The security of practical quantum key distribution

Valerio Scarani

Centre for Quantum Technologies and Department of Physics, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore and Group of Applied Physics, University of Geneva, 20 rue de l'Ecole de Médicine, 1211 Geneva, Switzerland

Helle Bechmann-Pasquinucci

University of Pavia, Dipartimento di Fisica "A. Volta," via Bassi 6, I-27100 Pavia, Italy and UCCI.IT, via Olma 26, I-23888, Rovagnate (LC), Italy

Nicolas J. Cerf

Quantum Information and Communication, Ecole Polytechnique, Université Libre de Bruxelles, Avenue F. D. Roosevelt 50, B-1050 Brussels, Belgium

Miloslav Dušek

Department of Optics, Faculty of Science, Palacký University, 17. listopadu 12, 772 00, Olomouc, Czech Republic

Norbert Lütkenhaus

Institute for Quantum Computing and Department for Physics and Astronomy, University of Waterloo, 200 University Avenue W., Waterloo, ON N2L 3G1, Canada and Max Planck Research Group, Institute for Optics, Information and Photonics, University of Erlangen-Nuremberg, Staudtstrasse 7/B2, 91058 Erlangen, Germany

Momtchil Peev

Quantum Technologies, Smart Systems Division, Austrian Research Centers GmbH ARC, Donau-City, Strasse 1, 1220 Vienna, Austria

(Published 29 September 2009)

Quantum key distribution (QKD) is the first quantum information task to reach the level of mature technology, already fit for commercialization. It aims at the creation of a secret key between authorized partners connected by a quantum channel and a classical authenticated channel. The security of the key can in principle be guaranteed without putting any restriction on an eavesdropper's power. This article provides a concise up-to-date review of QKD, biased toward the practical side. Essential theoretical tools that have been developed to assess the security of the main experimental platforms are presented (discrete-variable, continuous-variable, and distributed-phase-reference protocols).

CONTENTS

I. INTRODUCTION

A. Cryptography

Cryptography is a field of applications that provides privacy, authentication, and confidentiality to users. An important subfield is that of secure communication, aiming at allowing confidential communication between different parties such that no unauthorized party has access to the content of the messages. This field has a long history of successes and failures, as many methods to encode messages emerged throughout the centuries, with the codes always broken some time later.

History need not repeat itself forever, though. In 1917, Vernam invented the so-called *one-time pad* encryption, which uses a symmetric, random secret key shared between sender and receiver (Vernam, 1926). This scheme cannot be broken in principle, provided the parties do not reuse their key. Three decades later, Shannon proved that the Vernam scheme is optimal: there is no encryption method that requires less key (Shannon, 1949). This means that the key is being used up in the process. To employ this scheme, therefore, the communicating parties must have a secure method to share a

key that is as long as the text to be encrypted. Because of this limitation, which becomes severe when large amounts of information have to be securely transmitted, most cryptographic applications nowadays are based on other schemes, whose security cannot be proved in principle, but is rather based on our experience that some problems are hard to solve. In other words, these schemes can be broken, but with a substantial amount of computational power. One can therefore set a security parameter to a value such that the amount of required computational power lies beyond the amount deemed to be available to an adversary; the value can be adjusted in time, along with technological advances.

The picture has changed in the last two decades, thanks to unexpected inputs from *quantum physics.* In the early 1980s, Bennett and Brassard proposed a solution to the key distribution problem based on quantum physics (Bennett and Brassard, 1984); this idea, independently rediscovered by Ekert a few years later (Ekert, 1991), was the beginning of *quantum key distribution* (QKD), which was to become the most promising task of *quantum cryptography*.[1] Since then, QKD devices have continuously increased their key generation rate and have started approaching maturity, ready for implementation in realistic settings.

In an intriguing independent development, ten years after the advent of QKD, Peter Shor discovered that large numbers can in principle be factorized efficiently if one can perform coherent manipulations on many quantum systems (Shor, 1994, 1997). The factorization of large numbers is an example of a mathematical task considered classically hard to solve and for this reason related to a class of cryptographic schemes which are currently widely used. Although quantum computers have not been realized yet, the mere fact that they could be

---

[1]Quantum cryptography is often identified with QKD, but actually comprises all possible tasks related to secrecy that are implemented with the help of quantum physics. The first appearance of a link between secrecy and quantum physics was Wiesner's idea of *quantum money*, which dates back to the early 1970s although published a decade later (Wiesner, 1983). To our knowledge, nothing else appeared before the Bennett and Brassard first QKD protocol. In 1999, two new tasks were invented and both were given the same name, *quantum secret sharing*. In one case, the protocol is a multipartite generalization of key distribution (Hillery, Bužek, and Berthiaume, 1999; Karlsson, Koashi, and Imoto, 1999); in the other case, it refers to the sharing of secret quantum information, i.e., the goal is for the authorized partners to share quantum information (instead of a list of classical random variables) known only to them (Cleve, Gottesman, and Lo, 1999; Crépeau, Gottesman, and Smith, 2005). Other examples of cryptographic tasks are bit commitment or oblivious transfer; for these tasks, in contrast to the case of QKD and secret sharing, quantum physics cannot guarantee unconditional security (Lo, 1997; Lo and Chau, 1997; Mayers, 1997) and therefore their interest seems limited—though new paradigms such as "bounded-storage models" may change this perception in the future (Damgaard *et al.*, 2005, 2007; Wehner, Schaffner, and Terhal, 2008).
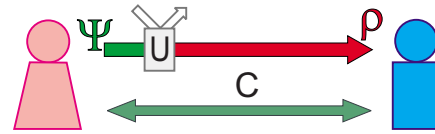
FIG. 1. (Color online) The setting of QKD: Alice and Bob are connected by a quantum channel, into which Eve can tap without any restriction other than the laws of physics; and by an authenticated classical channel, into which Eve can only listen to.

built might threaten the security of some cryptographic schemes.[2]

This review focuses therefore on the cryptographic task of key distribution, and in particular on its realization using quantum physics. Note that a secret key serves many useful purposes in cryptography other than message encryption: it can be used, for example, to authenticate messages, that is, to prove that a message has indeed been sent by the claimed sender.

B. Basics of quantum key distribution

Here, we introduce the basic elements of QKD, for the sake of those readers who are not familiar with the field. Alternative presentations of this material are available in many sources, ranging from books (Lo, 1998; Ekert *et al.*, 2001; Le Bellac, 2006; Scarani, 2006) to other review articles (Gisin, Ribordy, Tittel, and Zbinden, 2002; Dušek, Lütkenhaus, and Hendrych, 2006; Lo and Zhao, 2008).

1. Generic setting

The generic settings of QKD are shown in Fig. 1. The two *authorized partners*, those that want to establish a secret key at a distance, are traditionally called Alice and Bob. They need to be connected by two channels: a quantum channel, allowing them to share quantum signals, and a classical channel, on which they can send classical messages forth and back.

The classical channel needs to be authenticated: this means that Alice and Bob identify themselves; a third person can listen to the conversation but cannot participate in it. The quantum channel, however, is open to any possible manipulation from a third person. Specifically, the task of Alice and Bob is to guarantee security against an adversarial *eavesdropper*, usually called Eve,[3] tapping into the quantum channel and listening to the exchanges on the classical channel.

By a guarantee of security we mean that a non secret key is never used: either the authorized partners can create a secret key (a common list of secret bits known

---

[2]This issue will be discussed in more detail in Sec. VIII.B.

[3]The name, obtained from assonance with the English term "eavesdropping," is well suited for someone whose task is to mess things up.

only to themselves) or they abort the protocol.[4] Therefore, after the transmission of a sequence of symbols, Alice and Bob must estimate how much information about their lists of bits has leaked out to Eve. Such an estimate is obviously impossible in classical communication: if someone is tapping into a telephone line, or when Eve listens to the exchanges on the classical channel for that matter, the communication goes on unmodified. This is where quantum physics comes into the game: in a quantum channel, leakage of information is quantitatively related to degradation of the communication. Next we delve a bit deeper into the physical reasons for this statement.

2. The origin of security

The origin of the security of QKD can be traced back to some fundamental principles of quantum physics. One can argue, for instance, that any action by which Eve extracts some information out of quantum states is a generalized form of measurement; and a well-known tenet of quantum physics says that measurement in general modifies the state of the measured system. Alternatively, one may think that Eve's goal is to have a perfect copy of the state that Alice sends to Bob; this, however, is forbidden by the *no-cloning theorem* (Wootters and Zurek, 1982), which states that one cannot duplicate an unknown quantum state while keeping the original intact. Both these arguments already appeared in the seminal paper of Bennett and Brassard (1984); they lead to the same formalization. A third physical argument can be invoked, which is usually considered rather as a fact than as a principle, but a very deep one: quantum correlations obtained by separated measurements on members of entangled pairs violate Bell'sinequalities and cannot therefore have been created by preestablished agreement. In other words, the outcomes of the measurements did not exist before the measurements; but then, in particular, Eve could not know them (Ekert, 1991). This argument supposes that QKD is implemented with entangled states.

The fact that security can be based on general principles of physics suggests the possibility of *unconditional security*, i.e., the possibility of guaranteeing security without imposing any restriction on the power of the eavesdropper (see Sec. II.C.1). Indeed currently unconditional security has been proved for several QKD protocols.

3. The choice of light

In general, quantum information processing can be implemented with any system, and indeed there are proposals to implement quantum computing with ions, atoms, light, spins, etc. Abstractly, this is the case also for QKD: one could imagine performing a QKD experiment with electrons, ions, and molecules; however, *light* is the only practical choice. Indeed, the task of key distribution makes sense only if Alice and Bob are separated by a macroscopic distance: if they are in the same room, they have much easier ways of generating a common secret key.

Now, as is well known, light does not interact easily with matter; therefore quantum states of light can be transmitted to distant locations basically without decoherence, in the sense that small perturbation is expected in the definition of the optical mode. The problem with light is scattering, i.e., *losses*: quite often, the photons just do not arrive. The way losses affect QKD varies with the protocol and the implementation; we deal with these issues later, but it is useful to give here a rapid overview. First, losses impose bounds on the secret key rate (which cannot scale with the distance better than the transmittivity of the line) and on the achievable distance (where losses are so large that the signal is lost in spurious events, the "dark counts"). Second, losses may leak information to the eavesdropper, according to the nature of the quantum signal: for coherent pulses this is certainly the case; for single photons it is not; the case for entangled beams is more subtle. A third basic difference is determined by the detection scheme. Implementations that use photon counters rely on postselection: if a photon does not arrive, the detector does not click and the event is simply discarded.[5] On the contrary, implementations that use homodyne detection always give a signal; therefore losses translate as additional noise.

In summary, QKD is always implemented with light and there is no reason to believe that things will change in the future. As a consequence, the quantum channel is any medium that propagates light with reasonable losses: typically, either an optical fiber or just free space provided Alice and Bob have a line of sight.

4. The BB84 protocol

All the points and concepts introduced above will be dealt with later in this review. We first apply the generic

---

[4]No physical principle can prevent an adversary from cutting the channels, thus blocking all transfer of information between Alice and Bob. Stepping back then, one can imagine the following eavesdropping strategy (suggested by A. Beveratos): Eve systematically cuts all QKD channels, until Alice and Bob, who after all want to communicate, opt for less secure methods—and then Eve gets the information. There is obviously some humor in this idea but, given that Eve has no hope if QKD is used correctly, this strategy may indeed be the most effective.

[5]Note that this is possible because the task is to distribute a random key. In the early days of development of quantum information theory, some considered the possibility of sending the message directly via the quantum channel (Beige *et al.*, 2002; Boström and Felbinger, 2002). This task has been called "quantum secure direct communication" and has generated some interest. However, it was soon recognized that the idea suffers from two major defaults with respect to standard QKD: (i) It is obviously not robust against losses: you cannot afford to lose a significant amount of the message. (ii) It allows no analog of privacy amplification: if an eavesdropper obtains information, it is information on the message itself and of course cannot be erased.

ideas to a very concrete example: the first QKD protocol, published by Bennett and Brassard in 1984 and called therefore BB84 (Bennett and Brassard, 1984).

Suppose Alice holds a source of single photons. The spectral properties of the photons are sharply defined so the only degree of freedom left is polarization. Alice and Bob align their polarizers and agree to use either the horizontal or vertical $(+)$ basis, or the complementary basis of linear polarizations, i.e., $+45/-45$ $(\times)$. Specifically, the coding of bits is

$$|H\rangle, \quad \text{codes for } 0_+,$$

$$|V\rangle, \quad \text{codes for } 1_+,$$

$$|+45\rangle, \quad \text{codes for } 0_\times,$$

$$|-45\rangle, \quad \text{codes for } 1_\times. \tag{1}$$

We see that both bit values 0 and 1 are coded in two possible ways, or more precisely in nonorthogonal states because

$$|\pm 45\rangle = (1/\sqrt{2})(|H\rangle \pm |V\rangle). \tag{2}$$

Given this coding, the BB84 protocol goes as follows:

(1) Alice prepares a photon in one of the four states above and sends it to Bob on the quantum channel. Bob measures it in either the $+$ or the $\times$ basis. This step is repeated N times. Both Alice and Bob now have a list of N pairs (bit, basis).

(2) Alice and Bob communicate over the classical channel and compare the "basis" value of each item, discarding those instances in which they have used different bases. This step is called *sifting*. At its end, Alice and Bob have a list of approximately $N/2$ bits, with the promise that for each of them Alice's coding matched Bob's measurement. This list is called the *raw key*.

(3) Alice and Bob now reveal a random sample of the bits of their raw keys and estimate the error rate in the quantum channel, and thus in turn Eve's information. In the absence of errors, the raw key is identical for Alice and Bob and Eve has no information: in this case, the raw key is already the secret key. If there are errors, however, Alice and Bob have to correct them and to erase the information that Eve could have obtained.[6] Both tasks can be performed by communication in the classical channel, so this part of the protocol is called *classical postprocessing*. At the end of this processing, Alice and Bob share either a truly secret key or nothing at all (if Eve's information was too large).

---

[6]Historical note: the procedure that erases the information obtained by the eavesdropper was not discussed by Bennett and Brassard (1984) and first appeared a few years later (Bennett, Brassard, and Robert, 1988).

5. An example of eavesdropping

A particularly simple eavesdropping strategy is the one called *intercept resend*. To obtain information, Eve does the same as Bob: she intercepts the photon coming from Alice and measures it either in the $+$ or in the $\times$ basis. But Bob is waiting for some signal to arrive. We then suppose that Eve resends the same photon to Bob (Eve is limited only by the laws of physics: therefore, in particular, she can perform a quantum nondemolition measurement). If Eve has measured in the basis of Alice's preparation, the photon is intact: in such instances, Eve has obtained full information on Alice's bit without introducing any errors. However, when Eve has chosen the wrong basis, her result is uncorrelated with Alice's bit; moreover, she has modified the state so that, even if Bob uses the same basis as Alice, half of the time he will get the wrong result.

On average, over long keys, this particular attack gives Eve full information on half of the bits of the raw key $(I_E=0.5)$ at the price of introducing an error rate $Q=0.25$. Can a secure key be extracted under such conditions? One has to know how to quantify the length of the final key that can be extracted. For this particular case, under some assumptions on the classical postprocessing, it holds (Csiszár and Körner, 1978), that

$$r = \max\{I(A:B) - I_E, 0\}, \tag{3}$$

where $I(A:B) = H(A) + H(B) - H(AB)$ is the mutual information between Alice's and Bob's raw keys (H is Shannon entropy). Assuming that both bit values are equally probable, i.e., $H(A) = H(B) = 1$, one has $I(A:B) = 1 - h(Q)$, where h is the binary entropy. Having these elements, one can replace the values obtained for the intercept-resend attack and find that $I(A:B) < I_E$: Eve has more information on Alice's string than Bob: therefore no secret key can be extracted.[7]

Another simple exercise consists in supposing that Eve perform the intercept-resend attack only on a fraction p of the photons sent by Alice, and leaves the others untouched. Then obviously $Q = p/4$ and $I_E = p/2 = 2Q$; this leads to the conclusion that, if $Q \gtrsim 17\%$, a secure key cannot be extracted from the BB84 protocol—at least if the classical postprocessing is done according to the assumptions of Csiszár and Körner (1978).

6. Beyond the example: The field of QKD

The basic example just presented suggests a number of important questions.

---

[7]This conclusion is valid for all protocols: no secret key can be extracted if the observed statistics are compatible with Eve performing the intercept-resend attack (Curty, Lewenstein, and Lütkenhaus, 2004). The reason is that this attack "breaks" the quantum channel into two pieces, in which case the correlations between Alice and Bob can always be obtained with classical signals; and no secrecy can be distributed with classical communication.

- The adversary is clearly not restricted to performing the intercept-resend attack. What is the maximal amount of information Eve can possibly obtain, if she is allowed to do anything that is compatible with the laws of physics? This is a question about the possibility of proving unconditional security.

- The BB84 protocol is just a particular protocol. What about other forms of coding and/or of processing the data?

- The protocol supposed that the quantum signal is a *qubit*—explicitly, a bimodal single photon, i.e., an elementary excitation of the light field in only two modes (polarization in the explicit example). How close can an implementation come to this? And, after all, should any implementation of QKD actually aim at coming close to this?

- In a real device, information may leak out in channels that are neglected in a theoretical description. What are the potential threats in an implementation?

The whole field of QKD has developed by answering these and similar questions.

C. Scope of this review

1. Focus

The label "quantum cryptography" applies nowadays to a very wide range of interests, going from abstract mathematical considerations to strictly technological issues.

This review focuses somewhere in the middle of this range, in the realm where theoretical and experimental physics meet, which we call *practical QKD*. There, theorists cannot pursue pure formal elegance and are compelled to complicate their models in order to take real effects into account; and experimentalists must have a serious grasp of theoretical issues in order to choose the right formulas and make the correct claims about the security of their devices. Specifically, we want to address the following two concerns:

(1) On the one hand, the theoretical tools have reached a rather satisfactory level of development; but from outside the restricted group of experts, it has become almost impossible to follow this development. This is also because quite a few strong security claims made in the past had to be reconsidered in the light of better understanding. As theorists involved in the development of security proofs, we want to provide an updated review of the status of such proofs.

(2) On the other hand, several competing experimental platforms exist nowadays. It is desirable to have a synthetic view of those, highlighting the interest and possible shortcomings of each choice. Also, we want to raise awareness of the complexity of any comparison: "physical" figures of merit such as the secret key rate or the maximal achievable distance are in competition with "practical" figures of merit such as stability and cost.

Throughout the review, we also make reference to some strictly mathematical or strictly technological progress, but without any claim of exhaustiveness.

2. Outline

The review is structured as follows. Section II introduces the basic elements of practical QKD. Section III is devoted to the rate at which a secret key is produced: this is the fundamental parameter of QKD, and depends both on the speed and efficiency of the devices and on the intrinsic security of the protocol against eavesdropping. The next three sections provide a detailed analysis, with a consistent set of explicit formulas, for the three main families of protocols: those based on discrete-variable coding (Sec. IV), those based on continuous-variable coding (Sec. V), and those based on the more recent distributed-phase-reference coding (Sec. VI). In Sec. VII, we put everything together and sketch some directions for comparison of different experimental platforms. Finally, in Sec. VIII, we discuss future perspectives for QKD, both as a field in itself and in the broader context of key distribution.

II. ELEMENTS OF PRACTICAL QKD

A. Milestones

1. Foundations: 1984–1995

Quantum key distribution unfolded with the presentation of the first complete protocol (Bennett and Brassard, 1984), which was based on earlier ideas by Wiesner (1983). In the BB84 protocol, bits are coded in two complementary bases of a two-level system (qubit); this qubit is sent by Alice to Bob, who measures it. The no-cloning theorem is explicitly mentioned as the reason for security. This work was published in conference proceedings and was largely unknown to the community of physicists. It was not until 1991, when Artur Ekert, independently from the earlier developments, published a paper on quantum key distributions that the field gained rapid popularity (Ekert, 1991). Ekert's argument for security had a different flavor: an eavesdropper introduces "elements of reality" into the correlations shared by Alice and Bob; so, if they observe correlations that violate a Bell inequality, the communication cannot have been completely broken by Eve. Shortly thereafter, Bennett, Brassard, and Mermin argued[8] that entanglement-based protocols, such as E91, are equivalent to prepare-and-

---

[8] The argument is correct under some assumptions; only around 2006 was it fully realized that Ekert's view is qualitatively different and allows the set of assumptions about Alice's and Bob's devices to be reduced; see Sec. VIII.A.3. This is also why the Ekert protocol was not implemented as such in an experiment until very recently (Ling *et al.*, 2008).

measure protocols, such as the BB84 protocol (Bennett, Brassard, and Mermin, 1992). The same year 1992 witnessed two additional milestones: the invention of the B92 protocol (Bennett, 1992) and the very first in-principle experimental demonstration (Bennett, Bessette, *et al.*, 1992). One can reasonably conclude the foundational period of QKD with the definition of *privacy amplification*, the classical postprocessing needed to erase Eve's information from the raw key (Bennett *et al.*, 1995).

2. The theory-experiment gap opens: 1993–2000

After these foundational works, the interest and feasibility of QKD became apparent to many. Improved experimental demonstrations took place, first in the laboratory with a growing distance of optical fiber from the optical table (Townsend, Rarity, and Tapster, 1993; Bréguet, Muller, and Gisin, 1994; Franson and Ilves, 1994), and then in installed optical fibers (Muller, Zbinden, and Gisin, 1995), thereby demonstrating that QKD can be made sufficiently robust for a real-world implementation. In this development, an obvious milestone is the invention of the so-called *plug-and-play setups* by the Geneva group (Muller *et al.*, 1997; Ribordy *et al.*, 1998). By 2000, QKD over large distances was also demonstrated with entangled photons (Jennewein *et al.*, 2000; Naik *et al.*, 2000; Tittel *et al.*, 2000).

Theorists became very active too. New protocols were proposed. For instance, the elegant six-state protocol, first mentioned back in 1984 as a possible extension of BB84 (Bennett *et al.*, 1984), was rediscovered and studied in greater detail (Bruß, 1998; Bechmann-Pasquinucci and Gisin, 1999). But a much more complex task was at stake: the derivation of *rigorous security proofs* that would replace the intuitive arguments and the first, obviously suboptimal, estimates. The first such proof was by Mayers, who included even advanced features such as the analysis of finite key effects (Mayers, 1996, 2001). However, this proof is not very intuitive, and other proofs emerged, starting from the basic principle of entanglement distillation (Deutsch *et al.*, 1996) which were put into a rigorous framework by Lo and Chau (1999). These entanglement-based proofs would require the ability to perform quantum logic operations on signals. At present, we do not have the experimental capability to do so. Therefore the result by Shor and Preskill (2000) provided a step forward, as it combined the property of Mayers' result of using only classical error correction and privacy amplification with a very intuitive way of proving the security of the BB84 protocol. That result uses the ideas of quantum error correction methods, and reduces the corresponding quantum protocol to classically assisted prepare-and-measure protocol.

As of 2000 therefore, both experimental and theoretical QKD had made very significant advances. However, almost inevitably, a gap had opened between the two: security proofs had been derived only for very idealized schemes; setups had been made practical without paying attention to all the security issues.

3. Closing the gap: 2000 to the present

Awareness of the gap was triggered by the discovery of *photon-number-splitting* (PNS) *attacks* (Brassard, Lütkenhaus, *et al.*, 2000) which had actually been anticipated years before (Bennett, 1992; Huttner *et al.*, 1995; Dušek, Haderka, and Hendrych, 1999) but had passed rather unnoticed. The focus is on the source: the theoretical protocols supposed single-photon sources, but experiments were using attenuated laser pulses, with average photon numbers below 1. In these pulses, photons are distributed according to Poissonian statistics: in particular, there are sometimes two or more photons, and this opens an important loophole. Security proofs can be adapted to deal with the case (Lütkenhaus, 2000; Gottesman, Lo, Lütkenhaus, and Preskill, 2004; Inamori, Lütkenhaus, and Mayers, 2007): the extractable secret key rate was found to scale much more poorly with the distance than for single-photon sources (t^2 compared to t, where t is the transmittivity of the quantum channel).

It took a few years to realize that methods can be devised to reduce the power of PNS attacks while keeping the very convenient laser sources. One improvement can be made by a mere change of software by modifying the announcements of the BB84 protocol (Scarani, Acín, Ribordy, and Gisin, 2004): in this SARG04 protocol, the key rate scales as $t^{3/2}$ (Koashi, 2005; Kraus, Gisin, and Renner, 2005). Another significant improvement can be made by an easy change of hardware: by varying the quantum state throughout the protocol (*decoy states*), one can perform a more complete test of the quantum channel (Hwang, 2003). When the decoy state idea is applied to laser sources, the key rate scales as t (Lo, Ma, and Chen, 2005; Wang, 2005).

Parallel to this development, the field of practical QKD[9] has grown in breadth and maturity. New families of protocols have proposed, notably *continuous-variable protocols* (Ralph, 1999; Hillery, 2000; Cerf, Lévy, and Van Assche, 2001; Gottesman and Preskill, 2001; Grosshans and Grangier, 2002; Silberhorn *et al.*, 2002) and the more recent *distributed-phase-reference protocols* (Inoue, Waks, and Yamamoto, 2002; Stucki *et al.*, 2005). Critical thinking on existing setups has led to the awareness that security against Eve tapping into the quantum channel is not all that should be considered: one should also protect the devices against more commonplace *hacking attacks* and verify that information does not leak out in *side channels* (Makarov and Hjelme, 2005). Recently, QKD has also reached the commercial market: at least three companies[10] are offering working QKD devices. New questions can now be addressed: in which applications QKD can help (Alléaume *et al.*,

---

[9]The whole field of QKD witnessed many other developments, especially in theoretical studies, which are not discussed here but are mentioned later.

[10]idQuantique, Geneva (Switzerland) (www.idquantique.com); MagiQ Technologies, Inc., New York (www.magiqtech.com); and Smartquantum, Lannion (France) (www.smartquantum.com).

2007), how a network of QKD systems can be implemented,[11] how QKD devices can be certified for commercial markets (including the verification that these devices indeed satisfy the specifications of the corresponding security proofs), etc.

B. Generic QKD protocol

1. Classical and quantum channels

As mentioned in Sec. I.B, Alice and Bob need to be connected by two channels. On the quantum channel, Alice can send quantum signals to Bob. Eve can interact with these signals, but if she does, the signals are changed because of the laws of quantum physics—the essence of QKD lies precisely here.

On the classical channel, Alice and Bob can send classical messages back and forth. Eve can listen without penalty to all communication that takes place on this channel. However, in contrast to the quantum channel, the classical channel is required to be authenticated so that Eve cannot change the messages that are being sent on this channel. Failure to authenticate the classical channel can lead to a situation where Eve impersonates one of the parties to the other, thus entirely compromising the security. Unconditionally secure authentication[12] of the classical channel requires Alice and Bob to pre-share an initial secret key or at least partially secret but identical random strings (Renner and Wolf, 2005). QKD therefore does not create a secret key out of nothing: rather, it expands a short secret key into a long one, so strictly speaking it is a method of key growing. This remark calls for two comments. First, key growing cannot be achieved by use of classical means alone, whence QKD offers a real advantage. Second, it is important to show that the secret key emerging from QKD is *composable*, that is, it can be used like a perfect random secret key in any task (see Sec. II.C.2) because one has to use a part of it as authentication key for the next round.

2. Quantum information processing

The first step of a QKD protocol is the exchange and measurement of signals on the quantum channel. Alice's role is *encoding*: the protocol must specify which quantum state $|\Psi(\mathcal{S}_n)\rangle$ codes for the sequence of n symbols $\mathcal{S}_n = \{s_1, \ldots, s_n\}$. In most protocols, but not in all, the state $|\Psi(\mathcal{S}_n)\rangle$ has the tensor product form $|\psi(s_1)\rangle \otimes \cdots$

$\otimes |\psi(s_n)\rangle$. In all cases, it is crucial that the protocol uses a set of nonorthogonal states,[13] otherwise Eve could decode the sequence without introducing errors by measuring in the appropriate basis (in other words, a set of orthogonal states can be perfectly cloned). Bob's role is twofold: his measurements of course allow the signal to be *decoded*, but also an estimation of the loss of quantum coherence and therefore Eve's information. For this to be possible, noncompatible measurements must be used.

We have described the quantum coding of QKD protocols with the language of prepare-and-measure (P&M) schemes: Alice chooses actively the sequence $\mathcal{S}_n$ she wants to send, prepares the state $|\Psi(\mathcal{S}_n)\rangle$, and sends it to Bob, who performs some measurement. Any such scheme can be immediately translated into an *entanglement-based* (EB) scheme: Alice prepares the entangled state

$$|\Phi^n\rangle_{AB} = \frac{1}{\sqrt{d_n}} \sum_{\mathcal{S}_n} |\mathcal{S}_n\rangle_A \otimes |\Psi(\mathcal{S}_n)\rangle_B, \qquad (4)$$

where d_n is the number of possible $\mathcal{S}_n$ sequences and $|\mathcal{S}_n\rangle_A$ form an orthogonal basis. By measuring in this basis, Alice learns one $\mathcal{S}_n$ and prepares the corresponding $|\Psi(\mathcal{S}_n)\rangle$ on the subsystem that is sent to Bob: from Bob's point of view, nothing changes. This formal translation does not mean that both realizations are equally practical or even feasible with present-day technology. However, it implies that the security proof for the EB protocol translates immediately to the corresponding P&M protocol and vice versa.

A frequently quoted statement concerning the role of entanglement in QKD says that "entanglement is a necessary condition to extract a secret key" (Curty, Lewenstein, and Lütkenhaus, 2004; Acín and Gisin, 2005). Two important comments have to be made to understand this correctly. First, this is not a statement about implementations, but about the quantum channel: it says that no key can be extracted from an entanglement-breaking channel.[14] In particular, the statement does not say that entanglement-based implementations are the only secure ones.

Second, as formulated above, the statement has been derived under the assumption that Eve holds a purifica-

---

[12]Authentication schemes that do not rely on preshared secrecy exist, but are not unconditionally secure. Since we aim at unconditional security for QKD, the same level of security must in principle be guaranteed in all auxiliary protocols. However, breaking the authentication code after one round of QKD does not threaten security of the key that has been produced; one may therefore consider authentication schemes that guarantee security only for a limited time, e.g., those based on complexity assumptions.

[13]There is only one exception (Goldenberg and Vaidman, 1995) when Alice uses just two orthogonal states. Alice prepares a qubit in one of the two orthogonal superpositions of two spatially separated states; then—at a random time instant—she sends one component of this superposition to Bob. Only later does she send the second component. Precise time synchronization between Alice and Bob is crucial. See also Peres (1996), Goldenberg and Vaidman (1996), and a related discussion (Koashi and Imoto, 1997). Unconditional security has not been proved for this protocol.

[14]As the name indicates, a channel $\rho \to \rho' = C(\rho)$ is called *entanglement breaking* if $(1 \otimes C)|\Psi\rangle_{AB}$ is separable for any input $|\Psi\rangle_{AB}$. A typical example of such a channel is obtained by performing a measurement on half of the entangled pair.

tion of ρ_{AB}, where A and B are the degrees of freedom that Alice and Bob are going to measure. One may ask a more general question, namely, how to characterize the *private states*, i.e., the states out of which secrecy can be extracted (Horodecki *et al.*, 2005, 2008a, 2008b). It was realized that, in the most general situation, Alice and Bob may control some additional degrees of freedom A' and B'; thus, Eve is not given a purification of ρ_{AB}, but of $\rho_{AA'BB'}$. In such a situation, it turns out that ρ_{AB} can even be separable; as for $\rho_{AA'BB'}$, it must be entangled, but may even be bound entangled. The reason is quite clear: A' and B' shield the meaningful degrees of freedom from Eve's knowledge. We do not consider this most general approach in what follows[15] because currently no practical QKD scheme with shielding systems has been proposed.

3. Classical information processing

Once a large number N of signals have been exchanged and measured on the quantum channel, Alice and Bob start processing their data by exchanging communication via the classical channel. In all protocols, Alice and Bob estimate the statistics of their data; in particular, they can extract the meaningful parameters of the quantum channel: error rate in decoding, loss of quantum coherence, transmission rate, detection rates, etc. This step, called parameter estimation, may be preceded in some protocols by a sifting phase, in which Alice and Bob agree to discard some symbols (typically, because Bob learns that he has not applied the suitable decoding on those items). After parameter estimation and possibly sifting, both Alice and Bob hold a list of $n \leq N$ symbols, called raw keys. These raw keys are only partially correlated and only partially secret. Using some classical information post-processing (see Sec. III.B.1), they can be transformed into a fully secure key K of length $\ell \leq n$. The length ℓ of the final secret key depends of course on Eve's information about the raw keys.

4. Secret fraction and secret key rate

In the asymptotic case $N \to \infty$ of infinitely long keys, the meaningful quantity is the secret fraction[16]

$$r = \lim_{N \to \infty} \ell/n. \tag{5}$$

The secret fraction is clearly the heart of QKD: this is the quantity for which the security proofs Sec. II.C.3 must provide an explicit expression. However, a more prosaic parameter must also be taken into account as well in practical QKD: namely, the raw-key rate R, i.e., the length of the raw key that can be produced per unit time. This rate depends partly on the protocol: for in-

stance, it contains the sifting factor, i.e., the fraction of exchanged symbols that is discarded in a possible sifting phase. But certainly its largest dependence is on the details of the setup: repetition rate of the source, losses in the channel, efficiency and dead time of the detectors, possible duty cycle, etc. In conclusion, in order to assess the performances of practical QKD systems, it is natural to define the secret key rate as the product

$$K = Rr. \tag{6}$$

Section III presents a detailed discussion of this quantity.

As we mentioned, these definitions hold in the asymptotic regime of infinitely long keys. When finite-key corrections are taken into account, a reduction in the secret fraction is expected, mainly for two reasons. On the one hand, parameter estimation is made on a finite number of samples, and consequently one has to consider the worst possible values compatible with statistical fluctuations. On the other hand, the yield of the classical postprocessing contains terms that vanish only in the asymptotic limit; intuitively, these correction take care of the fact that security is never absolute: the probability that Eve knows an n-bit key is at least 2^{-n}, which is strictly positive. In this review, we restrict our attention to the asymptotic case, not because finite-key corrections are negligible—quite the opposite seems to be true[17]—but because their estimate is still the object of ongoing research (see Sec. VIII.A.1 for the state of the art).

C. Notions of security

1. Unconditional security and its conditions

The appeal of QKD comes mainly from the fact that, in principle, it can achieve *unconditional security*. This technical term means that security can be proved without imposing any restriction on the computational resources or the manipulation techniques that are available to the eavesdropper acting on the signal. The possibility of achieving unconditional security in QKD is deeply rooted in quantum physics. To learn something about the key, Eve must interact with the quantum system; now, if the coding uses randomly chosen nonorthogonal states, Eve's intervention necessarily modifies the state on average, and this modification can be observed by the parties. As discussed in Sec. I.B, there are many equivalent formulations of this basic principle. However formulated it must be stressed that this criterion can be made quantitative: the observed perturbations in the quantum channel allow computation of a bound on the information that Eve might have obtained.

Like many other technical terms, "unconditional security" has to be used in its precise meaning given above, and not as a synonym for "absolute security"—

---

[15]Smith, Renes, and Smolin (2008) used the formalism of private states to study preprocessing (see Sec. III.B.1).
[16]Often, especially in theoretical studies, this quantity is called the "secret key rate." Here we reserve this term for Eq. (6), which is more meaningful for practical QKD.

[17]For instance, in the only experiment analyzed with finite-key formalism to date (Hasegawa *et al.*, 2007), the authors extracted $r \approx 2\%$, whereas, for the observed error rate, the asymptotic bound would have yielded $r \gtrsim 40\%$.

something that does not exist. As a matter of fact, the unconditional security of QKD holds under some conditions. First, there are some compulsory requirements:

(1) Eve cannot intrude into Alice's and Bob's devices to access either the emerging key or their choices of settings (in Sec. III.B.4 we show how complex it is to check this point thoroughly).

(2) Alice and Bob must trust the random number generators that select the state to be sent or the measurement to be performed.

(3) The classical channel is authenticated with unconditionally secure protocols, which exist (Carter and Wegman, 1979; Wegman and Carter, 1981; Stinson, 1995).

(4) Eve is limited by the laws of physics. This requirement can be sharpened: in particular, one can ask whether security can be based on a restricted set of laws.[18] In this review, as in the whole field of practical QKD, we assume that Eve has to obey the whole of quantum physics.

We take these requirements, the failure of which would obviously compromise any security, as granted. Even so, many other issues have to be settled before unconditional security is claimed for a given protocol: for instance, the theoretical description of the quantum states must match the signals that are really exchanged; the implementations must be proved free of unwanted information leakage through side channels or back doors, against which no theoretical protection can be invoked.

2. Definition of security

The security of a key $\mathcal{K}$ can be parametrized by its deviation ε from a perfect key, which is defined as a list of perfectly correlated symbols shared between Alice and Bob, about which Eve has no information (in particular, all possible lists must be equally probable *a priori*). A definition of security is a choice of the quantity

that is required to be bounded by ε; a key that deviates by ε from a perfect key is called ε secure. The main property that a definition of security must satisfy is composability, meaning that the security of the key is guaranteed whatever its application may be—more precisely if an ε-secure key is used in an ε'-secure task,[19] composability ensures that the whole procedure is at least $\varepsilon + \varepsilon'$ secure.

A composable definition of security is the one based on the trace norm (Ben-Or *et al.*, 2005; Renner and König, 2005): $\frac{1}{2}\|\rho_{\mathcal{K}E} - \tau_{\mathcal{K}} \otimes \rho_E\|_1 \leqslant \varepsilon$, where $\rho_{\mathcal{K}E}$ is the actual state containing some correlations between the final key and Eve, $\tau_{\mathcal{K}}$ is the completely mixed state on the set $\mathcal{K}$ of possible final keys, and ρ_E is any state of Eve. In this definition, the parameter ε has a clear interpretation as the maximum failure probability of the process of key extraction. As shown, the issue of composability was raised rather late in the development of QKD. Most, if not all, of the early security studies had adopted a definition of security that is not composable, but the asymptotic bounds that were derived can be "redeemed" using a composable definition.[20]

3. Security proofs

Once the security criterion is defined, one can derive a full security proof, leading to an explicit (and hopefully computable) expression for the length of the extractable secret key rate. Several techniques have been used:

- The very first proofs by Mayers were somehow based on the uncertainty principle (Mayers, 1996, 2001).

---

[18]As we have seen (Sec. I.B.2), intuition suggests that the security of QKD can be traced back to a few specific principles or laws like "no-cloning" or "nonlocality without signaling." One may ask whether this intuition can be made fully rigorous. Concretely, since any theory that does not allow signaling and is nonlocal exhibits a no-cloning theorem (Barnum *et al.*, 2006; Masanes, Acín, and Gisin, 2006), and since nonlocality itself can be checked, one may hope to derive security only from the physical law of *no signaling*. In this framework, unconditional security has been proved only in the case of strictly error-free channels and for a key of vanishing length (Barrett, Hardy, and Kent, 2005). Only limited security has been proved in more realistic cases (Acín, Gisin, and Masanes, 2006; Scarani *et al.*, 2006). Recently, Masanes showed that unconditional composable security can be proved if no-signaling is assumed not only between Alice and Bob, but also among the systems that are measured by each partner (Masanes, 2008).

[19]For instance, the one-time pad is a 0-secure task, while any implementation of channel authentication, for which a part of the key is used (Sec. II.B.1), must allow for a nonzero ε'.

[20]The early proofs defined security by analogy with the classical definition: Eve, who holds a quantum state ρ_E, performs the measurement $\mathcal{M}$ which maximizes her mutual information with the key $\mathcal{K}$. This defines the so-called *accessible information* $I_{\mathrm{acc}}(\mathcal{K}:\rho_E) = \max_{E=\mathcal{M}(\rho_E)} I(\mathcal{K}:E)$, and the security criterion reads $I_{\mathrm{acc}}(\mathcal{K}:\rho_E) \leqslant \varepsilon$. As for the history of claims, it is quite intricate. Accessible information was first claimed to provide composable security (Ben-Or *et al.*, 2005). The proof is correct, but composability follows from the use of two-universal hashing in the privacy amplification step (see Sec. III.B.1), rather than from the properties of accessible information itself. Indeed, shortly thereafter, an explicit counterexample showed that accessible information is in general not composable for any choice of the security parameter ε (König *et al.*, 2007). The reason why accessible information is not composable can be explained qualitatively: this criterion supposes that Eve performs a measurement to guess the key at the end of the key exchange. But Eve may prefer not to measure her systems until the key is actually used in a further protocol: for instance, if a plaintext attack can reveal some information, Eve should certainly adapt her measurement to this additional knowledge. The counterexample also implies that the classical results on privacy amplification by two-universal hashing (Bennett *et al.*, 1995) do not apply and have to be replaced by a quantum version of the statement (Renner and König, 2005).

This approach has been revived recently by Koashi (2006a, 2007).

- Most of the subsequent security proofs have been based on the correspondence between entanglement distillation and classical post processing, generalizing the techniques of Shor and Preskill (2000). For instance, the most developed security proofs for imperfect devices follow this pattern (Gottesman, Lo, Lütkenhaus, and Preskill, 2004).

- The most recent techniques use instead information-theoretical notions (Ben-Or, 2002; Kraus, Gisin, and Renner, 2005; Renner, 2005; Renner, Gisin, and Kraus, 2005).

A detailed description of how a security proof is built goes beyond the scope of this review. The core lies in relating the security requirement $\frac{1}{2}\|\rho_{\mathcal{K}E} - \tau_{\mathcal{K}} \otimes \rho_E\|_1 \leqslant \varepsilon$ to a statement about the length ℓ of the secret key that can be extracted. This step is achieved using inequalities that can be seen as a generalization of the Chernoff bound. In other words, one must use or prove an inequality of the form

$$\text{Prob}(\|\rho_{\mathcal{K}E} - \tau_{\mathcal{K}} \otimes \rho_E\|_1 > 2\varepsilon) \lesssim e^{\ell - F(\rho_{\mathcal{K}E}, \varepsilon)}, \tag{7}$$

where we omitted constant factors. From such an inequality, one can immediately see that the security requirement will fail with exponentially small probability provided $\ell \lesssim F(\rho_{\mathcal{K}E}, \varepsilon)$. Explicit security bounds will be provided below (Sec. III.B) for the asymptotic limit of infinitely long keys—note that in this limit one can take $\varepsilon \to 0$, whence no explicit dependence on ε is manifest in those expressions.

D. Explicit protocols

1. Three families

The number of explicit QKD protocols is virtually infinite: after all, Bennett has proved that security can be obtained when a bit is coded in just two nonorthogonal quantum states (Bennett, 1992). But as a matter of fact this possible variety has crystallized into three main families: discrete-variable coding (Sec. II.D.2), continuous-variable coding (Sec. II.D.3), and more recently distributed-phase-reference coding (Sec. II.D.4). The crucial difference is the detection scheme: discrete-variable coding and distributed-phase-reference coding use photon counting and postselect the events in which a detection has effectively taken place, while continuous-variable coding is defined by the use of homodyne detection (detection techniques are reviewed in Sec. II.G).

Discrete-variable coding is the original one. Its main advantage is that protocols can be designed in such a way that, in the absence of errors, Alice and Bob immediately share a perfect secret key. They are still the most frequently implemented QKD protocols. Any discrete quantum degree of freedom can be chosen in principle, but the most frequent ones are polarization for free-space implementations and phase coding in fiber-based implementations.[21] The case for continuous-variable coding stems from the observation that photon counters normally feature low quantum efficiencies, high dark count rates, and rather long dead times, while these inconveniences can be overcome using homodyne detection. The price to pay is that the protocol provides Alice and Bob with correlated but rather noisy realization of a continuous random variable, because losses translate into noise (see Sec. I.B.3): as a consequence, a significant amount of error correction must be used. In short, the issue is whether it is better to build up a noiseless raw key slowly or a noisy one rapidly. As for distributed-phase-reference coding, its origin lies in the efforts of some experimental groups toward a more practical implementation. From the point of view of detection, these protocols produce a discrete-valued result; but the nature of the quantum signals is very different from that in discrete-variable coding, and this motivates a separate treatment.

Despite the differences originating from the use of a different detection device, there is a strong conceptual unity underlying discrete- and continuous-variable QKD. To take just one example, in both cases the ability to distribute a quantum key is closely related to the ability to distribute entanglement, regardless of the detection scheme used and even if no actual entanglement is present. These similarities are not very surprising since it has long been known that the quantum features of light may be revealed either via photon counting (e.g., antibunching or anticorrelation experiments) or via homodyne detection (e.g., squeezing experiments). Since QKD is a technique that exploits these quantum features of light, there is no reason for it to be restricted to the photon-counting regime. Surprisingly, just as antibunching (or a single-photon source) is not even needed in photon-counting-based QKD, squeezing is shown not needed in homodyne-detection-based QKD. The only quantum feature that happens to be needed is the nonorthogonality of light states.

2. Discrete-variable protocols

a. BB84-BBM

The best known discrete-variable protocol is of course BB84 (Bennett and Brassard, 1984), which we introduced in Sec. I.B. The corresponding EB protocol is known as BBM (Bennett, Brassard, and Mermin, 1992); the E91 protocol (Ekert, 1991) is equivalent to it when implemented with qubits. Alice prepares a single particle in one of the four states

$$|+x\rangle, |-x\rangle, \quad \text{eigenstates of } \sigma_x,$$

$$|+y\rangle, |-y\rangle, \quad \text{eigenstates of } \sigma_y, \qquad (8)$$

where σ's are Pauli operators. The states with $+$ code for the bit value 0, the states with $-$ for the bit value 1. Bob measures either σ_x or σ_y. In the absence of errors, measurement in the correct basis reveals the bit value encoded by Alice. The protocol includes a sifting phase: Alice reveals the basis, X or Y, of each of her signals; Bob accepts the values for which he has used the same basis and discards the others.[22]

Unconditional security of the BB84-BBM protocols has been proved with many different techniques (Mayers, 1996, 2001; Lo and Chau, 1999; Shor and Preskill, 2000; Kraus, Gisin, and Renner, 2005). The same coding can be implemented with other sources, leading to a family of BB84-like protocols. We review them in Sec. IV.B.

b. SARG04

The SARG04 protocol (Acín, Gisin, and Scarani, 2004; Scarani, Acín, Ribordy, and Gisin, 2004) uses the same four states Eq. (8) and the same measurements on Bob's side as BB84, but the bit is coded in the basis rather than in the state (basis X codes for 0 and basis Y codes for 1). Bob has to choose his bases with probability $\frac{1}{2}$. The creation of the raw key is slightly more complicated than in BB84. Suppose for definiteness that Alice sends $|+x\rangle$: in the absence of errors if Bob measures X, he gets $s_b = +$; if he measures Y, he may get both $s_b = +/-$ with equal probability. In the sifting phase, Bob reveals s_b; Alice tells him to accept if she had prepared a state with $s_a \neq s_b$, in which case Bob accepts the bit corresponding to the basis he has not used. The reason is clear in the example above: in the absence of errors, $s_b = -$ singles out the wrong basis.[23]

SARG04 was invented for implementations with attenuated laser sources because it is more robust than BB84 against the PNS attacks. Unconditional security has been proved; the main results are reviewed in Sec. IV.D.

---

[22]In the original version of BB84, both bases are used with the same probability so that the sifting factor is $p_{\text{sift}} = 1/2$, i.e., only half of the detected bits will be kept in the raw key. But the protocol can be made asymmetric without changing the security (Lo, Chau, and Ardehali, 2005): Alice and Bob can agree on using one basis with probability $1 - \epsilon$, where ϵ can be taken as small as one wants, so as to have $p_{\text{sift}} \approx 1$ [recall that we are considering only asymptotic bounds; in the finite-key regime, the optimal value of ϵ can be computed (Scarani and Renner, 2008)].

[23]In an alternative version of the sifting, Alice reveals that the state she sent belongs to one of the two sets $\{|s_a x\rangle, |s_a y\rangle\}$, and Bob accepts it if he has detected a state $s_b \neq s_a$. This is a simplified version with respect to the original proposal, where Alice could declare any of the four sets of two nonorthogonal states. The fact that the two versions are equivalent in terms of security was not clear when the first rigorous bounds were derived (Branciard *et al.*, 2005), but was verified later.

c. Other discrete-variable protocols

A large number of other discrete-variable protocols have been proposed; all of them have features that makes them less interesting for practical QKD than BB84 or SARG04.

The *six-state protocol* (Bennett *et al.*, 1984; Bruß, 1998; Bechmann-Pasquinucci and Gisin, 1999) follows the same structure as BB84, to which it adds the third mutually unbiased basis Z defined by the Pauli matrix σ_z. Its unconditional security was proved quite early (Lo, 2001). The interest of this protocol lies in the fact that the channel estimation becomes "tomographically complete," that is, the measured parameters completely characterize the channel. As a consequence, more noise can be tolerated than with the BB84 or SARG04 protocols. However, noise is quite low in optical setups, while losses are a greater concern (see Sec. II.F). In this respect, the six-state protocol perform worse because it requires additional lossy optical components. Similar considerations apply to the six-state version of the SARG04 coding (Tamaki and Lo, 2006) and to the Singapore protocol (Englert *et al.*, 2004).

The coding of BB84 and six-state protocols has been generalized to larger dimensional quantum systems (Bechmann-Pasquinucci and Peres, 2000; Bechmann-Pasquinucci and Tittel, 2000). For any d, protocols that use either two or $d+1$ mutually unbiased bases have been defined (Cerf *et al.*, 2002). Unconditional security was not studied; for restricted attacks, the robustness to noise increases with d. Time-bin coding allows d-dimensional quantum states of light to be produced in a rather natural way (De Riedmatten, Marcikic, *et al.*, 2004; Thew *et al.*, 2004). However, the production and detection of these states requires d-arm interferometers with couplers or switches, which must moreover be kept stable. Thus, again, the possible advantages are overcome by the practical issues of losses and stability.

Finally, we mention the B92 protocol (Bennett, 1992), which uses only two nonorthogonal states, each one coding for one bit value. In terms of encoding, this is obviously the most economic possibility. Unfortunately, B92 is a rather sensitive protocol: as noticed in the original paper, this protocol is secure only if some other signal (e.g., a strong reference pulse) is present along with the two states that code the bit. Unconditional security has been proved for single-photon implementations (Tamaki, Koashi, and Imoto, 2003; Tamaki and Lütkenhaus, 2004) and for some implementations with a strong reference pulse (Koashi, 2004; Tamaki *et al.*, 2006). Incidentally, the SARG04 protocol may be seen as a modified B92, in which a second set of nonorthogonal states is added—actually, an almost forgotten protocol served as a link between the two (Huttner *et al.*, 1995).

3. Continuous-variable protocols

Discrete-variable coding can be implemented with several sources, but requires photon-counting techniques. An alternative approach to QKD has been suggested, in which the photon counters are replaced by

standard telecom *p-i-n* photodiodes, which are faster (gigahertz instead of megahertz) and more efficient (typically 80% instead of 10%). The corresponding measurement schemes are then based on homodyne detection (Sec. II.G.2) and involve measuring data that are real amplitudes instead of discrete events; hence these schemes are named continuous-variable (CV) QKD.

The first proposals suggesting the use of homodyne detection in QKD are due to Ralph (1999), Hillery (2000) and Reid (2000). In particular, a squeezed-state version of BB84 was proposed by Hillery (2000), where Alice's basis choice consists of selecting whether the state of light sent to Bob is squeezed in the quadrature $q=x$ or $q=p$. Next, this q-squeezed state is displaced in q by either $+c$ or $-c$ depending on a random bit chosen by Alice, where c is an appropriately chosen constant. Bob's random basis choice defines whether it is the x or p quadrature that is measured. The sifting simply consists in keeping only the instances where Alice and Bob's chosen quadratures coincide. In this case, the value measured by Bob is distributed according to a Gaussian distribution centered on the value ($+c$ or $-c$) sent by Alice. In some sense, this protocol can be viewed as "hybrid" because Alice's data are binary while Bob's data are real (Gaussian distributed).

These early proposals and their direct generalization are called CV protocols with discrete modulation; at the same time, another class of CV protocols was proposed that instead use a continuous modulation, in particular a Gaussian modulation. Although CV protocols are much more recent than discrete-variable protocols, their security proofs have been progressing steadily over recent years, and are now close to reaching a comparable status, see Sec. V.A

a. Gaussian protocols

The first proposed Gaussian QKD protocol was based on squeezed states of light, which are modulated with a Gaussian distribution in the x or p quadrature by Alice, and are measured via homodyne detection by Bob (Cerf, Lévy and Van Assche, 2001). This protocol can be viewed as the proper continuous-variable counterpart of BB84 in the sense that the average state sent by Alice is the same regardless of the chosen basis (it is a thermal state, replacing the maximally mixed qubit state in BB84). The security of this protocol can be analyzed using the connection with continuous-variable cloning (Cerf, Ipe, and Rottenberg, 2000); using a connection with quantum error-correcting codes, unconditional security was proved when the squeezing exceeds 2.51 dB (Gottesman and Preskill, 2001). The main drawback of this protocol is the need for a source of squeezed light.

A second Gaussian QKD protocol was therefore devised, in which Alice generates coherent states of light, which are then Gaussian modulated in both x and p, while Bob still performs homodyne detection (Grosshans and Grangier, 2002a). A first proof-of-principle experiment, supplemented with the technique of reverse

reconciliation,[24] was run with bulk optical elements on an optics table (Grosshans, Van Assche, *et al.*, 2003). Subsequent experiments have used optical fibers and telecom wavelengths. The scheme was thus implemented over distances up to 14 km using a plug-and-play configuration (Legré, Zbinden, and Gisin, 2006); then up to 25 km by time multiplexing the local oscillator pulses with the signal pulses in the same optical fiber and using an improved classical postprocessing (Lodewyck *et al.*, 2005; Lodewyck, Bloch, *et al.*, 2007). Another fiber-based implementation over 5 km has been reported (Qi, Fung, *et al.*, 2007).

Note that, in these two first protocols, Bob randomly chooses to homodyne one quadrature, either x or p. In the squeezed-state protocol, this implies the need for sifting. Bob indeed needs to reject the instances where he measured the other quadrature rather than the one modulated by Alice, which results in a decrease in the key rate by a factor of 2 (this factor may actually be reduced arbitrarily close to 1 by making an asymmetric choice between x and p, provided that the key length is sufficiently large) (Lo, Chau, and Ardehali, 2005). In the coherent-state protocol, Alice simply forgets the quadrature that is not measured by Bob, so that all pulses do carry useful information that is exploited to establish the final secret key.

The fact that Alice, in this second protocol, discards half of her data may look like a loss of efficiency since some information is transmitted and then lost. A third Gaussian QKD protocol was therefore proposed (Weedbrook *et al.*, 2004), in which Alice still transmits doubly modulated coherent states drawn from a bivariate Gaussian distribution, but Bob performs heterodyne instead of homodyne measurements,[25] that is, he measures both x and p quadratures simultaneously. At first sight, this seems to imply that the rate is doubled since Bob then acquires a pair of quadratures (x,p). Actually, since heterodyne measurement effects one additional unit of vacuum noise on the measured quadratures, the two quadratures received by Bob are noisier than the single quadrature in the homodyne-based protocol. The net effect, however, is often an increase in the key rate when the two quadratures are measured simultaneously. In addition, a technological advantage of this heterodyne-based coherent-state protocol is that there is no need to choose a random quadrature at Bob's side (that is, no active basis choice is needed). The experiment has been realized (Lance *et al.*, 2005).

Finally, a fourth Gaussian QKD protocol was introduced recently (García-Patrón, 2007), which completes

---

[24]In all Gaussian QKD protocols, reversing the one-way reconciliation procedure (i.e., using Bob's measured data instead of Alice's sent data as the raw key) is beneficial in terms of attainable range, provided that the noise is not too large. We return to this point in Sec. V.

[25]This possibility was also suggested for postselection-based protocols by Lorenz, Korolkova, and Leuchs (2004), and the experiment has been performed (Lorenz *et al.*, 2006).

this family of Gaussian QKD protocols. Here Alice sends again squeezed states, as in the protocol of Cerf, Lévy, and Van Assche (2001), but Bob performs heterodyne measurements, as in the protocol of Weedbrook *et al.* (2004). This protocol is associated with the highest rate and range among all Gaussian QKD protocols, but requires a source of squeezed light.

As seen in the above discussion about BB84 and SARG04 protocols, it turns out for the CV QKD protocols that classical processing is also an essential element of the protocol. As discussed later (Sec. V.A), the performance of CV-QKD protocols depends crucially on the exact protocol that extracts the secret key from the experimental data. Two important tools here are reverse reconciliation (Grosshans and Grangier, 2002a) and postselection (Silberhorn *et al.*, 2002). As shown by Heid and Lütkenhaus (2007), the combination of both will lead to the optimal key rate.

b. Discrete-modulation protocols

For practical implementation, it is desirable to keep the number of signals as low as possible, and to minimize the number of parameters in the detection process that need to be monitored. The reason behind this is that in practical implementation at some stage one has to consider finite-size effects in the statistics and in the security proof stage. For a continuous family of signals, it will be intuitively harder to determine these finite-size effects and to include statistical fluctuations of observations in a full security proof.

For this reason, it is interesting to study QKD systems that combine a finite number of signals with the continuous-variable detection schemes: discrete-modulation protocols have been devised following this proposal, some based on coherent states instead of squeezed states (Silberhorn *et al.*, 2002). The signals consist here of a weak coherent state together with a strong phase reference. The signal is imprinted onto the weak coherent state by setting the relative optical phase between weak coherent state and reference pulse to either 0 or π. Schematically, the strong phase reference could be represented by two local oscillators, e.g., phase-locked lasers at the sending and receiving stations. These types of signals were already used in the original B92 protocol (Bennett, 1992). The receiver then uses the local oscillator in the homodyne or heterodyne measurement. The security of this protocol is still based on the fact that the weak signal pulses represent nonorthogonal signal states.

On the receiver side, homodyne detection is performed by choosing at random one of the two relevant quadrature measurement (one quadrature allows measurement of the bit values; the other serves the purpose of monitoring the channel to limit possible eavesdropping attacks). Alternatively, a heterodyne measurement can monitor both quadratures. Consider for definiteness a simple detection scheme, in which bit values are assigned by the sign of the detection signal, $+$ or $-$, with respect to the half planes in the quantum optical phase space in which the two signals reside. As a result, both
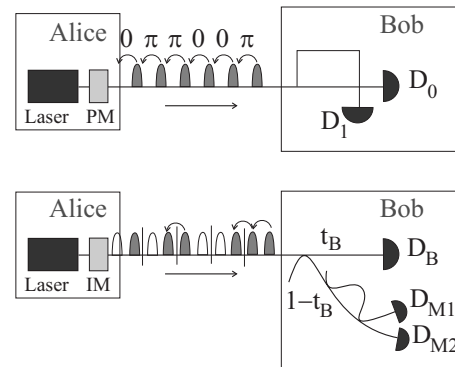
FIG. 2. The two-distributed-phase reference protocol: differential phase shift (DPS, top) and coherent one-way (COW, bottom). Legend: PM, phase modulator; IM, intensity modulator. See text for description.

sender and receiver have binary data at hand. As in the case of Gaussian modulation, they can now perform postselection of data, and use error correction and privacy amplification to extract secret keys from these data.

4. Distributed-phase-reference protocols

Both discrete- and continuous-variable protocols were invented by theorists. Some experimental groups, in their developments toward practical QKD systems, have conceived new protocols, which do not fit in the categories above. In these, as in discrete-variable protocols, the raw keys are made up of realizations of a discrete variable (a bit) and are already perfectly correlated in the absence of errors. However, the quantum channel is monitored using the properties of coherent states—more specifically, by observing the phase coherence of subsequent pulses; whence the name distributed-phase-reference protocols.

The first such protocol has been called the differential phase shift (DPS) (Inoue, Waks, and Yamamoto, 2002, 2003). Alice produces a sequence of coherent states of the same intensity,

$$|\Psi(\mathcal{S}_n)\rangle = \cdots |e^{i\varphi_{k-1}}\sqrt{\mu}\rangle|e^{i\varphi_k}\sqrt{\mu}\rangle|e^{i\varphi_{k+1}}\sqrt{\mu}\rangle\cdots, \qquad (9)$$

where each phase can be set at $\varphi=0$ or π (Fig. 2). The bits are encoded in the difference between two successive phases: $b_k=0$ if $e^{i\varphi_k}=e^{i\varphi_{k+1}}$ and $b_k=1$ otherwise. This can be unambiguously discriminated using an unbalanced interferometer. The complexity in the analysis of this protocol lies in the fact that $|\Psi(\mathcal{S}_n)\rangle \neq |\psi(b_1)\rangle \otimes \cdots \otimes |\psi(b_n)\rangle$: the kth pulse contributes to both the kth and $(k+1)$st bits. The DPS protocol has already been the object of several experiments (Takesue *et al.*, 2005, 2007; Diamanti *et al.*, 2006).

In the protocol called coherent one way (COW) (Gisin *et al.*, 2004; Stucki *et al.*, 2005), each bit is encoded in a sequence of one nonempty and one empty pulse,

$$|0\rangle_k = |\sqrt{\mu}\rangle_{2k-1}|0\rangle_{2k}, \quad |1\rangle_k = |0\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}. \qquad (10)$$

These two states can be unambiguously discriminated in an optimal way by measuring the time of arrival

(Fig. 2). For the channel estimation, one checks the coherence between two successive nonempty pulses; these can be produced on purpose as a "decoy sequence" $|\sqrt{\mu}\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}$, or can happen as $|\sqrt{\mu}\rangle_{2k}|\sqrt{\mu}\rangle_{2k+1}$ across a bit separation, when a sequence $|1\rangle_k|0\rangle_{k+1}$ is coded. This last check, important to detect PNS attacks, implies that the phase between any two successive pulses must be controlled; therefore, as happens for DPS, the whole sequence must be considered as a single signal. A prototype of a full QKD system based on COW has been reported recently (Stucki *et al.*, 2008).

Both DPS and COW are P&M schemes, tailored for laser sources. It has not yet been possible to derive a bound for unconditional security because the existing techniques apply only when $|\Psi(\mathcal{S}_n)\rangle$ can be decomposed into independent signals. We review the status of partial security proofs in Sec. VI.

E. Sources

1. Lasers

Lasers are the most practical and versatile light sources available today. For this reason, they are chosenby the vast majority of groups working in the field. Of course, all implementations in which the source is a laser are P&M schemes. For the purposes of this review, we do not delve deep into laser physics. The output of a laser in a given mode is described by a coherent state of the field,

$$|\sqrt{\mu}e^{i\theta}\rangle \equiv |\alpha\rangle = e^{-\mu/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{11}$$

where $\mu = |\alpha^2|$ is the average photon number (also called the intensity). The phase factor $e^{i\theta}$ is accessible if a reference for the phase is available; if not, the emitted state is instead described by the mixture

$$\rho = \int_0^{2\pi}\frac{d\theta}{2\pi}|\alpha\rangle\langle\alpha| = \sum_n P(n|\mu)|n\rangle\langle n| \tag{12}$$

with

$$P(n|\mu) = e^{-\mu}\mu^n/n!. \tag{13}$$

Since two equivalent decompositions of the same density matrix cannot be distinguished, one may say that, in the absence of a phase reference, the laser produces a Poissonian mixture of number states.

The randomization of θ generalizes to multimode coherent states (Mølmer, 1997; van Enk and Fuchs, 2002). Consider, for instance, the two-mode coherent state $|\sqrt{\mu}e^{i(\theta+\varphi)}\rangle|\sqrt{\mu'}e^{i\theta}\rangle$ which may describe, for instance, a weak pulse and a reference beam. The phase φ is the relative phase between the two modes and is well defined, but the common phase θ is random. One can then carry out the same integration as before; the resulting ρ is the Poissonian mixture with average photon number $\mu + \mu'$ and the number states generated in the mode described by the creation operator $A^\dagger = (e^{i\varphi}\sqrt{\mu}a_1^\dagger + \sqrt{\mu'}a_2^\dagger)/\sqrt{\mu+\mu'}$.

We turn now to QKD. The existence of a reference for the phase is essential in both continuous-variable and distributed-phase-reference protocols: after all, these protocols have been designed having the laser specifically in mind as a source. On the contrary, when attenuated lasers are used to approximate qubits in discrete protocols, the phase reference does not play any role. In these implementations, ρ given in Eq. (12) is generically[26] an accurate description of the quantum signal outside Alice's laboratory. Since ρ commutes with the measurement of the number of photons, this opens the possibility of photon-number-splitting attacks (Bennett, 1992; Brassard, Lütkenhaus, *et al.*, 2000; Lütkenhaus, 2000), a major concern in practical QKD which is addressed in Sec. III.B.3.

2. Sub-Poissonian sources

Sub-Poissonian sources (sometimes called "single-photon sources") come closer to a single-photon source than an attenuated laser, in the sense that the probability of emitting two photons is smaller. The quantum signal in each mode is taken to be a photon-number diagonal mixture with a very small contribution of the multiphoton terms. The quality of a sub-Poissonian source is usually measured through the second-order correlation function

$$g_2(\tau) = \frac{\langle :I(t)I(t+\tau):\rangle}{\langle I(t)\rangle^2}, \tag{14}$$

where $I(t)$ is the signal intensity emitted by the source and $::$ denotes normal ordering of the creation and annihilation operators. In particular, $g_2(0) \approx 2p(2)/p(1)^2$, while $p(n)$ is the probability that the source emits n photons. For Poissonian sources, $g_2(0) = 1$; the smaller $g_2(0)$, the closer the source is to an ideal single-photon source. It has been noticed that knowledge of the efficiency and g_2 is enough to characterize the performance of such a source in an implementation of BB84 (Waks, Santori, and Yamamoto, 2002a).

Sub-Poissonian sources have been the object of intensive research; recent reviews cover the most meaningful developments (Lounis and Orrit, 2005; Shields, 2007). In the context of QKD, the discovery of PNS attacks triggered much interest in sub-Poissonian sources because they would reach much higher secret fractions. QKD experiments have been performed with such sources (Beveratos *et al.*, 2002; Waks, Inoue, *et al.*, 2002; Al-

---

[26]One must be careful due to the fact that the phase reference is not used in the protocol does not necessarily mean that such a reference is physically not available. In particular, such reference is available for some sources, e.g., when a mode-locked laser is used to produce pulses. In such cases, even though Alice and Bob do not use the phase coherence in the protocol, the signal is no longer correctly described by Eq. (12), and Eve can in principle take advantage of the existing coherence to obtain more information (Lo and Preskill, 2007). Therefore it is necessary to implement active randomization (Gisin *et al.*, 2006; Zhao, Qi, and Lo, 2007).

léaume *et al.*, 2004), and also in fibers (Intallura *et al.*, 2007) thanks to the development of sources at telecom wavelengths (Ward *et al.*, 2005; Saint-Girons *et al.*, 2006, Zinoni *et al.*, 2006). Currently this interest has significantly dropped, as it was shown that the same rate can be achieved with lasers using decoy states (see Secs. IV.B.3 and IV.B.4). But the situation may turn again in the near future, for applications in QKD with quantum repeaters (Sangouard *et al.*, 2007).

3. Sources of entangled photons

Entangled photon pairs suitable for entanglement-based protocols or for heralded sub-Poissonian sources are mostly generated by spontaneous parametric down-conversion (SPDC) (Mandel and Wolf, 1995). In this process some photons from a pump laser beam are converted into pairs of photons with lower energies due to nonlinear interaction in an optical crystal.[27] The total energy and momentum are conserved. In QKD devices, cw-pumped sources are predominantly used.

In the approximation of two output modes, the state behind the crystal can be described as follows:

$$|\psi\rangle_{\mathrm{PDC}} = \sqrt{1-\lambda^2} \sum_{n=0}^{\infty} \lambda^n |n_A, n_B\rangle, \qquad (15)$$

where $\lambda = \tanh \xi$ with ξ proportional to the pump amplitude, and where $|n_A, n_B\rangle$ denotes the state with n photons in the mode destined to Alice and n photons in the other mode going to Bob. This is the so-called two-mode squeezed vacuum.

The photons are entangled in time and in frequencies (energies); one can also prepare pairs of photons correlated in other degrees of freedom: polarization (Kwiat *et al.*, 1995, 1999), time bins (Brendel *et al.*, 1999; Tittel *et al.*, 2000), momenta (directions), or orbital angular momenta (Mair *et al.*, 2001).

The state (15) can be directly utilized in continuous-variable protocols. In the case of discrete-variable protocols, one would prefer only a single pair of photons per signal; however, SPDC always produces multi-pair components, whose presence must be taken into account. We describe this in the four-mode approximation, which is sufficient for the description of fs-pulse-pumped SPDC (Li *et al.*, 2005). An ideal two-photon maximally entangled state reads $|\Psi_2\rangle = \frac{1}{\sqrt{2}}(|1,0\rangle_A |1,0\rangle_B + |0,1\rangle_A |0,1\rangle_B)$, where each photon can be in two different modes (orthogonal polarizations, different time bins, etc.). This state can be approximately achieved if $\lambda \ll 1$, i.e., if the mean pair number per pulse $\mu = 2\lambda^2/(1-\lambda^2)$

$\ll 1$. But there are multipair components: in fact, as in the case of a four-mode approximation, the generated state reads

$$|\Psi\rangle \approx \sqrt{p(0)}|0\rangle + \sqrt{p(1)}|\Psi_2\rangle + \sqrt{p(2)}|\Psi_4\rangle, \qquad (16)$$

where $p(1) \approx \mu$ and $p(2) \approx 3/4 \mu^2$, $|0\rangle$ is the vacuum state, and the four-photon state is $|\Psi_4\rangle = 1/\sqrt{3}(|0,2\rangle|0,2\rangle + |2,0\rangle|2,0\rangle + |1,1\rangle|1,1\rangle)$. We recall that this description is good for short pump pulses; when a cw-pumped source is used (or a pulse-pumped source with the pulse duration much larger than the coherence time τ of the down-converted photons) the four-mode approximation is not applicable and a continuum of frequency modes must be taken into account. The multiple excitations created during the coherence time τ are coherent and partially correlated: in this case, the four-photon state is a fully entangled state that cannot be written as "two pairs"—see $|\Psi_4\rangle$ above.[28] However, τ is usually much shorter than the typical time Δt that one can discriminate, this time being defined as the time resolution of the detectors for cw-pumped sources[29] or as the duration of a pulse for pulsed sources. This implies that, when two photons arrive "at the same time," they may actually arise from two incoherent processes, and in this case the observed statistics corresponds to that of two independent pairs. This physics has been the object of several studies (Tapster and Rarity, 1998; Ou, Rhee, and Wang, 1999; De Riedmatten, Scarani; *et al.*, 2004, Eisenberg *et al.*, 2004; Tsujino *et al.*, 2004; Scarani *et al.*, 2005).

What concerns us here is the advantage that Eve may obtain, and in particular the efficiency of PNS attacks. If the source is used in a P&M scheme as a heralded single-photon source, then the PNS attack is effective as usual, because all photons that travel to Bob have been actively prepared in the same state (Lütkenhaus, 2000); ideas inspired by decoy states can be used to detect it (Adachi *et al.*, 2007; Mauerer and Silberhorn, 2007). In an EB scheme, the PNS attack is effective on the fraction $\zeta \approx \tau/\Delta t$ of coherent four-photon states; in addition, all multipair contributions inevitably produce errors in the correlations between Alice and Bob. We return to these points in Sec. IV.B.5.

F. Physical channels

As far as the security is concerned, the quantum channel must be characterized only *a posteriori* because Eve has full freedom of action on it. However, knowledge of the *a priori* expected behavior is important at the time of designing a setup. We review here the physics of the

---

[27]Crystals such as $KNbO_3$, $LiIO_3$, $LiNbO_3$, $\beta-BaB_2O_4$, etc. Periodically poled nonlinear materials are very promising (Tanzilli *et al.*, 2001). Besides the spontaneous parametric down-conversion, new sources of entangled photons based on quantum dots have been tested (Young *et al.*, 2006). But these sources are still at an early stage of development. Their main drawback is the need for a cryogenic environment.

[28]Although a nuisance in qubit-based protocols, the existence of such four photon components can lead to new opportunities for QKD, as pointed out Brassard, Mor, and Sabders (2000) and Durkin *et al.* (2002).

[29]However, a recent entanglement-swapping experiment combined fast detectors and narrow filters to achieve $\Delta t < \tau$ in cw-pumped SPDC (Halder *et al.*, 2007).

two main quantum channels used for light, namely, optical fibers and free-space beams.

An important parameter of the quantum channel is the amount of loss. Certainly, a key can be built by postselecting only those photons that have actually been detected. But since quantum signals cannot be amplified, the raw key rate decreases with the distance as the transmission t of the channel; in addition, at some point the detection rate reaches the level of the dark counts of the detectors, and this effectively limits the maximal achievable distance. Finally, in general the lost photons are correlated with the signal and thus must be counted as information that leaked to Eve.

Concerning the interaction of photons with the environment in the channel, the effect of *decoherence* depends strongly on the quantum degree of freedom that is used; therefore, although weak in principle, it cannot be fully neglected and may become critical in some implementations.

1. Fiber links

The physics of optical fibers has been explored in depth because of its importance for communication (Agrawal, 1997). When we quote a value, we refer to the specifications of the standard fiber Corning SMF-28;[30] obviously, the actual values must be measured in any experiment.

Losses are due to random scattering processes and depend therefore exponentially on the length ℓ,

$$t = 10^{-\alpha\ell/10}. \tag{17}$$

The value of α is strongly dependent on the wavelength and is minimal in the two "telecom windows" around 1330 nm ($\alpha \simeq 0.34$ dB/km) and 1550 nm ($\alpha \simeq 0.2$ dB/km).

The decoherence channels and their importance vary with the coding of the information. Two main effects modify the state of light in optical fibers. The first effect is chromatic dispersion different wavelengths travel at slightly different velocities, thus leading to an incoherent temporal spread of a light pulse. This may become problematic as soon as subsequent pulses start to overlap. However, chromatic dispersion is a fixed quantity for a given fiber, and can be compensated (Fasel, Gisin, Ribordy, and Zbinden, 2004). The second effect is polarization mode dispersion (PMD) (Gisin and Pellaux, 1992; Galtarossa and Menyuk, 2005). This is a birefringent effect, which defines a fast and a slow polarization mode orthogonal to one another, so that any pulse tends to split into two components. This induces a depolarization of the pulse. Moreover, the direction of the birefringence may vary in time due to environmental factors: as thus, it cannot be compensated statically. Birefringence effects induce decoherence in polarization coding, and may be problematic for all implementations that require a control on polarization. The importance of such effects

---

[30]See www.ee.byu.edu/photonics/connectors.parts/smf28.pdf

depends on the fibers and on the sources; recent implementations can be made stable, even though they use a rather broadband source (Hübel *et al.*, 2007).

2. Free-space links

A free-space QKD link can be used in several very different scenarios, from short-distance line-of-sight links with small telescopes mounted on rooftops in urban areas to ground-space or even space-space links, involving the use of astronomical telescopes (see also Sec. VIII.A.4). Free-space QKD has been demonstrated in both the prepare-and-measure (Buttler *et al.*, 1998; Rarity, Gorman, and Tapster, 2001; Hughes *et al.*, 2002; Kurtsiefer *et al.*, 2002) and the entanglement-based configurations (Marcikic, Lamas-Linares, and Kurtsiefer, 2006; Ursin *et al.*, 2007 Erven *et al.*, 2008; Ling *et al.*, 2008).

The decoherence of polarization or of any other degree of freedom is practically negligible. The losses can roughly be divided into geometric and atmospheric. The geometric losses are related to the apertures of the receiving telescopes and with the effective aperture of the sending telescope (the one perceived by the receiving telescope, which is influenced by alignment, moving buildings, atmospheric turbulence, etc.). The atmospheric losses are due to scattering and to scintillation. Concerning scattering, within the 700–10 000 nm wavelength range there are several "atmospheric transmission windows," e.g., 780–850 nm and 1520–1600 nm, which have an attenuation $\alpha < 0.1$ dB/km in clear weather. Obviously, the weather conditions influence such losses heavily; numerical values are available [see, e.g., Kim and Korevaar (2001) and Bloom *et al.*, (2003)]. A simple model of the losses for a line-of-sight free-space channel of length ℓ is therefore given by $t \approx [d_r/(d_s + D\ell)]^2 \times 10^{-\alpha\ell/10}$, where the first term is an estimate of the geometric losses (d_s and d_r are the apertures of the sending and receiving telescopes; D is the divergence of the beam) and the second describes scattering (α is the atmospheric attenuation). We note that this formula does not account for scintillation, which is often the most critical factor in practice.

G. Detectors

1. Photon counters

Discrete-variable protocols use photon counters as detectors. The main quantities characterizing photon counters are the quantum efficiency η, which represents the probability of a detector click when the detector is hit by a photon, and the dark count rate p_d, characterizing the noise of the detector—dark counts are events when a detector sends an impulse even if no photon has entered it. An important parameter is also the dead time of the detector, i.e., the time it takes to reset the detector after a click. These three quantities are not independent. Most often, the overall repetition rate at which the detector can be operated is determined by the dead time.

TABLE I. Typical parameters of single-photon detectors: detected wavelength λ, quantum efficiency η, fraction of dark counts p_d, repetition rate, maximum count rate, jitter, and temperature of operation T; the last column refers to the possibility of distinguishing the photon numbers. For acronyms and references, see text.

Name	λ (nm)	η	p_d	Rep. (MHz)	Count (MHz)	Jitter (ps)	T (K)	n
			APDs					
Si	600	50%	100 Hz	cw	15	50–200	250	N
InGaAs	1550	10%	10^{-5} per gate	10	0.1	500	220	N
Self-differencing				1250	100	60		
			Others					
VLPC	650	58–85 %	20 kHz	cw	0.015	N.A.	6	Y
SSPD	1550	0.9%	100 Hz	cw	N.A.	68	2.9	N
TES	1550	65%	10 Hz	cw	0.001	9×10^4	0.1	Y

For each of the detectors discussed below, the meaningful parameters are listed in Table I.

The most commonly used photon counters in discrete-variable systems are avalanche photodiodes (APDs). Specifically, for wavelengths in the interval approximately 400–1000 nm Si APDs can be used; for wavelengths from about 950 to 1650 nm, including telecom wavelengths, InGaAs/InP diodes are most often applied. A whole literature on the use of APDs has originated in the field of QKD (Gisin, Ribordy, Tittel, and Zbinden, 2002; Cova *et al.*, 2004). Because they can be operated with thermoelectric cooling, these detectors are an obvious choice for practical QKD, and in particular for commercial devices (Ribordy *et al.*, 2004; Trifonov *et al.*, 2004). Two recent developments are worth mentioning. First, instead of directly using InGaAs APDs, one can detect signals at telecom wavelengths (1310 and 1550 nm) by applying parametric frequency up-conversion and then using efficient silicon APDs (Diamanti *et al.*, 2005; Thew *et al.*, 2006). These up-conversion detectors have lower quantum efficiency than InGaAs APDs, but could in principle be operated in continuous mode, thus leading to higher repetition rates (gigahertz); however, currently, they suffer from an intrinsic noise source that leads to high dark count rates. Second, more recently, an improvement of the repetition rate and count rate by several orders of magnitude has been obtained using a circuit that compares the output of the APD with that in the preceding clock cycle; such devices have been named self-differencing APDs (Yuan, Kardynal, *et al.*, 2007).

Single-photon detectors other than APDs have been and are being developed. For instance, visible light photon counters (VLPCs) are semiconductor detectors that can also distinguish the number of impinging photons (Kim *et al.*, 1999; Waks *et al.*, 2003; Waks, Diamanti, and Yamamoto, 2006). Other photon counters are based on superconductors, for instance superconducting single-photon detectors (SSPDs) (Verevkin *et al.*, 2002, 2004) and transition edge sensors (TESs) (Miller *et al.*, 2003; Rosenberg *et al.*, 2005); both types have already been used in QKD experiments (Hadfield *et al.*, 2006; Hiskett

et al., 2006; Rosenberg *et al.*, 2007, 2008). Each type has its own strong and weak features; in particular, all of them must be operated at cryogenic temperatures.

2. Homodyne detection

Continuous-variable QKD is based on the measurement of quadrature components of light. This can conveniently be done by means of optical homodyne detection. This detection scheme uses two beams of the same frequency: the signal and the so-called local oscillator (much stronger and therefore often treated as classical). The beams are superimposed at a balanced beam splitter. The intensity of light in each of the output modes is measured with proportional detectors, and the difference between the resulting photocurrents is recorded. If the amplitude and the phase of the local oscillator are stable, the differential current carries information about a quadrature component of the input signal—what quadrature component is actually measured depends on the phase difference between the signal and local oscillator. To keep this phase difference constant, the signal and local oscillator are usually derived from the same light source: the local oscillator beam needs to be transmitted along with the signal from Alice to Bob; in practice, they are actually sent through the same channel so that they experience the same phase noise and the relative phase remains unaltered—note, however, that this practical change may render the scheme completely insecure, unless additional measurements are performed to verify the character of both the weak and strong signals (Häseler, Moroder, and Lütkenhaus, 2008).

The intensities are measured by *p-i-n* diodes, which provide high detection efficiency (typically 80%) and relatively low noise. Therefore homodyne detection could in principle operate at gigahertz repetition rates (Camatel and Ferrero, 2006) in contrast to photon counters based on APDs, whose detection rate is limited by the detector dead time.

The use of such a high-rate homodyne detection technique unfortunately comes with a price. Because of the uncertainty principle, the measurement of complemen-

tary quadratures is intrinsically noisy. The vacuum noise (or intrinsic noise) is the noise obtained when there is vacuum in the signal port (only the local oscillator is present). Now, the unavoidable transmission losses in the optical line, which simply cause "missing clicks" in photon-counting-based schemes, result in a decrease in the signal-to-noise ratio in homodyne-detection-based schemes. The vacuum noise is responsible for a rather significant added noise in continuous-variable QKD, which needs to be corrected during the classical postprocessing stage: an additional computing effort in continuous-variable QKD.

In addition to the vacuum noise, excess noise is generated, mainly by the detectors themselves and by the subsequent electronics. In real systems, it is possible to reduce the excess noise even 20 dB below the shot noise; but this ratio depends on the width of the spectral window, and narrow spectral windows bound the modulation frequencies (i.e., the repetition rates).

H. Synchronization and alignment

1. Generalities

The problem of the *synchronization* of two distant clocks, in itself, is a technical matter that has been solved efficiently in several different ways; basically, either one sends out a synchronization signal at regular intervals during the whole protocol or one relies on an initial synchronization of two sufficiently stable clocks. In the context of QKD, one has to consider possible hacking attacks that would exploit this channel (see Sec. III.B.4).

The physical meaning of *alignment* depends on the coding. For coding in polarization, it obviously means that Alice and Bob agree on the polarization directions. For phase coding, it refers rather to the stabilization of interferometers. Both procedures are most often performed by sending a space signal at a different frequency than the quantum signal, taking advantage of the bandwidth of the optical channel. Alternatively, self-stabilized setups have been proposed: this is the so-called plug-and-play configuration, described next in the context of phase coding.

Before that, we have to mention that quantum mechanics also allows for a coding that does not require any alignment by exploiting the so-called "decoherence-free subspaces" (Zanardi and Rasetti, 1997; Boileau *et al.*, 2004). However, although demonstrated in some proof-of-principle experiments (Bourennane *et al.*, 2004; Chen *et al.*, 2006), such coding is highly impractical, as it requires the preparation and measurement of complex multiphoton states; moreover, it is very sensitive to losses.[31]
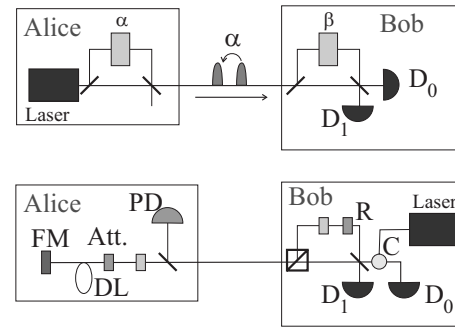

FIG. 3. Comparison of the one-way and two-way configurations for phase coding. The one-way configuration is called double Mach-Zehnder (top). Alice splits each laser pulse into two pulses with relative phase α; if Bob's phase is such that $\alpha - \beta = 0$ modulo π, the outcome is deterministic in the absence of errors. In the two-way configuration, or plug-and-play (bottom), the source of light is on Bob's side. In detail, an intense laser pulse is sent through a circulator (C) into Bob's interferometer. The phase modulator is passive at this stage, but a polarization rotation (R) is implemented so that all the light finally couples in the fiber. On Alice's side, part of the light is deflected to a proportional detector (PD) that is used to monitor Trojan horse attacks. The remaining light goes to a Faraday mirror (FM) that sends each polarization to the orthogonal one. On the way back, the pulses are attenuated down to a suitable level; then the coding is done as above. The role of the delay line (DL) is explained in the text.

2. Phase coding: Two configurations

We consider P&M schemes with phase coding. This coding has been the preferential choice in fiber implementations and has given rise to two possible configurations (Fig. 3). In the configuration called *one-way*, the laser is on Alice's side; it is typically realized with a double Mach-Zehnder interferometer (Bennett, 1992; Townsend, Rarity, and Tapster, 1993). The other possible configuration has been called plug-and-play configuration (Muller *et al.*, 1997; Ribordy *et al.*, 1998). As the name suggests, the goal of the plug-and-play configuration is to achieve *self-alignment* of the system. In contrast to the one-way configuration, the plug-and-play configuration puts the source of light on Bob's side: a strong laser pulse travels in the quantum channel from Bob to Alice. Alice attenuates this light to a suitable weak intensity (less than one photon per pulse on average; a more precise estimate is given below and in Sec. IV.B.4), codes the information, and sends the remaining light back to Bob, who detects. The coded signal goes as usual from Alice to Bob; but the same photons have first

---

[31]The simplest example is the singlet state of two qubits: when both qubits are sent into the quantum channel, the state is robust against any misalignment U since $U \otimes U|\Psi^-\rangle = |\Psi^-\rangle$. With *four* physical qubits, there are two orthogonal states such that $U \otimes U \otimes U \otimes U|\psi_{0,1}\rangle = |\psi_{0,1}\rangle$; therefore, one can form an ef-

fective logical qubit $|0\rangle \equiv |\psi_0\rangle$ and $|1\rangle \equiv |\psi_1\rangle$ that is insensitive to misalignments. The states $|\psi_{0,1}\rangle$ are not easy to prepare and to detect. As a matter of fact, the available experiments did not produce those states: they produced a quite complex photonic state that gives the required statistics conditioned on the observation of a specific detection pattern. In turn, this implies that all four photons must be transmitted and detected; therefore losses lead to a very fast decrease in the detection rate.

traveled through the line going from Bob to Alice. In this way, the interferometers become self-stabilized because the light passes through them twice; if the reflection on Alice's side is done with a Faraday mirror, polarization effects in the channel are compensated as well. These two configurations have shaped the beginning of practical QKD; we refer the reader to a previous review (Gisin, Ribordy, Tittel, and Zbinden, 2002) for a thorough discussion.

It is useful here to address some problems that are specific for the plug-and-play configuration since they illustrate the subtleties of practical QKD. The system has an intrinsic duty cycle, which limits the rate at long distances: Bob must wait through a go-and-return cycle before sending other strong signals, otherwise the weak signal coded by Alice will be overwhelmed by the back-scattered photons of the new strong ones.[32] This nuisance has been reduced by having Bob send not just one pulse, but a train of pulses; on Alice's side, a sufficiently long delay line must be added: all pulses must have passed the phase modulator before the first one comes back and is coded. Still, this duty cycle is a serious bottleneck compared to one-way configurations.

Two specific security concerns also arise for the plug-and-play configuration. First, in full generality, there is no reason to assume that Eve interacts only with the signal going from Alice to Bob; she might as well modify the signal going from Bob to Alice. A simple argument suggests that this is not helpful for Eve: Alice attenuates the light strongly and should actively randomize the global phase; then, whatever the state of the incoming light, the outgoing coded light consists of weak signals with almost exact Poissonian statistics (Gisin *et al.*, 2006). Indeed, a rigorous analysis shows that unconditional security can be proved if the global phase is actively randomized, and that the resulting secret fractions are only slightly lower than those achievable with the one-way configuration (Zhao, Qi, and Lo, 2008). The second concern is that, since Alice's box must allow two-way transit of light, Trojan horse attacks (see III.B.4) must be monitored actively, whereas in one-way setups they can be avoided by use of passive optical isolators. In practice, this may decrease the limiting distance.[33]

---

[32]As a matter of fact, backscattering and the corresponding duty cycle could be avoided, but at the price of attenuating the pulses at Bob's side. In turn, this implies that (i) a different channel should be used for synchronization and (ii) the maximal operating distance is reduced in practice, especially if one takes Trojan horse attacks into account (see below). Such a setup has been demonstrated (Bethune and Risk, 2000).

[33]The argument goes as follows: upon receiving Bob's pulse, Alice attenuates it down to the desired intensity μ. Now, it turns out that a simple error by a factor of 2, i.e., sending out 2μ instead of μ, would spoil all security (see Sec. IV.B.4). This implies that the intensity of the input pulse must be monitored to a precision far better than this factor 2. This precision may be hard to achieve at long distances, when Bob's pulse has already been significantly attenuated by transmission.

It is not obvious what the future perspectives of the plug-and-play configuration will be: recently, stabilized one-way configurations have been demonstrated, which can also reach optical visibilities larger than 99% and have a less constraining duty cycle (Gobby, Yuan, and Shields, 2004). Still, the plug-and-play configuration is an important milestone in practical QKD: in particular, the first commercial QKD systems are based on it.[34]

III. SECRET KEY RATE

We have seen in Sec. II.B.4 that the secret key rate K is the product of two terms [Eq. (6)], the raw key rate R and the secret fraction r. This section is devoted to a detailed study of these two factors. Clearly, the latter is by far the more complex one, and most security studies are devoted only to it; however, the raw key rate is crucial as well in practice and its proper description involves some subtleties as well. We therefore start with this description.

A. Raw key rate

The raw key rate reads

$$R = \nu_S \, \text{Prob(Bob accepts)}. \tag{18}$$

The second factor depends both on the protocol and on the hardware (losses and detectors) and will be studied for each specific case. The factor ν_S is the repetition rate.

In the case of pulsed sources ν_S is the repetition rate of the source of pulses. Of course, $\nu_S \leq \nu_S^{\max}$, the maximal repetition rate allowed by the source itself; but two other limitations may become important in limiting cases, so that the correct expression reads

$$\nu_S^{\text{pulse}} = \min(\nu_S^{\max}, 1/\tau_d \mu t t_B \eta, 1/T_{\text{dc}}). \tag{19}$$

We now explain what the two last terms mean.

The first limitation is due to the dead time of the detectors τ_d. In fact, it is useless to send more light than can actually be detected (worse, an excess of light may even give an advantage to Eve). One can require that at most one photon is detected in an interval of time τ_d; the detection probability is Prob(Bob detects)$\approx \mu t t_B \eta$ with $\mu = \langle n \rangle \leq 1$ the average number of photons produced by the source, t the transmittivity of the quantum channel, t_B the losses in Bob's device, and η the efficiency of the detector. Therefore, $\nu_S \leq (\tau_d \mu t t_B \eta)^{-1}$. It is clear that this limitation plays a role only at short distances: as soon as there are enough losses in the channel, fewer photons will arrive at Bob than can actually be detected.

The second limitation is associated with the existence of a duty cycle: two pulses cannot be sent at a time interval smaller than a time T_{dc} determined by the setup.

---

[34]The configuration has also been used for continuous-variable coding (Legré, Zbinden, and Gisin, 2006), for a distributed-phase-reference protocol (Zhou *et al.*, 2003), and for noncryptographic quantum information tasks (Brainis *et al.*, 2003).

The expression for T_{dc} depends on the details of the setup. In plug-and-play configurations, for instance, one cannot send the next train of bright pulses before the weak signal of the earlier train has returned (Sec. II.H.2): the effect becomes important at long distance. Another example of a duty cycle is the one introduced by a stabilization scheme for one-way configurations, in which each coded signal is preceded by a strong reference signal (Yuan and Shields, 2005). Note, finally, that in any implementation with time-bin coding, the advanced component of the next signal must not overlap with the delayed component of the previous one.

In the case of heralded photon sources or entanglement-based schemes working in a continuous-wave (cw) regime it is reasonable to define ν_S as the average rate of Alice's detections; thus[35]

$$\nu_S^{cw} = \min(\eta_A t_A \mu', 1/\tau_d^A, 1/\tau_d t t_B \eta, 1/\Delta t). \tag{20}$$

Here $\eta_A t_A \mu'$ is the trigger rate with which Alice announces the pair creations to Bob, with μ' the pair-generation rate of the source, t_A is the overall transmittance of Alice's part of the apparatus, and η_A is the efficiency of Alice's detectors. Of course, in practice this rate is limited by the dead time of Alice's detectors τ_d^A. The whole repetition rate is limited by Bob's detector dead time τ_d and by the width of the coincidence window Δt (usually $\Delta t \ll \tau_d$).

B. Secret fraction

1. Classical information postprocessing

To extract a short secret key from the raw key, classical postprocessing is required. This is the subject of this section [for more details see Renner (2005) and Van Assche (2006)]. The security bounds for the secret fraction crucially depend on how this step is performed.

a. One-way postprocessing

These are the most studied and best-known procedures. One of the partners, the one who is chosen to hold the reference raw key, sends classical information through the public channel to the other one, who acts according to the established procedure on his data but never gives feedback. If the sender in this procedure is the same as the sender of the quantum states (Alice with our convention), one speaks of direct reconciliation; in the other case, of reverse reconciliation. The optimal one-way postprocessing has been characterized and consists of two steps.

The first step is error correction (EC), also called information reconciliation, at the end of which the lists of symbols of Alice and Bob have become shorter but perfectly correlated. As proved by Shannon, the fraction of

perfectly correlated symbols that can be extracted from a list of partially correlated symbols is bounded by the mutual information $I(A:B) = H(A) + H(B) - H(AB)$, where H is the entropy of the probability distribution. In the context of one-way procedures with a sender S and a receiver R, it is natural to write $I(A:B)$ in the apparently asymmetric form $H(S) - H(S|R)$. This formula has an intuitive interpretation, if one remembers that the entropy is a measure of uncertainty: the sender must reveal an amount of information at least as large as the uncertainty the receiver has on the reference raw key.

The second step is privacy amplification (PA). This procedure is aimed at destroying Eve's knowledge of the reference raw key. Of course, Alice and Bob will have chosen as a reference raw key the one on which Eve has the smallest information: here is where the choice between direct and reverse reconciliation becomes meaningful.[36] The fraction to be further removed can therefore be written $\min(I_{EA}, I_{EB})$, where $I_{E.}$ is Eve's information about the raw key of Alice or Bob, which will be defined more precisely in Sec. III.B.2 PA was first mentioned by Bennett, Brassard, and Robert (1988), and then established by Bennett *et al.* (1995). This reference has been considered as valid for one decade but, after the notion of universally composable security was introduced (see Sec. II.C.2), it had to be replaced by a generalized version (Renner and König, 2005). Currently the only PA procedure that works in a provable way is the one based on two-universal hash functions.[37] Also, for composability, the protocol must be symmetric under permutations; in particular, the pairs for the parameter estimation must be chosen at random, and the hash function has to be symmetric (as it is usually).

In summary, the expression for the secret fraction extractable using one-way classical postprocessing reads

$$r = I(A:B) - \min(I_{EA}, I_{EB}). \tag{21}$$

---

[35]The source is assumed to be safe at Alice's side. It is supposed that Alice's detectors are still "open" (not gated). Dark counts and multipair contributions were neglected in the estimation of ν_S^{cw}.

[36]Note that, $I(A:B)$ being symmetric, there is no difference between direct and reverse reconciliation at the level of EC, as expected from the nature of the task.

[37]A set $\mathcal{F}$ of functions $f : X \rightarrow Z$ is called two-universal if $\Pr[f(x) = f(x')] \leq 1/|Z|$ for $x \neq x'$ and f chosen at random with uniform probability. It is instructive to see why this definition is meaningful for privacy amplification. After EC, Alice and Bob share the same list of bits x; Eve has an estimate x' of this list. For PA, Alice chooses f from the two-universal set and announces it publicly to Bob. Both Alice and Bob end up with the shorter key $z = f(x)$; but the probability that Eve's estimate $z' = f(x')$ coincides with z is roughly $1/|Z|$: Eve might as well choose randomly out of the set Z of possible final keys. Two-universal hash functions, e.g., in the form of matrix multiplication, can be implemented efficiently (Carter and Wegman, 1979; Wegman and Carter, 1981). The size of the matrices is proportional to the length N of the raw key. Against a classical adversary, other *extractors* exist whose size grows only as $\log N$; but at currently, it is not known whether a similar construction exists in the case where the adversary is quantum (König and Renner, 2007).

b. Remarks on practical EC

As mentioned above, the performance of EC codes is bounded by Shannon's mutual information. Practical EC codes, however, do not reach the Shannon bound. For *a priori* theoretical estimates, it is fair to increase the number of bits to be removed by 10–20 %; more precise estimates are available (Lütkenhaus, 1999) but ultimately the performance must be evaluated on each code. We take this correction explicitly into account in Sec. IV–VII.

In addition, most of the efficient EC codes that are actually implemented, e.g., CASCADE (Brassard and Salvail, 1994), use two-way communication. To fit these two-way EC codes in the framework of one-way postprocessing, one can give the position of the errors to Eve and treat all communication as one-way communication by (Lütkenhaus, 1999). Alternatively, one can use encryption of the EC data, as suggested by Lütkenhaus (1999) and formally proved by Lo (2003).

Note finally that it is not necessary to estimate the error rate with a small sample of the data: instead, the parties learn naturally the precise number of errors during the EC procedure.

c. Other forms of postprocessing

Bounds can be improved by two-way postprocessing, which refers to any possible procedure in which both partners are allowed to send information. Since its first appearance in QKD (Gisin and Wolf, 1999; Chau, 2002; Gottesman and Lo, 2003), this possibility has been the object of several studies.[38] Contrary to the one-way case, the optimal procedure is still not known, basically because of the complexity of taking feedback into account.

More recently, another way to improve bounds was found, called preprocessing: before postprocessing, the sender (for one way) or both partners (for two way) can add locally some randomness to their data. Of course, this decreases the correlations between them, but it decreases Eve's information as well, and, remarkably, the overall effect may be positive (Kraus, Gisin, and Renner, 2005; Renner, Gisin, and Kraus, 2005).

Both preprocessing and two-way post-processing are easy to implement and allow a secret key to be extracted in a parameter region where one-way postprocessing would fail; in particular, the critical tolerable error rate is pushed much higher.[39] To our knowledge though, they

have been implemented only once in real systems (Ma *et al.*, 2006). The reason is that, in terms of secret key rate, an improvement can be appreciated only when the dark counts become dominant,[40] a regime in which few systems tend to operate—see, however, Rosenberg *et al.* (2008), Tanaka *et al.* (2008), and Yuan *et al.* (2008). Therefore, in what follows, we present only bounds for one-way classical postprocessing without preprocessing.

2. Individual, collective, and coherent attacks

As stressed from the beginning (Sec. II.C.1), one aims ultimately at proving unconditional security, i.e., security bounds in the case where Eve's attack on the quantum channel is not restricted. Such a *lower bound* for security was elusive for many years (Sec. II.A); it has nowadays been proved for many protocols, but is still missing for others. In order to provide an ordered view of the past, as well as to keep ideas that may also be useful in the future, we discuss now several levels of security.

a. Individual (or incoherent) attacks

This family describes the most constrained attacks that have been studied. They are characterized by the following properties:

(I1) Eve attacks each of the systems going from Alice to Bob independently of all others, using the same strategy.[41] This property is easily formalized in the EB scheme: the state of n symbols for Alice and Bob has the form $\rho_{AB}^n = (\rho_{AB})^{\otimes n}$.

(I2) Eve must measure her ancillas before the classical postprocessing. This means that, at the beginning of the classical postprocessing, Alice, Bob, and Eve share a product probability distribution of classical symbols.

In this case, the security bound for one-way postprocessing is the Csiszár-Körner bound, given by Eq. (21) with

$$I_{AE} = \max_{\text{Eve}} I(A{:}E) \quad \text{(individual attacks)}, \tag{22}$$

---

[38]We note that some of the security claims in the first paper dealing with advantage distillation (Gisin and Wolf, 1999) were imprecise. These works have also had an intriguing offspring, the conjecture of the existence of "bound information" (Gisin and Wolf, 2000), later proved for three-partite distributions (Acín, Cirac, and Masanes, 2004).

[39]The order of magnitude of the improvements is roughly the same for all examples that have been studied. Consider, e.g., BB84 in a single-photon implementation and security against the most general attacks: the critical quantum bit error rate (QBER) for one-way postprocessing without preprocessing is 11% (Shor and Preskill, 2000). Bitwise preprocessing brings

this value up to 12.4% (Kraus, Gisin, and Renner, 2005); more complex preprocessing up to 12.9% (Smith, Renes, and Smolin, 2008). Two-way postprocessing can increase it significantly further, at least up to 20.0%, but at the expenses of drastically reduced key rate (Chau, 2002; Gottesman and Lo, 2003; Bae and Acín, 2007). In weak-coherent-pulse implementations, preprocessing increases the critical distance of BB84 and SARG04 protocols by a few kilometers, for security to against both individual (Branciard *et al.*, 2005) and most general attacks (Kraus, Branciard, and Renner, 2007).

[40]Recall that optical error is routinely kept far below 5%; therefore, the total error rate exceeds ~10% when the error is largely due to the dark counts.

[41]We note here that this "same strategy" may be probabilistic (with probability p_1, Eve does something; with probability p_2, something else; etc.), provided the probabilities are fixed during the whole key exchange. From the standpoint of practical QKD, an attack in which Eve would simply stop attacking for a while, belongs to the family of the most general attacks.

and of course similarly for I_{BE} (Csiszár and Körner, 1978). Here $I(A:E)$ is the mutual information between the classical symbols; the notation $\max_{\text{Eve}}$ recalls that one must maximize this mutual information over Eve's strategies. There is actually an ambiguity in the literature as to the moment where Eve is forced to perform her measurement: namely, whether she is forced to measure immediately after the interaction (Lütkenhaus, 1996; Curty and Lütkenhaus, 2005; Bechmann-Pasquinucci, 2006) or whether she can keep the signals in a quantum memory until the end of the sifting and error correction phase (Fuchs *et al.*, 1997; Bruß, 1998; Slutsky *et al.*, 1998; Bechmann-Pasquinucci and Gisin, 1999; Lütkenhaus, 1999; Brassard, Lütkenhaus, *et al.*, 2000; Cerf *et al.*, 2002; Herbauts *et al.*, 2008). The first case is associated with the hardware assumption that Eve is restricted not to have a quantum memory.[42] The second case is associated with the hardware assumption that Eve cannot perform arbitrary coherent measurements and can be useful as a step on the way to unconditional security proofs. However, we stress that the bound for collective attacks can nowadays be calculated more easily and gives more powerful results.[43]

An important subfamily of individual attacks are the intercept-resend (IR) attacks. As the name indicates, Eve intercepts the quantum signal flying from Alice to Bob, performs a measurement on it, and, conditioned on the result she obtains, she prepares a new quantum signal that she sends to Bob. If performed identically on all items, this is an individual attack. Moreover, it obviously realizes an entanglement-breaking channel between Alice and Bob, thus providing an easily computed upper bound on the security of a protocol (Curty and Lütkenhaus, 2005; Bechmann-Pasquinucci, 2006).

b. Collective attacks

This notion was first proposed by Biham, and co-workers, who proved the security of BB84 against them and conjectured that the same bound would hold for the most general attacks (Biham and Mor, 1997; Biham *et al.*, 2005). Collective attacks are defined as follows:

(C1) The same as (I1).

(C2) Eve can keep her ancillas in a quantum memory until the end of the classical postprocessing, and more generally until any later time convenient to her (for instance, if the key is used to encode a message, part of which is vulnerable to plain-text attack, Eve may delay her measurement until she obtains the information coming from this attack). She can then perform the best measurement compatible with what she knows. In general, this will be a collective measurement.

Only (C1) is an assumption on Eve's power. The generic bound for the secret key fraction achievable using one-way postprocessing (*Devetak-Winter bound*) is given by Eq. (21) with

$$I_{AE} = \max_{\text{Eve}} \chi(A:E) \quad \text{(collective attacks)}, \qquad (23)$$

and I_{BE} defined in the analogous way (Devetak and Winter, 2005). Here $\chi(A:E)$ is the so-called Holevo quantity (Holevo, 1973),

$$\chi(A:E) = S(\rho_E) - \sum_a p(a) S(\rho_{E|a}), \qquad (24)$$

where S is von Neumann entropy, a is a symbol of Alice's classical alphabet distributed with probability $p(a)$, $\rho_{E|a}$ is the corresponding state of Eve's ancilla, and $\rho_E = \Sigma_a p(a) \rho_{E|a}$ is Eve's partial state. The Holevo quantity bounds the capacity of a channel, in which a classical value (here a) is encoded into a family of quantum states (here, $\rho_{E|a}$): in this sense, it is the natural generalization of the mutual information.

As mentioned, it is actually easier to compute Eq. (23) than Eq. (22). The reason lies in the optimization of Eve's strategy. In fact, the Holevo quantity depends only on Eve's states $\rho_{E|a}$, that is, on the unitary operation with which she couples her ancilla to the system flying to Bob. In contrast to that, the mutual information depends both on Eve's states and on the best measurement that Eve can perform to discriminate them, which can be constructed only for very specific examples of the set of states (Helstrom, 1976).

c. General (or coherent) attacks

Eve's most general strategy includes so many possible variations (she may entangle several systems flying from Alice to Bob, she may modify her attack according to the result of an intermediate measurement, etc.) that it cannot be efficiently parametrized. A brute force optimization is therefore impossible. Nevertheless, as mentioned, bounds for unconditional security have been found in many cases. In all these cases, it turns out that the bound is the same as for collective attacks. This result calls for several comments.

First, this result has an intuitive justification. If the state $|\Psi(\mathcal{S}_n)\rangle$ that codes the sequence $\mathcal{S}_n$ has the tensor product form $|\psi(s_1)\rangle \otimes \cdots \otimes |\psi(s_n)\rangle$, then the states passing from Alice to Bob are uncorrelated in the quantum channel; therefore Eve does not seem to have any advantage in introducing artificial correlations at this

---

[42]Generalizing (Wang, 2001), it is conjectured that individual attacks should be optimal under the weaker assumption of a quantum memory that is bounded, either in capacity or in lifetime; but only rougher bounds have been derived so far (Damgaard *et al.*, 2005, 2007; König and Terhal, 2008).

[43]Currently there is still something that is known only for individual attacks, and this is Eve's full strategy; the optimal procedures have been found both for the scenarios both without quantum memory (Lütkenhaus, 1996) and with it (Lütkenhaus, 1999; Herbauts *et al.*, 2008). On the contrary, the bound for collective and coherent attacks is computed by optimizing the Holevo bound over all possible interactions between the signal and Eve's ancillas (see below): one implicitly assumes that suitable measurements and data processing exist, which will allow Eve to extract that amount of information. It would be interesting to exhibit explicit procedures also for more general attacks.

point.[44] However, correlations do appear later, during the classical postprocessing of the raw key, such that, in fact, the final key is determined by the relations between the symbols of the raw key, rather than by those symbols themselves. Thus, Eve must not try to guess the value of each symbol of the raw key, but rather some relation between them—and this is typically a situation in which entanglement is powerful. This vision also clarifies why unconditional security is still elusive for those protocols for which $|\Psi(\mathcal{S}_n)\rangle$ is not of the tensor product form (see Sec. VI.A).

Second, for BB84, six-state, and other protocols, assuming the squashing property of detectors (see Sec. IV.A.2), this result is a consequence of the internal symmetries (Kraus, Gisin, and Renner, 2005; Renner, Gisin, and Kraus, 2005). The explicit calculations are given in Appendix A. In a more general framework, the same conclusion can be reached by invoking the exponential De Finetti theorem (Renner, 2005, 2007). This theorem says that, after some suitable symmetrization, the statistics of the raw key are never significantly different from those that would be obtained under constraint (I1). This is a powerful result, but again does not solve all the issues: for instance, because the actual exponential bound depends on the dimension of the Hilbert space of the quantum signals, it cannot be applied to continuous-variable QKD (see, however, the "Note added" at the end of this paper). Also recall that we consider only the asymptotic bound: the finite-key bounds obtained by invoking the De Finetti theorem are overpessimistic (Scarani and Renner, 2008).

3. Quantum side channels and zero-error attacks

The possibility of zero-error attacks seems to be at odds with the fundamental tenet of QKD, namely, that Eve must introduce modifications in the state as soon as she obtains some information. However, there is no contradiction: for instance, in the presence of losses the quantum signal is also changed between the source and the receiver. Even if in most protocols (see discussion in Sec. I.B.3) losses do not lead to errors in the raw key, some information about the value of the coded symbol may have leaked to Eve.

Losses are the most universal example of leakage of information in a quantum side channel, i.e., in some degree of freedom other than the one that is monitored. We stress that the existence of side channels does not compromise security, provided the corresponding attacks are taken into account in the privacy amplification.

A beam-splitting (BS) attack translates the fact that the light that is lost in the channel must be given to Eve: specifically, Eve could be simulating the losses by putting a beam splitter just outside Alice's laboratory, and then forwarding the remaining photons to Bob on a lossless line. The BS attack does not modify the optical mode that Bob receives: it is therefore always possible for lossy channels and does not introduce any error .[45] For an explicit computation of BS attacks, see Sec. VI.B.

When the signal can consist of more than one photon, Eve can count the number of photons in each signal and act differently according to the result *n* of this measurement. Such attacks are called photon-number splitting (PNS) attacks (Bennett, 1992; Dušek, Haderka, and Hendrych, 1999; Brassard, Lütkenhaus, *et al.*, 2000; Lütkenhaus, 2000) and can be much more powerful than the BS attack. They were discovered as zero-error attacks against BB84 implemented with weak laser pulses; in the typical parameter regime of QKD, even the Poissonian photon-number distribution can be preserved (Lütkenhaus and Jahma, 2002), so that the PNS attack cannot be detected even in principle as long as one known signal intensity is used. Use of different intensities in order to detect PNS attacks is the idea behind the decoy-states method (Hwang, 2003; Lo, Ma, and Chen, 2005; Wang, 2005). The distributed-phase-reference protocols also detect PNS attacks (Inoue and Honjo, 2005; Stucki *et al.*, 2005).

Finally, we mention the possibility of attacks based on unambiguous state discrimination (USD) followed by resending of a signal (Dušek, Jahma, and Lütkenhaus, 2000). These can be part of a PNS attack (Scarani, Acín, Ribordy, and Gisin, 2004) or can define attacks alone (Branciard *et al.*, 2007; Curty *et al.*, 2007); they are clearly zero-error attacks and modify the photon-number statistics in general.

Of course, a quantum side channel may hide in any imperfect component of the device (e.g., a polarizer which would also distort the wave function according to the chosen polarization). The list of possibilities is unbounded, whence the need for careful testing.[46]

4. Hacking attacks on practical QKD

In practical QKD, the security concerns are not limited to the computation of security bounds for Eve's action on the quantum channel. Any specific implementation must be checked against hacking attacks and classical leakage of information.

Hacking attacks are related to the weaknesses of an implementation. A first common feature of hacking attacks is that they are feasible, or almost feasible, with present-day technology. The best-known example is the family of Trojan horse attacks, in which Eve probes the settings of Alice's and/or Bob's devices by sending some light into them and collecting the reflected signal (Vakhitov, Makarov, and Hjelme, 2001). Actually, the first kind of hacking attack that was considered is a form of Trojan

---

[44]Of course, one is not saying that Eve does satisfy (I1): Eve can do whatever she wants; but there exists an attack that satisfies (I1) and that performs as well as the best possible attack.

[45]For some sources, this attack simply does not give Eve any information: for a perfect single-photon source, if the photon goes to Eve, nothing goes to Bob, and vice versa.

[46]Some very specific protocols and the corresponding security proofs can be made robust against such imperfections (Acín *et al.*, 2007).

horse that would come for free: it was noticed that some photon counters (silicon-based avalanche photodiodes) emit some light at various wavelengths when they detect a photon (Kurtsiefer *et al.*, 2001). If this light carries some information about which detector has fired, it must be prevented from propagating out, where Eve could detect it. In these two examples, one also sees the second common feature of all hacking attacks, namely, that once they have been noticed, they can be countered by adding some component. In all setups where light goes only one way (out of Alice's and into Bob's laboratory), the solution against Trojan horse attacks consists in simply using an optical isolator; in implementations where light must go both ways (typically, the plug-and-play setups), the solution is provided by an additional monitoring detector (Gisin *et al.*, 2006).

Apart from Trojan horses, other hacking attacks have been invented to exploit potential weaknesses of specific implementations, e.g., faked state attacks (Makarov and Hjelme, 2005; Makarov *et al.*, 2006; Makarov and Skaar, 2008), phase-remapping attacks (Fung *et al.*, 2007), and time-shift attacks (Qi, Fung, *et al.*, 2007; Zhao, Fung, *et al.*, 2007).It has also been noticed that a too precise timing disclosed in the Alice-Bob synchronization protocol may give information about which detector actually fired (Lamas-Linares and Kurtsiefer, 2007).

5. A crutch: The uncalibrated-device scenario

As we have stressed, the errors and losses in the quantum channel must be attributed to Eve's intervention. But in a real experiment, there are errors and losses also inside the devices of the authorized partners. In particular, the detectors have finite efficiency (losses) and dark counts (errors); these values are known to the authorized partners, through calibration of their devices. A security proof should take this fact into account.

The task of integrating this knowledge into security proofs, however, has proved harder than one might think. In general, the naive approach, consisting in taking an attack and removing the device imperfections from the parameters used in privacy amplification, gives only an upper bound, even at the level of individual attacks.[47] In particular, unconditional security proofs,

whenever available, have been provided only under the assumption that all the losses and all the errors are attributed to Eve and must therefore be taken into account in privacy amplification. We refer to this assumption as to the uncalibrated-device scenario, because it implies that Alice and Bob have no means of distinguishing the losses and errors of their devices from those originating in the channel.[48] These issues have been raised in a nonuniform way in the literature. Most of the discussions have taken place for discrete-variable protocols; the security studies of distributed-phase-reference protocols are in too early a stage, but will surely have to address the question. The case of CV QKD may prove different because of the difference in the detection process (homodyne detection instead of photon counting).

Currently the uncalibrated-device scenario is still a necessary condition to derive lower bounds. In the following sections, we work with this scenario. In Sec. IV.C and VII.B.2, we compare the best available lower bounds with the upper bounds obtained with a naive approach to calibrated devices: we show that in some cases the two bounds coincide for every practical purpose. In Sec. VIII.A.2, we summarize the status of this open problem.

IV. DISCRETE-VARIABLE PROTOCOLS

A. Generic assumptions and tools

As argued in Sec. III.B.5, in order to present lower bounds as they are available today, we work systematically in the uncalibrated-device scenario; Sec. IV.C will present the derivation of an upper bound for calibrated devices.

1. Photon-number statistics

We suppose that each signal is represented by a diagonal state in the photon-number basis, or, in other words, that there is no phase reference available and no coherence between successive signals.[49] Thus, Alice's source can be described as sending out a pulse that contains n photons with probability $p_A(n)$; Eve can learn n without modifying the state, so this step is indeed part of

---

[47]Consider a PNS attack (Sec. III.B.3) on BB84 implemented with weak coherent pulses, and focus on the pulses for which Eve has $n=2$ photons. The obvious PNS attack consists in Eve keeping one photon in a quantum memory and sending the other one to Bob because in this case she obtains full information and introduces no error. But there is no information on nondetected photons: in particular, if Eve cannot control the losses in Bob's apparatus, t_B, and the detector efficiency η, her information rate on such events will be $I_{2\rightarrow1+1}=t_B\eta$. Now, consider another strategy: Eve applies a quantum cloner $2\rightarrow3$, keeps one photon, and sends the other two to Bob. Since no perfect cloning is possible, this introduces an error ε_2 on Bob's side, and Eve's information on each detected bit is $I(\varepsilon_2)<1$. But Eve's information rate is $I_{2\rightarrow2+1}=[1-(1-t_B\eta)^2]I(\varepsilon_2)$ $\approx2t_B\eta I(\varepsilon_2)$ and can therefore become larger than $I_{2\rightarrow1+1}$. The full analysis must be done carefully, taking into account the

observed total error rate; in the family of individual attacks, the cloning strategy performs better than for typical values of $t_B\eta$ (Curty and Lütkenhaus, 2004; Niederberger, Scarani, and Gisin, 2005). Note that there is no claim of optimality in this example: another attack may be found that performs still better.

[48]The name uncalibrated-device scenario is proposed here for the first time. In the literature, the assumption used to be named the untrusted-device scenario; but this name is clearly inadequate (see Sec. II.C.1 for the elements that must always be trusted in a QKD setup, and Sec. VIII.A.3 for those that may not be trusted in some very specific protocols).

[49]In some cases such as plug-and-play implementations, the randomization of the phase should in principle be ensured actively (Gisin *et al.*, 2006; Zhao, Qi, and Lo, 2008).

the optimal collective attack (Eve may always choose not to take advantage of this information).

The statistical parameters that describe a key exchange are basically detection rates and error rates.[50] Here are the main notations: R, total detection rate; R_n, detection rate for the events when Alice sent n photons ($\Sigma_n R_n = R$); $Y_n = R_n/R$ a convenient notation ($\Sigma_n Y_n = 1$); R_n^w wrong counts among the R_n; $\varepsilon_n = R_n^w/R_n$ the error rate on the n photon signals; and $Q = \Sigma_n Y_n \varepsilon_n$ the total error rate (QBER). Concerning photon statistics on Bob's side, it is important to notice the following. If the channel introduces random losses, the photons that enter Bob's device are distributed according to $p_B^t(k) = \Sigma_{n \geq k} p_A(n) C_n^k t^k (1-t)^{n-k}$, where $C_n^k = k!/n!(n-k)!$ is the binomial factor; one could compute R_n from this value and the details of the protocol. However, Eve can adapt her strategy to the value of n, so the photon-number statistics $p_B(k)$ on Bob's side may be completely different from $p_B^t(k)$ (Lütkenhaus and Jahma, 2002).

2. Qubits and modes

Many, although not all, security proofs can be obtained by finding qubit protocols in the optical implementations that work with optical modes.

a. Sources: Tagging

On the source side, this can be done with "tagging," by assuming that all multiphoton signals (with respect to the total signal) becoming fully known to an eavesdropper. This leaves us effectively with qubits, using single photons and the coding degree of freedom, for example, polarization or relative phase between two modes. This method has been used by Lütkenhaus (2000) and Inamori, Lütkenhaus, and Mayers (2007), but the term tagging was introduced only by Gottesman, Lo, Lütkenhaus, and Preskill (2004). Note that security proofs can be made without this assumption, e.g., in the case of the SARG protocol.

b. Detectors: Squashing

Detectors act on optical modes, and typically threshold detectors are used that cannot resolve the incoming photon number. Some security proofs (Mayers, 1996, 2001; Koashi, 2006a) can deal directly with this situation. In other security proofs one has to search through all possible photon numbers of arriving signals to prove that it is Eve's optimal strategy to send preferentially single photons to Bob (Lütkenhaus, 1999). It was realized there that double clicks in detection devices, resulting from multiphoton signals or dark counts, cannot be simply ignored, as this would open up a security

loophole.[51] As a countermeasure, Lütkenhaus (1999, 2000) introduced the concept of assigning double clicks at random to the values corresponding to single-click events.

The concept of squashing, originally introduced in a continuous-variable context (Gottesman and Preskill 2001), was coined by Gottesman, Lo, Lütkenhaus, and Preskill (2004), where it is assumed that the detection device can be described by a two-step process: in a first step, the optical signal is mapped (squashed) into a single photon (qubit), and then the ideal measurement in the qubit description is performed. Only recently has it been shown that a squashing model actually exists for the BB84 protocol (Beaudry, Moroder, and Lütkenhaus, 2008a; Tsurumaru and Tamaki, 2008) with the given assignment of double clicks to random single detector clicks. Actually, Beaudry, Moroder, and Lütkenhaus (2008a), developed squashing maps for different detector setups, including the implementation of passive basis choice in the BB84 protocols via a beam splitter. Note that the existence of a squashing model should not be taken for granted, as, for example, the six-state protocol does not admit a squashing model. However, a six-state protocol measurement with a passive basis choice via a linear optics array admits a squashing model for suitable assignment of multiclicks. (Beaudry *et al.*, 2008b).

It is not necessary to find a squashing model to prove security, but it is certainly an elegant shortcut, as now the combination of tagging in the source and squashing in the detector allows a reduction of the security analysis of QKD to qubit protocols. For the remainder of this review, however, we adopt the squashing model view.

3. Secret key rate

The bound for the secret fraction is Eq. (21). In the case of the protocols under study, $H(A) = H(B) = 1$ and $H(A|B) = H(B|A) = h(Q)$, where h is binary entropy and Q is the QBER. Therefore $I(A:B) = 1 - h(Q)$. However, we want to provide formulas that take imperfect error correction into account. Therefore we use

$$K = R[1 - \text{leak}_{EC}(Q) - I_E] \tag{25}$$

with $\text{leak}_{EC}(Q) \geq h(Q)$ and $I_E = \min(I_{AE}, I_{BE})$. We study this last term. Eve gains information only on the non-empty pulses, and provided Bob detects the photon she has forwarded. Since, due to the squashing model, the exponential De Finetti theorem applies to discrete-variable protocols (see discussion in Sec. III.B.2), and since the optimal collective attack includes the measure-

---

[50]We assume that these parameters are independent of Bob's measurements, either because they are really measured to be the same for all bases (a reasonable case in practice), or because, after the sifting procedure, Alice and Bob forget from which measurement each bit was derived and work with average values.

[51]A simple attack exploiting this loophole goes as follows: Eve performs an intercept-resend attack and resends a pulse containing a large number of photons in the detected polarization. If Bob measures in the same basis as Eve, he will receive a single detector click, about which Eve has full information. If Bob measures in a different basis, he will almost always receive double clicks, which he discards. Therefore Eve has perfect information about all signals retained by Eve, allowing her to break the QKD scheme.

ment of the number of photons, the generic structure for Eve's information reads[52]

$$I_E = \max_{\text{Eve}} \sum_n Y_n I_{E,n}, \qquad (26)$$

where the maximum is to be taken on all Eve's attacks compatible with the measured parameters.

B. BB84 coding: Lower bounds

In the BB84 coding, the probability that Bob accepts an item depends only on the fact that he has used the same basis as Alice, which happens with probability p_{sift}. Therefore, writing $\tilde{\nu}_S = \nu_S p_{\text{sift}}$, we have

$$R_n = \tilde{\nu}_S p_A(n) f_n, \qquad (27)$$

where f_n is the probability that Eve forwards some signal to Bob for n-photon pulses. Eve's attack must be optimized over the possible $\{f_n\}_{n \geq 0}$ compatible with $\Sigma_n R_n = R$. Now we consider different implementations of this coding.

1. Prepare-and-measure: Generalities

In P&M BB84, $I_{AE} = I_{BE}$. On the events when Alice sends no photons ($n=0$) but Bob has a detection, the intuitive result $I_{E,0} = 0$ (Lo, 2005) has indeed been proved (Koashi, 2006b). On the single-photon pulses, Eve can gain information only at the expense of introducing an error ε_1; the maximal information that she can obtain in this way is $I_{E,1} = h(\varepsilon_1)$, where h is the binary entropy (Shor and Preskill, 2000). A possible demonstration of this well-known result is given in Appendix A. For multiphoton pulses, the best attack is the PNS attack in which Eve forwards one photon to Bob and keeps the others: i.e., for $n \geq 2$, $\varepsilon_n = 0$, and $I_{E,n} = 1$ (Gottesman, Lo, Lütkenhaus, and Preskill, 2004; Fung, Tamaki, and Lo, 2006; Kraus, Branciard, and Renner, 2007). Therefore Eq. (26) becomes

$$I_E = \max_{\text{Eve}}[Y_1 h(\varepsilon_1) + (1 - Y_0 - Y_1)]$$

$$= 1 - \min_{\text{Eve}}\{Y_0 + Y_1[1 - h(\varepsilon_1)]\}. \qquad (28)$$

2. P&M without decoy states

In P&M schemes without decoy states, the only measured parameters are R and Q. We have to assume $\varepsilon_{n \geq 2} = 0$; therefore we obtain $\varepsilon_1 = Q/Y_1$. From this and

Eq. (28), we see[53] that Eve's optimal attack compatible with the measured parameters is the one which minimizes Y_1, a situation which is obviously achieved by setting $f_0 = 0$ and $f_{n \geq 2} = 1$. One finds then

$$Y_1 = 1 - (\tilde{\nu}_S/R)p_A(n \geq 2). \qquad (29)$$

As a conclusion, for BB84 in a P&M scheme without decoy states, the quantity to be subtracted in PA is

$$I_E = 1 - Y_1[1 - h(Q/Y_1)]. \qquad (30)$$

The corresponding achievable secret key rate (25) is

$$K = R\{Y_1[1 - h(Q/Y_1)] - \text{leak}_{EC}(Q)\}, \qquad (31)$$

where Y_1 is given in Eq. (29). As expected, K contains only quantities that are known either from calibration or from the parameter estimation of the protocol (R, Q).

3. P&M with decoy states

The idea of decoy states is simple and deep. Alice changes the nature of the quantum signal at random during the protocol; at the end of the quantum signal exchange, she will reveal which state she sent in each run. Thus, Eve cannot adapt her attack to Alice's state, but in the postprocessing Alice and Bob can estimate their parameters conditioned on that knowledge. The first proposal using one- and two-photon signals (Hwang, 2003) was rapidly modified to the more realistic implementation in which Alice modulates the intensity of the laser (Lo, Ma, and Chen, 2005; Wang, 2005). As mentioned, several experiments have already been performed (Ma *et al.*, 2006; Zhao *et al.*, 2006; Peng *et al.*, 2007; Rosenberg *et al.*, 2007; Yuan, Sharpe, and Shields, 2007), more recently even including finite-key effects (Hasegawa *et al.*, 2007).

Let ξ be some tunable parameter(s) in the source, the typical example being $\xi = \mu$, the intensity (mean photon number) of a laser. Alice changes the value of ξ randomly from one pulse to the other; at the end of the exchange of quantum signals, Alice reveals the list of values of $\xi \in \mathcal{X}$, and the data are sorted in order to estimate the parameters separately for each value. With this simple method, Alice and Bob measure $2|\mathcal{X}|$ parameters, namely, the R^ξ and the Q^ξ.

The set $\mathcal{X}$ is publicly known as part of the protocol, but if $|\mathcal{X}| > 1$, Eve cannot adapt her strategy to the actual value of ξ in each pulse because she does not know it. Therefore, f_n and ε_n are independent of ξ; in particular, $R_n^\xi = \tilde{\nu}_S p_A(n|\xi) f_n$. The measured parameters

$$R^\xi = \sum_{n \geq 0} R_n^\xi \quad \text{and} \quad Q^\xi = \sum_{n \geq 0} (R_n^\xi/R^\xi)\varepsilon_n \qquad (32)$$

define a linear system with $2|\mathcal{X}|$ equations for f_n and ε_n. The optimization in Eq. (28) must then be performed using the lower bound for Y_1^ξ and the upper bound for ε_1 as obtained from the measured quantities $\{R^\xi, Q^\xi\}_{\xi \in \mathcal{X}}$

---

[52]More explicitly, this formula should read $I_E = \min(I_{AE}, I_{BE})$ with $I_{AE} = \max_{\text{Eve}} \Sigma_n Y_n I_{AE,n}$ and similarly for I_{BE}. In the development of QKD, this formula was derived first for BB84 (Gottesman, Lo, Lütkenhaus, and Preskill, 2004), then for SARG04 (Fung, Tamaki, and Lo, 2006), and then generalized to all discrete-variable protocols (Kraus, Branciard, and Renner, 2007).

[53]First proved by Inamori, Lütkenhaus, and Mayers (2007) in the context of unconditional security.

(Tsurumaru, Soujaeff, and Takeuchi, 2008). In practice, the meaningful contributions are typically the $n=0,1,2$ terms, and a decoy-state protocol with $|\mathcal{X}|=3$ comes very close to an exact determination (Hayashi, 2007b). For simplicity, here we suppose that all f_n and ε_n have been determined exactly.[54] Also, we consider a protocol in which the classical postprocessing that extracts a key is done separately on the data that correspond to different ξ. For each ξ, the quantity to be subtracted in PA is[55]

$$I_E^\xi = 1 - Y_0^\xi - Y_1^\xi [1 - h(\varepsilon_1)] \qquad (33)$$

with $Y_{0,1}^\xi = R_{0,1}^\xi / R^\xi$, and the corresponding achievable secret key rate is

$$K^\xi = R^\xi \{ Y_0^\xi + Y_1^\xi [1 - h(\varepsilon_1)] - \text{leak}_{EC}(Q^\xi) \}. \qquad (34)$$

The total secret key rate is $K = \Sigma_\xi' K^\xi$, where the sum is taken on all values of ξ such that $K^\xi \geq 0$. If the classical postprocessing were done on the whole raw key, the total secret key rate would read $K = R[1 - \text{leak}_{EC}(Q)] - \Sigma_\xi R^\xi I_E^\xi$. The two expressions coincide if there exists a ξ that is used almost always.

4. P&M: Analytical estimates

Alice and Bob can optimize K by playing with the parameters of the source, typically the intensity. A rigorous optimization can be done only numerically. In this section, we rederive some often-quoted results for P&M implementations of BB84. For this *a priori* estimate, one has to assume that some "typical" values for R_n and Q_n will be observed. As stressed above, security must be based on the actually measured values: what follows provides only guidelines to start working with the correct orders of magnitude. Here we chose to work in a regime in which the rate of detection of true photons is much larger than the dark count rate. For simplicity, we also assume optimal error correction, so that $\text{leak}_{EC}(Q) = h(Q)$.

The reference case is the case of single-photon sources, for which the meaningful scheme is P&M without decoy states. For this source, $p_A(1) = 1$ and therefore $Y_1 = 1$; the expected detection rate is $R = \tilde{\nu}_S t t_B \eta$, and Eq. (31) yields immediately

$$K \approx \tilde{\nu}_S t t_B \eta [1 - 2h(Q)] \quad \text{(single photon)}. \qquad (35)$$

As expected, K scales linearly with the losses in the line and the efficiency of the detector.

The most widespread sources in P&M schemes are attenuated lasers. The estimate can be made by considering only the single-photon and two-photon emissions: $p_A(1) = \mu e^{-\mu}$ and $p_A(2) = \mu^2 e^{-\mu}/2$. The expected detection rate is $R = \tilde{\nu}_S \mu t t_B \eta$. The important feature that is absent in the study of single-photon sources is the existence of

an optimal value for the intensity μ, a compromise between a large R and a small $p_A(2)$. We focus first on implementations without decoy states. We can set $p_A(1) \approx \mu$ and $p_A(2) \approx \mu^2/2$, but still the optimal value of μ cannot be estimated exactly in general, because $Y_1 = 1 - \mu/2 t t_B \eta$ depends on μ and appears in a nonalgebraic function. We then consider first the limiting case $Q = 0$: Eq. (31) becomes $K/\tilde{\nu}_S \approx \mu t t_B \eta - \mu^2/2$, whose maximal value is $\frac{1}{2}(t t_B \eta)^2$, obtained for $\mu_0 = t t_B \eta$ (Lütkenhaus, 2000). To obtain estimates for the $Q > 0$ case, we can make the approximation of using μ_0 to compute Y_1, i.e., to set $Y_1 = \frac{1}{2}$. Then, the optimization of Eq. (31) is also immediate: writing $F(Q) = 1 - h(2Q) - h(Q)$, the highest achievable secret key rate is

$$K/\tilde{\nu}_S t t_B \eta \approx \tfrac{1}{2} \mu_{\text{opt}} F(Q) \quad \text{(laser, no decoy)} \qquad (36)$$

obtained for the optimal mean photon number

$$\mu_{\text{opt}} \approx t t_B \eta F(Q)/[1 - h(2Q)]. \qquad (37)$$

We now perform the estimate for an implementation using decoy states. The decoy consists in varying the intensity of the laser from one pulse to another so that the general parameter ξ is in fact μ. We suppose that a given value μ is used almost always (and this one we want to optimize), while sufficiently many decoy values are used in order to provide a full parameter estimation. The expected values are $R^\mu = \tilde{\nu}_S \mu t t_B \eta$, $R_1^\mu = \tilde{\nu}_S \mu e^{-\mu} t t_B \eta$, and $\varepsilon_1 = Q$. Inserted into Eq. (34), one obtains $K \approx \tilde{\nu}_S \mu t t_B \eta \{ e^{-\mu} [1 - h(Q)] - h(Q) \}$; using $e^{-\mu} \approx 1 - \mu$, this expression reaches the maximal value

$$K/\tilde{\nu}_S t t_B \eta \approx \tfrac{1}{2} \mu_{\text{opt}} [1 - 2h(Q)] \quad \text{(laser, decoy)} \qquad (38)$$

for the optimal mean photon number

$$\mu_{\text{opt}} \approx \frac{1}{2} \left(1 - \frac{h(Q)}{1 - h(Q)} \right). \qquad (39)$$

We now summarize. Without decoy states, $\mu_{\text{opt}} \sim t$ and consequently $K \propto t^2$: the larger the losses, the more attenuated must the laser be. The reason are PNS attacks: Alice must ensure that Eve cannot reproduce the detection rate at Bob's using only photons that come from two-photon pulses (on which she has full information). With decoy states, one can determine the fraction of detections that involve photons coming from two-photon pulses; if this fraction is as low as expected, one can exclude a PNS attack by Eve—as a benefit, the linear scaling $K \propto t$ is recovered. This is the same scaling obtained with single-photon sources, with the obvious benefit that lasers are much more versatile and well developed than strongly sub-Poissonian sources. Another interesting remark is that, both with and without decoy states, $\mu_{\text{opt}} \approx \frac{1}{2} \mu_{\text{crit}}$, where the critical value μ_{crit} is defined as the one for which $K \approx 0$. In other words, an intensity double the optimal one is already enough to spoil all security. In implementations without decoy states, where μ decreases with increasing t, this calibration may be critical at long distances.

---

[54]As a side remark, one might find $\varepsilon_{n \geq 2} > 0$, but this does not modify the discussion in Sec. IV.B.1 about the optimal attack. Indeed, Eve might have performed the attack that gives $\varepsilon_{n \geq 2} = 0$ and then added some errors "for free."

[55]Note the presence of Y_0^ξ in the next two equations.

5. Entanglement based

If Alice holds the down-conversion source, as is the case in almost all EB QKD experiments performed to date,[56] an EB scheme is equivalent to a P&M one (see Sec. II.B.2) so the corresponding security proofs could be applied. The only specific difference to address concerns the events in which more than one pair is produced inside a coincidence window. As described in Sec. II.E.3, two kinds of such contributions exist and Eve is able to distinguish between them.

- A fraction of the multipair events contain partial correlations in the degrees of freedom used for symbol encoding; thus, Eve can obtain information on the key bit by some form of PNS attack. This situation is similar to the multiphoton case in P&M schemes, although here it is difficult to determine exactly the amount of information that leaks out. To be on the safe side we suppose that Eve can obtain full information without introducing any errors.

- The other, usually much larger, fraction of multipair events consists of independent uncorrelated pairs. In this case Eve cannot obtain any information about Bob's symbol using the PNS attack. She can only apply the "standard" single-particle attack. We suppose that Eve can somehow find out which one of multiple pairs was selected by Alice's detector, so we treat all such multipair contributions as if they were single pairs.

Therefore Eq. (28) is replaced by

$$I_E \leqslant Y_m' + Y_1' h(Q/Y_1'), \tag{40}$$

where Y_1' is the fraction of single-pair plus uncorrelated multipair events and Y_m' is the fraction of multipair events that are (partially) correlated in the degree of freedom in which the information is encoded. Explicitly,

$$Y_m' = p_A(n \geqslant 2) \frac{\tilde{\nu}_S \zeta}{R} \tag{41}$$

with ζ the ratio of the number of partially correlated multipair contributions to all multipair contributions (see Sec. II.E.3). In total $Y_m' + Y_1' = 1$. Finally, the achievable secret key rate reads

$$K = R\{Y_1'[1 - h(Q/Y_1')] - \text{leak}_{EC}(Q)\}. \tag{42}$$

Recall that these formulas apply to implementations in which the source is safe on Alice's side. Notice also that two different sorts of multipair contribution are considered and for each of them a different eavesdropping strategy is assumed. However, in reality there is a smooth transition between correlated and uncorrelated pairs. All multipair events that exhibit non-negligible correlations must be counted as correlated.

Recently security has also been demonstrated for EB systems, in which the source is under Eve's control (Ma, Fung, and Lo, 2007). They describe the conditions under which the whole object "Eve's state preparation and Alice's measurement" behaves like an uncharacterized source in the sense of Koashi and Preskill (2003). Alice has a box where she can dial a basis and she gets an information bit from her box indicating which signal (0 or 1) was sent. Whatever state Eve prepares, when she puts one part into Alice's box and Alice chooses a measurement, then the average density matrix outside this box is independent of this choice (assuming that the no-click event probability is basis independent).[57] On Alice's side no Hilbert space argument is needed, but on Bob's side the squashing property of the detection is required (see Sec. IV.A.2). The formula for the achievable secret key rate then reads

$$K = R[1 - h(Q) - \text{leak}_{EC}(Q)]. \tag{43}$$

Formally, this is the same as obtained in a P&M scheme using single photons [Eq. (31) with $Y_1 = 1$]. As such, it is a remarkable result: it states that, under the assumptions listed above, all deviations from a perfect two-photon source—in particular, the presence of multiphoton components—are taken care of by measuring the error rate Q (Koashi and Preskill, 2003). In addition, it has been found that the EB QKD can tolerate higher losses if the source is placed in the middle between Alice and Bob rather than if it is on Alice's side (Waks, Zeevi, and Yamamoto, 2002; Ma, Fung, and Lo, 2007).

Finally, we note that very recently another proof of the security of entanglement-based systems with real detectors was proposed, which does not rely on the squashing property but rather on the measurement of the double-click rate (Koashi *et al.*, 2008).

C. BB84 coding: Upper bounds incorporating the calibration of the devices

As explained in Sec. III.B.5, the bounds for unconditional security are always found for the uncalibrated-device scenario, which is overly pessimistic. It is instructive to present some upper bounds that take the calibration of the devices into account: the comparison between these and the lower bounds will determine the "realm of hope," i.e., the range in which improvements on K may yet be found. Clearly, the contribution $\text{leak}_{EC}(Q)$ of error correction is independent of the scenario: one has to correct for all errors, whatever their origin. The difference appears in the quantity to be removed in privacy amplification.

---

[56]We are aware of a single case in which the source was in the middle (Erven *et al.*, 2008). As discussed below in this section, security proofs have been provided also for this situation.

[57]This is clearly true for an active basis choice. In the case of passive basis selection some additional assumptions on the detection may be necessary.

1. Statistical parameters

In order to single out the parameters of the devices, one has first to recast the general notations (Sec. IV.A.1) in a more elaborated form. The detection rates must be explicitly written as

$$R_n = R_{n,p} + R_{n,d}, \tag{44}$$

where $R_{n,p}$ is the contribution of detections and $R_{n,d}$ is the contribution of dark counts. Since Eve can act only on the first part, it is convenient to redefine $Y_n = R_{n,p}/R$ so that $\Sigma_n Y_n \equiv Y < 1$. The errors on the line ε_n are introduced only on the photon contribution, while the dark counts always give an error rate of $\frac{1}{2}$; therefore the total error is

$$Q = Y\varepsilon + \delta, \tag{45}$$

where $\varepsilon = \Sigma_{n \geqslant 1}(Y_n/Y)\varepsilon_n$ and $\delta = (1-Y)/2$.

Note that the content of this section is not specific to the BB84 protocol; but all that follows is.

2. Upper bounds

To derive an upper bound, we use a simple recipe, which consists in following closely the calculations of the previous section (Sec. IV.B) and making the necessary modifications, although this is known to be suboptimal and no squashing model is known in this situation to justify the assumption. In particular, Eve is still supposed to forward to Bob at most one photon, although this is known to be suboptimal. Therefore

$$R_{n,p} = \tilde{\nu}_S p_A(n) f_n t_B \eta, \tag{46}$$

$$R_{n,d} = \tilde{\nu}_S p_A(n)(1 - f_n t_B \eta) 2 p_d, \tag{47}$$

where p_d is the dark count rate. Note the presence of $t_B \eta$ in these formulas: the detector efficiency has not been incorporated into f_n. Extracting $f_n t_B \eta$ from these equations, one finds

$$Y = (1 - 2 p_d \tilde{\nu}_S/R)/(1 - 2 p_d), \tag{48}$$

which means that the ratio between detections and dark counts depends only on the total detection rate R. Also, for our simple recipe, it is immediate that the modification of the general expression (28) reads

$$\begin{aligned} I_E &= \max_{\text{Eve}}[Y_1 h(\varepsilon_1) + (Y - Y_1)] \\ &= Y - \min_{\text{Eve}} Y_1[1 - h(\varepsilon_1)]. \end{aligned} \tag{49}$$

We restrict the discussion now to the P&M schemes. In the implementation with decoy states, Y_n and ε_n are known, so the only difference from the uncalibrated-device formula (34) is the role of the dark counts,

$$K^\xi = R^\xi \{ Y_1^\xi [1 - h(\varepsilon_1)] + 2\delta^\xi - \text{leak}_{EC}(Q^\xi) \}, \tag{50}$$

where Y_0 is replaced by the slightly larger term[58] $2\delta^\xi = 1 - Y^\xi$. Things are different for the implementation

without decoy states, because now Y_1 and ε_1 are not directly measured; only R and Q are. Since we are supposing that the optimal strategy is still such that $\varepsilon_{n \geqslant 2} = 0$ and $f_{n \geqslant 2} = 1$, we have

$$Y_1 = Y - t_B \eta \frac{\tilde{\nu}_S}{R} p_A(n \geqslant 2) \quad \text{and} \quad \varepsilon_1 = \frac{Q - \delta}{Y_1}. \tag{51}$$

Note that Y_1 can be significantly larger than in the uncalibrated-device scenario [Eq. (29)]: in fact, although Y is slightly smaller than 1, the term to be subtracted is multiplied by $t_B \eta$. This difference is specifically due to the fact that Eve is not supposed to influence the efficiency of the detector. Finally, one obtains

$$K = R\{ Y_1[1 - h(\varepsilon_1)] + 2\delta - \text{leak}_{EC}(Q) \} \tag{52}$$

with Eq. (51) and $2\delta = 1 - Y$.

D. Bounds for the SARG04 coding

We sketch here the analysis of the SARG04 protocol because it contains a certain number of instructive differences with respect to BB84. We note that $\tilde{\nu}_S = \nu_S/2$ because Bob must always choose the bases with probability $\frac{1}{2}$, even if Alice almost always uses the same set of states. The raw key rates are different from those of BB84. For definiteness, suppose that Alice sends $|+x\rangle$ so the bit is accepted if Bob finds $-$. If Bob measures X, he accepts the bit only if he obtains $-$, but this can only be due to an error. We write $R_n^w = \tilde{\nu}_S p_A(n) f_n \tilde{\varepsilon}_n$, where the relation of $\tilde{\varepsilon}_n$ to the induced error rate ε_n will be computed below. If Bob measures Y, he gets $-$ in half of the cases[59] and the bit value is correct. As a result,

$$R_n = \tilde{\nu}_S p_A(n) f_n (\tfrac{1}{2} + \tilde{\varepsilon}_n). \tag{53}$$

We see that the detection rate increases in the presence of errors, in contract to the situation in BB84, where the detection rate is determined only by p_{sift}. The error rate is

$$\varepsilon_n = \tilde{\varepsilon}_n \left/ \left(\frac{1}{2} + \tilde{\varepsilon}_n \right) \right.; \tag{54}$$

for a given perturbation $\tilde{\varepsilon}_n$ in the quantum channel, the error introduced in SARG04 is roughly twice the error $\varepsilon_n = \tilde{\varepsilon}_n$ that would be introduced in BB84.

The protocol can be analyzed following the same pattern as the one presented for BB84. Here we review the main results.

---

[58] In the notation here the previous Y_0 would read $R_0/R = R_{0,d}/R$; while $2\delta = \Sigma_{n \geqslant 0} R_{n,d}/R$. Note that, strictly speaking,

[footnote continued in right column]

$R_0 = R_{0,d}$ is an assumption: *a priori* one can imagine that Eve creates some photons to send to Bob also when Alice is sending no photons—but we do not consider here such a highly artificial situation.

[59] This statement contains an assumption about Eve's attack, namely, $\text{Tr}[\sigma_y \rho(\pm x)] = 0$, where $\rho(\pm x)$ is the state received by Bob after Eve's intervention, when Alice has sent $|\pm x\rangle$. But the result holds in general for the average detection rate, if Alice prepares all four states with equal probability.

- SARG04 was invented as a method to reduce the effect of PNS attacks, taking advantage of the fact that Eve cannot extract full information from the two-photon pulses (Acín, Gisin, and Scarani, 2004; Scarani, Acín, Ribordy, and Gisin, 2004). This initial intuition has been confirmed by all subsequent, more rigorous studies. In particular, it was proved that a fraction of the fully secure secret key can be extracted from the two-photon pulses (Tamaki and Lo, 2006), and that in implementations using weak coherent lasers and without decoy states, for a small error rate, SARG04 indeed performs better than BB84 and shows a scaling $\sim t^{3/2}$ as a function of the distance (Branciard *et al.*, 2005; Koashi, 2005; Kraus, Branciard, and Renner, 2007). In the literature one finds the claim that, when implemented with decoy states, SARG04 performs worse than BB84 (Fung, Tamaki, and Lo, 2006; Kraus, Branciard, and Renner, 2007). This must be properly understood: decoy states are a method to gain additional knowledge about Eve's attack. If this method does not reveal any PNS attack (as will be the case in most experiments because losses appear random and therefore Eve is acting as a beam splitter), indeed the BB84 rate is better than that of SARG04. However, if Eve is actually performing a PNS attack, SARG04 will of course be more robust, consistently with what we wrote in the previous item.

- An interesting case arises if one considers implementations with single-photon sources. The first unconditional security bound yielded that the SARG04 protocol tolerates a smaller QBER than BB84 (Tamaki and Lo, 2006). But this bound was improved shortly thereafter: the optimal $I_{E,1}$, which is not known analytically but can easily be computed numerically, goes to zero for $\varepsilon_1 \approx 11.67\%$ (Kraus, Branciard, and Renner, 2007). This improved value is slightly better than the corresponding value for BB84, $\varepsilon_1 \approx 11.0\%$: it seems therefore that SARG04 would perform better than BB84 in a single-photon implementation also. The picture is different, however, if one relates the error rate to parameter of the channel, typically the visibility of interference fringes: this parameter is related to the ones introduced here through $\tilde{\varepsilon}_1 = (1 - V)/2$. For BB84, $\tilde{\varepsilon}_1 = \varepsilon_1$ and consequently the critical visibility is $V \approx 78\%$; while for SARG04, because of Eq. (54), the critical visibility is worse, namely, $V \approx 87\%$.

V. CONTINUOUS-VARIABLE PROTOCOLS

A. Status of security proofs

In the case of Gaussian modulation, security has been proved against collective attacks (García-Patrón and Cerf, 2006; Navascués, Grosshans, and Acín, 2006). We present this bound below (Sec. V.B) and use it for comparison with the other platforms (Sec. VII). There is some hope that the same bound would also hold for the most general attack, as it is the case for discrete-variable systems: in particular, we note that the "intuitive" reason behind that equivalence (Sec. III.B.2) would apply also to CV protocols. Unfortunately, the exponential De Finetti bound (Renner, 2007) does not help because it explicitly depends on the dimension of the quantum signals. For more on this issue, see the "Note added" at the end of this paper.

In the case of discrete modulation, the security status is even less advanced. Technically, the difficulty lies in the fact that the raw key is made up of discrete variables for Alice, while Bob has a string of real numbers. A full analysis has been possible only in the case where the quantum channel does not add excess noise to the signal, so that the observed conditional variances still describe minimum-uncertainty states. In this case, the eavesdropper's attack is always describable as a generalized beam-splitting attack, simulating the observed loss. The corresponding key rates depend on the classical communication protocols chosen (with or without postselection of data, in reverse or direct reconciliation); the best-known protocol involves a combination of postselection and reverse reconciliation, especially when the error-correction algorithms work away from the asymptotic Shannon efficiency (Heid and Lütkenhaus, 2006). In the presence of excess noise, the formula for the key rate is the object of ongoing research; it has at least been possible to derive entanglement witnesses (Rigas, Gühne, and Lütkenhaus, 2006). Entanglement verification has been performed and has shown that excess noise in typical installations does not wipe out the quantum correlation within the experimentally accessible domain (Lorenz *et al.*, 2006).

Finally, in all works on CV QKD, with no exception, it has been assumed that Eve does not act on the local oscillator[60]—of course, she is allowed to have access to it in order to measure quadratures. Since the local oscillator travels through Eve's domain, this assumption opens a security loophole.[61] Note that a similar situation burdened until recently the security of plug-and-play configurations, for which finally unconditional security was proved (see Sec. II.H.2); it is not clear, however, that the same approach will work here since the strong pulses

---

[60]This amounts to viewing the local oscillator as an *authenticated* channel, building on the closeness to classical signals. In an alternative setup, this problem can be circumvented by Bob measuring the phase of the local oscillator, followed by the recreation within Bob's detector of a local oscillator with the measured phase (Koashi, 2004).

[61]For the setups as they have been implemented, all observed correlations are compatible with an intercept-resend attack involving both the signal and the local oscillator. Security against this specific attack can be easily recovered by simple modifications of the setups; for example, the independent measurement of the intensity of the phase reference pulse and the signal pulse (Häseler, Moroder, and Lütkenhaus, 2008).

have very different roles in the two schemes. In any case, the open issue just discussed together with the fact that the existing exponential De Finetti theorem does not apply to infinitely dimensional systems are the main reasons that unconditional security proofs are not available yet for CV QKD.

As mentioned earlier (Sec. II.D.3), continuous-variable protocols also show interesting features in the classical part. In contrast to typical discrete-variable protocols, where losses simply reduce the number of detected signals, continuous-variable protocols will always detect a result so that loss corresponds now to increased noise in the signal. Two main methods have been formulated to deal with this situation at the protocol level: reverse reconciliation (Grosshans and Grangier, 2002) and postselection (Silberhorn *et al.*, 2002). The first method can be realized using one-way EC schemes, but turns out to be sensitive to the efficiency of those schemes. Its main advantage is that its security can be rigorously assessed versus general collective attacks (and has been conjectured to hold even for coherent attacks). In contrast, the second method can use both one-way and two-way EC schemes, and is fairly stable even if those schemes do not perform at the Shannon limit. However, its security can be analyzed only by making assumptions about Eve's interception (see below). The status of its security is not clear even for general individual attacks. Note that, for close-to-perfect EC, reverse reconciliation outperforms postselection. While progress is being made in the efficiency of EC schemes, it turns out that a combination of postselection and reverse reconciliation provides a practical solution to obtain reasonable rates with current technology, both for discrete-modulation (Heid and Lütkenhaus, 2006) and for Gaussian-modulation protocols (Heid and Lütkenhaus, 2007).

B. Bounds for Gaussian protocols

1. Generalities

As discussed, we provide an explicit security bound for the coherent-state homodyne-detection protocol of Grosshans and Grangier (2002a). Like all Gaussian protocols, this prepare-and-measure protocol can be shown to be equivalent to an entanglement-based scheme (Grosshans, Cerf, *et al.*, 2003). In such a scheme, Alice prepares an Einstein-Podolsky-Rosen (EPR) state—more precisely, the two-mode squeezed vacuum state (15). By applying a heterodyne measurement on mode A, she prepares in the second mode of the EPR pair a coherent state, whose displacement vector is Gaussian distributed in x and p. Then, Bob applies a homodyne measurement on mode B, measuring quadrature x or p. It can be shown that reverse reconciliation is always favorable for Alice and Bob, so we have to compute Eq. (21) with I_{EB} on the right-hand side.

It has been proved that Eve's optimal attack is Gaussian for both individual (Grosshans and Cerf, 2004; García-Patrón, 2007; Lodewyck, Debuisschert, *et al.*,

2007) and collective attacks (García-Patrón and Cerf, 2006; Navascués, Grosshans, and Acín, 2006). We can therefore assume that Eve effects a Gaussian channel so that the quantum state ρ_{AB} just before Alice and Bob's measurements can be assumed to be a Gaussian two-mode state with zero mean value and covariance matrix γ_{AB}.

The Gaussian channel is characterized by two parameters: the transmittance, which here, since we work in the uncalibrated-device scenario, is $t\eta$ with η the efficiency of the detectors; and the noise δ referred to the input of the channel.[62] Since the two-mode squeezed state (15) is also symmetric and has no correlations between x and p, the resulting covariance matrix of modes A and B can be written in a block-diagonal form,

$$\gamma_{AB} = \begin{pmatrix} \gamma_{AB}^x & 0 \\ 0 & \gamma_{AB}^p \end{pmatrix} \tag{55}$$

with

$$\gamma_{AB}^{x(p)} = \begin{pmatrix} v & \pm\sqrt{t\eta(v^2-1)} \\ \pm\sqrt{t\eta(v^2-1)} & t\eta(v+\delta) \end{pmatrix}, \tag{56}$$

where the signs $+$ and $-$ correspond to γ_{AB}^x and γ_{AB}^p, respectively. Here v is the variance of both quadratures of Alice's output thermal state expressed in shot-noise units, that is, $v = v_A + 1$, with v_A the variance of Alice's Gaussian modulation.

For what follows, it is convenient to define $v_{X|Y}$, the conditional variance that quantifies the remaining uncertainty on X after the measurement of Y,

$$v_{X|Y} = \langle x^2 \rangle - \langle xy \rangle^2 / \langle y^2 \rangle, \tag{57}$$

expressed in shot-noise units.

2. Modeling the noise

The noise δ is the total noise of the Alice-Bob channel. It can be modeled as the sum of three terms,

$$\delta = (1-t)/t + \delta_h/t + \epsilon. \tag{58}$$

The first term $(1-t)/t$ stands for the loss-induced vacuum noise (referred to the input); this term is at the origin of the higher sensitivity to losses of continuous-variable QKD. The second term stands for the noise added by the imperfection of the homodyne detection. This is modeled by assuming that the signal reaching Bob's station is attenuated by a factor η (detection efficiency) and mixed with some thermal noise v_{el} (electronic noise of the detector), giving[63]

---

[62]The observed noise in channels such as optical fibers is typically symmetric and uncorrelated in both quadratures x and p (there is no preferred phase) so we restrict consideration to this case here.

[63]Replacing the expression for δ_h into Eq. (58), one obtains $\delta = (1-t\eta+v_{el})/t\eta + \epsilon$, which depends only on $t\eta$, as it should in the uncalibrated-device scenario.

$$\delta_h = (1 + v_{el})/\eta - 1. \tag{59}$$

The third term ϵ is the excess noise (referred to the input) that is not due to line losses nor detector imperfections. For a perfect detector, it can be viewed as the continuous-variable counterpart of the QBER in discrete-variable QKD; it is zero for a lossy but noiseless line.

3. Alice-Bob information

In the EB version of the coherent-state protocol considered here (Grosshans and Grangier, 2002a), Alice performs heterodyne detection so her uncertainty on Bob's quadratures is expressed as

$$v_{B|A_M} = t\eta(\delta + 1). \tag{60}$$

The mutual information between Alice and Bob is therefore given by

$$I(A:B) = \frac{1}{2}\log_2\left(\frac{v_B}{v_{B|A_M}}\right) = \frac{1}{2}\log_2\left(\frac{\delta + v}{\delta + 1}\right). \tag{61}$$

As mentioned above, the main bottleneck of continuous-variable QKD schemes comes from the heavy postprocessing that is needed in order to correct the errors due to the vacuum noise that is induced by the line losses. In practice, the amount of information left after error correction will be a fraction β of $I(A:B)$. This value has an important effect on the achievable secret key rate and the limiting distance (as discussed below, for $\beta=1$ a secure key can in principle be extracted for arbitrarily large distances). This provides a strong incentive for developing better reconciliation algorithms. The first technique that was proposed to perform continuous-variable error correction relied on a so-called "sliced reconciliation" method (Van Assche, Cardinal, and Cerf, 2004), and gave an efficiency $\beta \approx 80\%$. These algorithms have been improved using turbo codes (Nguyen, Van Assche, and Cerf, 2004) and low-density parity codes (LDPCs) (Bloch *et al.* 2005), which both allow working with noisy data, hence longer distances. More recently, multidimensional reconciliation algorithms have been introduced, which allow even noisier data to be dealt with; while keeping similar or higher reconciliation efficiencies (Leverrier, Alleaume, *et al.*, 2008).

4. Individual attacks

To become familiar with the security analysis, we first present individual attacks. In order to address the security of the protocol, we assume as usual that Eve holds the purification of ρ_{AB}. Then, by measuring their systems, Alice and Eve project Bob's share of the joint pure state $|\Psi_{ABE}\rangle$ onto another pure state [we may assume without loss of generality that Eve's projection results from a rank-1 positive-operator-valued measure (POVM)]. Applying the Heisenberg uncertainty relation on the pure state held by Bob conditionally on Alice and Eve's measurements, we have

$$v_{X_B|E}v_{P_B|A} \geqslant 1, \quad v_{P_B|E}v_{X_B|A} \geqslant 1, \tag{62}$$

where X_B and P_B are the canonically conjugate quadratures of Bob's mode. Equation (62) can be written as a single uncertainty relation

$$v_{B|E}v_{B|A} \geqslant 1, \tag{63}$$

where B stands for any quadrature of Bob's mode. This inequality can be used to put a lower bound on the uncertainty of Eve's estimate of the key in reverse reconciliation, that is, when the key is made out of Bob's data while Alice and Eve compete to estimate it.

Now, $v_{B|A}$ is not necessarily given by Eq. (60): Eve's attack cannot depend on how the mixed state sent by Alice (i.e., the thermal state) has been prepared, since all possible ensembles are indistinguishable. An acceptable possibility is that Alice performs homodyne measurement, or, equivalently, prepares squeezed states just as in the protocol of Cerf, Lévy, and Van Assche (2001); in which case we obtain

$$v_{B|A} = t\eta(\delta + 1/v). \tag{64}$$

It can be shown that this is the lowest possible value of $v_{B|A}$; hence from Eq. (63)

$$v_{B|E} \geqslant 1/t\eta(\delta + 1/v). \tag{65}$$

This gives a bound for $I(B:E)$, so the extractable secret key rate under the assumption of individual attacks becomes

$$r = I(A:B) - I(E:B) = \frac{1}{2}\log_2\left(\frac{v_{B|E}}{v_{B|A_M}}\right)$$
$$\geqslant \frac{1}{2}\log_2\left(\frac{1}{(t\eta)^2(\delta + 1/v)(\delta + 1)}\right) \tag{66}$$

as shown by Grosshans, Van Assche, *et al.* (2003). Note that the scheme that implements the optimal attack (saturating this bound) is the entanglement cloner defined by Grosshans and Grangier (2002b). Using Eq. (58), in the case of high losses ($t\eta \to 0$) and large modulation ($v \to \infty$), the secret key rate r remains nonzero provided that the excess noise satisfies $\epsilon < 1/2$. This is a remarkable result due to reverse reconciliation: for direct reconciliation, obviously there can be no security when Eve has as much light as Bob, i.e., for $t\eta \leqslant \frac{1}{2}$.

A similar reasoning can be followed to derive the security of all Gaussian QKD protocols against individual attacks (García-Patrón, 2007). The only special case concerns the coherent-state heterodyne-detection protocol, whose security study against individual attacks is more involved (Lodewyck and Grangier, 2007; Sudjana *et al.*, 2007).

5. Collective attacks

The security of the coherent-state homodyne-detection scheme against the class of collective attacks has been fully studied. The corresponding rates were first provided assuming that Eve's collective attack is

Gaussian (Grosshans, 2005; Navascués and Acín, 2005). Later on, it was proved that this choice is actually optimal (García-Patrón, and Cerf, 2006; Navascués, Grosshans, and Acín, 2006). This implies that it remains sufficient to assess the security against Gaussian collective attacks, which are completely characterized by the covariance matrix γ_{AB} estimated by Alice and Bob. A long but straightforward calculation shows that

$$\chi(B\!:\!E) = g(\tilde{\lambda}_1) + g(\tilde{\lambda}_2) - g(\tilde{\lambda}_3), \tag{67}$$

where $g(x) = (x+1)\log_2(x+1) - x\log_2 x$ is the entropy of a thermal state with a mean photon number of x and $\tilde{\lambda}_k = (\lambda_k - 1)/2$, where

$$\lambda_{1,2}^2 = \frac{1}{2}(A \pm \sqrt{A^2 - 4B}), \quad \lambda_3^2 = v\frac{1 + v\delta}{v + \delta} \tag{68}$$

with $A = v^2(1 - 2t\eta) + 2t\eta + [t\eta(v+\delta)]^2$ and $B = [t\eta(v\delta + 1)]^2$.

In conclusion, the secret key rate achievable against collective attacks is obtained by inserting Eqs. (61) and (67) into

$$K = R[\beta I(A\!:\!B) - \chi(B\!:\!E)]. \tag{69}$$

Finally, we note that the optimality of Gaussian attacks is actually valid for protocols that use heterodyne detection; a bound for security against Gaussian collective attacks in these protocols has been provided recently (Pirandola, Braunstein, and Lloyd, 2008).

6. Collective attacks and postselection

In the case where all observed data are Gaussian, including the observed noise, we can provide a security proof which also allows the inclusion of postselection of data in the procedure. The starting point of this security proof is a protocol with Gaussian distribution of the amplitude together with heterodyne detection by Bob. In this case, in a collective attack scenario, we can assume a product structure of the subsequent signals, and the density matrix ρ_{AB} of the joint state of Alice and Bob is completely determined due to the tomographic structure of the source replacement picture and the measurement. In this scenario, we can therefore determine the quantum states in the hand of the eavesdropper as Eve holds the system E of the purification $|\Psi\rangle_{ABE}$ of ρ_{AB}.

We consider the situation where all observed data in this scenario are Gaussian distributions, which is the typical observation made in experiments. Note that this is an assumption that can be verified in each run of the QKD protocol. In principle, one can use the standard formula for the key rate in the collective scenario [Eq. (69)]. However, we introduce a postselection procedure (Silberhorn *et al.*, 2002) to improve the stability of the protocol against imperfections in the error-correction protocol.

To facilitate the introduction of postselection, we add further public announcements to the CV QKD protocol: Alice makes an announcement "a" consistent with the imaginary component α_y and the modulus of the real component $|\alpha_x|$ of the complex amplitude α of her signals. That leaves two possible signals state open. Similarly, Bob makes an announcement "b" which contains again the complex component β_y and the modulus $|\beta_x|$ of the complex measurement result β of her heterodyne measurement. That leaves, again, two possible measurements from Eve's point of view. For any announcement combination (a,b) we have therefore an effective binary channel between Alice and Bob. As the purification of the total state ρ_{AB} is known, we can calculate for each effective binary channel a key rate

$$\Delta I(a,b) = \max\{1 - f(e^{a,b})h[e^{a,b}] - \chi^{a,b}, 0\}. \tag{70}$$

This expression contains the postselection idea in the way that whenever $1 - h[e^{a,b}] - \chi^{a,b}$ is negative, the data are discarded, leading to a zero contribution of the corresponding effective binary channel to the overall key rate. The expressions for $\chi^{a,b}$ have been calculated analytically by Heid and Lütkenhaus (2007), which is possible since the conditional states of Eve, as calculated from the purification of ρ_{AB}, are now at most of rank 4. Several scenarios have been considered there, but the one that is of highest interest is the combination of postselection with reverse reconciliation. The explicit expressions are omitted here, as they do not give additional insight. The evaluation of the overall key rate

$$K = R \int da\, db\, \Delta I(a,b) \tag{71}$$

is then done numerically.

VI. DISTRIBUTED-PHASE-REFERENCE PROTOCOLS

A. Status of security proofs

As discussed in Sec. II.D.4, distributed-phase-reference protocols were invented by experimentalists, looking for practical solutions. Only later was it noticed that these protocols, in addition to be practical, may even yield better rates than the traditional discrete-variable protocols, i.e., rates comparable to those of decoy-state implementations. The reason is that the PNS attacks are no longer zero-error attacks for either DPS (Inoue and Honjo, 2005) for COW (Gisin *et al.*, 2004; Stucki *et al.*, 2005). In fact, the number of photons in a given pulse and the phase coherence between pulses are incompatible physical quantities. Currently no lower bound is known for the unconditional security of DPS or COW, but several restricted attacks have been studied (Curty, Tamaki, and Moroder, 2005; Waks, Takesue, and Yamamoto, 2006; Branciard *et al.*, 2007; Curty *et al.*, 2007; Tsurumaru, 2007; Branciard, Gisin, and Scarani, 2008; Gomez-Sousa and Curty, 2008). In these studies, it has also been noticed that DPS and especially COW can be modified in a way that does not make them more complicated, but may make them more robust (Branciard, Gisin, and Scarani, 2007). Since this point has not been fully developed, we restrict our attention to the original version of these protocols.

B. Bounds for DPS and COW

1. Collective beam-splitting attack

We present the calculation of the simplest zero-error collective attack, namely, the beam-splitting attack (Branciard, Gisin, and Scarani, 2008). For both DPS and COW, Alice prepares a sequence of coherent states $\otimes_k |\alpha(k)\rangle$: each $\alpha(k)$ is chosen in $\{+\alpha, -\alpha\}$ for DPS, in $\{+\alpha, 0\}$ for COW. Eve simulates the losses with a beam splitter, keeps a fraction of the signal, and sends the remaining fraction $\tau = tt_B\eta$ to Bob on a lossless line—note that, although this security study does not provide a lower bound, we work in the uncalibrated-device scenario for the sake of comparison with the other protocols. Bob receives the state $\otimes_k |\alpha(k)\sqrt{\tau}\rangle$: in particular, Bob's optical mode is not modified, i.e., BSA introduces no error.[64] Eve's state is $\otimes_k |\alpha(k)\sqrt{1-\tau}\rangle$; we introduce the notations $\alpha_E = \alpha\sqrt{1-\tau}$ and

$$\gamma = e^{-|\alpha_E|^2} = e^{-\mu(1-\tau)}. \tag{72}$$

When Bob announces a detection involving pulses $k-1$ and k, Eve tries to learn the value of his bit by looking at her systems. Assuming that each bit value is equally probable, Eve's information is given by $I_{\text{Eve}} = S(\rho_E) - \frac{1}{2}S(\rho_{E|0}) - \frac{1}{2}S(\rho_{E|1})$ with $\rho_E = \frac{1}{2}\rho_{E|0} + \frac{1}{2}\rho_{E|1}$.

The information available to Eve differs for the two protocols because of the different coding of the bits. In DPS, the bit is 0 when $\alpha(k-1) = \alpha(k)$ and is 1 when $\alpha(k-1) = -\alpha(k)$. So, writing P_ψ the projector on $|\psi\rangle$, the state of two consecutive pulses reads $\rho_{E|0} = \frac{1}{2}P_{+\alpha_E, +\alpha_E} + \frac{1}{2}P_{-\alpha_E, -\alpha_E}$ and $\rho_{E|1} = \frac{1}{2}P_{+\alpha_E, -\alpha_E} + \frac{1}{2}P_{-\alpha_E, +\alpha_E}$; therefore, noticing that $|\langle +\alpha_E| -\alpha_E\rangle| = \gamma^2$, we obtain

$$I_{E,\text{BS}}^{\text{DPS}}(\mu) = 2h[(1-\gamma^2)/2] - h[(1-\gamma^4)/2], \tag{73}$$

where h is the binary entropy function, and

$$K(\mu) = \nu_S(1 - e^{-\mu tt_B\eta})[1 - I_{E,\text{BS}}^{\text{DPS}}(\mu)]. \tag{74}$$

In COW, the bit is 0 when $\alpha(k-1) = \sqrt{\mu}$, $\alpha(k) = 0$ and is 1 when $\alpha(k-1) = 0$, $\alpha(k) = \sqrt{\mu}$; so, with similar notations as above, $\rho_{E|0} = P_{+\alpha_E, 0}$ and $\rho_{E|1} = P_{0, +\alpha_E}$; therefore, noticing that $|\langle +\alpha_E|0\rangle| = \gamma$, we obtain

$$I_{E,\text{BS}}^{\text{COW}}(\mu) = h[(1-\gamma)/2]. \tag{75}$$

The secret key rate is given by

$$K(\mu) = \tilde{\nu}_S(1 - e^{-\mu tt_B\eta})[1 - I_{E,\text{BS}}^{\text{COW}}(\mu)], \tag{76}$$

where $\tilde{\nu}_S = \nu_S(1-f)/2$, because the fraction f of decoy sequences does not contribute to the raw key, and half of the remaining pulses are empty.

---

[64]Apart from BSA, other attacks exist that do not introduce errors: for instance, photon-number-splitting attacks over the whole key, preserving the coherence (these are hard to parametrize and have never been studied in detail). For COW, there also exist attacks based on unambiguous state discrimination (Branciard *et al.*, 2007).

2. More sophisticated attacks

For the purpose of comparison with other protocols later in this review, it is useful to move away from the strictly zero-error attacks. As mentioned above, several examples of more sophisticated attacks have indeed been found. Instead of looking for the exact optimum among those attacks, we prefer to keep the discussion simple, bearing in mind that all available bounds are to be replaced one day by unconditional security proofs.

We consider attacks in which Eve interacts coherently with pairs of pulses (Branciard, Gisin, and Scarani, 2008). Upper bounds have been provided in the limit $\mu t \ll 1$ of not-too-short distances. Even within this family, a simple formula is available only for COW. For COW, there is no *a priori* relation between the error on the key ε and the visibility V observed on the interferometer. If $e^{-\mu} \leq \xi \equiv 2\sqrt{V(1-V)}$, one finds $I_E^{\text{COW}}(\mu) = 1$: μ is too large and no security is possible. If, on the contrary, $e^{-\mu} > \xi$, the best attack in the family yields

$$I_E^{\text{COW}}(\mu) = \varepsilon + (1-\varepsilon)h\left(\frac{1 + F_V(\mu)}{2}\right) \tag{77}$$

with $F_V(\mu) = (2V-1)e^{-\mu} - \xi\sqrt{1-e^{-2\mu}}$. Therefore

$$K(\mu) = R[1 - I_E^{\text{COW}}(\mu) - \text{leak}_{EC}(Q)], \tag{78}$$

where the value of R is constrained by the definition of the attack to be $\tilde{\nu}_S(\mu tt_B\eta + 2p_d)$.

As for DPS, numerical estimates show that its robustness under the same family of attacks is very similar (slightly better) than that of COW. Therefore, we use Eq. (78) as an estimate of the performances of distributed-phase-reference protocols in the presence of errors; again, for the sake of comparison with the other protocols, we have adopted the uncalibrated-device scenario here.[65]

VII. COMPARISON OF EXPERIMENTAL PLATFORMS

A. Generalities

After having presented the various forms that practical QKD can take, we now try and draw some comparison. If one disposed of unlimited financial means and manpower, then obviously the best platform would be the one that maximizes the secret key rate K for the desired distance. A choice in the real world will obviously put other parameters in the balance, like simplicity, stability, cost, etc. Some partial comparisons are

---

[65]For the family of attacks under study, the rate scales linearly with the losses; therefore the difference between calibrated and uncalibrated devices is due only to the dark counts. We have to warn that the attacks based on unambiguous state discrimination, which have been studied explicitly for calibrated devices (Branciard *et al.*, 2007), are expected to become significantly more critical in the uncalibrated-device scenario. However, this more complex family of attacks can be further restricted by a careful statistical analysis of the data: we can therefore omit it out, which is in any case very partial.

available in the literature; but this is the first systematic attempt to compare the most meaningful platforms at practical QKD. Of course, any attempt at putting all platforms on equal footing contains elements of arbitrariness. Also, we are bounded by the state of the art, concerning both the performance of the devices and the development of the security proofs, as discussed in the previous sections. We have chosen to compare the best available bounds, which, however, do not correspond to the same degree of security: for the implementations of the BB84 coding, we have bounds for unconditional security; for continuous-variable systems, we have security against collective attacks; for the new protocols such as COW and DPS, we have security only against specific families of attacks. Also, one must be reminded that all security proofs hold under some assumptions: these have been discussed in Secs. IV–VI; it is crucial to check if they apply correctly to any given implementation.

As stressed many times, the security of a given QKD realization must be assessed using *measured* values. Here we present some *a priori* estimates: they necessarily involve choices, which have some degree of arbitrariness. The first step is to provide a model for the channel: the one that we give (Sec. VII.A.1) corresponds well to what is observed in all experiments and is therefore rather universally accepted as an *a priori* model. We stress that the actual realization of this specific channel is not a condition for security: Eve might realize a completely different channel, and the general formulas for security apply to any case.[66] Once the model of the channel accepted, one still has to choose the numerical values for all the parameters.

1. Model for the source and channel

We assume that the detection rates are those that are expected in the absence of Eve, given the source and the distance between Alice and Bob. As for the error rates, we consider a depolarizing channel with visibility V. For an *a priori* choice, the modeling of the channel just sketched is rather universally accepted. In detail, it gives the following.

(a) *Discrete-variable protocols, P&M.* We consider implementations of the BB84 coding. The rate is estimated by $R = \tilde{\nu}_S(\mathcal{P} + \mathcal{P}_d)$, with $\mathcal{P} = \Sigma_{n \geq 1} p_A(n)[1 - (1 - tt_B \eta)^n]$ and $\mathcal{P}_d = 2p_d \Sigma_{n \geq 0} p_A(n)(1 - tt_B \eta)^n$. The error rate in the channel is $\varepsilon = (1 - V)/2$, so the expected error rate is $Q = (\varepsilon \mathcal{P} + \mathcal{P}_d/2)/(R/\tilde{\nu}_S)$. For weak coherent pulses without decoy states, $p_A(1)$

$= e^{-\mu}\mu$, $p_A(n \geq 2) = 1 - e^{-\mu}(1 + \mu)$, and we optimize K, given by Eq. (31), over μ. For weak coherent pulses with decoy states, we consider an implementation in which one value of μ is used almost always, while sufficiently many others are used, so that all the parameters are exactly evaluated. The statistics of the source are as above; Y_0 is estimated by $\tilde{\nu}_S 2p_d p_A(0)/R$, Y_1 by $\tilde{\nu}_S p_A(1)tt_B \eta/R$, and we optimize K given by Eq. (34) over μ. For perfect single-photon sources, $p_A(1) = 1$ and $p_A(n \geq 2) = 0$; we compute Eq. (31), as there is nothing to optimize.

(b) *Discrete-variable protocols, EB.* Again, we consider implementations of the BB84 coding. Since most of the experiments have been performed using cw-pumped sources, we restrict consideration to this case.[67] For such sources, the probability of having multiple pairs is $\zeta = 0$ with good precision; therefore the bounds (42) and (43) for K are identical. K will be optimized over μ', the mean pair-generation rate of the source. Note that ν_S^{cw} given by Eq. (20) depends on μ'; given this, one has $p_A(1) \approx 1$ and $p_A(2) \approx \mu' \Delta t$ if $\mu' \Delta t \ll 1$: indeed, neglecting dark counts, whenever any of Alice's detectors fires there is at least one photon going to Bob; and the probability that another pair appears during the coincidence window Δt is approximately $\mu' \Delta t$. The total expected error is $Q = [(\varepsilon + \varepsilon')\mathcal{P} + \mathcal{P}_d/2]/(R/\tilde{\nu}_S)$, where $\varepsilon = (1 - V)/2$ as above and $\varepsilon' \approx \mu' \Delta t/2$ is the error rate due to double-pair events.

(c) *Continuous-variable protocols.* We consider the protocol that uses coherent states with Gaussian modulation, and compute the best available bound [Eq. (69)], which give security against collective attacks. The reference beam is supposed to be so intense that there is always a signal arriving at the homodyne detector, so $R = \tilde{\nu}_S$. The error is modeled by Eq. (58). Now, just as for discrete-variable protocols one can optimize K over the mean number of photons (or of pairs) μ for each distance, here one can optimize K over the variance v of the modulation. Note that this optimization outputs rather demanding values so that only recently has it become possible to implement them in practice, thanks to the latest developments in error-correction codes (Leverrier, Alleaume, *et al.*, 2008).

---

[66]The attacks we studied against DPS and COW (Sec. VI), do suppose a model of the channel. This is a signature of the incompleteness of such studies. Security can be guaranteed by adding that, if the channel deviates from the expected one, the protocol is aborted. A full assessment of the channel requires additional tests: the fact that data can be reproduced by a channel model does not imply that the channel model is correct (for instance, in weak-coherent-pulse implementations of BB84 without decoy states, the observed parameters are compatible with both a BS and a PNS attack).

[67]Pulsed sources can be treated in a similar way. For short-pulse schemes, one would have $p_A(1) \approx \mu$ and $p_A(2) \approx 3\mu^2/4$ if $\mu \ll 1$; for long-pulse pumping, the statistics of pairs is approximately Poissonian, $p_A(1) \approx \mu$ and $p_A(2) \approx \mu^2/2$ if $\mu \ll 1$, and most of the multipair events are uncorrelated. In both cases, the intrinsic error rate due to double-pair events is $\varepsilon' \approx \mu/2$ (Eisenberg *et al.*, 2004; Scarani *et al.*, 2005). Note that the parameter ζ may be different from 0 in the case of short-pulse schemes.

TABLE II. Parameters used for the *a priori* plots. See text for notations and comments. The entry (opt.) means that the parameter will be varied as a function of the distance in order to optimize K.

Platform	Parameter	Set 1	Set 2
BB84, COW	μ (mean intensity)	(Opt.)	(Opt.)
	V (visibility): P&M	0.99	0.99
	V (visibility): EB	0.96	0.99
	t_B (transmission in Bob's device)	1	1
	η (detector efficiency)	0.1	0.2
	p_d (dark counts)	10^{-5}	10^{-6}
	ε (COW) (bit error)	0.03	0.01
	ζ (EB) (coherent four photons)	0	0
	Leak (EC code)	1.2	1
CV	$v = v_A + 1$ (variance)	(Opt.)	(Opt.)
	ε (optical noise)	0.005	0.001
	η (detector efficiency)	0.6	0.85
	v_{el} (electronic noise)	0.01	0
	β (EC code)	0.9	0.9

(d) *Distributed-phase-reference protocols.* As mentioned, apart from the errorless case, a simple formula exists only for COW, which moreover is valid only at not-too-short distances. We use this bound to represent distributed-phase-reference protocols in this comparison, keeping in mind that DPS performs slightly better, but that in any case only upper bounds are available. Specifically, we have $R \approx \tilde{\nu}_S(\mu t t_B \eta + 2 p_d)$; we optimize then $K(\mu)$ given by Eq. (78) over μ, and keep the value only if $\mu_{\text{opt}} t \leq 0.1$. The expected error rate is formally the same as for the P&M BB84 protocol; recall, however, that here the bit error ε is not related to the visibility of the channel and must be chosen independently.

2. Choice of the parameters

We use two sets of parameters (Table II): set 1 corresponds to today's state of the art, while set 2 reflects a more optimistic but not unrealistic development. Moreover, we make the following choices:

- Unless specified otherwise (see Sec. VII.B.2), the plots use the formulas for the uncalibrated-device scenario. The reason for this choice is the same as discussed in Sec. III.B.5: unconditional security has been proved only in this overly-pessimistic scenario.

- Since we are using formulas that are valid only in the asymptotic regime of infinitely long keys, we remove the nuisance of sifting by allowing an asymmetric choice of bases or of quadratures. Specifically, this leads to $\tilde{\nu}_S = \nu_S$ for both BB84 and continuous-variable protocols. Similarly, for COW we can set $f = 0$, whence $\tilde{\nu}_S = \nu_S/2$.
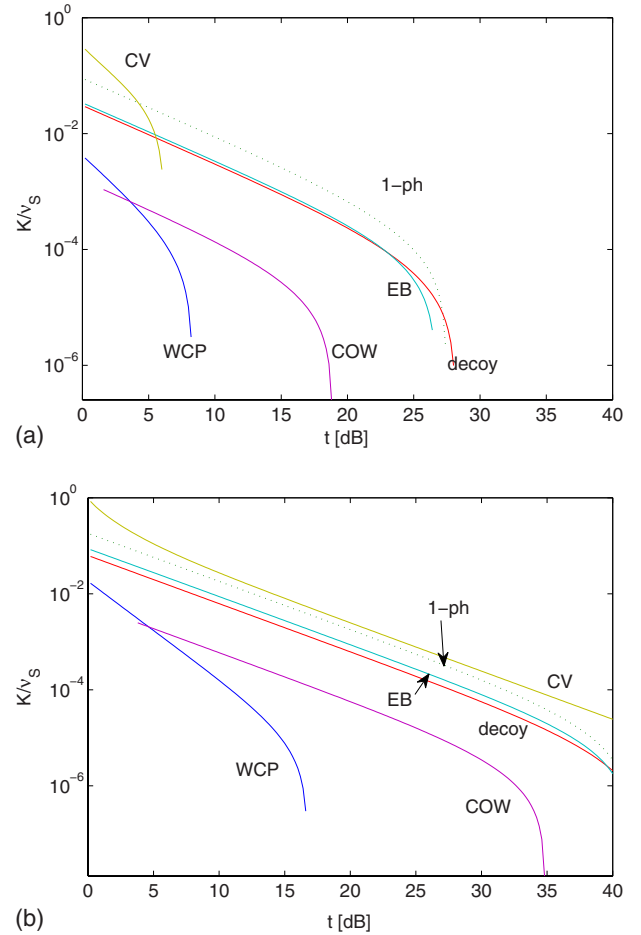

FIG. 4. (Color online) K/ν_S as a function of the transmittivity t, for all the platforms. Legend: 1-ph, perfect single-photon source, unconditional; WCP, weak coherent pulses without decoy states, unconditional; decoy, weak coherent pulses with decoy states, unconditional; EB, entanglement-based, unconditional; CV, continuous variables with Gaussian modulation, security against collective attacks; COW, coherent one way, security against the restricted family of attacks described in Sec. VI.B.2. Parameters from Table II: set 1, upper graph; set 2, lower graph.

- For definiteness, we consider fiber-based implementations; in particular, the relation between distance and transmission will be Eq. (17) with $\alpha = 0.2$ *d*B/km; and the parameters for photon counters are given at telecom wavelengths (Table II). The reader must keep in mind that, in free-space implementations, where one can work with other frequencies, the rates and the achievable distance may be larger.

B. Comparisons based on K

1. All platforms on a plot

As a first case study, we compare all platforms on the same basis by plotting K/ν_S as a function of the transmittivity t of the channel. The result is shown in Fig. 4. We stress the elements of arbitrariness in this compari-
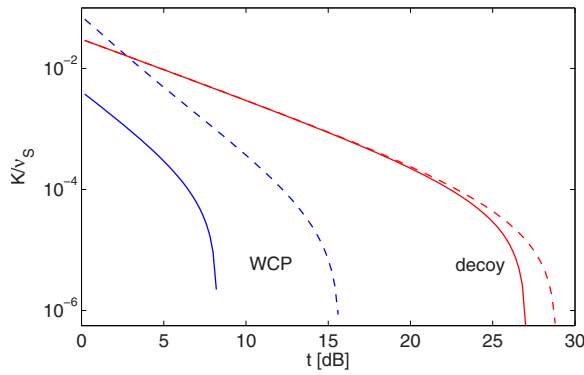
FIG. 5. (Color online) K/ν_S as a function of the transmission t for the P&M implementations of BB84 with weak coherent pulses: comparison between the lower bound (solid lines, same as in Fig. 4, upper graph) and the upper bound for calibrated devices (dashed lines). Legend as in Fig. 4. Parameters from Table II, set 1.
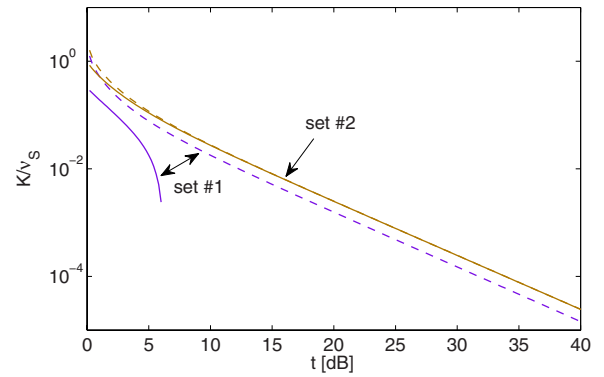

FIG. 6. (Color online) K/ν_S as a function of the transmission t for CV QKD with Gaussian modulation and security against collective attacks: comparison between the lower bound (solid lines, same as in Fig. 4) and the upper bound for calibrated devices (dashed lines) for both sets of parameters from Table II. Compared to Fig. 4, the color of the lines of set 1 was changed for clarity.

son (in addition to the choices discussed above). First, we recall that the curves do not correspond to the same degree of security (see Sec. VII.A). Second, we have considered "steady-state" key rates, because we have neglected the time needed for the classical postprocessing; this supposes that the setup is stable enough to run in that regime (and it is fair to say that many of the existing platforms have not reached this stage of stability yet). Third, the *real* performance is of course K: in particular, if some implementations have bottlenecks at the level of ν_S (see Sec. III.A), the order of the curves may change significantly.

2. Upper bound incorporating the calibration of the devices

As a second case study, we show the difference between the lower bounds derived in the uncalibrated-device scenario and some upper bounds that incorporate the calibration of the devices.

We focus first on BB84 implemented with weak coherent pulses; the upper bounds under study have been derived in Sec. IV.C. The plots in Fig. 5 show how much one can hope to improve the unconditional security bounds from their present status. As expected, the plot confirms that basically no improvement is expected for implementations with decoy states, because there only the treatment of dark counts is different; while the bound for implementations without decoy states may still be the object of significant improvement.

We turn now to CV QKD with Gaussian modulation. Bounds for the security against collective attacks assuming calibrated devices are given in Eqs. (5)–(12) of Lodewyck, Bloch, *et al.* (2007). The plots are shown in Fig. 6. One sees that the difference between the two scenarios is significant for set 1 of parameters, but is negligible for the more optimistic set 2. This is interesting, given that the efficiency η of the detectors is "only" 85% in set 2.

C. Comparison based on the "cost of a linear network"

We consider a linear chain of QKD devices, aimed at achieving a secret key rate K_{target} over a distance L. Many devices can be put in parallel, and trusted repeater stations are built at the connecting points. Each individual QKD device is characterized by the point-to-point rate $K(\ell)$ it can achieve as a function of the distance ℓ, and by its cost C_1. We need $N = (L/\ell)K_{target}/K(\ell)$ devices to achieve the goal, so the cost of the network is[68]

$$C_{tot}[\ell] = C_1 \frac{L}{\ell} \frac{K_{target}}{K(\ell)}. \tag{79}$$

The best platform is the one that minimizes this cost, i.e., the one that maximizes $F(\ell) = \ell K(\ell)$. This quantity, normalized to ν_S, is plotted in Fig. 7 as a function of the distance for both sets of parameters defined in Table II. Of course, this comparison presents the same elements of arbitrariness as the previous one.

The optimal distances are quite short, and this can be understood from a simple analytical argument. Indeed, typical behaviors are $K(\ell) \propto t$ (single-photon sources, attenuated lasers with decoy states, and strong reference pulses) and $K(\ell) \propto t^2$ (weak coherent pulses without decoy states). Using $t = 10^{-\alpha \ell/10}$, it is easy to find ℓ_{opt} that maximizes $F(\ell)$,

$$K(\ell) \propto t^k \rightarrow \ell_{opt} = 10/k\alpha \ln 10. \tag{80}$$

In particular, for $\alpha \approx 0.2$ dB/km, one has $\ell_{opt} \approx 20$ km for $k = 1$ and $\ell_{opt} \approx 10$ km for $k = 2$.

In conclusion, our toy model suggests that, in a network environment, one might not be interested in pushing the maximal separation of the devices; in particular,

---

[68]In this first toy model, we neglect the cost of the trusted repeater stations; see Alléaume *et al.* (2008) for a more elaborated model.
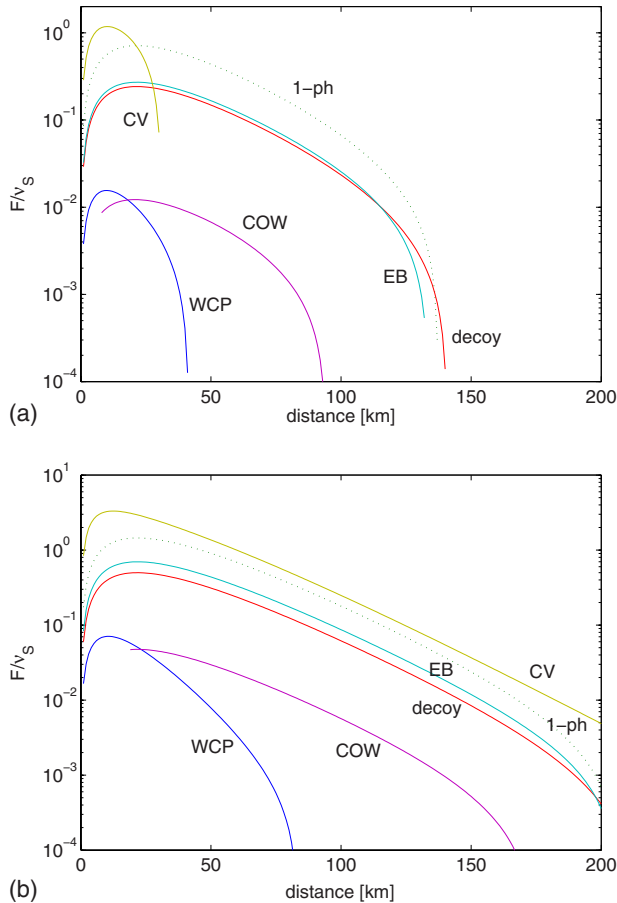
FIG. 7. (Color online) F/ν_S as a function of the distance ℓ for all platforms. Legend as in Fig. 4. Parameters from Table II: set 1, upper graph; set 2, lower graph.

detector saturation (which we neglected in the plots above) may become the dominant problem instead of dark counts.

VIII. PERSPECTIVES

A. Perspectives within QKD

1. Finite-key analysis

As we have stressed, all the security bounds presented in this review are valid only in the asymptotic limit of infinitely long keys. Proofs of security for finite-length keys are a crucial tool for practical QKD. The estimate of finite-key effects, unfortunately, has received very limited attention so far. The pioneering works (Mayers, 1996; Inamori, Lütkenhaus and Mayers, 2007); as well as some subsequent ones (Watanabe *et al.*, 2004; Hayashi, 2006), have used noncomposable definitions of security (see Sec. II.C.2). This is a problem because the security of a finite key is never perfect, so one needs to know how it composes with other tasks. Others studied a new formalism but failed to prove unconditional security (Meyer *et al.*, 2006). The most recent works comply with the requirements (Hayashi, 2007a; Scarani and Renner, 2008); finite statistics have been incorporated in the

analysis of an experiment (Hasegawa *et al.*, 2007). Without going into details, all these works estimate that no key can be extracted if fewer than $N \approx 10^5$ signals are exchanged.

2. Open issues in unconditional security

As stated above that, for CV QKD and distributed-phase-reference protocols, no unconditional security proof is available yet. However, there is an important difference between these cases. In the existing CV QKD protocols, the information is coded in independent signals; because of this, it is believed that unconditional security proofs can be built as generalizations of the existing ones (see also the "Note added" below). On the contrary, the impossibility of identifying signals with qubits in distributed-phase reference protocols will require a completely different approach, which nobody has been currently able to devise.

As explained in Sec. III.B.5, all unconditional security proofs have been derived under the overconservative assumption of uncalibrated devices. Ideally, such an assumption should be removed: one should work out unconditional security proofs taking into account the knowledge about the detectors; this would lead to better rates. A possible solution is to include the calibration of the devices in the protocol itself; the price to pay seems to be a complication of the setup (Qi, Zhao, *et al.*, 2007). The idea is somewhat similar to the one used in decoy states. We also discussed how calibrated-device proofs may ultimately provide significant improvement only for some protocols (see Sec. VII.B.2). The difference between protocols can be understood from the fact that typically $K \sim t^\alpha$, where t is the transmittance and $\alpha \geq 1$. When $\alpha = 1$, the only advantage of calibrating the devices can come from the dark count contribution. If, on the contrary, $\alpha > 1$ (weak coherent pulses without decoy states: $\alpha = 2$ for BB84, $\alpha = 3/2$ for SARG04), then the difference is much larger because it matters whether or not $t_B \eta$ is included in the losses. The urgency of this rather ungrateful[69] task is therefore relative to the choice of a protocol.

---

[69]Here is an example of the complications that might appear. When taking the calibration into account, it is often assumed that the dark counts do not enter in Eve's information. Actually, things are more subtle. On the one hand, most of the dark counts will actually *decrease* Eve's information, because she does not know if a detection is due to the physical signal (about which she has gained some information) or is a completely random event. On the other hand, if a detection happens shortly after a previous one, Eve may guess that the second event is in fact a dark count triggered by an afterpulse, and therefore learn about some correlations between the two results. Admittedly, these are fine-tuning corrections, and have never been fully discussed in the literature; but if one wants to prove unconditional security, these marginal issues must be also properly addressed.

3. Black-box security proofs

The development of commercial QKD systems makes it natural to ask whether the "quantumness" of such devices can be proved in a black-box approach. Of course, the compulsory requirements (Sec. II.C.1) must hold. For instance, the random number generator cannot be within the black box because it must be trusted; one must also make sure that no output port is diffusing the keys on the internet; and so on. Remarkably though, all the quantum part can in principle be kept in a black box. The idea is basically the one that triggered Ekert's discovery (Ekert, 1991), although Ekert himself did not push it so far: the fact that Alice and Bob observe correlations that violate a Bell inequality is enough to guarantee entanglement, independent of the nature of the quantum signals and even of the measurements that are performed on them. This has been called "device-independent security"; a quantitative bound was computed for collective attacks on a modification of Ekert's protocol, but the goal of proving unconditional security is still unattained (Acín *et al.*, 2007). Device-independent security can be proved only for entanglement-based schemes: for this definition of security, the equivalence of EB and P&M presented in Sec. II.B.2 does not hold. As long as the detection loophole is open, these security proofs cannot be applied to any system; but if some knowledge of the devices is reintroduced, they might provide a good tool for disposing of all quantum side channels (Sec. III.B.4).

4. Toward longer distances: Satellites and repeaters

The attempt to achieve efficient QKD over long distances is triggering ambitious experimental developments. Basically, two solutions are being envisaged. The first is to use the techniques of free space quantum communication to realize ground-to-satellite links (Buttler *et al.*, 1998; Rarity *et al.*, 2002; Aspelmeyer *et al.*, 2003). The main challenges are technical: to adapt the existing optical tracking techniques to the needs of quantum communication, and to build devices that can operate in a satellite without need of maintenance.

The second solution is to use quantum repeaters (Briegel *et al.*, 1998; Dür *et al.*, 1999). The basic idea is the following: the link A-B is cut in segments A-C_1, C_1-$C_2, \ldots, C_n$-B. On each segment independently, the two partners exchange pairs of entangled photons, which may of course be lost; but whenever both partners receive the photon, they store it in a quantum memory. As soon as there is an entangled pair on each link, the intermediate stations perform a Bell measurement, thus ultimately swapping all the entanglement into A-B. Actually, variations of this basic scheme may be more practical (Duan *et al.*, 2001). Whatever the exact implementation, the advantage is clear: one does not have to ensure that all the links are active simultaneously; but the advantage can be achieved only if quantum memories are available. The experimental research in quantum memories has increased over recent years, but applications in practical QKD are still far away because the requirements are challenging (see Appendix B).

Teleportation-based links have also been studied in the absence of quantum memories (quantum relays). They are rather inefficient, but allow reduction of the nuisance of the dark counts and therefore increase the limiting distance (Jacobs, Pittman, and Franson, 2002; Collins, Gisin, and de Riedmatten, 2005); however, it seems simpler and more cost effective to solve the same problem using cryogenic detectors (see Sec. II.G).

5. QKD in networks

QKD is a point-to-point link between two users. But only a tiny fraction of all communication occurs in dedicated point-to-point links; most communication takes place in networks, where many users are interconnected. Note that one-to-many connectivity between QKD devices can be obtained with optical switching (Townsend *et al.*, 1994; Elliott, 2002; Elliott *et al.*, 2005).

In all models of QKD networks, the nodes are operated by authorized partners, while Eve can eavesdrop on all links. If the network is built with quantum repeaters or quantum relays, no secret information is available to the nodes: indeed, the role of these nodes is to perform entanglement swapping so that Alice and Bob end up with a maximally entangled—and therefore fully private—state. Since production of quantum repeaters is still a challenge, trusted-relays QKD networks have been considered. In this case, the nodes learn secret information during the protocol. In the simplest model, a QKD key is created between two consecutive nodes and a message is encrypted and decrypted hop by hop. This model has been adopted by BBN Technologies and by the SECOQC QKD networks (Elliott, 2002; Elliott *et al.*, 2005; Dianati and Alléaume, 2006; Alléaume *et al.*, 2007; Dianati *et al.*, 2008). Alternatively, the trusted relays can perform an intercept-resend chain at the level of the quantum signal (Bechmann-Pasquinucci and Pasquinucci, 2005).

B. QKD versus other solutions

Information-theoretically (unconditionally) secure key distribution (key agreement) is a cryptographic task that, as is well known, cannot be solved by public communication alone, i.e. without employing additional resources or relying on additional assumptions. In addition to QKD (the additional resource in this case being the quantum channel), a number of alternative schemes to this end have been put forward (Wyner, 1975; Csiszár and Körner, 1978; Ahlswede and Csiszár, 1993; Maurer, 1993), among which one can also count the traditional trusted-courier approach (Alléaume *et al.*, 2007). While the latter is still used in certain high-security environments, QKD is the sole automatic, practically feasible, and efficient information-theoretically secure key agreement technology, where in the point-to-point setting limitations of distance and related key rate apply. These limitations can be lifted using QKD networks (see Sec. VIII.A.1).

With this in mind, we address below typical secure communication solutions in order to relate then subsequently to the assets offered by QKD. Secure communication in general requires encrypted (and authentic) transition of communication data. In current standard cryptographic practice, neither the encryption schemes nor the key agreement protocols used (whenever needed) are unconditionally secure. While there is really a very broad range of possible alternatives and combinations, the most typical pattern for confidential communication is the following: public key exchange protocols are used to ensure agreement of two identical keys; the encryption itself is done using symmetric-key algorithms. In particular, most often some realization of the Diffie-Hellman algorithm (Diffie and Hellman, 1976) is used in the key agreement phase. The symmetric-encryption algorithms most widely used today belong to the block-cipher class and are typically Triple Data Encryption Standard (3DES) (Coppersmith *et al.*, 1996) or Advanced Encryption Standard (AES) (Daemen and Rijmen, 2001).

The security of the Diffie-Hellman algorithm is based on the assumption that the so-called Diffie-Hellman problem is hard to solve, the complexity of this problem being ultimately related to the hardness of the discrete-logarithm problem [see Maurer and Wolf (1999, 2000) for a detailed discussion]. It is widely believed, although it was never proven, that the discrete-logarithm problem is classically hard to solve. This is not true in the quantum case since a quantum computer, if available, can execute a corresponding efficient algorithm by Peter Shor (Shor, 1994, 1997), which is based on the same fundamental approach as is the Shor factoring algorithm, already mentioned in Sec. I.A.

It should be further noted that, similarly to QKD, the Diffie-Hellman protocol can trivially be broken if the authenticity of the communication channel is not ensured. There are many means to guarantee communication authenticity with different degrees of security but in any case additional resources are needed. In current common practice, public-key infrastructures are employed, which in turn rely on public-key cryptographic primitives (digital signatures), i.e., on similar assumptions as for the Diffie-Hellman protocol itself, and on trust in external certifying entities.

Turning now to encryption, it should be highlighted that the security of a block-cipher algorithm is based on the assumption that it has no structural weaknesses, i.e., that only a brute force attack amounting to a thorough search of the key space (utilizing pairs of cipher texts and corresponding known or even chosen plain texts) can actually reveal the secret key. The cost of such an attack on a classical computer is $O(N)$ operations, where N is the dimension of the key space. The speedup of a quantum computer in this case is moderate, the total number of operations to be performed being $O(\sqrt{N})$ (Grover, 1996, 1997). The assumption of the lack of structural weaknesses itself is not related to any particular class of mathematical problems and in the end relies merely on the fact that such a weakness is not

(yet) known. Cryptographic practice suggests that for a block-cipher algorithm such weaknesses are in fact discovered at the latest a few decades after its introduction.[70]

Before turning to a direct comparison of the described class of secure communication schemes with QKD-based solutions, it should be explained why public-key-based generation combined with symmetric-key encryption is actually the most proliferated solution. The reason is that currently AES or 3DES encryption, in contrast to direct public-key (asymmetric) encryption, can ensure a high encryption speed and appears optimal in this respect. Typically high speed is achieved by designing dedicated hardware devices, which can perform encryption at very high rate and ensure a secure throughput of up to 10 Gb per second. Such devices are offered by an increasing number of producers (see, e.g., ATMedia GmbH, www.atmedia.de) and it is beyond the scope of the current article to address them in any detail. We, however, underline an important side aspect. In general, security of encryption in the described scenario is increased by changing the key "often," the rate of change being proportional to the dimension of the key space. In practice, however, even in the high-speed case the key is changed at a rate lower than once per minute (often once per day or even more seldom). The reason for this is twofold: on the one hand, public-key-agreement algorithms are generally slow and, on the other hand, the current design of dedicated encryption devices is not compatible with a rapid key change.

The question now is how QKD compares with the standard practice as outlined above. It is often argued that QKD is too slow for practical uses and that the limited distance due to the losses is a limitation to the system as such. In order to allow for a correct comparison one has to define the relevant secure communication scenarios. There are two basic possibilities: (i) QKD is used in conjunction with one-time pad or (ii) QKD is used together with some high-speed encryptor (we note in passing that the second scenario appears to be the main target for the few QKD producers).

The rate as a function of distance has been discussed in detail in the preceding sections. Here we consider an "average" modern QKD device operating in the range of 1–10 kilobytes per second (kbps) over 25 km; the maximal distance of operation at above 100 bps being around 100 km.

Case (i) obviously offers information-theoretic security of communication if the classical channel, in both the key generation and the encryption phases, is additionally authenticated with the same degree of security. As the overhead for this is negligible, the QKD generation rates as presented above are also the rates for secure communication. Obviously this is not sufficient for broadband data transmission but quite adequate for communicating very highly sensitive data. Another ad-

---

[70]See Rijmen (2007).

vantage of this combination is the fact that keys can be stored for later use.

The security of the case (ii) is equivalent to the security of the high-speed encryption, which we addressed above, while all threats related to the key generation phase are eliminated. At 25 km the QKD speed would allow key refreshment (e.g., in the case of AES with 256 bit key length) several times per second. This is remarkable for two reasons: first, this is at or rather beyond the key-exchange capacity of current high-speed encryptors; second, it compares also to the performance of high-level classical link encryptors, which refresh AES keys a few times per second using Diffie-Hellman elliptic curve cryptography for key generation. So in the second scenario QKD outperforms the standard solution at 25 km distance in terms of both speed and security.

Regarding the distance, an interesting point is that classical high-end encryptors use direct dark fibers, not for reasons related to security but to achieve maximal speed, which also gives them a limitation in distance. However, classical key generation performed in software is naturally not bounded by the distance. In this sense standard public-key-based key agreement appears superior. This is, however, a QKD limitation typical for the point-to-point regime. As mentioned above, it is lifted in QKD networks.

Note added in proof. One of the pending issues toward unconditional security proofs of CV QKD, namely, the fact that the security bound for collective and general attacks should coincide asymptotically, has been solved (Renner and Cirac, 2009). The solution makes use of a exponential De Finetti–type theorem. Another approach, which would reach the same conclusion based only on the symmetries of the protocol, is being pursued (Leverrier, Karpov, Grangier, and Cerf, 2008).

APPENDIX A: UNCONDITIONAL SECURITY BOUNDS FOR BB84 AND SIX-STATE SINGLE-QUBIT SIGNALS

In this appendix, we present a derivation of the unconditional security bounds for the BB84 (Shor and Preskill, 2000) and six-state protocols (Lo, 2001) for the case where each quantum signal is a single qubit, or more generally when the quantum channel is a qubit channel followed by a qubit detection.[71]

As usual, the proof is done in the EB scheme, the application to the P&M case following immediately as discussed in Sec. II.B.2. Alice produces the state $|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$; she keeps the first qubit and sends the other one to Bob. This state is such that $\langle \sigma_z \otimes \sigma_z \rangle = \langle \sigma_x \otimes \sigma_x \rangle = +1$ (perfectly correlated outcomes) and $\langle \sigma_y \otimes \sigma_y \rangle = -1$ (perfectly anticorrelated outcomes); to have perfect correlation in all three bases, Bob flips his result when he measures σ_y. We suppose an asymmetric implementation of the protocols: the key is extracted only from the measurements in the Z basis, which is used almost always; the other measurements are used to estimate Eve's knowledge of the Z basis, and will be used on a negligible sample (recall that we work in the asymptotic regime of infinitely long keys).

Now we follow the techniques of Kraus, Gisin, and Renner (2005) and Renner, Gisin, and Kraus (2005). Without loss of generality, the symmetries of the BB84 and six-state protocols[72] imply that one can compute the bound by restricting consideration to collective attacks, and, even further, to those collective attacks such that the final state of Alice and Bob is Bell diagonal,

$$\rho_{AB} = \lambda_1 |\Phi^+\rangle\langle\Phi^+| + \lambda_2 |\Phi^-\rangle\langle\Phi^-| + \lambda_3 |\Psi^+\rangle\langle\Psi^+| + \lambda_4 |\Psi^-\rangle\langle\Psi^-|, \tag{A1}$$

with $\Sigma_i \lambda_i = 1$. Since $|\Phi^\pm\rangle$ give perfect correlations in the Z basis, while $|\Psi^\pm\rangle$ give perfect anticorrelations, the QBER ε_z is given by

$$\varepsilon_z = \lambda_3 + \lambda_4. \tag{A2}$$

The error rates in the other bases are

$$\varepsilon_x = \lambda_2 + \lambda_4, \quad \varepsilon_y = \lambda_2 + \lambda_3. \tag{A3}$$

Eve's information is given by the Holevo bound (24) $I_E = S(\rho_E) - \frac{1}{2}S(\rho_{E|0}) - \frac{1}{2}S(\rho_{E|1})$ since both values of the bit are equiprobable in this attack. Since Eve has a purification of ρ_{AB}, $S(\rho_E) = S(\rho_{AB}) = H(\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}) \equiv H(\underline{\lambda})$ where H is Shannon entropy. The computation of $\rho_{E|b}$ is made in two steps. First, one writes down explicitly the

---

[71]For real optical channels, we therefore assume the tagging method for real sources and the squashing model for the detection; see Sec. IV.A.2.

[72]Actually, a lower bound can be computed in the same way for a very general class of protocols; but it may not be tight, as explicitly found in the case of SARG04 (Branciard *et al.*, 2005; Kraus, Branciard, and Renner, 2007).

purification[73] $|\Psi\rangle_{ABE} = \Sigma_i \sqrt{\lambda_i}|\Phi_i\rangle_{AB}|e_i\rangle_E$, where we used a change of notation for the Bell states, and where $\langle e_i|e_j\rangle = \delta_{ij}$. Then, one traces out Bob and projects Alice on $|+z\rangle$ for $b=0$ and on $|-z\rangle$ for $b=1$. All calculations done, the result is $S(\rho_{E|0}) = S(\rho_{E|1}) = h(\varepsilon_z)$. So we have obtained

$$I_E(\underline{\lambda}) = H(\underline{\lambda}) - h(\varepsilon_z). \tag{A4}$$

Now we have to particularize to the two protocols under study.

We start with the six-state protocol. In this case, both ε_x and ε_y are measured, so all four λ's are directly determined. After some algebra, one finds

$$I_E(\underline{\varepsilon}) = \varepsilon_z h\left(\frac{1 + (\varepsilon_x - \varepsilon_y)/\varepsilon_z}{2}\right)$$
$$+ (1 - \varepsilon_z)h\left(\frac{1 - (\varepsilon_x + \varepsilon_y + \varepsilon_z)/2}{1 - \varepsilon_z}\right). \tag{A5}$$

Under the usual assumption of a depolarizing channel, $\varepsilon_x = \varepsilon_y = \varepsilon_z = Q$, this becomes

$$I_E(Q) = Q + (1-Q)h\left(\frac{1 - 3Q/2}{1-Q}\right). \tag{A6}$$

The corresponding secret fraction (one-way postprocessing, no preprocessing, and perfect error correction) is $r = 1 - h(Q) - I_E(Q)$, which goes to 0 for $Q \approx 12.61\%$.

The calculation is slightly more complicated for the BB84 protocol because there only ε_x is measured; therefore, there is still a free parameter, which must be chosen so as to maximize Eve's information. The simplest way of performing this calculation consists in writing $\lambda_1 = (1-\varepsilon_z)(1-u)$, $\lambda_2 = (1-\varepsilon_z)u$, $\lambda_3 = \varepsilon_z(1-v)$, and $\lambda_4 = \varepsilon_z v$, where $u, v \in [0,1]$ are subject to the additional constraint

$$(1-\varepsilon_z)u + \varepsilon_z v = \varepsilon_x. \tag{A7}$$

Under this parametrization, $H(\underline{\lambda}) = h(\varepsilon_z) + (1-\varepsilon_z)h(u) + \varepsilon_z h(v)$ and consequently

$$I_E(\underline{\lambda}) = (1-\varepsilon_z)h(u) + \varepsilon_z h(v), \tag{A8}$$

to be maximized under the constraint (A7). This can be done by inserting $v = v(u)$ and taking the derivative with respect to u. The result is that the optimal choice is $u = v = \varepsilon_x$ so that

$$I_E(\underline{\varepsilon}) = h(\varepsilon_x). \tag{A9}$$

The usual case is $\varepsilon_x = \varepsilon_z = Q$, which, however, here does not correspond to the depolarizing channel: the relations above imply $\varepsilon_y = 2Q(1-Q)$, which corresponds to the application of the so-called "phase-covariant cloning machine" (Griffiths and Niu, 1997; Bruß *et al.*, 2000). The corresponding secret fraction (again for one-way postprocessing, no preprocessing, and perfect error correc-

---

---

[73]All purifications are equivalent under a local unitary operation on Eve's system, so Eve's information does not change with the choice of the purification.
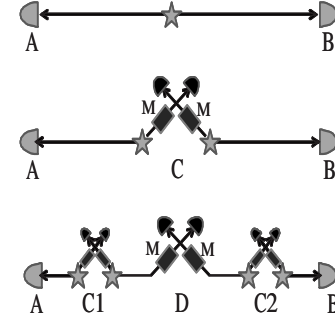

FIG. 8. Three configurations for quantum repeaters: direct link, two-link repeater, and four-link repeater.

tion) is $r = 1 - h(Q) - I_E(Q)$, which goes to 0 for $Q \approx 11\%$.

APPENDIX B: ELEMENTARY ESTIMATES FOR QUANTUM REPEATERS

1. Quantum memories

A quantum memory is a device that can store an incoming quantum state (typically, of light) and reemit it on demand without loss of coherence. A full review of the research in quantum memories is clearly beyond our scope. Experiments are being pursued using several techniques, such as atomic ensembles (Julsgaard *et al.*, 2004; Chou *et al.*, 2007), NV centers (Childress *et al.*, 2006), and doped crystals (Alexander *et al.*, 2006; Staudt *et al.*, 2007).

Two characteristics of quantum memories are especially relevant for quantum repeaters. A memory is called multimode if it can store several light modes and one can select which mode to reemit; multimode memories are being realized (Simon *et al.*, 2007). A memory is called heralded if its status (loaded or not loaded) can be learned without perturbation; there is no current proposal on how to realize such a memory, and repeater schemes have been found that work without heralded memories (Duan *et al.*, 2001).

2. Model of quantum repeater

Here we present a comparison of the direct link with the two-link repeater and discuss the advantages and problems that arise in more complex repeaters. We consider the architecture sketched in Fig. 8, corresponding to the original idea (Briegel *et al.*, 1998).

a. Definition of the model

Our elementary model is described as follows:

- Source: Perfect two-photon source with repetition rate ν_S.

- Quantum channel: The total distance between Alice and Bob is ℓ. The channel is noiseless; its losses are characterized by α, and we denote by $t = 10^{-\alpha\ell/10}$ the total transmittivity.

- Detectors of Alice and Bob: Efficiency η; dark counts, dead time, and other nuisances are neglected.

- Quantum memories: Multimode memories that can store N modes. We write as p_M the probability that a photon is absorbed and then reemitted on demand (contains all the losses due to coupling with other elements). The memory has a typical time T_M, which we consider as a lifetime.[74]

- Bell measurement: Linear optics, i.e., the probability of success is $\frac{1}{2}$. The fidelity is F and the noise is depolarized [i.e., a detection comes from the desired Bell state with probability F; from any of the others with equal probability $(1-F)/3$]. The detectors have efficiency η_M and no dark counts.

b. Detection rates

For the direct link, the key rate is the detection rate in our simplified model,

$$K_1 = R_1 = \nu_S t \eta^2. \tag{B1}$$

In the two-link repeater, the central station (Christoph) holds the two sources and the memories. Consider one of the links, say with Alice. The source produces groups of N pairs, each pair in a different mode; one photon per pair is kept in the memory, the other is sent to Alice. Alice announces whether she has detected at least one photon: if she has, Christoph notes which one; if she has not, Christoph releases the memory and starts the protocol again. The same is happening on the other link, the one with Bob, independently. As soon as both partners have announced a detection, Christoph releases the corresponding photons, performs the Bell measurement and communicates the result to Alice and Bob, who postselect their results accordingly.[75] Note that the memories need not be heralded in this scheme.

Here is the quantitative analysis of the two-link repeater. Any elementary run takes the time for the photon to go from the source to the detector, then for the communication to reach back Christoph, i.e., ℓ/c. In each run, the probability of a detection is $1-(1-\sqrt{t}\eta)^N \approx N\sqrt{t}\eta$. Then, on average, the Bell measurement will be

FIG. 9. Comparison of K_1 (straight line) and K_2. For all curves, $\nu_S = 10$ GHz, $\eta = 0.5$, $\eta_M = 0.9$, $p_M = 0.9$, $\alpha = 0.2$ dB/km (fibers), $T_M = 10$ s. Line (a), best case, $N = 1000$, $F = 0.95$; line (b), $N = 1000$, fidelity reduced to $F = 0.9$; line (c), supported modes reduced to $N = 100$, $F = 0.95$.

performed after a time[76] $\tau \approx \frac{3}{2}\ell/c/N\sqrt{t}\eta$. Consequently,

$$R_2 = \begin{cases} \tau^{-1}\frac{1}{2}p_M^2\eta_M^2 & \text{if } \tau < T_M \\ 0 & \text{otherwise,} \end{cases} \tag{B2}$$

where we have supposed that the memory time T_M defines a sharp cut, which is another simplification. This is the expected result: R_2 scales with $\sqrt{t}\eta$ and not with $t\eta^2$ because each link can be activated independently. Finally, in our model, the error rate is uncorrelated with the other parameters and only due to the fidelity of the Bell measurement; so

$$K_2 = R_2[1 - 2h(\varepsilon)] \tag{B3}$$

with $\varepsilon = \frac{2}{3}(1-F)$ because one of the "wrong" Bell states nevertheless gives the correct bit correlations. In particular, the fidelity of a Bell measurement must exceed 83.5% to have $K_2 > 0$.

Some plots of K_1 and K_2 as a function of the distance are shown in Fig. 9. The chosen values are already optimistic extrapolations of what could be achieved in the not too distant future. We notice that quantum repeaters overcome the direct link for $\ell \gtrsim 500$ km in fibers; with $\eta = 0.5$ and $N = 1000$, this requires $T_M \approx 10$ s. Also, the number of modes supported by the memory is a more critical parameter than the fidelity of the Bell measure-

---

[74]That is, photons may be lost but do not decohere in the memory. Note that this can be the case even if the atoms, which form the memory, do undergo some decoherence (Staudt *et al.*, 2007).

[75]Recall that there is no time ordering in quantum correlations, so this procedure gives exactly the same statistics as the "usual" entanglement swapping, in which the Bell measurement is made beforehand.
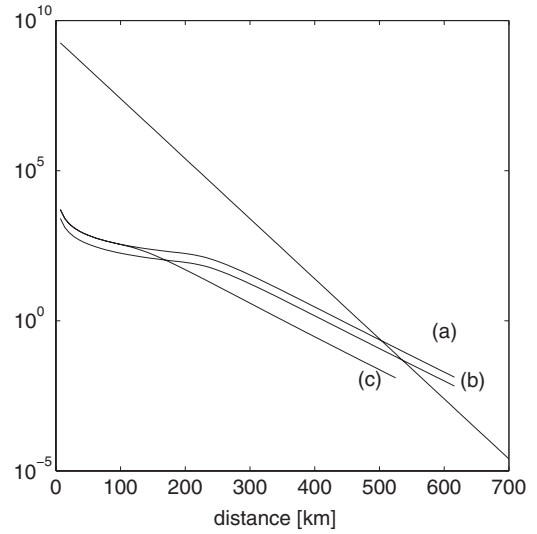
---

[76]In fact, let $x = 1-(1-\sqrt{t}\eta)^N$: the probability that Alice's (Bob's) detector is activated by the mth group of N pairs is $p_1(m) = x(1-x)^{m-1}$. Therefore, the probability that both links are activated exactly by the nth repetition is $p(n) = 2p_1(n)p_1(<n) + p_1(n)^2 = x(1-x)^{n-1}[2-(2-x)(1-x)^{n-1}]$ with $p_1(<n) = \sum_{m=1}^{n-1}p_1(m)$. Finally, the number of repetitions needed to establish the link is $\langle n \rangle = \sum_n np(n) = (1/x)[(3-2x)/(2-x)]$.

ment. This analysis provides a rough idea of the performances to be reached in order for quantum repeaters to be useful.

For the next step, the four-link repeater, we content ourselves with a few remarks. The four-link repeater allows one in principle to reach the scaling $R_4 \propto t^{1/4}$. The requirements for a practical implementation, however, become more stringent: the four memories must be released before T_M; there are three Bell measurements, so $\varepsilon < 11\%$ requires $F \gtrsim 95\%$; also, $p_{M'} \approx p_M t^{1/4}$. Moreover, it is easy to realize that the basic scheme (Fig. 8) requires heralded memories, although other schemes do not (Duan *et al.*, 2001).

REFERENCES

Acín, A., N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, 2007, Phys. Rev. Lett. **98**, 230501.

Acín, A., J. I. Cirac, and L. Masanes, 2004, Phys. Rev. Lett. **92**, 107903.

Acín, A., and N. Gisin, 2005, Phys. Rev. Lett. **94**, 020501.

Acín, A., N. Gisin, and L. Masanes, 2006, Phys. Rev. Lett. **97**, 120405.

Acín, A., N. Gisin, and V. Scarani, 2004, Phys. Rev. A **69**, 012309.

Adachi, Y., T. Yamamoto, M. Koashi, and N. Imoto, 2007, Phys. Rev. Lett. **99**, 180503.

Agrawal, G. P., 1997, *Fiber-Optic Communication Systems* (Wiley, New York).

Ahlswede, R., and I. Csiszár, 1993, IEEE Trans. Inf. Theory **39**, 1121.

Alexander, A. L., J. J. Longdell, M. J. Sellars, and N. B. Manson, 2006, Phys. Rev. Lett. **96**, 043602.

Alléaume, R., 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, and A. Zeilinger, 2007, e-print arXiv:quant-ph/0701168.

Alléaume, R., F. Roueff, E. Diamanti, and N. Lütkenhaus, 2009, e-print arXiv:0903.0839.

Alléaume, R., F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J.-P. Poizat, and P. Grangier, 2004, New J. Phys. **6**, 92.

Aspelmeyer, M., T. Jennewein, M. Pfennigbauer, W. Leeb, and A. Zeilinger, 2003, IEEE J. Sel. Top. Quantum Electron. **9**, 1541.

Bae, J., and A. Acín, 2007, Phys. Rev. A **75**, 012334.

Barnum, H., J. Barrett, M. Leifer, and A. Wilce, 2006, e-print arXiv:quant-ph/0611295.

Barrett, J., L. Hardy, and A. Kent, 2005, Phys. Rev. Lett. **95**, 010503.

Beaudry, N. J., T. Moroder, and N. Lütkenhaus, 2008a, Phys. Rev. Lett. **101**, 093601.

Beaudry, N. J., T. Moroder, and N. Lütkenhaus, 2008b, unpublished.

Bechmann-Pasquinucci, H., 2006, Phys. Rev. A **73**, 044305.

Bechmann-Pasquinucci, H., and N. Gisin, 1999, Phys. Rev. A **59**, 4238.

Bechmann-Pasquinucci H., and A. Pasquinucci, 2005, e-print arXiv:quant-ph/0505089.

Bechmann-Pasquinucci, H., and A. Peres, 2000, Phys. Rev.

Lett. **85**, 3313.

Bechmann-Pasquinucci, H., and W. Tittel, 2000, Phys. Rev. A **61**, 062308.

Beige, A., B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, 2002, Acta Phys. Pol. A **101**, 357.

Bennett, C. H., 1992, Phys. Rev. Lett. **68**, 3121.

Bennett, C. H., F. Bessette, L. Salvail, G. Brassard, and J. Smolin, 1992, J. Cryptology **5**, 3.

Bennett, C. H. and G. Brassard, 1984, *Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York), p. 175.

Bennett, C. H., G. Brassard, S. Bredibart, and S. Wiesner, 1984, IBM Tech. Discl. Bull. **26**, 4363.

Bennett, C. H., G. Brassard, C. Crépeau, and U. Maurer, 1995, IEEE Trans. Inf. Theory **41**, 1915.

Bennett, C. H., G. Brassard, and N. D. Mermin, 1992, Phys. Rev. Lett. **68**, 557.

Bennett, C. H., G. Brassard, and J.-M. Robert, 1988, SIAM J. Comput. **17**, 210.

Ben-Or, M., 2002, Security of BB84 QKD Protocol.

Ben-Or, M., M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, 2005, *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005*, Lecture Notes in Computer Science Vol. 3378 (Springer Verlag, Berlin), p. 387.

Bethune, D., and W. Risk, 2000, IEEE J. Quantum Electron. **36**, 340.

Beveratos, A., R. Bruori, T. Gacoin, A. Villing, J. P. Poizat, and P. Grangier, 2002, Phys. Rev. Lett. **89**, 187901.

Biham, E., M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, 2005, Algorithmica **34**, 372.

Biham, E., and T. Mor, 1997, Phys. Rev. Lett. **78**, 2256.

Bloch, M., A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, 2005, e-print arXiv:cs.IT/0509041.

Bloom, S., E. Korevaar, J. Schuster, and H. Willebrand, 2003, J. Opt. Netw. **2**, 178.

Boileau, J. C., D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, 2004, Phys. Rev. Lett. **92**, 017901.

Boström, K., and T. Felbinger, 2002, Phys. Rev. Lett. **89**, 187902.

Boucher, W., and T. Debuisschert, 2005, Phys. Rev. A **72**, 062325.

Bourennane, M., M. Eibl, S. Gaertner, C. Kurtsiefer, A. Cabello, and H. Weinfurter, 2004, Phys. Rev. Lett. **92**, 107901.

Brainis, E., L.-P. Lamoureux, N. J. Cerf, P. Emplit, M. Haelterman, and S. Massar, 2003, Phys. Rev. Lett. **90**, 157902.

Branciard, C., N. Gisin, B. Kraus, and V. Scarani, 2005, Phys. Rev. A **72**, 032301.

Branciard, C., N. Gisin, N. Lütkenhaus, and V. Scarani, 2007, Quantum Inf. Comput. **7**, 639.

Branciard, C., N. Gisin, and V. Scarani, 2008, New J. Phys. **10**, 013031.

Brassard, G., N. Lütkenhaus, T. Mor, and B. C. Sanders, 2000, Phys. Rev. Lett. **85**, 1330.

Brassard, G., T. Mor, and B. C. Sanders, 2000, in *Quantum Communication, Computing and Measurement 2*, edited by P. Kumar, G. M. D'Ariano, and O. Hirota (Kluwer Academic/ Plenum, New York), pp. 381–386.

Brassard, G., and L. Salvail, 1994, *Advances in Cryptology— EUROCRYPT '93*, Lecture Notes in Computer Science Vol. 765 (Springer Verlag, Berlin), pp. 410–423.

Bréguet, J., A. Muller, and N. Gisin, 1994, J. Mod. Opt. **41**, 2405.

Brendel, J., N. Gisin, W. Tittel, and H. Zbinden, 1999, Phys.

Rev. Lett. **82**, 2594.

Briegel, H.-J., W. Dür, J. I. Cirac, and P. Zoller, 1998, Phys. Rev. Lett. **81**, 5932.

Bruß, D., 1998, Phys. Rev. Lett. **81**, 3018.

Bruß, D., M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, 2000, Phys. Rev. A **62**, 012302.

Buttler, W. T., R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, 1998, Phys. Rev. Lett. **81**, 3283.

Camatel, S., and V. Ferrero, 2006, IEEE Photonics Technol. Lett. **18**, 142.

Carter, J. L., and M. N. Wegman, 1979, J. Comput. Syst. Sci. **18**, 143.

Cerf, N. J., M. Bourennane, A. Karlsson, and N. Gisin, 2002, Phys. Rev. Lett. **88**, 127902.

Cerf, N. J., A. Ipe, and X. Rottenberg, 2000, Phys. Rev. Lett. **85**, 1754.

Cerf, N. J., M. Lévy, and G. Van Assche, 2001, Phys. Rev. A **63**, 052311.

Chau, H. F., 2002, Phys. Rev. A **66**, 060302(R).

Chen, T.-Y., J. Zhang, J.-C. Boileau, X.-M. Jin, B. Yang, Q. Zhang, T. Yang, R. Laflamme, and J.-W. Pan, 2006, Phys. Rev. Lett. **96**, 150504.

Childress, L., J. M. Taylor, A. S. Sorensen, and M. D. Lukin, 2006, Phys. Rev. Lett. **96**, 070504.

Chou, C.-W., J. Laurat, H. Deng, K. S. Choi, H. de Riedmatten, D. Felinto, H. J. Kimble, 2007, Science **316**, 1316.

Cleve, R., D. Gottesman, and H.-K. Lo, 1999, Phys. Rev. Lett. **83**, 648.

Collins D., N. Gisin, and H. de Riedmatten, 2005, J. Mod. Opt. **52**, 735.

Coppersmith, D., D. B. Johnson, and S. M. Matyas, 1996, IBM J. Res. Dev. **40**, 253.

Cova, S., M. Ghioni, A. Lotito, I. Rech, and F. Zappa, 2004, J. Mod. Opt. **51**, 1267.

Crépeau, C., D. Gottesman, and A. Smith, 2005, *Advances in Cryptology—EUROCRYPT 2005*, Lecture Notes in Computer Science Vol. 3494 (Springer Verlag, Berlin), pp. 285–301.

Csiszár, I., and J. Körner, 1978, IEEE Trans. Inf. Theory **24**, 339.

Curty, M., M. Lewenstein, and N. Lütkenhaus, 2004, Phys. Rev. Lett. **92**, 217903.

Curty, M., and N. Lütkenhaus, 2004, Phys. Rev. A **69**, 042321.

Curty, M., and N. Lütkenhaus, 2005, Phys. Rev. A **71**, 062301.

Curty, M., K. Tamaki, and T. Moroder, 2008, Phys. Rev. A **77**, 052321.

Curty, M., L. Zhang, H.-K. Lo, and N. Lütkenhaus, 2007, Quantum Inf. Comput. **7**, 665.

Daemen, J., and V. Rijmen, 2001, Dr. Dobb's J. **26**, 137.

Damgaard, I. B., S. Fehr, R. Renner, L. Salvail, and C. Schaffner, 2007, *CRYPTO 2007*, Lecture Notes in Computer Science Vol. 4622 (Springer Verlag, Berlin).

Damgaard, I. B., S. Fehr, L. Salvail, and C. Schaffner, 2005, Proceedings of the 46th IEEE Symposium on Foundations of Computer Science—FOCS 2005 (unpublished), p. 449

De Riedmatten, H., I. Marcikic, V. Scarani, W. Tittel, H. Zbinden, and N. Gisin, 2004, Phys. Rev. A **69**, 050304(R).

De Riedmatten, H., V. Scarani, I. Marcikic, A. Acín, W. Tittel, H. Zbinden, and N. Gisin, 2004, J. Mod. Opt. **51**, 1637.

Deutsch, D., A. K. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, 1996, Phys. Rev. Lett. **77**, 2818.

Devetak, I., and A. Winter, 2005, Proc. R. Soc. London, Ser. A

461, 207.

Diamanti, E., H. Takesue, T. Honjo, K. Inoue, and Y. Yamamoto, 2005, Phys. Rev. A **72**, 052311.

Diamanti, E., H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, 2006, Opt. Express **14**, 13073.

Dianati, M., and R. Alléaume, 2006, e-print arXiv:quant-ph/0610202.

Dianati, M., R. Alléaume, M. Gagnaire, and X. Shen, 2008, Secur. Commun. Netw. **1**, 57.

Diffie, W., and M. E. Hellman, 1976, IEEE Trans. Inf. Theory **IT-22**, 644.

Duan, L. M., M. D. Lukin, J. I. Cirac, and P. Zoller, 2001, Nature (London) **414**, 413.

Dür, W., H.-J. Briegel, J. I. Cirac, and P. Zoller, 1999, Phys. Rev. A **59**, 169.

Durkin, G. A., C. Simon, and D. Bouwmeester, 2002, Phys. Rev. Lett. **88**, 187902.

Dušek, M., O. Haderka, and M. Hendrych, 1999, Opt. Commun. **169**, 103.

Dušek, M., M. Jahma, and N. Lütkenhaus, 2000, Phys. Rev. A **62**, 022306.

Dušek, M., N. Lütkenhaus, and M. Hendrych, 2006, in *Progress in Optics*, edited by E. Wolf (Elsevier, New York), Vol. 49, p. 381.

Eisenberg, H. S., G. Khoury, G. A. Durkin, C. Simon, and D. Bouwmeester, 2004, Phys. Rev. Lett. **93**, 193901.

Ekert, A. K., 1991, Phys. Rev. Lett. **67**, 661.

Ekert, A. K., N. Gisin, B. Huttner, H. Inamori, and H. Weinfurter, 2001, in *The Physics of Quantum Information*, edited by D. Bouwmeester, A. K. Ekert, and A. Zeilinger (Springer Verlag, London).

Elliott, C., 2002, New J. Phys. **4**, 46.

Elliott, C., A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, 2005, e-print arXiv:quant-ph/0503058.

Englert, B.-G., D. Kaszlikowski, H. K. Ng, W. K. Chua, J. Rehácek, and J., Anders, 2004, e-print arXiv:quant-ph/0412075.

Erven, C., C. Couteau, R. Laflamme, and G. Weihs, 2008, e-print arXiv:0807.2289.

Fasel, S., N. Gisin, G. Ribordy, and H. Zbinden, 2004, Eur. Phys. J. D **30**, 143.

Franson, J. D., and H. Ilves, 1994, J. Mod. Opt. **41**, 2391.

Fuchs, C. A., N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, 1997, Phys. Rev. A **56**, 1163.

Fung, C.-H. F., B. Qi, K. Tamaki, and H.-K. Lo, 2007, Phys. Rev. A **75**, 032314.

Fung, C.-H. F., K. Tamaki, and H.-K. Lo, 2006, Phys. Rev. A **73**, 012337.

Galtarossa, A., and C. R. Menyuk, 2005, *Polarization Mode Dispersion* (Springer, Berlin).

García-Patrón, R., 2007, Ph.D. thesis (Université Libre de Bruxelles).

García-Patrón, R., and N. J. Cerf, 2006, Phys. Rev. Lett. **97**, 190503.

Gisin, N., S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, 2006, Phys. Rev. A **73**, 022320.

Gisin, N., and J. P. Pellaux, 1992, Opt. Commun. **89**, 316.

Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden, 2002, Rev. Mod. Phys. **74**, 145.

Gisin, N., G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, 2004, e-print arXiv:quant-ph/0411022.

Gisin, N., and S. Wolf, 1999, Phys. Rev. Lett. **83**, 4200.

Gisin, N., and S. Wolf, 2000, *Proceedings of CRYPTO 2000*, Lecture Notes in Computer Science Vol. 1880 (Springer Ver-

lag, Berlin), p. 482.

Gobby, C., Z. L. Yuan, and A. J. Shields, 2004, Appl. Phys. Lett. **84**, 3762.

Goldenberg, L., and L. Vaidman, 1995, Phys. Rev. Lett. **75**, 1239.

Goldenberg, L., and L. Vaidman, 1996, Phys. Rev. Lett. **77**, 3265.

Gomez-Sousa, H., and M. Curty, 2009, Quant. Inf. Comput. **9**, 62.

Gottesman, D., and H.-K. Lo, 2003, IEEE Trans. Inf. Theory **49**, 457.

Gottesman, D., H.-K. Lo, N. Lütkenhaus, and J. Preskill, 2004, Quantum Inf. Comput. **4**, 325.

Gottesman, D., and J. Preskill, 2001, Phys. Rev. A **63**, 022309.

Griffiths, R. B., and C.-S. Niu, 1997, Phys. Rev. A **56**, 1173.

Grosshans, F., 2005, Phys. Rev. Lett. **94**, 020504.

Grosshans, F., and N. J. Cerf, 2004, Phys. Rev. Lett. **92**, 047905.

Grosshans, F., N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, 2003, Quantum Inf. Comput. **3**, 535.

Grosshans, F., and P. Grangier, 2002a, Phys. Rev. Lett. **88**, 057902.

Grosshans, F., and P. Grangier, 2002b, *Proceedings of the Sixth International Conference on Quantum Communications, Measurement, and Computing (QCMC'02)* (Rinton Press, Princeton, NJ).

Grosshans, F., G. Van Assche, J. Wenger, R. Tualle-Brouri, N. J. Cerf, and P. Grangier, 2003, Nature (London) **421**, 238.

Grover, L. K., 1996, *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, STOC'96* (ACM, New York), p. 212.

Grover, L. K., 1997, Phys. Rev. Lett. **79**, 325.

Hadfield, R. H., J. L. Habif, J. Schlafer, R. E. Schwall, and S. W. Nam, 2006, Appl. Phys. Lett. **89**, 241129.

Halder, M., A. Beveratos, N. Gisin, V. Scarani, C. Simon, and H. Zbinden, 2007, Nat. Phys. **3**, 692.

Hasegawa, J., M. Hayashi, T. Hiroshima, A. Tanaka, and A. Tomita, 2007, e-print arXiv:0705.3081.

Häseler, H., T. Moroder, and N. Lütkenhaus, 2008, Phys. Rev. A **77**, 032303.

Hayashi, M., 2006, Phys. Rev. A **74**, 022307.

Hayashi, M., 2007a, Phys. Rev. A **76**, 012329.

Hayashi, M., 2007b, New J. Phys. **9**, 284.

Heid, M., and N. Lütkenhaus, 2006, Phys. Rev. A **73**, 052316.

Heid, M., and N. Lütkenhaus, 2007, Phys. Rev. A **76**, 022313.

Helstrom, C. W., 1976, *Quantum Detection and Estimation Theory* (Academic, New York).

Herbauts, I. M., S. Bettelli, H. Hübel, and M. Peev, 2008, Eur. Phys. J. D **46**, 395.

Hillery, M., 2000, Phys. Rev. A **61**, 022309.

Hillery, M., V. Bužek, and A. Berthiaume, 1999, Phys. Rev. A **59**, 1829.

Hiskett, P. A., D. Rosenberg, C. G. Peterson, R. J. Hughes, S. W. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, 2006, New J. Phys. **8**, 193.

Holevo, A. S., 1973, Probl. Inf. Transm. **9**, 177.

Horodecki, K., M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, 2008a, IEEE Trans. Inf. Theory **54**, 2604.

Horodecki, K., M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, 2008b, Phys. Rev. Lett. **100**, 110502.

Horodecki, K., M. Horodecki, P. Horodecki, and J. Oppenheim, 2005, Phys. Rev. Lett. **94**, 160502.

Hübel, H., M. R. Vanner, T. Lederer, B. Blauensteiner, T. Lorünser, A. Poppe, and A. Zeilinger, 2007, Opt. Express **15**, 7853.

Hughes, R. J., J. E. Nordholt, D. Derkacs, and C. G. Peterson, 2002, New J. Phys. **4**, 43.

Huttner, B., N. Imoto, N. Gisin, and T. Mor, 1995, Phys. Rev. A **51**, 1863.

Hwang, W.-Y., 2003, Phys. Rev. Lett. **91**, 057901.

Inamori, H., N. Lütkenhaus, and D. Mayers, 2007, Eur. Phys. J. D **41**, 599.

Inoue, K., and T. Honjo, 2005, Phys. Rev. A **71**, 042305.

Inoue, K., E. Waks, and Y. Yamamoto, 2002, Phys. Rev. Lett. **89**, 037902.

Inoue, K., E. Waks, and Y. Yamamoto, 2003, Phys. Rev. A **68**, 022317.

Intallura, P. M., M. B. Ward, O. Z. Karimov, Z. L. Yuan, P. See, A. J. Shields, P. Atkinson, and D. A. Ritchie, 2007, Appl. Phys. Lett. **91**, 161103.

Jacobs, B. C., T. B. Pittman, and J. D. Franson, 2002, Phys. Rev. A **66**, 052307.

Jennewein, T., C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, 2000, Phys. Rev. Lett. **84**, 4729.

Julsgaard, B., J. Sherson, J. I. Cirac, J. Fiurasek, and E. S. Polzik, 2004, Nature (London) **432**, 482.

Karlsson, A., M. Koashi, and N. Imoto, 1999, Phys. Rev. A **59**, 162.

Kim, I. I., and E. Korevaar, 2001, http://www.freespaceoptic.com/WhitePapers/SPIE2001b.pdf.

Kim, J., S. Takeuchi, Y. Yamamoto, and H. Hogue, 1999, Appl. Phys. Lett. **74**, 902.

Koashi, M., 2004, Phys. Rev. Lett. **93**, 120501.

Koashi, M., 2005, e-print arXiv:quant-ph/0507154.

Koashi, M., 2006a, J. Phys.: Conf. Ser. **36**, 98.

Koashi, M., 2006b, e-print arXiv:quant-ph/0609180.

Koashi, M., 2007, e-print arXiv:0704.3661.

Koashi, M., Y. Adachi, T. Yamamoto, and N. Imoto, 2008, e-print arXiv:0804.0891.

Koashi, M., and N. Imoto, 1997, Phys. Rev. Lett. **79**, 2383.

Koashi, M., and J. Preskill, 2003, Phys. Rev. Lett. **90**, 057902.

König, R., and R. Renner, 2007, e-print arXiv:0712.4291.

König, R., R. Renner, A. Bariska, and U. Maurer, 2007, Phys. Rev. Lett. **98**, 140502.

König, R., and B. Terhal, 2008, IEEE Trans. Inf. Theory **54**, 749.

Kraus, B., C. Branciard, and R. Renner, 2007, Phys. Rev. A **75**, 012316.

Kraus, B., N. Gisin, and R. Renner, 2005, Phys. Rev. Lett. **95**, 080501.

Kurtsiefer, C., P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, 2002, Nature (London) **419**, 450.

Kurtsiefer, C., P. Zarda, S. Mayer, and H. Weinfurter, 2001, J. Mod. Opt. **48**, 2039.

Kwiat, P. G., K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, 1995, Phys. Rev. Lett. **75**, 4337.

Kwiat, P. G., E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, 1999, Phys. Rev. A **60**, R773.

Lamas-Linares, A., and C. Kurtsiefer, 2007, Opt. Express **15**, 9388.

Lance, A. M., T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, 2005, Phys. Rev. Lett. **95**, 180503.

Laurent, S., S. Varoutsis, L. Le Gratiet, A. Lemaître, I. Sagnes, F. Raineri, J. A. Levenson, I. Robert-Philip, and I. Abram, 2005, Appl. Phys. Lett. **87**, 163107.

Le Bellac, M., 2006, *A Short Introduction to Quantum Infor-*

mation and Quantum Computation (Cambridge University Press, Cambridge).

Legré, M., H. Zbinden, and N. Gisin, 2006, Quantum Inf. Comput. **6**, 326.

Leverrier, A., R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, 2008, Phys. Rev. A **77**, 042325.

Leverrier, A., E. Karpov, P. Grangier, and N. J. Cerf, 2008, e-print arXiv:0809.2252.

Li, Y., H. Mikami, H. Wang, and T. Kobayashi, 2005, Phys. Rev. A **72**, 063801.

Ling, A., M. P. Peloso, I. Marcikic, V. Scarani, A. Lamas-Linares, and C. Kurtsiefer, 2008, Phys. Rev. A **78**, 020301(R).

Lo, H.-K., 1997, Phys. Rev. A **56**, 1154.

Lo, H.-K., 1998, in *Introduction to Quantum Computation and Information*, edited by H.-K. Lo, S. Popescu, and T. Spiller (World Scientific, Singapore).

Lo, H.-K., 2001, Quantum Inf. Comput. **1**, 81.

Lo, H.-K., 2003, New J. Phys. **5**, 36.

Lo, H.-K., 2005, Quantum Inf. Comput. **5**, 413.

Lo, H.-K., and H. F. Chau, 1997, Phys. Rev. Lett. **78**, 3410.

Lo, H.-K., and H. F. Chau, 1999, Science **283**, 2050.

Lo, H.-K., H. F. Chau, and M. Ardehali, 2005, J. Cryptology **18**, 133.

Lo, H.-K., X. Ma, and K. Chen, 2005, Phys. Rev. Lett. **94**, 230504.

Lo, H.-K., and J. Preskill, 2007, Quantum Inf. Comput. **8**, 431.

Lo, H.-K., and Y. Zhao, 2008, e-print arXiv:0803.2507.

Lodewyck, J., M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, 2007, Phys. Rev. A **76**, 042305.

Lodewyck, J., T. Debuisschert, R. García-Patrón, R. Tualle-Brouri, N. J. Cerf, and P. Grangier, 2007, Phys. Rev. Lett. **98**, 030503.

Lodewyck, J., T. Debuisschert, R. Tualle-Brouri, and P. Grangier, 2005, Phys. Rev. A **72**, 050303(R).

Lodewyck, J., and P. Grangier, 2007, Phys. Rev. A **76**, 022332.

Lorenz, S., N. Korolkova, and G. Leuchs, 2004, Appl. Phys. B: Lasers Opt. **79**, 273.

Lorenz, S., J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs, 2006, Phys. Rev. A **74**, 042326.

Lounis, B., and M. Orrit, 2005, Rep. Prog. Phys. **68**, 1129.

Lütkenhaus, N., 1996, Phys. Rev. A **54**, 97.

Lütkenhaus, N., 1999, Phys. Rev. A **59**, 3301.

Lütkenhaus, N., 2000, Phys. Rev. A **61**, 052304.

Lütkenhaus, N., and M. Jahma, 2002, New J. Phys. **4**, 44.

Ma, X., C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, 2006, Phys. Rev. A **74**, 032330.

Ma, X., C.-H. F. Fung, and H.-K. Lo, 2007, Phys. Rev. A **76**, 012307.

Mair, A., A. Vaziri, G. Weihs, and A. Zeilinger, 2001, Nature (London) **412**, 3123.

Makarov, V., A. Anisimov, and J. Skaar, 2006, Phys. Rev. A **74**, 022313.

Makarov, V., and D. R. Hjelme, 2005, J. Mod. Opt. **52**, 691.

Makarov, V., and J. Skaar, 2008, Quantum Inf. Comput. **8**, 622.

Mandel, L., and E. Wolf, 1995, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge).

Marcikic, I., A. Lamas-Linares, and C. Kurtsiefer, 2006, Appl. Phys. Lett. **89**, 101122.

Masanes, L., 2009, Phys. Rev. Lett. **102**, 140501.

Masanes, L., A. Acín, and N. Gisin, 2006, Phys. Rev. A **73**, 012112.

Mauerer, W., and C. Silberhorn, 2007, Phys. Rev. A **75**, 050305(R).

Maurer, U. M., 1993, IEEE Trans. Inf. Theory **39**, 733.

Maurer, U. M., and S. Wolf, 1999, SIAM J. Comput. **28**, 1689.

Maurer, U. M., and S. Wolf, 2000, Designs, Codes, Cryptogr. **19**, 147.

Mayers, D., 1996, *Advances in Cryptology: Proceedings of Crypto '96* (Springer Verlag, Berlin), p. 343.

Mayers, D., 1997, Phys. Rev. Lett. **78**, 3414.

Mayers, D., 2001, J. ACM **48**, 351.

Mérolla, J.-M., Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes, 1999, Phys. Rev. Lett. **82**, 1656.

Meyer, T., H. Kampermann, M. Kleinmann, and D. Bruß, 2006, Phys. Rev. A **74**, 042340.

Miller, A. J., S. W. Nam, J. M. Martinis, and A. V. Sergienko, 2003, Appl. Phys. Lett. **83**, 791.

Mølmer, K., 1997, Phys. Rev. A **55**, 3195.

Muller, A., T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, 1997, Appl. Phys. Lett. **70**, 793.

Muller, A., H. Zbinden, and N. Gisin, 1995, Nature (London) **378**, 449.

Naik, D. S., C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, 2000, Phys. Rev. Lett. **84**, 4733.

Navascués, M., and A. Acín, 2005, Phys. Rev. Lett. **94**, 020505.

Navascués, M., F. Grosshans, and A. Acín, 2006, Phys. Rev. Lett. **97**, 190502.

Nguyen, K.-C., G. Van Assche, and N. J. Cerf, 2004, Proceedings of International Symposium on Information Theory and its Applications (ISITA), Parma, 2004 (unpublished).

Niederberger, A., V. Scarani, and N. Gisin, 2005, Phys. Rev. A **71**, 042316.

Ou, Z. Y., J.-K. Rhee, and L. J. Wang, 1999, Phys. Rev. A **60**, 593.

Peng, C.-Z., J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wand, and J.-W. Pan, 2007, Phys. Rev. Lett. **98**, 010505.

Peres, A., 1996, Phys. Rev. Lett. **77**, 3264.

Pirandola, S., S. L. Braunstein, and S. Lloyd,, 2008, Phys. Rev. Lett. **101**, 200504.

Qi, B., C. H. F. Fung, H.-K. Lo, and X. Ma, 2007, Quantum Inf. Comput. **7**, 73.

Qi, B., L.-L. Huang, L. Qian, and H.-K. Lo, 2007, Phys. Rev. A **76**, 052323.

Qi, B., Y. Zhao, X. Ma, H.-K. Lo, and L. Qian, 2007, Phys. Rev. A **75**, 052304.

Ralph, T. C., 1999, Phys. Rev. A **61**, 010303(R).

Rarity, J. G., P. M. Gorman, and P. R. Tapster, 2001, Electron. Lett. **37**, 512.

Rarity, J. G., P. R. Tapster, P. M. Gorman, and P. Knight, 2002, New J. Phys. **4**, 82.

Reid, M. D., 2000, Phys. Rev. A **62**, 062308.

Renner, R., 2005, Ph.D. thesis, ETH Zürich.

Renner, R., 2007, Nat. Phys. **3**, 645.

Renner, R., and J. I. Cirac, 2009, Phys. Rev. Lett. **102**, 110504.

Renner, R., N. Gisin, and B. Kraus, 2005, Phys. Rev. A **72**, 012332.

Renner, R., and R. König, 2005, *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005*, Lecture Notes in Computer Science Vol. 3378 (Springer, Berlin), p. 407.

Renner, R., and S. Wolf, 2005, *Advances in Cryptology: CRYPTO 2003*, Lecture Notes in Computer Science Vol. 2729 (Springer, Berlin), p. 78.

Ribordy, G., J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, 1998, Electron. Lett. **34**, 2116.

Ribordy, G., N. Gisin, O. Guinnard, D. Stucki, M. Wegmüller, and H. Zbinden, 2004, J. Mod. Opt. **51**, 1381.

Rigas, J., O. Gühne, and N. Lütkenhaus, 2006, Phys. Rev. A **73**, 012341.

Rijmen, V., 2007, private communication.

Rosenberg, D., J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, 2007, Phys. Rev. Lett. **98**, 010503.

Rosenberg, D., A. E. Lita, A. J. Miller, and S. W. Nam, 2005, Phys. Rev. A **71**, 061803(R).

Rosenberg, D., C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. W. Nam, B. Baek, R. H. Hadfield, R. J. Hughes, and J. E. Nordholt, 2009, New J. Phys. **11**, 045009.

Saint-Girons, G., N. Chauvin, A. Michon, G. Patriarche, G. Beaudoin, B. Bremond, C. Bru-Chevalier, and I. Sagnes, 2006, Appl. Phys. Lett. **88**, 133101.

Sangouard, N., C. Simon, J. Minar, H. Zbinden, H. De Riedmatten, and N. Gisin, 2007, Phys. Rev. A **76**, 050301(R).

Scarani, V., 2006, *Quantum Physics—A First Encounter* (Oxford University Press, Oxford).

Scarani, V., A. Acín, G. Ribordy, and N. Gisin, 2004, Phys. Rev. Lett. **92**, 057901.

Scarani, V., H. De Riedmatten, I. Marcikic, H. Zbinden, and N. Gisin, 2005, Eur. Phys. J. D **32**, 129.

Scarani, V., N. Gisin, N. Brunner, L. Masanes, S. Pino, and A. Acín, 2006, Phys. Rev. A **74**, 042339.

Scarani, V., and R. Renner, 2008, Phys. Rev. Lett. **100**, 200501.

Shannon, C. E., 1949, Bell Syst. Tech. J. **28**, 656.

Shields, A. J., 2007, Nat. Photonics **1**, 215.

Shor, P. W., 1994, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Santa Fe* (IEEE Computer Society, Los Alamitos), p. 124.

Shor, P. W., 1997, SIAM Sci. Stat. Comput. **26**, 1484.

Shor, P. W., and J. Preskill, 2000, Phys. Rev. Lett. **85**, 441.

Silberhorn, C., T. C. Ralph, N. Lütkenhaus, and G. Leuchs, 2002, Phys. Rev. Lett. **89**, 167901.

Simon, C., H. De Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, 2007, Phys. Rev. Lett. **98**, 190503.

Slutsky, B. A., R. Rao, P.-C. Sun, and Y. Fainman, 1998, Phys. Rev. A **57**, 2383.

Smith, G., J. M. Renes, and J. A. Smolin, 2008, Phys. Rev. Lett. **100**, 170502.

Staudt, M. U., S. R. Hastings-Simon, M. Nilsson, M. Afzelius, V. Scarani, R. Ricken, H. Suche, W. Sohler, W. Tittel, and N. Gisin, 2007, Phys. Rev. Lett. **98**, 113601.

Stinson, D. R., 1995, *Cryptography, Theory and Practice* (CRC, Boca Raton).

Stucki, D., C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, 2008, e-print arXiv:0809.5264.

Stucki, D., N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, 2005, Appl. Phys. Lett. **87**, 194108.

Sudjana, J., L. Magnin, R. Garcia-Patron, and N. J. Cerf, 2007, Phys. Rev. A **76**, 052301.

Takesue, H., E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto, 2005, New J. Phys. **7**, 232.

Takesue, H., S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, 2007, Nat. Photonics **1**, 343.

Tamaki, K., M. Koashi, and N. Imoto, 2003, Phys. Rev. Lett. **90**, 167904.

Tamaki, K., and H.-K. Lo, 2006, Phys. Rev. A **73**, 010302(R).

Tamaki, K., and N. Lütkenhaus, 2004, Phys. Rev. A **69**, 032316.

Tamaki, K., N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, 2006, e-print arXiv:quant-ph/0607082.

Tanaka, A., 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, 2008, e-print arXiv:0805.2193.

Tanzilli, S., H. De Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D. B. Ostrowsky, and N. Gisin, 2001, Electron. Lett. **37**, 26.

Tapster, P. R., and J. G. Rarity, 1998, J. Mod. Opt. **45**, 595.

Thew, R., A. Acín, H. Zbinden, and N. Gisin, 2004, Quantum Inf. Comput. **4**, 93.

Thew, R., S. Tanzilli, L. Krainer, S. C. Zeller, A. Rochas, I. Rech, S. Cova, H. Zbinden, and N. Gisin, 2006, New J. Phys. **8**, 32.

Tittel, W., J. Brendel, H. Zbinden, and N. Gisin, 2000, Phys. Rev. Lett. **84**, 4737.

Townsend, P. D., S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, 1994, Electron. Lett. **30**, 1875.

Townsend, P. D., J. G. Rarity, and P. R. Tapster, 1993, Electron. Lett. **29**, 1291.

Trifonov, A., D. Subacius, A. Berzanskis, and A. Zavriyev, 2004, J. Mod. Opt. **51**, 1399.

Tsujino, K., H. F. Hofmann, S. Takeuchi, and K. Sasaki, 2004, Phys. Rev. Lett. **92**, 153602.

Tsurumaru, T., 2007, Phys. Rev. A **75**, 062319.

Tsurumaru, T., A. Soujaeff, and S. Takeuchi, 2008, Phys. Rev. A **77**, 022319.

Tsurumaru, T., and K. Tamaki, 2008, Phys. Rev. A **78**, 032302.

Ursin, R., 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, and A. Zeilinger, 2007, Nat. Phys. **3**, 481.

Vakhitov, A., V. Makarov, and D. R. Hjelme, 2001, J. Mod. Opt. **48**, 2023.

Van Assche, G., 2006, *Quantum Cryptography and Secret-Key Distillation* (Cambridge University Press, Cambridge).

Van Assche, G., J. Cardinal, and N. J. Cerf, 2004, IEEE Trans. Inf. Theory **50**, 394.

van Enk, S. J., and C. A. Fuchs, 2002, Quantum Inf. Comput. **2**, 151.

Verevkin, A., A. Pearlmany, W. Slyszyz, J. Zhangy, M. Currie, A. Korneev, G. Chulkova, O. Okunev, P. Kouminov, K. Smirnov, B. Voronov, G. N. Goltsman, and R. Sobolewskiy, 2004, J. Mod. Opt. **51**, 1447.

Verevkin, A., J. Zhang, R. Sobolewski, A. Lipatov, O. Okunev, G. Chulkova, A. Korneev, K. Smirnov, G. N. Goltsman, and A. Semenov, 2002, Appl. Phys. Lett. **80**, 4687.

Vernam, G. S., 1926, J. Am. Inst. Elec. Eng. **55**, 109.

Waks, E., E. Diamanti, and Y. Yamamoto, 2006, New J. Phys. **8**, 4.

Waks, E., K. Inoue, W. D. Oliver, E. Diamanti, and Y. Yamamoto, 2003, IEEE J. Sel. Top. Quantum Electron. **9**, 1502.

Waks, E., K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. Solomon, and Y. Yamamoto, 2002, Nature (London) **420**, 762.

Waks, E., C. Santori, and Y. Yamamoto, 2002, Phys. Rev. A **66**, 042315.

Waks, E., H. Takesue, and Y. Yamamoto, 2006, Phys. Rev. A **73**, 012344.

Waks, E., A. Zeevi, and Y. Yamamoto, 2002, Phys. Rev. A **65**, 052310.

Wang, X.-B., 2001, e-print arXiv:quant-ph/0110089.

Wang, X.-B., 2005, Phys. Rev. Lett. **94**, 230503.

Ward, M. B., O. Z. Karimov, D. C. Unitt, Z. L. Yuan, P. See, D. G. Gevaux, A. J. Shields, P. Atkinson, and D. A. Ritchie, 2005, Appl. Phys. Lett. **86**, 201111.

Watanabe, S., R. Matsumoto, and T. Uyematsu, 2004, e-print arXiv:quant-ph/0412070.

Weedbrook, C., A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, 2004, Phys. Rev. Lett. **93**, 170504.

Wegman, M. N., and J. L. Carter, 1981, J. Comput. Syst. Sci. **22**, 265.

Wehner, S., C. Schaffner, and B. Terhal, 2008, Phys. Rev. Lett. **100**, 220502.

Wiesner, S., 1983, SIGACT News **15**, 78.

Wootters, W. K., and W. H. Zurek, 1982, Nature (London) **299**, 802.

Wyner, A. D., 1975, Bell Syst. Tech. J. **54**, 1355.

Young, R. J., R. M. Stevenson, P. Atkinson, K. Cooper, D. A. Ritchie, and A. J. Shields, 2006, New J. Phys. **8**, 29.

Yuan, Z. L., A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, 2008, Appl. Phys. Lett. **92**, 201104.

Yuan, Z. L., B. E. Kardynal, A. W. Sharpe, and A. J. Shields, 2007, Appl. Phys. Lett. **91**, 011114.

Yuan, Z. L., A. W. Sharpe, and A. J. Shields, 2007, Appl. Phys. Lett. **90**, 011118.

Yuan, Z. L., and A. J. Shields, 2005, Opt. Express **13**, 660.

Zanardi, P., and M. Rasetti, 1997, Phys. Rev. Lett. **79**, 3306.

Zhao, Y., C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, 2008, Phys. Rev. A **78**, 042333.

Zhao, Y., B. Qi, and H.-K. Lo, 2007, Appl. Phys. Lett. **90**, 044106.

Zhao, Y., B. Qi, and H.-K. Lo, 2008, Phys. Rev. A **77**, 052327.

Zhao, Y., B. Qi, X. Ma, H.-K. Lo, and L. Qian, 2006, Phys. Rev. Lett. **96**, 070502.

Zhou, C., G. Wu, X. Chen, and H. Zeng, 2003, Appl. Phys. Lett. **83**, 1692.

Zinoni, C., B. Alloing, C. Monat, V. Zwiller, L. H. Li, A. Fiore, L. Lunghi, A. Gerardino, H. de Riedmatten, H. Zbinden, and N. Gisin, 2006, Appl. Phys. Lett. **88**, 131102.