used with. Indeed a composably secure primitive can be used as a standard security building block, in contrast to the case when the security of each application as a whole needs always to be proven from scratch. For key generation composability simply means that the key remains secure (is not leaked) irrespective of the encryption method.

In the case of QKD it was noticed that accessible information based proofs lack composability. In fact it is the requirement on the adversary to **measure** at the end of the key generation process that potentially can weaken the security proof. The eavesdropper can in principle retain his quantum state, choose to measure later on, during transmission of the encrypted communication, and for some old style security proofs, indeed break the combined security application (QKD + encryption).

It was realized that it is the attacker's state that must be ϵ-near, in terms of Hilbert space distance, to an ideal target state (the latter can yield no information on the key whatsoever). This condition, together with the requirement that Alice and Bob can arbitrarily reduce the probability of not sharing a common key, while believing to do so, as well as the probability that their QKD protocol outputs no key when there is no disturbance on the quantum channel, is the objective of a QKD security proof in the modern sense. A protocol that can be demonstrated to satisfy this objective, outputs composably ϵ-secure key.

Fortunately, it has been shown that the secure key generation rate in the old- and

new-style proofs coincide in the "asymptotic regime", i.e., in case a single key generation run generates infinite amount of key. As this is naturally impossible, it is practically important to estimate precisely by how much the key rate needs to be reduced, as a function of the length key output of a single protocol run, to remain composably ϵ-secure. This is the goal of the study of the so called "finite size effects" that is still an object of analysis for different types of QKD protocols.

4.2 Physical limits of QKD

The most significant limit for QKD in the foreseeable future is imposed by the attenuation in the propagation medium used by the quantum channel, which limits the maximum achievable distance with a practical secure key rate. The typical carrier of quantum signals in QKD are states of light (photons) and the propagation media is either air —termed free space QKD— or optical fiber. Since the secrecy of the key is guaranteed by the detection of any modification of the emitted qubits, any change has to be ascribed to a potential attacker, following the "paranoid" approach discussed above. Whenever the error rate is beyond the limits that guarantee that some secret information can be extracted from the set of received signals, the QKD system is no longer useful. In practice, this is even more restrictive, since getting close to the error threshold has a dramatic effect on the achievable secret key rate due to the postprocessing step (Section 5), further reducing the throughput to a level that is not useful for practical purposes.

The intensity of signals that propagate in homogeneous media like (in first approximation) air or optical fiber, suffer an exponential attenuation with the length. Typically such transmitting media present a variable attenuation as a function of the wavelength of the light. Free air propagation has a clear optical window where attenuation is low, from ≈ 300 to about ≈ 1100 nm. The best wavelength in optical fiber is around 1550 nm, where absorption is as low as 0.2 dB/km. In the end, together with the fact that signals sent need to be weak (below some intensity threshold) to be quantum, this means that there is a limit to the maximum achievable distance of a QKD system. Still there have been significant experiments demonstrating the transmission and detection of quantum signals over 300 km [44] and of QKD systems working over distances of $\approx 250 - 300$ km [45, 46]. These, however, employ technology that is presently difficult to deploy in a commercial setting (e.g., special low loss fibers or superconducting detectors) and were designed more to demonstrate state of the art technological capability rather than commercial availability. In Fig. 2, a typical curve of achievable secret key rate is shown. The exponential decrease of key rate with distance (absorptions) and the final drop, due to the high error rate, that precludes the distillation of secret key, are clearly seen. The best current practical QKD systems using fiber have a loss budget of around 30 dB, meaning that they are able to create key in the order of tens of Kbits per second over distances of around 100 km in optical fiber. Remarkable free space experiments spanning distances from 150 to 300 km, designed primarily to demonstrate the feasibility of a ground to satellite link, were performed in 2007 [32, 33].

High tolerance to losses has been achieved in modern QKD systems mainly through

the improvements of detectors. Most of the detectors used are avalanche photo diodes (APDs). APDs work in Geiger mode: the semiconductor crystal is subject to a voltage, usually during a short period of time (gated mode) such that an incoming photon ejects an electron from an atom, the electron is accelerated in the electric field and gets enough energy to remove more electrons from other atoms, thus producing an avalanche that is finally detected. Then the detector is quenched to remove all the free charge. This mode of operation has several shortcomings: On one hand, the voltage is adjusted to a level that can easily trigger the avalanche, but this can also remove an electron from an atom without an incoming photon, thus producing a false count also referred to as *darkcount*. On the other hand, an electron from a previous cascade that has not been fully dissipated will produce an avalanche as soon as the voltage is applied again, also without an incoming photon, referred to as *afterpulse*. The usual solution to avoid the latter problem has been to leave some time without applying any voltage pulse to the crystal. It was not unusual to use values for this so called dead time of the order of a hundred microseconds, thus limiting the maximum possible effective signal detection rate to the order of few Kbps. New methods to limit the accumulation of charge in the crystal [47, 48] and discriminating the probability that a given avalanche comes from previously accumulated charge [49] have improved greatly on this magnitude, allowing for detectors working in the Gbps range.

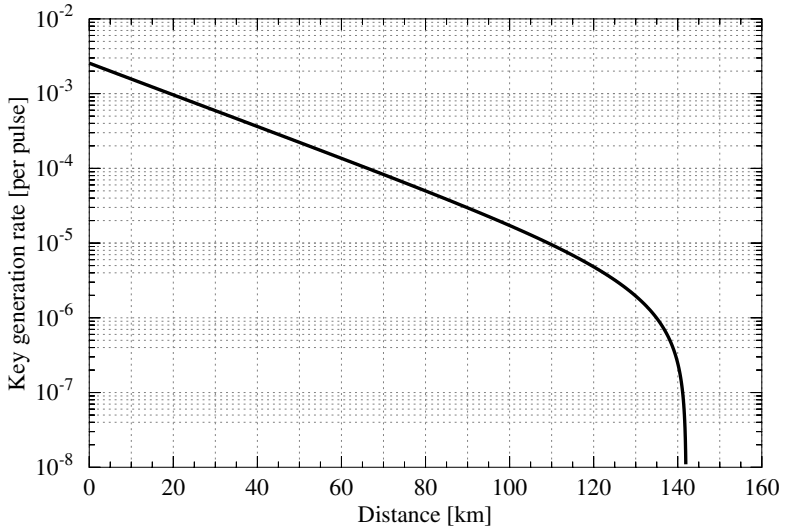

Figure 2: Typical secret key rate (per pulse) of a QKD system as a function of the length of the optical fibre (equivalently, losses, with a conversion of 0.2 dB per Km) connecting the emitter (Alice) with the receiver (Bob). Note the exponential decrease of the secret key and the final collapse, due mainly to reaching a point where the high QBER (Quantum Bit Error Rate, see Section 5) implies that the possible leakage of information to an eavesdropper is too high and that key distillation is not possible anymore.

Real single photon on demand sources, as required by the original QKD protocol designs, have been harder to produce. Typical QKD systems have resorted to the use of

weak coherent pulses. A laser pulse is attenuated to a level such that it carries only one (or less) photon on average. In practice this means that about 90% of the pulses carry no photon and also that about 5% of the pulses carry more than one photon. Although, in principle, lasers can be pulsed at a very high frequency, thus compensating for such a low efficiency, there is a limit to this because the detector has to wait for the arrival of a possible photon in the same time interval, so that it must be opened at the same frequency and thus increasing the probability of having counts without a photon actually arriving. Furthermore, the existence of multi photon pulses must be taken into account in the key distillation phase, since these can render the system completely insecure, adding another source of inefficiency. The production of single photons on demand at the wavelengths needed by QKD systems is currently an active research field.

Even in the case in which perfect emitters and detectors exist, attenuation will eventually set a hard limit that cannot be beaten. With the current fiber infrastructure, practical limits will be in the order of just a few hundreds of kilometers. To go to unlimited distance requires either quantum repeaters [14], or trusted intermediate nodes [24]. The former, as already mentioned are devices that can forward the information encoded in the qubit without actually measuring or copying it. Thus without additional disturbance, implying without information leakage. The latter are devices that measure the qubit —hence destroying it and gaining full information, thus the trust requirement— and then repeating the same protocol with either the receiving end or with another trusted repeater. Quantum repeaters are the subject of intense research, but their feasibility in practical networks has yet to be demonstrated.

4.3 The original protocol

The BB84 was the first QKD protocol devised. To encode the bits of information, it uses qubits prepared in two mutually non-orthogonal bases, that act as conjugate variables: A measurement in one produces an indeterminacy in the other. In the typical arrangement, the angle between the bases is $\pi/2$. Assuming that there is no interaction with the environment, the measurement of a bit encoded in a qubit prepared in one of the two base states in one of the two basis has a probability $1/2$ of producing the correct encoded value when measured in the other base and $1/2$ of producing the wrong value. This pairs of basis are called conjugate after the work of Wiesner [17]. When the qubit is measured in the same base than the used for its preparation, the measurement will always produce the correct value.

Following the original proposal, that used the polarization as the degree of freedom in which to encode the information, we will call "R" —rectilinear— to the first polarization basis, for which an arbitrary direction in space is chosen and "D" —diagonal— to the second basis, rotated $\pi/4$ from the chosen direction. The two basis states for each of the 2-dimensional Hilbert space will be also chosen orthogonal. We will use these states to encode the logical "0" and "1". Following the standard notation in quantum mechanics, we will denote $|0\rangle_R$ and $|1\rangle_R$ to the basis states in the rectilinear base and, analogously, $|0\rangle_D$ and $|1\rangle_D$ in the diagonal base. When we analyze, for example, the state $|0\rangle_R$ in the rectilinear base (e.g., by using a polarization filter oriented according to the base) we will

get as a result the logical "0" with certainty (using a perfect apparatus and assuming no decoherence, i.e., noise). The same will happen with the rest of states whenever the preparation and measurement basis are the same. If they differ, no information is obtained at all: measuring the same $|0\rangle_R$ state in the diagonal basis will produce either a "0" or a "1" with equal probability.

With this element one step of the quantum part of the BB84 protocol is executed as follows. As it is customary, Alice is the emitter and Bob the receiver.

- Alice draws a random bit to encode.
- Alice draws a random bit to choose between the "R" and "D" basis.
- Alice encodes the chosen bit in the chosen basis and send the resulting qubit to Bob using the quantum channel.
- Bob draws a random bit to choose the measurement basis.
- Bob measures in the chosen basis the incoming qubit.

In absence of any source of decoherence in the quantum channel and with perfect preparation and measure, the protocol would require only a further step in which Bob posts, using the classical, public but authenticated and integrity preserving channel, the basis that he used to measure all the received signals. Then Alice would report back, using the same channel, the time slots in which she used the same basis. With this, it would be guaranteed that in these time slots the bits encoded by Alice would be the same than the bits read by Bob, thus having the same string of randomly produced bits.

Obviously, in a real setting, there are sources of error. Either the noise or an eavesdropper would introduce errors. Since they cannot be distinguished, all of them have to be attributed to a possible attacker. This makes necessary to further continue the protocol with the key distillation phase, a classical post-processing part that includes error correction and privacy amplification steps. During the error correction step, an estimate of the errors in the quantum channel is obtained. This QBER, Quantum Bit Error Rate, is the crucial magnitude that guides the process since it directly affects the amount of secret key rate. Beyond a certain threshold QBER it is not possible to distill a secret key. The important subject of key distillation will be treated in the next section.

In Fig. 3 the original published table with the execution of 15 rounds is displayed. The following postprocessing steps are not shown.

4.4 Other protocols

While the BB84 protocol has historically been the first one, different classes of protocols have been proposed and demonstrated later on. Most of these rely on single photon signals, or more realistically, on approximations thereof by means of weak coherent pulses. These are then called "discrete variable protocols".

As we have already mentioned, each discrete variable protocol is equivalent to an "entangled" protocol. The "entanglement based" protocols, require sources of quantum

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↙	↕	↘	↔	↕	↕	↔	↔	↘	↙	↕	↘	↙	↙	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Figure 3: The original BB84 protocol from Ref. [19].15 rounds of the of the BB84 protocol are depicted. Note that $\leftrightarrow = |0\rangle_R$, $\updownarrow = |1\rangle_R$, $\nearrow = |0\rangle_D$, $\searrow = |1\rangle_D$.

entanglement. It is beyond the scope of the present introduction to describe in detail the functionality of such devices. We would, however, point out that the majority of the pioneering experiments with entangled photons have been carried out using sources that utilize Spontaneous Parametric Down Conversion (SPDC), a non-linear optical process in appropriate birefringent materials [50]. In SPDC one (pump) photon generates two (down-converted) ones, whereby care is taken that the output state is a superposition of two pairs of generated photons. The constituents of the superposition are pairs that differ with respect to an additional degree of freedom, e.g., polarization. Note that each of the photons in a pair can be differentiated by the other by some physical parameter (e.g., energy or position of generation). In this sense one can view the entangled state as a single pair of two distinct photons that are entangled in the additional degree of freedom.

A potential measurement of the polarization of one of the photons of the entangled state in a particular basis, e.g., R, (i.e., generally measurement of the chosen degree of freedom in a specific setting) would yield a result, which quantum-mechanically is described by a projection of the entangled state. For this projection the result of a polarization measurement of the second photon is already uniquely fixed, provided the same basis is used. In other words the results of the measurements of both photons are rigidly correlated for identical settings. It is now almost obvious how to carry out QKD using an entangled photon source.

Each of the two photons of entangled pair is dispatched to one of the two legitimate parties Alice or Bob. If one of them, say Alice, measures the polarization of her photon from the entangled state in a selected basis, she can immediately infer with certainty what the outcome of the measurement of Bob will be, if he chooses the same measurement basis as her. The same holds for Bob. (The bases choice follows the pattern of the BB84 protocol, discussed above.) The two parties then, provided there had been no imperfections or third party interference, hold a perfectly correlated string of outcomes (bits) in case their measurement settings correspond one to the other. The non-corresponding settings (differing measurement bases) can be discarded and the output of this protocol, known as E91 [35] is identical to that of BB84.

The protocols are also truly equivalent for the following simple reason: In a prepare

and measure scheme, Alice draws two random numbers and then deterministically prepares a state by using one number to select a basis and one number to select a state out of the two basis vectors in the selected basis. However, one can imagine that actually Alice has an entangled source, and uses one random bit to select a measurement setting (i.e., one of the bases R or D). In this setting she measures one of the photons of the entangled pair and gets a number (a measurement result). The second photon of the entangled pair is sent to Bob. Based on her result and measurement setting, Alice perfectly knows what state is being sent to Bob. (This state is determined by the two numbers - the random one, for selecting the basis, and the measurement result telling which of the basis vectors is propagating to Bob.) Technically there is no difference if Alice draws two random numbers and using these prepares a fixed sate, or if she draws one random number (the measurement setting choice) and using an initial entangled state gets a second random number (the measurement result) that uniquely determines the state sent to Bob.

The advantage of entanglement is that SPDCs emit states that are better approximations of (pairs) of single photons in comparison with the weak coherent pulse sources. We caution here that we have been speaking above about "a photon that generates two ones" in the non-linear medium. In fact the impinging pump photon, typically a weak coherent pulse, generates in SPDC two entangled "squeezed states" that in addition to the entangled pair carry also four, six and higher numbers of photons, albeit with very low probability.

Entanglement sources are currently pretty robust [32, 33], however their pair-generation rate is limited, putting a restriction on the entanglement-based QKD key generation rate that is still lower than that of prepare and measure schemes.

While discrete variable protocols have been historically the first ones that have been put forward, other classes of protocols were proposed and demonstrated later on.

A well known class is that of Continuous Variable (CV) QKD. Taking inspiration from the fact that pin-photodiodes are significantly more efficient in registering light than single photon detectors, it has been contemplated to measure electric field amplitudes instead of registering arrivals of single photons. To this end homodyne detection has been considered and the two conjugate observables of the electromagnetic field (equivalent to the canonical operators $\hat{X}$ and $\hat{P}$) have been used to define the protocol. The fact that these observables do not commute is the corner stone that is used to derive the security of these QKD schemes.

There are many variations of CV QKD and numerous publications, discussing these. The two main branches of CV QKD based on so called coherent state signals, however, are Gaussian Modulation CV [51] and Discrete Modulation CV QKD [52].

4.5 QKD Networks

The point to point character and the requirements of single quantum transmission makes QKD a difficult technology to implement in practice. If a direct quantum channel is required for every possible pair of users in a network, the growth in the number of connections will be exponential with the number of users. Thus, we will need a means

to route the quantum signals. Since they cannot be disturbed, no signal amplification is possible in the quantum channel and the noise has to be kept as low as possible, otherwise the quantum bit error rate will increase, meaning a reduction in the amount of attainable secret key.

The standard way to implement a quantum channel is to use a dedicated dark fiber but, again, an all to all network of dark fibers is not feasible. The alternative, as in standard networks, is to use routing elements that can connect the points in the network that require a secret key. If the routing elements connect the end points to establish a single direct quantum channel between them, we speak of a switched QKD network. In this case an ITS key can be, in principle, generated. If the routing elements act as end points of the quantum channel themselves, establishing a secret key between the initial and end point requires a series of hops using quantum channels that connect, pairwise, the initial point with a routing element, between routing elements and then with the final point. In this case, an ITS key cannot be generated and trust relationships has to be assumed on the routing elements. This kind of networks are termed trusted node networks.

Switched networks are limited in distance due to the maximum tolerable absorption budget that QKD devices have. Note that switching elements have a probability to absorb a photon from the quantum channel, thus further limiting the range of these networks, that are typically restricted to metropolitan area. To give an idea, a modern QKD system can withstand about 30 dB losses. Typical, industrial grade, elements used in passive optical networks (PON) like Array Waveguide Gratings (32 ports) have an absorption of about $3-4$ dB. A 1:4 splitter is 6 dB and would add 3 dB each time its splitting ratio is doubled. Clean and well cared connectors are about 0.5 dB. Optical switches are between $1-2$ dB. Testbeds to demonstrate a QKD switching network and its integration in conventional telecommunications networks have been built as early as 2009. In particular [28] was specifically designed to share as much infrastructure as possible. It follows the same core and access structure and devices than conventional PON. Also, the same optical fiber is used to transmit the quantum and classical signals. More advanced switched networks where, by design, the user of a QKD device can decide with whom to grow a secret key [53] or use the network to distribute entanglement [54] have been also tested. More modern results in the case of a PON access network have been published in [55].

By contrast, trusted node networks (see Fig. 4) are not limited in distance, however they cannot guarantee ITS security. They can be composed by switched networks together with trusted nodes. A global, world-wide QKD trusted network has been envisioned using satellite links. Although no QKD satellite link has been demonstrated up to now, its feasibility has been studied in free space ground links in the Canary islands over 144 Km [32] and there are plans for its development [34].

A key aspect in the integration of QKD in telecommunications networks is the capability of sharing the installed infrastructure. In particular, the Total Cost of Ownership of the dark fiber required for the quantum channel over the several years that a QKD device might be operational, considerably exceeds the cost of the QKD device itself.

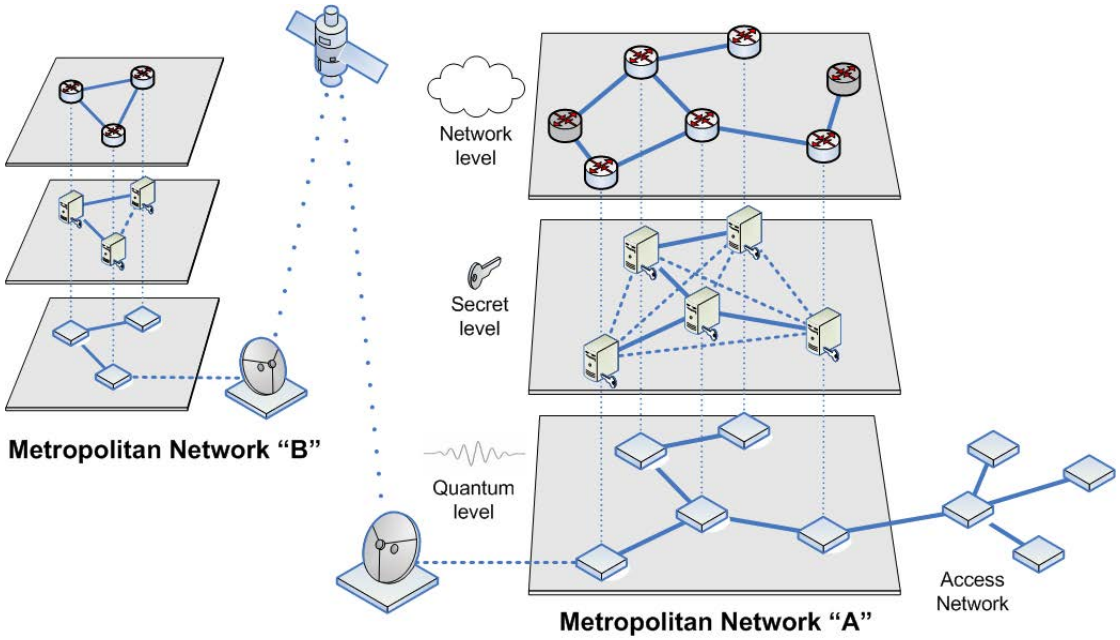

Figure 4: An hypothetical global trusted node quantum network is shown. A wide area QKD network (e.g., Metropolitan Network A or B) is composed by a set of quantum, point to point, nodes linked by quantum channels. These links could also include ITS switched networks, like the access network depicted at the lower rigth corner. The set of quantum nodes and links form the quantum level. Many of the quantum nodes will act as classical repeaters by retransmitting the keys distilled from the signals of one of the quantum links using another quantum link connected to the same node. Note that to do this, the key must be distilled (e.g., in A to B and B to C, since there is no direct quantum channel A-C, B will act as a trusted node), hence known to the two extremes of the quantum channel and retransmitted through other channel. The network loses then its ITS character and is secure as long as these nodes are secure, hence the name "trusted node". These set of links and keys conform the "secrets layer". Keys are managed at this level and the nodes are able to provide secret keys to applications in the nodes that require such a feature (the network layer). For long distance links a satellite, that is assumed to be a trusted node, is used.

To reduce the cost, the ability to use the same fiber for classical communications and the quantum channel or to use a single dark fiber to serve many quantum channels has been actively studied. It has been demonstrated that by a combination of reducing the total power in the fiber, filtering schemes and time rejection using very fast, gated detectors, it is possible to make compatible quantum and classical communications in the same dark fiber. Test beds to specifically demonstrate the integration of QKD in conventional telecommunications infrastructure have been built [28] and demonstrations of high speed classical and quantum communications over the same fiber have been carried out [49, 56, 57]. On the more industrial side, long term testbeds, with QKD systems working continuously without interruption during several months have also been demonstrated [27].

Trusted node networks have been also built. The first, more experimental ones were more focused on technological demonstration, using different types of QKD systems [23, 58]. The Vienna network [24] was a major demonstrator that not only showed very different technologies, including a free space link and a long distance one (80 Km), but also built the necessary SW layer to link all of them together in a common infrastructure. Later networks, like the Tokyo one [25, 26], are already approaching a real QKD network oriented more towards the provision of practical security services. New, very large, QKD networks are being built in China, USA and UK [29–31].

Networks capable of integrating quantum repeaters would be a definitive solution for the losses problem while keeping at the same time the ITS character of QKD. While a quantum repeater is, technologically, easier to build than a quantum computer, they are not expected to be available in the near future. Furthermore, the technologies currently used to study them are not easy to deploy in the field (ultra-cold atoms, superconducting devices...).

5 The classical part of a QKD protocol: Key Distillation

After the quantum phase of a QKD protocol the parties, named Alice and Bob, have to convert their strings into a secret key. These strings are sequences of key elements (symbols) that correspond to the outcomes of two correlated random sources X and Y, belonging to Alice and Bob, respectively. Typically, in discrete variable QKD, the key elements are bits, and the sequences are thus binary strings. This key post-processing is known as *secret key distillation* and typically involves two steps: information reconciliation (or error correction) and privacy amplification.

Firstly, the parties need to reconcile discrepancies in their strings to make them identical. This process, usually known as error correction but more appropriately referred to as *information reconciliation* or simply reconciliation, allows two legitimate parties to agree on a common —although not necessarily secret— string. Additional information from both strings needs then to be shared among the legitimate parties, for instance the parities of carefully chosen sets of bits in a binary string. This information is disclosed through a public (classical) channel, and therefore assumed to be known by everyone, including any potential adversary or eavesdropper. The eavesdropper gains then in-

formation, denoted by Z, about the shared strings both by wiretapping the quantum channel and listening the discussion in the public channel during reconciliation. Note, however, that the public channel is considered authenticated and error-free, such that an adversary cannot modify the information communicated between the parties and the parties know the origin of the information.

Additionally, for practical purposes an intermediate *confirmation* step must be also considered. This step, that should take place just after information reconciliation, aims to ensure (confirm) that the reconciled strings are indeed identical. Note that a typical reconciliation procedure does not guarantee that all discrepancies are reconciled after its completion, having always a non-negligible and unbounded failure or undetected error probability.

Finally, the parties must agree on a third procedure, called *privacy amplification*, for extracting an information-theoretic secret key from a common shared string, even in the presence of an eavesdropper. In privacy amplification the parties amplify the uncertainty of the eavesdropper (i.e., reduce his knowledge in order to make it negligible) about the shared strings at the expense of compressing and thus reducing the secret key length.

In the following, we delve into both steps, information reconciliation and privacy amplification, and the most interesting alternatives proposed to efficiently implement each of these steps. Note that the confirmation step can be easily attained using common cryptographic hash functions to verify a number of reconciled strings.

5.1 Information reconciliation

As described above, information reconciliation basically consists in exchanging messages over a public classical authenticated and integrity preserving channel with appropriate information to detect and correct discrepancies in two correlated strings. Let x and y be two strings, instances of two correlated sources X and Y, respectively. The information disclosed in the exchanged messages can be then described as a function of these strings $f(x, y)$. Roughly, the subsequent impact of reconciliation in the privacy amplification phase is a decrease of $|f(x, y)|$ symbols in the secret key length (a necessary but not sufficient condition to produce a secret key), where $|f(x, y)|$ is the number of symbols disclosed during the reconciliation. Consequently, an a priori *optimal reconciliation* procedure is the one that reveals the minimum amount of information needed for correcting all the discrepancies between two correlated strings, therefore minimizing the key material discarded in privacy amplification or equivalently maximizing the secret key length.

Formally, the problem of correcting discrepancies in correlated sources is equivalent to the encoding of such sources, a problem already studied by Slepian and Wolf in their seminal work [59]. In this contribution the authors demonstrate that two correlated sources can be encoded at a rate of $H(X, Y)$ [60] even when X and Y are encoded separately, where $H(X)$ is the Shannon entropy. A particular case of interest to the problem in hand is the well-known source coding with side information. In such a case, only X is to be recovered on the other side with information about Y, the amount of information needed to reconcile X given Y is then lower bounded by the conditional entropy $H(X|Y)$

[59]. Given this fundamental limit, an *efficiency* parameter f is commonly defined in information reconciliation as follows:

$$f = \frac{\ell}{H(X|Y)} \tag{1}$$

where ℓ is the ratio of information leakage, i.e., the actual amount of information disclosed per symbol during the reconciliation. As defined, the efficiency is always greater than 1, and equal only when the reconciliation is perfect.

In the case of discrete variable QKD, the outcomes of both correlated sources X and Y are two binary strings that can be regarded as the input and output of a binary symmetric channel (BSC) with the crossover probability ϵ. The conditional entropy coincides then with the binary Shannon entropy $h(\epsilon) = -\epsilon \log_2 \epsilon - (1-\epsilon) \log_2 (1-\epsilon)$ [61].

Note, however, that optimal reconciliation in terms of efficiency does not guarantee the best results in terms of secret key rate or *throughput* as originally discussed in [62]. There are other parameters to consider when analyzing and optimizing an information reconciliation procedure, such as the computational complexity, number of communication rounds and frame error rate [62, 63].

5.1.1 The Cascade protocol

Cascade [22] is undoubtedly the best-known protocol for information reconciliation, and probably the de-facto standard for practical implementations of QKD. It corrects discrepancies in two binary strings based on parity exchanges. Each string is divided into blocks of equal length, and the parity of each block is computed and exchanged simultaneously through the public channel. For each block with an odd number of errors a parity mismatch occurs and the parties perform a binary search to find and correct one error per block. The protocol works iteratively for a number of passes, shuffling synchronously the strings between successive passes and taking into account that each detected error produces side information that can be used to correct undetected errors of previous passes.

The block sizes are chosen accordingly to the estimated bit error rate ϵ (i.e., ratio of errors or discrepancies in the binary strings), and the number of passes completed. For instance, in its original description Cascade uses an initial block size of $k_1 \approx 0.73/\epsilon$ for the first pass, and doubles its size in successive passes $k_i = 2k_{i-1}$. Numerous optimizations have been proposed, most trying to optimize these block sizes, but recently it was shown that the optimum sizes correspond to power of two values [63]. Cascade is unfortunately a highly interactive protocol, i.e., the parties have to exchange a large number of messages (with its corresponding latency and consequently drop in the speed), however as recently shown in [63] the protocol is able to achieve a remarkable average efficiency of $f = 1.05$ in the error rate range of interest for QKD.

5.1.2 One-way reconciliation

A number of proposals aim to reduce the interactivity of Cascade using one-way (forward) error correcting methods. For instance, by replacing the binary search in Cascade with a Hamming code, such as in Winnow [64], or by directly using capacity approaching linear error correcting codes, such as turbo codes [65, 66] or the newly renowned low-density parity-check (LDPC) codes [67].

The idea underlying one-way reconciliation is as follows. The parties agree on a linear block code with information rate (code rate) adapted to the estimated error rate in the quantum channel or QBER (i.e., the ratio of discrepancies in the correlated sources X and Y). Let W denote the parity-check matrix of this code. Alice computes then the syndrome z, a compressed version of her string x, $z = Wx$, and sends it to Bob through the public noiseless channel. Finally, Bob uses the received syndrome to detect and correct any discrepancy in his string—in other words, he tries to recover x starting from y and considering that the error in the communication is given by Wy. Once completed, the parties share with high probability a common string. In such a way, the number of communications can be thereby reduced to a minimum, such that when using capacity approaching codes the problem now becomes how the parties can efficiently share an error correcting code adapted to a varying error rate in the quantum channel.

LDPC codes were originally proposed for high speed QKD on the DARPA quantum network [68]. However, although such codes can be easily adapted for the source coding problem, these are fixed-rate codes that rapidly becomes inefficient when the quantum bit error rate varies (see figure 4.1 in [67]). Moreover, the process of building a new LDPC code, and exchange it between the parties, is both computationally and time-wise costly, in particular for large block-length codes. For this reason, to achieve a good reconciliation efficiency it is essential to use these codes together with any rate adaptive technique. Therefore, the primary objective of highly efficient LDPC-based proposals is to dynamically adapt the rate of a single LDPC code using different coding techniques, such as puncturing or shortening, among others. Several reconciliation protocols have been proposed in this line using large block-length rate-adaptive binary [67, 69] and non-binary [70] LDPC codes.

Unfortunately, none of these proposals is appropriate for a hardware implementation, given that the length of the codes used is one or even two orders of magnitude higher than the longest code block-lengths considered for existing hardware (HW). Somehow as a proof of concept, these proposals aim to investigate the potential of LDPC codes applied to information reconciliation. The results of these proposals are even more optimistic since the error correcting process allows up to 200 decoding iterations (see sum-product algorithm in [67]), a figure much higher than the 10 or 20 iterations typically considered in HW implementations.

Fundamental limits of one-way reconciliation

At this point, it is then clear that for practical purposes shorter block or frame lengths have to be considered. For this, it is useful to know recent advances in understanding

the fundamental limits of forward error correction using finite resources. New limits in information reconciliation with finite block-length codes applied to quantum key distribution were recently developed in [71]. The following expression for the reconciliation leakage summarizes the most important result of this contribution:

$$\ell \approx \xi_1 h(\epsilon) + \xi_2 \sqrt{v(\epsilon)/n}\, \Phi^{-1}(1-F) \tag{2}$$

where $h(x)$ and ϵ are as in Eq. (1), $v(x) = x(1-x)\log^2(x/(1-x))$, n is the code block-length in bits, $\Phi(x)$ is the cumulative standard normal distribution, F is the frame error rate, and ξ_1 and ξ_2 are two efficiency constants satisfying $\xi_1, \xi_2 \geq 1$ and thus providing a new lower bound for the leakage when using a finite block-length of n bits.

Note that this expression coincides with that given in Eq. (1) for the case of discrete variable QKD if we consider $\xi_2 = 0$. Therefore, ξ_1 is in some sense a measure of the asymptotic reconciliation efficiency (i.e., the one considering a code of infinite block-length), while ξ_2 is a second order efficiency for the finite length case.

Further note that this equation also raises an important parameter already suggested above but not considered so far: *frame error rate* (FER) or ratio of strings that cannot be reconciled. Most of the early work on reconciliation considered a constant and low enough value for the FER, typically 10^{-3} or lower, but even worse this parameter has been sometimes ignored. However, when using an LDPC code in a higher FER region we increase the number of errors that can be reconciled with this code, improving thus the efficiency, at the expense of clearly increase also the ratio of strings that cannot be reconciled and must be then discarded. Any optimization of a reconciliation protocol should consider this trade off between efficiency and FER to improve the average efficiency and performance, as shown in [62, 63].

5.1.3 Blind reconciliation

Despite the above fundamental limit there still exist coding techniques that provide a good average efficiency even when using short block-length LDPC codes. A remarkable choice is provided by incremental redundancy hybrid automatic repeat request (H-ARQ) schemes, a combination of forward error correction and ARQ (acknowledgment messages). This is a coding scheme with retransmission, such that an improvement in efficiency is achieved at the expense of relaxing the condition of minimal interactivity. In [67, 72] the authors proposed a novel reconciliation protocol, named *blind reconciliation*, that significantly improves the efficiency of one-way reconciliation protocols using short block-length LDPC codes by allowing a limited interactivity, for instance between 3 and 5 rounds. Later, this protocol was also shown to be interesting not only in efficiency but from the throughput point of view [72].

5.2 Privacy Amplification

After the physical part of a QKD protocol and the basis and information reconciliation steps, the parties share two identical but partially secret strings. The parties need then to amplify their secrecy producing a provably uniformly random sequence, the secret

key, at the expense of reducing the length of their shared strings. This procedure is called privacy amplification. Intuitively, it makes use of a compressing function that generates a uniform output given as input the output of a weak randomness source, but also by taking advantage of an auxiliary random source. Such functions exist and are called (seeded) *randomness extractors* or simply extractors.

Some well-known randomness extractors suitable for privacy amplification in QKD are the almost two-universal families of hash functions and Trevisan's extractors, although here we focus only on the former given its simplicity and effectiveness. Universal hash functions were originally proposed by Wegman and Carter [38, 39], and firstly proposed for privacy amplification by Bennett et al. [20, 73]. Although initially these functions were proposed for the secret key agreement problem where an adversary is restricted to classical information processing, later it was also proved that these functions are also valid for the case where the side information known by an adversary is described by the state of a quantum system [74]. The procedure works as follows. A hash function is randomly chosen, by one of the parties, within a family or class of hash functions previously agreed between the parties. A description of the selected hash function is exchanged, such that both parties can then compute the same hash. It is obviously preferable a short description of this hash, or equivalently a short identifier within its family, in order to reduce the communication between the parties. Further note that, unlike in information reconciliation, they are not allowed to perform privacy amplification by dividing their strings into smaller blocks. Therefore, this step must be efficiently computed even when using large input and output sizes.

As suggested in [66], there are few universal families of hash functions suitable for privacy amplification. Notably, linear functions from $\mathcal{B}^n$ to $\mathcal{B}^k$ are two-universal [38], where $\mathcal{B}$ denotes the set of Boolean values $\{0, 1\}$, or equivalently the two-element Galois field $GF(2)$. These functions can be described by $n \times k$ binary matrices, such that $n \cdot k$ bits has to be transmitted to identify the chosen function and the hash is calculated as a common matrix multiplication procedure. Fortunately, the subset of binary matrices that are Toeplitz matrices is also universal [75]. This new class of functions is of particular interest since a Toeplitz matrix is completely determined by its first row and column, thus only $n + k - 1$ bits are needed to describe it. Furthermore, a Toeplitz matrix can be extended to a circular one, such that the product (i.e., the hash) can be efficiently implemented using the Fourier transform or its integer version, the number theoretic transform.

Acknowledgment

This work has been partially supported by the project Continuous Variables for Quantum Communications (CVQuCo), TEC2015-70406-R, funded by the Spanish Ministry of Economy and Competitiveness and QUITEMAD+, S2013-IC2801, funded by Comunidad Autónoma de Madrid.

References

[1] This assumption can be replaced by weaker ones as discussed for instance in [36].

[2] P. W. Shor, in *35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, Nov. 1994, doi:10.1109/SFCS.1994.365700.

[3] P. W. Shor, *SIAM Journal of Computing*, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, doi:10.1137/S0097539795293172.

[4] C. H. Bennett and G. Brassard, *Sigact News*, vol. 20, no. 4, pp. 78–82, Nov. 1989, doi:10.1145/74074.74087.

[5] ID quantique, www.idquantique.com.

[6] D. Boneh, *Notices of the American Mathematical Society*, vol. 46, no. 2, pp. 203–213, Feb. 1999.

[7] F. Koeune and F. X. Standaert, in *Foundations of Security Analysis and Design III*, *Lecture Notes in Computer Science*, vol. 3655, pp. 78–108, 2005, doi:10.1007/11554578_3.

[8] H.-K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130503, Mar. 2012, doi:10.1103/PhysRevLett.108.130503.

[9] S. L. Braunstein and S. Pirandola, *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130502, Mar. 2012, doi:10.1103/PhysRevLett.108.130502.

[10] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Phys. Rev. Lett.*, vol. 98, no. 23, p. 230501, June 2007, doi:10.1103/PhysRevLett.98.230501.

[11] N. I. of Standards and Technology, Federal information processing standard (FIPS) publication 140-2: Security requirements for cryptographic modules, May 2001, `http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf`.

[12] R. Alleaume, I. P. Degiovanni, A. Mink, T. E. Chapuran, N. Lutkenhaus, M. Peev, C. J. Chunnilall, V. Martin, M. Lucamarini, M. Ward, and A. Shields, in *2014 IEEE Globecom Workshops (GC Wkshps)*, pp. 656–661, Dec. 2014, doi:10.1109/GLOCOMW.2014.7063507.

[13] The signal attenuation in modern optical fiber is about 0.2 dB/Km in the clearest transmission window, around 1550 nm.

[14] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.*, vol. 81, no. 26, pp. 5932–5935, Dec. 1998, doi:10.1103/PhysRevLett.81.5932.

[15] H.-K. Lo, *Phys. Rev. A*, vol. 56, no. 2, p. 1154, August 1997, doi:10.1103/PhysRevA.56.1154.

[16] S. Wehner and B. M. Schaffner, Christian andTerhal, *Phys. Rev. Lett.*, vol. 100, no. 22, p. 220502, June 2008, doi:10.1103/PhysRevLett.100.220502.

[17] S. J. Wiesner, *Sigact News*, vol. 15, no. 1, pp. 78–88, Jan. 1983, doi:10.1145/1008908.1008920.

[18] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, in *Advances in Cryptology – Proceedings of Crypto 82*, pp. 267–275, Springer US, 1983, doi:10.1007/978-1-4757-0602-4_26.

[19] C. H. Bennett and G. Brassard, in *IEEE Int. Conf. on Computers, Systems, and Signal Processing*, pp. 175–179, Dec. 1984.

[20] C. H. Bennett, G. Brassard, and J.-M. Roberts, *SIAM J. Comput.*, vol. 17, no. 2, pp. 210–229, Apr. 1988, doi:10.1137/0217014.

[21] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Cryptology*, vol. 5, no. 1, pp. 3–28, Jan. 1992, doi:10.1007/BF00191318.

[22] G. Brassard and L. Salvail, in *Advances in Cryptology – Eurocrypt 93*, vol. 765, pp. 410–423, 1994, doi:10.1007/3-540-48285-7_35.

[23] C. Elliot, *New J. Phys.*, vol. 4, no. 1, pp. 46.1–46.12, July 2002, doi:10.1088/1367-2630/4/1/346.

[24] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, *New J. Phys.*, vol. 11, no. 7, p. 075001, July 2009, doi:10.1088/1367-2630/11/7/075001.

[25] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, *Opt. Express*, vol. 19, no. 11, pp. 10387–10409, May 2011, doi:10.1364/OE.19.010387.

[26] Tokyo QKD network, www.uqcc.org/QKDnetwork/.

[27] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, *New J. Phys.*, vol. 13, no. 12, p. 123001, Dec. 2011, doi:10.1088/1367-2630/13/12/123001.

[28] D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin, in *Quantum Communication and Quantum Networking*, vol. 36, pp. 142–149, 2010, doi:10.1007/978-3-642-11731-2_18.

[29] A. Morrow, D. Hayford, and M. Legre, in *2012 IEEE Conf. on Technologies for Homeland Security (HST)*, pp. 162–166, Nov. 2012, doi:10.1109/THS.2012.6459843.

[30] H. Xiang and Z.-F. Han, The chinese QKD networks, 2015, 3rd ETSI Quantum Safe Cryptography Workshop.

[31] UK quantum technology hub for quantum communications technologies, quantum-commshub.net.

[32] R. Ursin, F. Tiefenbacher1, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, *Nat. Phys.*, vol. 3, pp. 481–486, June 2007, doi:10.1038/nphys629.

[33] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein, and A. Zeilinger, *Nat. Phys.*, vol. 5, pp. 389–392, May 2009, doi:10.1038/nphys1255.

[34] China plans in space: Quantum experiments at space scale (QUESS), english.nssc.cas.cn/missions/FM/.

[35] A. K. Ekert, *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991, doi:10.1103/PhysRevLett.67.661.

[36] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sept. 2009, doi:10.1103/RevModPhys.81.1301.

[37] A. Einstein, B. Podolski, and N. Rosen, *Phys. Rev.*, vol. 47, no. 10, p. 777, May 1935, doi:10.1103/PhysRev.47.777.

[38] J. L. Carter and M. N. Wegman, *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143–154, Apr. 1979, doi:10.1016/0022-0000(79)90044-8.

[39] M. N. Wegman and J. L. Carter, *J. Comput. Syst. Sci.*, vol. 22, no. 3, pp. 265–279, June 1981, doi:10.1016/0022-0000(81)90033-7.

[40] W. K. Wootters and W. H. Zurek, *Nature*, vol. 299, pp. 802–803, Oct. 1982, doi:10.1038/299802a0.

[41] In view of Quantum Computing, it is also interesting to note that in spite of the restrictions of the no cloning theorem it is possible to correct errors in quantum memory registers.

[42] D. Mayers, in *Advances in Cryptology – Crypto 96*, pp. 343–357, 1996, doi:10.1007/3-540-68697-5_26.

[43] P. W. Shor and J. Preskill, *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, July 2000, doi:dx.doi.org/10.1103/PhysRevLett.85.441.

[44] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, *Opt. Express*, vol. 21, no. 20, pp. 23241–23249, 2013, doi:10.1364/OE.21.023241.

[45] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, *New J. Phys.*, vol. 11, no. 7, p. 075003, July 2009, doi:10.1088/1367-2630/11/7/075003.

[46] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, *Nat. Photonics*, vol. 9, pp. 163–168, Feb. 2015, doi:10.1038/nphoton.2014.327.

[47] Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, *Appl. Phys. Lett.*, vol. 91, p. 041114, 2007, doi:10.1063/1.2760135.

[48] N. Namekata, S. Sasamori, and S. Inoue, *Opt. Express*, vol. 14, no. 21, pp. 10043–10049, 2006, doi:10.1364/OE.14.010043.

[49] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, *Phys. Rev. X*, vol. 2, p. 041010, Nov. 2012, doi:10.1103/PhysRevX.2.041010.

[50] P. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. Sergienko, and Y. Shih, *Phys. Rev. Lett.*, vol. 75, no. 24, 1995, doi:10.1103/physrevlett.75.4337.

[51] F. Grosshans and P. Grangier, *Phys. Rev. Lett.*, vol. 88, no. 5, p. 057902, Jan. 2002, doi:10.1103/PhysRevLett.88.057902.

[52] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, *Phys. Rev. Lett.*, vol. 89, no. 16, p. 167901, Sept. 2002, doi:10.1103/PhysRevLett.89.167901.

[53] A. Ciurana, J. Martinez-Mateo, M. Peev, A. Poppe, H. Walenta, H. Zbiden, and V. Martin, *Opt. Express*, vol. 22, no. 2, pp. 1576–1593, Jan. 2014, doi:10.1364/OE.22.001576.

[54] A. Ciurana, V. Martin, J. Martinez-Mateo, B. Schrenk, M. Peev, and A. Poppe, *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, p. 6400212, May-June 2015, doi:10.1109/JSTQE.2014.2367241.

[55] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, S. W.-B. Tam, Z. Yuan, and A. J. Shields, *Sci. Rep.*, vol. 5, p. 18121, Dec. 2015, doi:10.1038/srep18121.

[56] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, *New J. Phys.*, vol. 12, no. 6, p. 063027, June 2010.

[57] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M. Legré, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H. Zbinden, *New J. Phys.*, vol. 16, no. 1, p. 013047, Jan. 2014.

[58] C. Elliot, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, in *Quantum Information and Computation III*, *Proc. SPIE*, vol. 5815, pp. 138–149, 2005, doi:10.1117/12.606489.

[59] D. S. Slepian and J. K. Wolf, *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, July 1973, doi:10.1109/TIT.1973.1055037.

[60] Note, it is clear that a rate $H(X,Y)$ is enough to jointly encode both sources, while a rate $R \geq H(X) + H(Y)$ is seemingly needed when X and Y are encoded separately.

[61] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley-Interscience, New York, NY, USA, 1991, doi:10.1002/047174882X.

[62] J. Martinez-Mateo, D. Elkouss, and V. Martin, *Sci. Rep.*, vol. 3, no. 1576, pp. 1–6, Apr. 2013, doi:10.1109/JSTQE.2014.2367241.

[63] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, *Quantum Inform. Comput.*, vol. 15, no. 5&6, pp. 453–477, May 2015, arXiv:1409.5965 [quant-ph].

[64] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, *Phys. Rev. A*, vol. 67, no. 5, p. 052303, May 2003, doi:10.1103/PhysRevA.67.052303.

[65] K.-C. Nguyen, G. Van Assche, and N. J. Cerf, in *2004 Int. Symp. on Information Theory and its Applications*, pp. 1274–1279, 2004.

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

[67] J. Martinez-Mateo, *Efficient Information Reconciliation for Quantum Key Distribution*, Ph.D. thesis, Universidad Politécnica de Madrid, Dec. 2011, oa.upm.es/9717.

[68] D. Pearson, in *7th Int. Conf. on Quantum Communication, Measurement and Computing*, vol. 734, pp. 299–302, Nov. 2004, doi:10.1063/1.1834439.

[69] D. Elkouss, J. Martinez-Mateo, and V. Martin, *Quantum Inform. Comput.*, vol. 11, no. 3&4, pp. 226–238, Apr.-May 2011, arXiv:1007.1616 [quant-ph].

[70] K. Kasai, R. Matsumoto, and K. Sakaniwa, in *2010 Int. Symp. on Information Theory and its Applications*, pp. 922–927, Oct. 2010, doi:10.1109/ISITA.2010.5649550.

[71] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, in *2014 IEEE Int. Symp. on Information Theory*, pp. 1469–1473, June-July 2014, doi:10.1109/ISIT.2014.6875077.

[72] J. Martinez-Mateo, D. Elkouss, and V. Martin, *Quantum Inform. Comput.*, vol. 12, no. 9&10, pp. 791–812, Sept.-Oct. 2012, arXiv:1205.5729 [quant-ph].

[73] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995, doi:10.1109/18.476316.

[74] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, *IEEE Trans. Inf. Theory*, vol. 57, no. 8, pp. 5524–5535, Aug. 2011, doi:10.1109/TIT.2011.2158473.

[75] H. Krawczyk, in *Advances in Cryptology – CRYPTO '94*, *Lecture Notes in Computer Science*, vol. 839, pp. 129–139, 1994, doi:10.1007/3-540-48658-5_15.