Quantum cryptography

Gisin, Nicolas; Ribordy, Grégoire; Tittel, Wolfgang; Zbinden, Hugo

How to cite

GISIN, Nicolas et al. Quantum cryptography. In: Reviews of modern physics, 2002, vol. 74, n° 1, p. 145–195. doi: 10.1103/RevModPhys.74.145

This publication URL: https://archive-ouverte.unige.ch//unige:36820
Publication DOI: 10.1103/RevModPhys.74.145

Quantum cryptography

Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden

Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland

(Published 8 March 2002)

Quantum cryptography could well be the first application of quantum mechanics at the single-quantum level. The rapid progress in both theory and experiment in recent years is reviewed, with emphasis on open questions and technological issues.

CONTENTS

I. INTRODUCTION

Electrodynamics was discovered and formalized in the 19th century. The 20th century was then profoundly affected by its applications. A similar adventure may be underway for quantum mechanics, discovered and formalized during the last century. Indeed, although the laser and semiconductor are already common, applications of the most radical predictions of quantum mechanics have only recently been conceived, and their full potential remains to be explored by the physicists and engineers of the 21st century.

The most peculiar characteristics of quantum mechanics are the existence of indivisible quanta and of entangled systems. Both of these lie at the root of quantum cryptography (QC), which could very well be the first commercial application of quantum physics at the single-quantum level. In addition to quantum mechanics, the 20th century has been marked by two other major scientific revolutions: information theory and relativity. The status of the latter is well recognized. It is less well known that the concept of information, nowadays measured in bits, and the formalization of probabilities are

quite recent,[1] although they have a tremendous impact on our daily life. It is fascinating to realize that QC lies at the intersection of quantum mechanics and information theory and that, moreover, the tension between quantum mechanics and relativity—the famous Einstein-Rosen-Podolsky (EPR) paradox (Einstein *et al.*, 1935)—is closely connected to the security of QC. Let us add a further point for young physicists. Unlike laser and semiconductor physics, which are manifestations of quantum physics at the ensemble level and can thus be described by semiclassical models, QC, and to an even greater extent quantum computers, require a full quantum-mechanical description (this may offer an interesting challenge for physicists well trained in the subtleties of their science).

This review article has several objectives. First, we present the basic intuition behind QC. Indeed, the basic idea is so beautiful and simple that every physicist and student should be given the pleasure of learning it. The general principle is then set in the broader context of modern cryptology (Sec. II.B) and made more precise (Sec. II.C). Section III discusses the main technological challenges. Then, Secs. IV and V present the most common implementations of QC: the use of weak laser pulses and photon pairs, respectively. Finally, the important and difficult problems of eavesdropping and security proofs are discussed in Sec. VI, where the emphasis is more on the diversity of the issues than on formal details. We have tried to write the different parts of this review in such a way that they can be read independently.

II. A BEAUTIFUL IDEA

The idea of quantum cryptography was first proposed in the 1970s by Stephen Wiesner[2] (1983) and by Charles H. Bennett of IBM and Gilles Brassard of The University of Montréal (1984, 1985).[3] However, this idea is so simple that any first-year student since the infancy of quantum mechanics could actually have discovered it! Nevertheless, it is only now that the field is mature enough and information security important enough that physicists are ready to consider quantum mechanics, not only as a strange theory good for paradoxes, but also as a tool for new engineering. Apparently, information theory, classical cryptography, quantum physics, and quantum optics first had to develop into mature sciences. It is certainly not a coincidence that QC and, more generally, quantum information were developed by a community including many computer scientists and more mathematically oriented young physicists: broader interests than traditional physics were needed.

A. The intuition

Quantum physics is well known for being counterintuitive or even bizarre. We teach students that quantum physics establishes a set of negative rules stating things that cannot be done. For example,

(1) One cannot take a measurement without perturbing the system.
(2) One cannot determine simultaneously the position and the momentum of a particle with arbitrarily high accuracy.
(3) One cannot simultaneously measure the polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis.
(4) One cannot draw pictures of individual quantum processes.
(5) One cannot duplicate an unknown quantum state.

This negative viewpoint of quantum physics, due to its contrast with classical physics, has only recently been turned positive, and QC is one of the best illustrations of this *psychological revolution*. Indeed, one could characterize quantum information processing as the science of turning quantum conundrums into potentially useful applications.

Let us illustrate this point for QC. One of the basic negative statements of quantum physics reads

One cannot take a measurement without perturbing the system (1)

(unless the quantum state is compatible with the measurement). The positive side of this axiom can be seen when applied to a communication between Alice and Bob (the conventional names of the sender and receiver, respectively), provided the communication is quantum, that is, quantum systems, for example, individual photons, carry the information. When this is the case, axiom (1) also applies to eavesdroppers, i.e., to a malicious Eve (the conventional name given to the adversary in cryptology). Hence Eve cannot get any information about the communication without introducing perturbations that would reveal her presence.

To make this intuition more precise, imagine that Alice codes information in individual photons, which she sends to Bob. If Bob receives the photons unperturbed, then, according to the basic axiom (1), the photons were not measured. No measurement implies that Eve did not get any information about the photons (note that acquiring information is synonymous with carrying out measurements). Consequently, after exchanging the photons,

[1]The Russian mathematician A. N. Kolmogorov (1956) is credited with being the first to have formulated a consistent mathematical theory of probabilities in the 1940s.

[2]S. Wiesner, then at Columbia University, was the first to propose ideas closely related to QC in the 1970s. However, his revolutionary paper did not appear until a decade later. Since it is difficult to find, we reproduce his abstract here: *The uncertainty principle imposes restrictions on the capacity of certain types of communication channels. This paper will show that in compensation for this "quantum noise," quantum mechanics allows us novel forms of coding without analogue in communication channels adequately described by classical physics*.

[3]Artur Ekert (1991) of Oxford University discovered QC independently, though from a different perspective (see Sec. II.D.3).

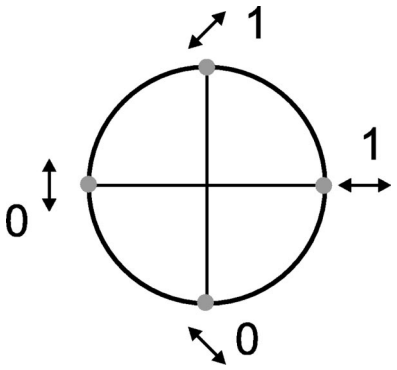

FIG. 1. Implementation of the Bennett and Brassard (BB84) protocol. The four states lie on the equator of the Poincaré sphere.

Alice and Bob can check whether someone "was listening": they simply compare a randomly chosen subset of their data using a public channel. If Bob received this subset unperturbed, then the logic goes as follows:

$$\text{No perturbation} \Rightarrow \text{No measurement} \Rightarrow \text{No eavesdropping.} \quad (2)$$

Actually, there are two more points to add. First, in order to ensure that axiom (1) applies, Alice encodes her information in nonorthogonal states (we shall illustrate this in Secs. II.C and II.D). Second, as we have presented it so far, Alice and Bob could discover any eavesdropper, but only after they have exchanged their message. It would of course be much better to ensure their privacy in advance and not afterwards. To achieve this, Alice and Bob complement the above idea with a second idea, again a very simple one, and one which is entirely classical. Alice and Bob do not use the quantum channel to transmit information, but only to transmit a random sequence of bits, i.e., a key. Now, if the key is unperturbed, then quantum physics guarantees that no one has gotten any information about this key by eavesdropping, i.e., measuring, the quantum communication channel. In this case, Alice and Bob can safely use this key to encode messages. If, on the other hand, the key turns out to be perturbed, then Alice and Bob simply disregard it; since the key does not contain any information, they have not lost any.

Let us make this general idea somewhat more precise, in anticipation of Sec. II.C. In practice, the individual quanta used by Alice and Bob, often called *qubits* (for quantum bits), are encoded in individual photons; for example, vertical and horizontal polarization code for bit values 0 and 1, respectively. The second basis can then be the diagonal one ($\pm 45°$ linear polarization), with $+45°$ coding for bit 1 and $-45°$ for bit 0, respectively (see Fig. 1). Alternatively, the circular polarization basis could be used as second basis. For photons the quantum communication channel can be either free space (see Sec. IV.E) or optical fibers—special fibers or the ones used in standard telecommunications (Sec. III.B). The communication channel is thus not really quantum. What is quantum are the information carriers.

Before continuing, we need to see how QC could fit into existing cryptosystems. For this purpose the next section briefly surveys some of the main aspects of modern cryptology.

B. Classical cryptography

Cryptography is the art of rendering a message unintelligible to any unauthorized party. It is part of the broader field of cryptology, which also includes cryptoanalysis, the art of code breaking (for a historical perspective, see Singh, 1999). To achieve this goal, an algorithm (also called a *cryptosystem* or cipher) is used to combine a message with some additional information—known as the key—and produce a *cryptogram*. This technique is known as *encryption*. For a cryptosystem to be secure, it should be impossible to unlock the cryptogram without the key. In practice, this requirement is often weakened so that the system is just extremely difficult to crack. The idea is that the message should remain protected at least as long as the information it contains is valuable. Although confidentiality is the traditional application of cryptography, it is used nowadays to achieve broader objectives, such as authentication, digital signatures, and nonrepudiation (Brassard, 1988).

1. Asymmetrical (public-key) cryptosystems

Cryptosytems come in two main classes—depending on whether Alice and Bob use the same key. Asymmetrical systems involve the use of different keys for encryption and decryption. They are commonly known as *public-key cryptosystems*. Their principle was first proposed in 1976 by Whitfield Diffie and Martin Hellman, who were then at Stanford University. The first actual implementation was then developed by Ronald Rivest, Adi Shamir, and Leonard Adleman of the Massachusetts Institute of Technology in 1978.[4] It is known as RSA and is still widely used. If Bob wants to be able to receive messages encrypted with a public-key cryptosystem, he must first choose a private key, which he keeps secret. Then he computes from this private key a public key, which he discloses to any interested party. Alice uses this public key to encrypt her message. She transmits the encrypted message to Bob, who decrypts it with the private key. Public-key cryptosystems are convenient and have thus become very popular over the last 20 years. The security of the Internet, for example, is partially based on such systems. They can be thought of as a mailbox in which anybody can insert a letter. Only the legitimate owner can then recover it, by opening it with his private key.

[4]According to the British Government, public-key cryptography was originally invented at the Government Communications Headquarters in Cheltenham as early as 1973. For an historical account, see, for example, the book by Simon Singh (1999).

The security of public-key cryptosystems is based on computational complexity. The idea is to use mathematical objects called one-way functions. By definition, it is easy to compute the function $f(x)$ given the variable x, but difficult to reverse the calculation and deduce x from $f(x)$. In the context of computational complexity, the word "difficult" means that the time required to perform a task grows exponentially with the number of bits in the input, while "easy" means that it grows polynomially. Intuitively, it is easy to understand that it takes only a few seconds to work out 67×71, but it takes much longer to find the prime factors of 4757. However, factoring has a "trapdoor," which means that it is easy to do the calculation in the difficult direction provided that you have some additional information. For example, if you were told that 67 was one of the prime factors of 4757, the calculation would be relatively simple. The security of RSA is actually based on the factorization of large integers.

In spite of its elegance, this technique suffers from a major flaw. It has not been possible yet to prove whether factoring is "difficult" or not. This implies that the existence of a fast algorithm for factorization cannot be ruled out. In addition, the discovery in 1994 by Peter Shor of a polynomial algorithm allowing fast factorization of integers with a quantum computer casts additional doubt on the nonexistence of a polynomial algorithm for classical computers.

Similarly, all public-key cryptosystems rely for their security on unproven assumptions, which could themselves be weakened or suppressed by theoretical or practical advances. So far, no one has proved the existence of any one-way function with a trapdoor. In other words, the existence of secure asymmetric cryptosystems is not proven. This poses a serious threat to these cryptosystems.

In a society like ours, where information and secure communication are of the utmost importance, one cannot tolerate such a threat. For instance, an overnight breakthrough in mathematics could make electronic money instantly worthless. To limit such economic and social risks, there is no alternative but to turn to symmetrical cryptosystems. QC has a role to play in such alternative systems.

2. Symmetrical (secret-key) cryptosystems

Symmetrical ciphers require the use of a single key for both encryption and decryption. These systems can be thought of as a safe in which the message is locked by Alice with a key. Bob in turns uses a copy of this key to unlock the safe. The *one-time pad*, first proposed by Gilbert Vernam of AT&T in 1926, belongs to this category. In this scheme, Alice encrypts her message, a string of bits denoted by the binary number m_1, using a randomly generated key k. She simply adds each bit of the message to the corresponding bit of the key to obtain the scrambled text ($s=m_1\oplus k$, where $\oplus$ denotes the binary addition modulo 2 without carry). It is then sent to Bob, who decrypts the message by subtracting the key ($s\ominus k=m_1\oplus k\ominus k=m_1$). Because the bits of the scrambled text are as random as those of the key, they do not contain any information. This cryptosystem is thus provably secure according to information theory (Shannon, 1949). In fact, it is the only provably secure cryptosystem known today.

Although perfectly secure, this system has a problem—it is essential for Alice and Bob to possess a common secret key, which must be at least as long as the message itself. They can only use the key for a single encryption—hence the name "one-time pad." If they used the key more than once, Eve could record all of the scrambled messages and start to build up a picture of the plain texts and thus also of the key. (If Eve recorded two different messages encrypted with the same key, she could add the scrambled texts to obtain the sum of the plain texts: $s_1\oplus s_2=m_1\oplus k\oplus m_2\oplus k=m_1\oplus m_2\oplus k\oplus k=m_1\oplus m_2$, where we use the fact that $\oplus$ is commutative.) Furthermore, the key has to be transmitted by some trusted means, such as a courier, or through a personal meeting between Alice and Bob. This procedure can be complex and expensive, and may even amount to a loophole in the system.

Because of the problem of distributing long sequences of key bits, the one-time pad is currently used only for the most critical applications. The symmetrical cryptosystems in use for routine applications such as e-commerce employ rather short keys. In the case of the Data Encryption Standard (also known as DES, promoted by the United States' National Institute of Standards and Technology), a 56-bit key is combined with the plain text divided into blocks in a rather complicated way, involving permutations and nonlinear functions to produce the cipher text blocks (see Stallings, 1999 for a didactic presentation). Other cryptosystems (e.g., IDEA, The International Data Encryption System, or AES, the Advanced Encryption Standard) follow similar principles. Like asymmetrical cryptosystems, they offer only computational security. However, for a given key length, symmetrical systems are more secure than their asymmetrical counterparts.

In practical implementations, asymmetrical algorithms are used not so much for encryption, because of their slowness, but rather for distribution of session keys for symmetrical cryptosystems such as DES. Because the security of those algorithms is not proven (see Sec. II.B.1), the security of the whole implementation can be compromised. If these algorithms were broken by mathematical advances, QC would constitute the only way to solve the key distribution problem.

3. The one-time pad as "classical teleportation"

The one-time pad has an interesting characteristic. Assume that Alice wants to transfer to Bob a faithful copy of a classical system, without giving any information to Eve about this system. For this purpose Alice and Bob have access only to an insecure classical channel. The operation is possible provided they share an arbitrarily long secret key. Indeed, in principle, Alice

can measure the state of her classical system with arbitrarily high precision and then use the one-time pad to securely communicate this information to Bob, who can then, in principle, reconstruct (a copy of) the classical system. This somewhat artificial use of the one-time pad has an interesting quantum relative (see Sec. II.E).

C. The BB84 protocol

1. Principle

The first protocol for QC was proposed in 1984 by Charles H. Bennett, of IBM and Gilles Brassard, of the University of Montreal, hence the name BB84, as this protocol is now known. They presented their work at an IEEE conference in India, quite unnoticed by the physics community at the term. This underscores the need for collaboration in QC between different communities, with different jargons, habits, and conventions.[5] The interdisciplinary character of QC is the probable reason for its relatively slow start, but it certainly has contributed to the rapid expansion of the field in recent years.

We shall explain the BB84 protocol using the language of spin $\frac{1}{2}$, but clearly any two-level quantum system would do. The protocol uses four quantum states that constitute two bases, for example, the states up $|\uparrow\rangle$, down $|\downarrow\rangle$, left $|\leftarrow\rangle$, and right $|\rightarrow\rangle$. The bases are maximally conjugate in the sense that any pair of vectors, one from each basis, has the same overlap, e.g., $|\langle\uparrow|\leftarrow\rangle|^2 = \frac{1}{2}$. Conventionally, one attributes the binary value 0 to states $|\uparrow\rangle$ and $|\rightarrow\rangle$ and the value 1 to the other two states, and calls the states qubits (for quantum bits). In the first step, Alice sends individual spins to Bob in states chosen at random among the four states (in Fig. 1 the spin states $|\uparrow\rangle$, $|\downarrow\rangle$, $|\rightarrow\rangle$, and $|\leftarrow\rangle$ are identified as the polarization states "horizontal," "vertical," "$+45°$," and "$-45°$," respectively). How she "chooses at random" is a delicate problem in practice (see Sec. III.D), but in principle she could use her free will. The individual spins could be sent all at once or one after the other (much more practical), the only restriction being that Alice and Bob be able to establish a one-to-one correspondence between the transmitted and the received spins. Next, Bob measures the incoming spins in one of the two bases, chosen at random (using a random-number generator independent from that of Alice). At this point, whenever they use the same basis, they get perfectly correlated results. However, whenever they use different bases, they get uncorrelated results. Hence, on average, Bob obtains a string of bits with a 25% error rate; called the *raw key*. This error rate is so high that standard error correction schemes would fail. But in this protocol, as we shall see, Alice and Bob know which bits are perfectly correlated (the ones for which Alice and Bob used the same basis) and which ones are completely uncorrelated (all the other ones). Hence a straightforward error correction scheme is possible: For each bit Bob announces publicly in which basis he measured the corresponding qubit (but he does not tell the result he obtained). Alice then reveals only whether or not the state in which she encoded that qubit is compatible with the basis announced by Bob. If the state is compatible, they keep the bit; if not, they disregard it. In this way about 50% of the bit string is discarded. This shorter key obtained after basis reconciliation is called the *sifted key*.[6] The fact that Alice and Bob use a public channel at some stage of their protocol is very common in cryptoprotocols. This channel does not have to be confidential, only authentic. Hence any adversary Eve can listen to all the communication on the public channel, but she cannot modify it. In practice Alice and Bob may use the same transmission channel to implement both the quantum and the classical channels.

Note that neither Alice nor Bob can decide which key results from the protocol.[7] Indeed, it is the conjunction of both of their random choices that produces the key.

Let us now consider the security of the above ideal protocol (ideal because so far we have not taken into account unavoidable noise in practice, due to technical imperfections). Assume that some adversary Eve intercepts a qubit propagating from Alice to Bob. This is very easy, but if Bob does not receive an expected qubit, he will simply tell Alice to disregard it. Hence Eve only lowers the bit rate (possibly down to zero), but she does not gain any useful information. For real eavesdropping Eve must send a qubit to Bob. Ideally she would like to send this qubit in its original state, keeping a copy for herself.

2. No-cloning theorem

Following Wootters and Zurek (1982) one can easily prove that perfect copying is impossible in the quantum world (see also the anticipatory intuition of Wigner in 1961, as well as Dieks, 1982 and Milonni and Hardies, 1982). Let ψ denote the original state of the qubit, $|b\rangle$ the blank copy,[8] and $|0\rangle \in \mathcal{H}_{QCM}$ the initial state of Eve's "quantum copy machine," where the Hilbert space $\mathcal{H}_{QCM}$ of the quantum cloning machine is arbitrary. The ideal machine would produce

[5]For instance, it is amusing to note that physicists strive to publish in reputable journals, while conference proceedings are of secondary importance. For computer scientists, in contrast, appearance in the proceedings of the best conferences is considered more important, while journal publication is secondary.

[6]This terminology was introduced by Ekert and Huttner in 1994.

[7]Alice and Bob can, however, determine the statistics of the key.

[8]$|b\rangle$ corresponds to the stock of white paper in an everyday photocopy machine. We shall assume that the machine is not empty, a purely theoretical assumption, as is well known.

$$\psi\otimes|b\rangle\otimes|0\rangle\rightarrow\psi\otimes\psi\otimes|f_\psi\rangle, \tag{3}$$

where $|f_\psi\rangle$ denotes the final state of Eve's machine, which might depend on ψ. Accordingly, using obvious notations,

$$|\uparrow,b,0\rangle\rightarrow|\uparrow,\uparrow,f_\uparrow\rangle, \tag{4}$$

and

$$|\downarrow,b,0\rangle\rightarrow|\downarrow,\downarrow,f_\downarrow\rangle. \tag{5}$$

By linearity of quantum dynamics it follows that

$$|\rightarrow,b,0\rangle=\frac{1}{\sqrt{2}}(|\uparrow\rangle+|\downarrow\rangle)\otimes|b,0\rangle \tag{6}$$

$$\rightarrow\frac{1}{\sqrt{2}}(|\uparrow,\uparrow,f_\uparrow\rangle+|\downarrow,\downarrow,f_\downarrow\rangle). \tag{7}$$

But the latter state differs from the ideal copy $|\rightarrow,\rightarrow,f_\rightarrow\rangle$, whatever the states $|f_\psi\rangle$ are.

Consequently, Eve cannot keep a perfect quantum copy, because perfect quantum copy machines cannot exist. The possibility of copying classical information is probably one of the most characteristic features of information in the everyday sense. The fact that quantum states, nowadays often called quantum information, cannot be copied is certainly one of the most specific attributes that make this new kind of information so different and hence so attractive. Actually, this negative capability clearly has its positive side, since it prevents Eve from perfect eavesdropping and hence makes QC potentially secure.

3. Intercept-resend strategy

We have seen that the eavesdropper needs to send a qubit to Bob while keeping a necessarily imperfect copy for herself. How imperfect the copy has to be, according to quantum theory, is a delicate problem that we shall address in Sec. VI. Here, let us develop a simple eavesdropping strategy, called intercept-resend. This simple and even practical attack consists of Eve's measuring each qubit in one of the two bases, precisely as Bob does. Then, she resends to Bob another qubit in the state corresponding to her measurement result. In about half of the cases, Eve will be lucky and choose the basis compatible with the state prepared by Alice. In these cases she resends to Bob a qubit in the correct state, and Alice and Bob will not notice her intervention. However, in the other half of the cases, Eve unluckily uses the basis incompatible with the state prepared by Alice. This necessarily happens, since Eve has no information about Alice's random-number generator (hence the importance of this generator's being truly random). In these cases the qubits sent out by Eve are in states with an overlap of $\frac{1}{2}$ with the correct states. Alice and Bob thus discover her intervention in about half of these cases, since they get uncorrelated results. Altogether, if Eve uses this intercept-resend strategy, she gets 50% information, while Alice and Bob have about a 25% error rate in their sifted key, i.e., after they eliminate the cases in which they used incompatible states, there is still about 25% error. They can thus easily detect the presence of Eve. If, however, Eve applies this strategy to only a fraction of the communication, say 10%, then the error rate will be only $\approx 2.5\%$, while Eve's information will be $\approx 5\%$. The next section explains how Alice and Bob can counter such attacks.

4. Error correction, privacy amplification, and quantum secret growing

At this point in the BB84 protocol, Alice and Bob share a so-called sifted key. But this key contains errors. The errors are caused by technical imperfections, as well as possibly by Eve's intervention. Realistic error rates in the sifted key using today's technology are of the order of a few percent. This contrasts strongly with the 10^{-9} error rate typical in optical communication. Of course, the few-percent error rate will be corrected down to the standard 10^{-9} during the (classical) error correction step of the protocol. In order to avoid confusion, especially among optical communication specialists, Beat Perny from Swisscom and Paul Townsend, then with British Telecommunications (BT), proposed naming the error rate in the sifted key QBER, for quantum bit error rate, to clearly distinguish it from the bit error rate (BER) used in standard communications.

Such a situation, in which legitimate partners share classical information with high but not 100% correlation and with possibly some correlation to a third party, is common to all quantum cryptosystems. Actually, it is also a standard starting point for classical information-based cryptosystems in which one assumes that somehow Alice, Bob, and Eve have random variables α, β, and ϵ, respectively, with a joint probability distribution $P(\alpha,\beta,\epsilon)$. Consequently, the last step in a QC protocol uses classical algorithms, first to correct the errors, and then reduce to Eve's information on the final key, a process called *privacy amplification*.

The first mention of privacy amplification appeared in Bennett, Brassard, and Robert (1988). It was then extended in collaboration with C. Crépeau from the University of Montreal and U. Maurer of ETH, Zürich, respectively (Bennett, Brassard, *et al.* 1995; see also Bennett, Bessette, *et al.*, 1992). Interestingly, this work motivated by QC found applications in standard information-based cryptography (Maurer, 1993; Maurer and Wolf, 1999).

Assume that a joint probability distribution $P(\alpha,\beta,\epsilon)$ exists. Near the end of this section, we shall comment on this assumption. Alice and Bob have access only to the marginal distribution $P(\alpha,\beta)$. From this and from the laws of quantum mechanics, they have to deduce constraints on the complete scenario $P(\alpha,\beta,\epsilon)$; in particular they have to bound Eve's information (see Secs. VI.E and VI.G). Given $P(\alpha,\beta,\epsilon)$, necessary and sufficient

conditions for a positive secret-key rate between Alice and Bob, $S(\alpha,\beta\|\epsilon)$, are not yet known. However, a useful lower bound is given by the difference between Alice and Bob's mutual Shannon information $I(\alpha,\beta)$ and Eve's mutual information (Csiszár and Körner, 1978, and Theorem 1 in Sec. VI.G):

$$S(\alpha,\beta\|\epsilon)\geqslant\max\{I(\alpha,\beta)-I(\alpha,\epsilon),I(\alpha,\beta)-I(\beta,\epsilon)\}. \quad (8)$$

Intuitively, this result states that secure-key distillation (Bennett, Bessette, *et al.*, 1992) is possible whenever Bob has more information than Eve.

The bound (8) is tight if Alice and Bob are restricted to one-way communication, but for two-way communication, secret-key agreement might be possible even when condition (8) is not satisfied (see Sec. II.C.5).

Without discussing any algorithm in detail, let us offer some idea of how Alice and Bob can establish a secret key when condition (8) is satisfied. First, once the sifted key is obtained (i.e., after the bases have been announced), Alice and Bob publicly compare a randomly chosen subset of it. In this way they estimate the error rate [more generally, they estimate their marginal probability distribution $P(\alpha,\beta)$]. These publicly disclosed bits are then discarded. Next, either condition (8) is not satisfied and they stop the protocol or condition (8) is satisfied and they use some standard error correction protocol to get a shorter key without errors.

With the simplest error correction protocol, Alice randomly chooses pairs of bits and announces their XOR value (i.e., their sum modulo 2). Bob replies either "accept" if he has the same XOR value for his corresponding bits, or "reject" if not. In the first case, Alice and Bob keep the first bit of the pair and discard the second one, while in the second case they discard both bits. In reality, more complex and efficient algorithms are used.

After error correction, Alice and Bob have identical copies of a key, but Eve may still have some information about it [compatible with condition (8)]. Alice and Bob thus need to reduce Eve's information to an arbitrarily low value using some privacy amplification protocols. These classical protocols typically work as follows. Alice again randomly chooses pairs of bits and computes their XOR value. But, in contrast to error correction, she does not announce this XOR value. She only announces which bits she chose (e.g., bits number 103 and 537). Alice and Bob then replace the two bits by their XOR value. In this way they shorten their key while keeping it error free, but if Eve has only partial information on the two bits, her information on the XOR value is even less. Assume, for example, that Eve knows only the value of the first bit and nothing about the second one. Then she has no information at all about the XOR value. Also, if Eve knows the value of both bits with 60% probability, then the probability that she correctly guesses the XOR value is only $0.6^2+0.4^2=52\%$. This process would have to be repeated several times; more efficient algorithms use larger blocks (Brassard and Salvail, 1994).

The error correction and privacy amplification algorithms sketched above are purely classical algorithms. This illustrates that QC is a truly interdisciplinary field.

Actually, the above scenario is incomplete. In this presentation, we have assumed that Eve measures her probe before Alice and Bob run the error correction and privacy amplification algorithms, hence that $P(\alpha,\beta,\epsilon)$ exists. In practice this is a reasonable assumption, but in principle Eve could wait until the end of all the protocols and then optimize her measurements accordingly. Such "delayed-choice eavesdropping strategies"[9] are discussed in Sec. VI.

It should by now be clear that QC does not provide a complete solution for all cryptographic purposes.[10] Actually, quite the contrary, QC can only be used as a complement to standard symmetrical cryptosystems. Accordingly, a more precise name for QC is *quantum key distribution*, since this is all QC does. Nevertheless, we prefer to keep the well-known terminology, which lends its name to the title of this review.

Finally, let us emphasize that every key distribution system must incorporate some authentication scheme: the two parties must identify themselves. If not, Alice could actually be communicating directly with Eve. A straightforward approach is for Alice and Bob initially to share a short secret. Then QC provides them with a longer one and they each keep a small portion for authentication at the next session (Bennett, Bessette, *et al.*, 1992). From this perspective, QC is a *quantum secret-growing* protocol.

5. Advantage distillation

QC has motivated and still motivates research in classical information theory. The best-known example is probably the development of privacy amplification algorithms (Bennett *et al.*, 1988, 1995). This in turn led to the development of new cryptosystems based on weak but classical signals, emitted for instance by satellites (Maurer, 1993).[11] These new developments required secret-key agreement protocols that could be used even when condition (8) did not apply. Such protocols, called *advantage distillation*, necessarily use two-way communication and are much less efficient than privacy amplification. Usually, they are not considered in the literature on QC, but conceptually they are remarkable from at least two points of view. First, it is somewhat surprising that secret-key agreement is possible even if Alice and Bob start with less mutual (Shannon) information than Eve. They can take advantage of the authenticated public

[9]Note, however, that Eve has to choose the interaction between her probe and the qubits before the public discussion phase of the protocol.

[10]For a while it was thought that *bit commitment* (see, for example, Brassard, 1988), a powerful primitive in cryptology, could be realized using quantum principles. However, Dominic Mayers (1996a, 1997) and Lo and Chau (1998) proved it to be impossible (see also Brassard *et al.*, 1998).

[11]Note that here confidentiality is not guaranteed by the laws of physics, but relies on the assumption that Eve's technology is limited, e.g., her antenna is finite, and her detectors have limited efficiencies.

channel to decide which series of realizations to keep, whereas Eve cannot influence this process[12] (Maurer, 1993; Maurer and Wolf, 1999).

Recently, a second remarkable feature of advantage distillation, connecting quantum and classical secret-key agreement, has been discovered (assuming one uses the Ekert protocol described in Sec. II.D.3): If Eve follows a strategy that optimizes her Shannon information, under the assumption that she attacks the qubits one at a time (the so-called individual attack; see Sec. VI.E), then Alice and Bob can use advantage distillation if and only if Alice and Bob's qubits are still entangled (they can thus use quantum privacy amplification; Deutsch *et al.*, 1996; Gisin and Wolf, 1999). This connection between the concept of *entanglement*, central to quantum information theory, and the concept of *intrinsic classical information*, central to classical information-based cryptography (Maurer and Wolf, 1999), has been shown to be general (Gisin and Wolf, 2000). The connection seems to extend even to *bound entanglement* (Gisin *et al.*, 2000).

D. Other protocols

1. Two-state protocol

In 1992 Bennett noticed that four states are more than are really necessary for QC: only two nonorthogonal states are needed. Indeed the security of QC relies on the inability of an adversary to distinguish unambiguously and without perturbation between the different states that Alice may send to Bob; hence two states are necessary, and if they are incompatible (i.e., not mutually orthogonal), then two states are also sufficient (Bennett, 1992). This is a conceptually important clarification. It also made several of the first experimental demonstrations easier (as is discussed further in Sec. IV.D). But in practice, it is not a good solution. Indeed, although two nonorthogonal states cannot be distinguished unambiguously without perturbation, one can unambiguously distinguish between them at the cost of some losses (Ivanovic, 1987; Peres, 1988). This possibility has been demonstrated in practice (Huttner, Gautier, *et al.*, 1996; Clarke *et al.*, 2000). Alice and Bob would have to monitor the attenuation of the quantum channel (and even this would not be entirely safe if Eve were able to replace the channel by a more transparent one; see Sec. VI.H). The two-state protocol can also be implemented using interference between a macroscopic bright pulse and a dim pulse with less than one photon on average (Bennett, 1992). The presence of the bright pulse makes this protocol especially resistant to eavesdropping, even in settings with high attenuation. Bob can monitor the bright pulses to make sure that Eve does not remove any. In this case, Eve cannot eliminate the dim pulse without revealing her presence, because the interference of the bright pulse with vacuum would introduce errors. A practical implementation of this so-called 892 protocol is discussed in Sec. IV.D. Huttner *et al.* extended this reference-beam monitoring to the four-state protocol in 1995.

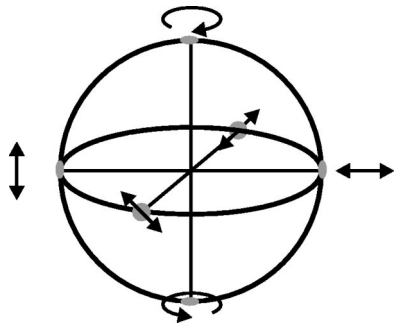

FIG. 2. Poincaré sphere with a representation of six states that can be used to implement the generalization of the BB84 protocol.

2. Six-state protocol

While two states are enough and four states are standard, a six-state protocol better respects the symmetry of the qubit state space; see Fig. 2 (Bruss, 1998; Bechmann-Pasquinucci and Gisin, 1999). The six states constitute three bases, hence the probability that Alice and Bob choose the same basis is only $\frac{1}{3}$, but the symmetry of this protocol greatly simplifies the security analysis and reduces Eve's optimal information gain for a given error rate QBER. If Eve measures every photon, the QBER is 33%, compared to 25% in the case of the BB84 protocol.

3. Einstein-Podolsky-Rosen protocol

This variation of the BB84 protocol is of special conceptual, historical, and practical interest. The idea is due to Artur Ekert (1991) of Oxford University, who, while elaborating on a suggestion of David Deutsch (1985), discovered QC independently of the BB84 paper. Intellectually, it is very satisfying to see this direct connection to the famous EPR paradox (Einstein, Podolski, and Rosen, 1935): the initially philosophical debate turned to theoretical physics with Bell's inequality (1964), then to experimental physics (Freedmann and Clauser, 1972; Fry and Thompson, 1976; Aspect *et al.*, 1982), and is now—thanks to Ekert's ingenious idea—part of applied physics.

The idea consists in replacing the quantum channel carrying two qubits from Alice to Bob by a channel carrying two qubits from a common source, one qubit to

[12]The idea is that Alice picks out several instances in which she got the same bit and communicates the instances—but not the bit—to Bob. Bob replies yes only if it happens that for all these instances he also has the same bit value. For high error rates this is unlikely, but when it does happen there is a high probability that both have the same bit. Eve cannot influence the choice of the instances. All she can do is use a majority vote for the cases accepted by Bob. The probability that Eve makes an error can be much higher than the probability that Bob makes an error (i.e., that all his instances are wrong), even if Eve has more initial information than Bob.

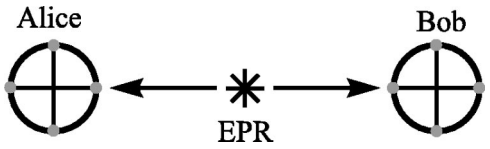

FIG. 3. Einstein-Podolsky-Rosen (EPR) protocol, with the source and a Poincaré representation of the four possible states measured independently by Alice and Bob.

Alice and one to Bob. A first possibility would be that the source always emits the two qubits in the same state chosen randomly among the four states of the BB84 protocol. Alice and Bob would then both measure their qubit in one of the two bases, again chosen independently and randomly. The source then announces the bases, and Alice and Bob keep the data only when they happen to have made their measurements in the compatible basis. If the source is reliable, this protocol is equivalent to that of BB84: It is as if the qubit propagates backwards in time from Alice to the source, and then forward to Bob. But better than trusting the source, which could be in Eve's hand, the Ekert protocol assumes that the two qubits are emitted in a maximally entangled state like

$$\phi^+ = \frac{1}{\sqrt{2}}(|\uparrow,\uparrow\rangle + |\downarrow,\downarrow\rangle). \tag{9}$$

Then, when Alice and Bob happen to use the same basis, either the x basis or the y basis, i.e., in about half of the cases, their results are identical, providing them with a common key. Note the similarity between the one-qubit BB84 protocol illustrated in Fig. 1 and the two-qubit Ekert protocol of Fig. 3. The analogy can be made even stronger by noting that for all unitary evolutions U_1 and U_2, the following equality holds:

$$U_1 \otimes U_2 \Phi^{(+)} = \mathbb{1} \otimes U_2 U_1^t \Phi^{(+)}, \tag{10}$$

where U_1^t denotes the transpose.

In his 1991 paper Ekert suggested basing the security of this two-qubit protocol on Bell's inequality, an inequality which demonstrates that some correlations predicted by quantum mechanics cannot be reproduced by any local theory (Bell, 1964). To do this, Alice and Bob can use a third basis (see Fig. 4). In this way the probability that they might happen to choose the same basis is reduced from $\frac{1}{2}$ to $\frac{2}{9}$, but at the same time as they establish a key, they collect enough data to test Bell's inequality.[13] They can thus check that the source really emits the entangled state (9) and not merely product states. The following year Bennett, Brassard, and Mermin (1992) criticized Ekert's letter, arguing that the violation of Bell's inequality is not necessary for the security of QC and emphasizing the close connection between the Ekert and the BB84 schemes. This criticism might be missing an important point. Although the exact relation between security and Bell's inequality is not yet fully known, there are clear results establishing fascinating connections (see Sec. VI.F). In October 1992, an article by Bennett, Brassard, and Ekert demonstrated that the founding fathers of QC were able to join forces to develop the field in a pleasant atmosphere (Bennett, Brassard, and Ekert, 1992).

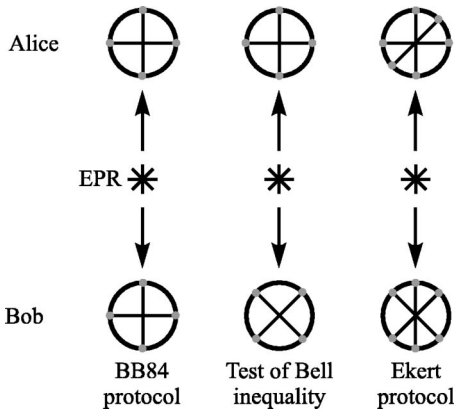

FIG. 4. Illustration of protocols exploiting EPR quantum systems. To implement the BB84 quantum cryptographic protocol, Alice and Bob use the same bases to prepare and measure their particles. A representation of their states on the Poincaré sphere is shown. A similar setup, but with Bob's bases rotated by 45°, can be used to test the violation of Bell's inequality. Finally, in the Ekert protocol, Alice and Bob may use the violation of Bell's inequality to test for eavesdropping.

4. Other variations

There is a large collection of variations on the BB84 protocol. Let us mention a few, chosen somewhat arbitrarily. First, one can assume that the two bases are not chosen with equal probability (Ardehali *et al.*, 1998). This has the nice consequence that the probability that Alice and Bob choose the same basis is greater than $\frac{1}{2}$, thus increasing the transmission rate of the sifted key. However, this protocol makes Eve's job easier, as she is more likely to guess correctly the basis that was used. Consequently, it is not clear whether the final key rate, after error correction and privacy amplification, is higher or not.

Another variation consists in using quantum systems of dimension greater than 2 (Bechmann-Pasquinucci and Peres, 2000; Bechmann-Pasquinucci and Tittel, 2000; Bourennane, Karlsson, and Björn, 2001). Again, the practical value of this idea has not yet been fully determined.

A third variation worth mentioning is due to Goldenberg and Vaidman of Tel Aviv University (1995). They suggested preparing the qubits in a superposition of two spatially separated states, then sending one component of this superposition and waiting until Bob receives it before sending the second component. This does not

[13]A maximal violation of Bell's inequality is necessary to rule out tampering by Eve. In this case, the QBER must necessarily be equal to zero. With a nonmaximal violation, as typically obtained in experimental systems, Alice and Bob can distill a secure key using error correction and privacy amplification.

sound of great practical value, but has the nice conceptual feature that the minimal two states do not need to be mutually orthogonal.

E. Quantum teleportation as a "quantum one-time pad"

Since its discovery in 1993 by a surprisingly large group of physicists, quantum teleportation (Bennett *et al.*, 1993) has received much attention from both the scientific community and the general public. The dream of beaming travelers through the universe is exciting, but completely out of the realm of any foreseeable technology. However, quantum teleportation can be seen as the fully quantum version of the one-time pad (see Sec. II.B.3), hence as the ultimate form of QC. As in "classical teleportation," let us assume that Alice aims to transfer a faithful copy of a quantum system to Bob. If Alice has full knowledge of the quantum state, the problem is not really a quantum one (Alice's information is classical). If, on the other hand, Alice does not know the quantum state, she cannot send a copy, since quantum copying is impossible according to quantum physics (see Sec. II.C.2). Nor can she send classical instructions, since this would allow the production of many copies. However, if Alice and Bob share arbitrarily many entangled qubits, sometimes called a quantum key, and share a classical communication channel, then the quantum teleportation protocol provides them with a means of transferring the quantum state of the system from Alice to Bob. In the course of running this protocol, Alice's quantum system is destroyed without Alice's having learned anything about the quantum state, while Bob's qubit ends in a state isomorphic to the state of the original system (but Bob does not learn anything about the quantum state). If the initial quantum system is a quantum message coded in the form of a sequence of qubits, then this quantum message is faithfully and securely transferred to Bob, without any information leaking to the outside world (i.e., to anyone not sharing the prior entanglement with Alice and Bob). Finally, the quantum message could be formed of a four-letter quantum alphabet consisting of the four states of the BB84 protocol. With futuristic but not impossible technology, Alice and Bob could keep their entangled qubits in their respective wallets and could enjoy totally secure communication at any time, without even having to know where the other is located (provided they can communicate classically).

F. Optical amplification, quantum nondemolition measurements, and optimal quantum cloning

After almost every general talk on QC, two questions arise: What about optical amplifiers? and What about quantum nondemolition measurements? In this section we briefly address these questions.

Let us start with the second one, as it is the easiest. The term "quantum nondemolition measurement" is simply confusing. There is nothing like a quantum measurement that does not perturb (i.e., modify) the quantum state, except if the state happens to be an eigenstate of the observable. Hence, if for some reason one conjectures that a quantum system is in some state (or in a state among a set of mutually orthogonal ones), one can in principle test this conjecture repeatedly (Braginsky and Khalili, 1992). However, if the state is only restricted to be in a finite set containing nonorthogonal states, as in QC, then there is no way to perform a measurement without "demolishing" (perturbing) the state. Now, in QC the term "nondemolition measurement" is also used with a different meaning: one measures the number of photons in a pulse without affecting the degree of freedom coding the qubit (e.g., the polarization; see Sec. VI.H), or one detects the presence of a photon without destroying it (Nogues *et al.*, 1999). Such measurements are usually called *ideal measurements*, or *projective measurements*, because they produce the least possible perturbation (Piron, 1990) and because they can be represented by projectors. It is important to stress that these "ideal measurements" do not invalidate the security of QC.

Let us now consider optical amplifiers (a laser medium, but without mirrors, so that amplification takes place in a single pass; see Desurvire, 1994). They are widely used in today's optical communication networks. However, they are of no use for quantum communication. Indeed, as seen in Sec. II.C, the copying of quantum information is impossible. Here we illustrate this characteristic of quantum information by the example of optical amplifiers: the necessary presence of spontaneous emission whenever there is stimulated emission prevents perfect copying. Let us clarify this important and often confusing point, following the work of Simon *et al.* (1999, 2000; see also De Martini *et al.*, 2000 and Kempe *et al.*, 2000). Let the two basic qubit states $|0\rangle$ and $|1\rangle$ be physically implemented by two optical modes: $|0\rangle \equiv |1,0\rangle$ and $|1\rangle \equiv |0,1\rangle$. Thus $|n,m\rangle_{ph} \otimes |k,l\rangle_a$ denotes the state of n photons in mode 1 and m photons in mode 2, while $k,l = 0(1)$ denotes the ground (or excited) state of two-level atoms coupled to mode 1 or 2, respectively. Hence spontaneous emission corresponds to

$$|0,0\rangle_{ph} \otimes |1,0\rangle_a \rightarrow |1,0\rangle_{ph} \otimes |0,0\rangle_a , \tag{11}$$

$$|0,0\rangle_{ph} \otimes |0,1\rangle_a \rightarrow |0,1\rangle_{ph} \otimes |0,0\rangle_a , \tag{12}$$

and stimulated emission to

$$|1,0\rangle_{ph} \otimes |1,0\rangle_a \rightarrow \sqrt{2}|2,0\rangle_{ph} \otimes |0,0\rangle_a , \tag{13}$$

$$|0,1\rangle_{ph} \otimes |0,1\rangle_a \rightarrow \sqrt{2}|0,2\rangle_{ph} \otimes |0,0\rangle_a , \tag{14}$$

where the factor of $\sqrt{2}$ takes into account the ratio of stimulated to spontaneous emission. Let the initial state of the atom be a mixture of the following two states, each with equal (50%) weight:

$$|0,1\rangle_a \text{ and } |1,0\rangle_a . \tag{15}$$

By symmetry, it suffices to consider one possible initial state of the qubit, e.g., one photon in the first mode $|1,0\rangle_{ph}$. The initial state of the photon+atom system is thus a mixture:

$$|1,0\rangle_{ph}\otimes|1,0\rangle_a \quad \text{or} \quad |1,0\rangle_{ph}\otimes|0,1\rangle_a . \tag{16}$$

This corresponds to the first-order term in an evolution with a Hamiltonian (in the interaction picture): $H=\chi(a_1^\dagger\sigma_1^- + a_1\sigma_1^\dagger + a_2^\dagger\sigma_2^- + a_2\sigma_2^\dagger)$. After some time the two-photon component of the evolved states becomes

$$\sqrt{2}|2,0\rangle_{ph}\otimes|0,0\rangle_a \quad \text{or} \quad |1,1\rangle_{ph}\otimes|0,0\rangle_a . \tag{17}$$

The correspondence with a pair of spin $\frac{1}{2}$ goes as follows:

$$|2,0\rangle=|\uparrow\uparrow\rangle, \quad |0,2\rangle=|\downarrow\downarrow\rangle, \tag{18}$$

$$|1,1\rangle_{ph}=\psi^{(+)}=\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle+|\downarrow\uparrow\rangle). \tag{19}$$

Tracing over the amplifier (i.e., the two-level atom), an (ideal) amplifier achieves the following transformation:

$$P_\uparrow \rightarrow 2P_{\uparrow\uparrow}+P_{\psi^{(+)}}, \tag{20}$$

where the P's indicate projectors (i.e., pure-state density matrices) and the lack of normalization results from the first-order expansion used in Eqs. (11)–(14). Accordingly, after normalization, each photon is in the state

$$\mathrm{Tr}_{1-ph\ mode}\left(\frac{2P_{\uparrow\uparrow}+P_{\psi^{(+)}}}{3}\right)=\frac{2P_\uparrow+\frac{1}{2}\mathbb{1}}{3}. \tag{21}$$

The corresponding fidelity is

$$F=\frac{2+\frac{1}{2}}{3}=\frac{5}{6}, \tag{22}$$

which is precisely the optimal fidelity compatible with quantum mechanics (Bužek and Hillery, 1996; Gisin and Massar, 1997; Bruss *et al.*, 1998). In other words, if we start with a single photon in an arbitrary state and pass it through an amplifier, then due to the effect of spontaneous emission the fidelity of the state exiting the amplifier, when it consists of exactly two photons, with the initial state will be equal to at most 5/6. Note that if it were possible to make better copies, then signaling at arbitrarily fast speed, using EPR correlations between spatially separated systems, would also be possible (Gisin, 1998).

III. TECHNOLOGICAL CHALLENGES

The very first demonstration of QC was a table-top experiment performed at the IBM laboratory in the early 1990s over a distance of 30 cm (Bennett, Bessette, *et al.*, 1992), marking the start of a series of impressive experimental improvements over the past few years. The 30-cm distance is of little practical interest. Either the distance should be even shorter [think of a credit card and an ATM machine (Huttner, Imoto, and Barnett, 1996), in which case all of Alice's components should fit on the credit card—a nice idea, but still impractical with present technology] or the distance should be much longer, at least in the kilometer range. Most of the research so far uses optical fibers to guide the photons from Alice to Bob, and we shall mainly concentrate on such systems here. There is also, however, some very significant research on free-space systems (see Sec. IV.E).

Once the medium has been chosen, there remain the questions of the source and detectors. Since they have to be compatible, the crucial choice is that of the wavelength. There are two main possibilities. Either one chooses a wavelength around 800 nm, for which efficient photon counters are commercially available, or one chooses a wavelength compatible with today's telecommunications optical fibers, i.e., near 1300 or 1550 nm. The first choice requires free-space transmission or the use of special fibers, hence the installed telecommunications networks cannot be used. The second choice requires the improvement or development of new detectors, not based on silicon semiconductors, which are transparent above a wavelength of 1000 nm.

In the case of transmission using optical fibers, it is still unclear which of the two alternatives will turn out to be the best choice. If QC finds niche markets, it is conceivable that special fibers will be installed for that purpose. But it is equally conceivable that new commercial detectors will soon make it much easier to detect single photons at telecommunications wavelengths. Actually, the latter possibility is very likely, as several research groups and industries are already working on it. There is another good reason to bet on this solution: the quality of telecommunications fibers is much higher than that of any special fiber; in particular, the attenuation is much lower (this is why the telecommunications industry chose these wavelengths): at 800 nm, the attenuation is about 2 dB/km (i.e., half the photons are lost after 1.5 km), while it is only of the order of 0.35 and 0.20 dB/km at 1300 and 1550 nm, respectively (50% loss after about 9 and 15 km).[14]

In the case of free-space transmission, the choice of wavelength is straightforward, since the region where good photon detectors exist—around 800 nm—coincides with that where absorption is low. However, free-space transmission is restricted to line-of-sight links and is very weather dependent.

In the next sections we successively consider the questions of how to produce single photons (Sec. III.A), how to transmit them (Sec. III.B), how to detect single photons (Sec. III.C), and finally how to exploit the intrinsic randomness of quantum processes to build random generators (Sec. III.D).

A. Photon sources

Optical quantum cryptography is based on the use of single-photon Fock states. Unfortunately, these states are difficult to realize experimentally. Nowadays, practical implementations rely on faint laser pulses or entangled photon pairs, in which both the photon and the photon-pair number distribution obey Poisson statistics.

[14]The losses in dB (l_{db}) can be calculated from the losses in percent ($l_{\%}$): $l_{dB}=-10\log_{10}[1-(l_{\%}/100)]$.

Hence both possibilities suffer from a small probability of generating more than one photon or photon pair at the same time. For large losses in the quantum channel, even small fractions of these multiphotons can have important consequences on the security of the key (see Sec. VI.H), leading to interest in "photon guns"; see Sec. III.A.3). In this section we briefly comment on sources based on faint pulses as well as on entangled photon pairs, and we compare their advantages and drawbacks.

1. Faint laser pulses

There is a very simple solution to approximate single-photon Fock states: coherent states with an ultralow mean photon number μ. They can easily be realized using only standard semiconductor lasers and calibrated attenuators. The probability of finding n photons in such a coherent state follows the Poisson statistics:

$$P(n,\mu)=\frac{\mu^n}{n!}e-\mu. \tag{23}$$

Accordingly, the probability that a nonempty weak coherent pulse contains more than one photon,

$$P(n>1|n>0,\mu)=\frac{1-P(0,\mu)-P(1,\mu)}{1-P(0,\mu)}$$

$$=\frac{1-e^{-\mu}(1+\mu)}{1-e^{-\mu}}\cong\frac{\mu}{2}, \tag{24}$$

can be made arbitrarily small. Weak pulses are thus extremely practical and have indeed been used in the vast majority of experiments. However, they have one major drawback. When μ is small, most pulses are empty: $P(n=0)\approx 1-\mu$. In principle, the resulting decrease in bit rate could be compensated for thanks to the achievable gigahertz modulation rates of telecommunications lasers. But in practice, the problem comes from the detectors' dark counts (i.e., a click without a photon's arriving). Indeed, the detectors must be active for all pulses, including the empty ones. Hence the total dark counts increase with the laser's modulation rate, and the ratio of detected photons to dark counts (i.e., the signal-to-noise ratio) decreases with μ (see Sec. IV.A). The problem is especially severe for longer wavelengths, at which photon detectors based on indium gallium arsenide semiconductors (InGaAs) are needed (see Sec. III.C), since the noise of these detectors explodes if they are opened too frequently (in practice with a rate larger than a few megahertz). This prevents the use of really low photon numbers, smaller than approximately 1%. Most experiments to date have relied on $\mu=0.1$, meaning that 5% of the nonempty pulses contain more than one photon. However, it is important to stress that, as pointed out by Lütkenhaus (2000), there is an optimal μ depending on the transmission losses.[15] After key distillation, the security is just as good with faint laser pulses as with Fock states. The price to pay for using such states is a reduction of the bit rate.

2. Photon pairs generated by parametric downconversion

Another way to create pseudo-single-photon states is the generation of photon pairs and the use of one photon as a trigger for the other one (Hong and Mandel, 1986). In contrast to the sources discussed earlier, the second detector must be activated only whenever the first one has detected a photon, hence when $\mu=1$, and not whenever a pump pulse has been emitted, therefore circumventing the problem of empty pulses.

The photon pairs are generated by spontaneous parametric downconversion in a $\chi^{(2)}$ nonlinear crystal.[16] In this process, the inverse of the well-known frequency doubling, one photon spontaneously splits into two daughter photons—traditionally called signal and idler photons—conserving total energy and momentum. In this context, momentum conservation is called phase matching and can be achieved despite chromatic dispersion by exploiting the birefringence of the nonlinear crystal. Phase matching allows one to choose the wavelength and determines the bandwidth of the downconverted photons. The latter is in general rather large and varies from a few nanometers up to some tens of nanometers. For the nondegenerate case one typically gets a bandwith of 5–10 nm, whereas in the degenerate case (where the central frequency of both photons is equal), the bandwidth can be as large as 70 nm.

This photon-pair creation process is very inefficient; typically it takes some 10^{10} pump photons to create one pair in a given mode.[17] The number of photon pairs per mode is thermally distributed within the coherence time of the photons and follows a Poissonian distribution for larger time windows (Walls and Milburn, 1995). With a pump power of 1 mW, about 10^6 pairs per second can be collected in single-mode fibers. Accordingly, in a time window of roughly 1 ns, the conditional probability of finding a second pair, having already detected one, is $10^6\times 10^{-9}\approx 0.1\%$. In the case of continuous pumping, this time window is given by the detector resolution. Tolerating, for example, 1% of these multipair events, one can generate 10^7 pairs per second using a realistic

[15]Contrary to a frequent misconception, there is nothing special about a μ value of 0.1, even though it has been selected by most experimentalists. The optimal value—i.e., the value that yields the highest key exchange rate after distillation—depends on the optical losses in the channel and on assumptions about Eve's technology (see Secs. VI.H and VI.I).

[16]For a review see Rarity and Tapster (1988), and for more recent developments see Kwiat *et al.* (1999), Tittel *et al.* (1999), Jennewein, Simon, *et al.* (2000), and Tanzilli *et al.* (2001).

[17]Recently we achieved a conversion rate of 10^{-6} using an optical waveguide in a periodically poled $LiNbO_3$ crystal (Tanzilli *et al.*, 2001).

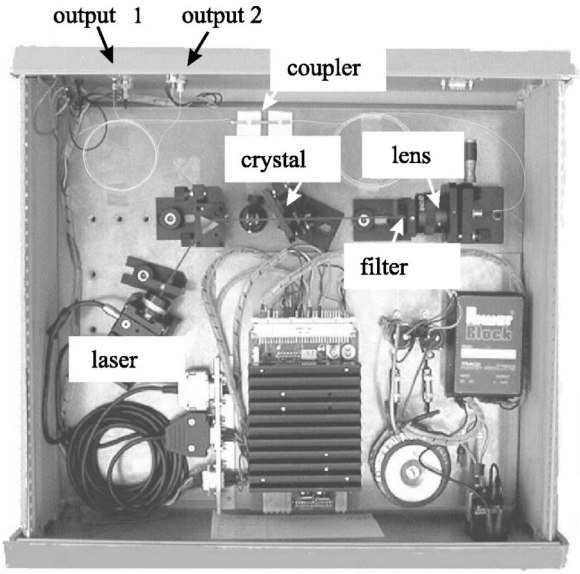

FIG. 5. Photo of our entangled photon-pair source as used in the first long-distance test of Bell's inequalities (Tittel *et al.*, 1998). Note that the whole source fits into a box only $40\times45\times15$ cm^3 in size and that neither a special power supply nor water cooling is necessary.

10-mW pump. To detect, for example, 10% of the trigger photons, the second detector has to be activated 10^6 times per second. In comparison, the example of 1% of multiphoton events corresponds in the case of faint laser pulses to a mean photon number of $\mu=0.02$. In order to get the same number (10^6) of nonempty pulses per second, a pulse rate of 50 MHz is needed. For a given photon statistics, photon pairs thus allow one to work with lower pulse rates (e.g., 50 times lower) and hence reduced detector-induced errors. However, due to limited coupling efficiency in optical fibers, the probability of finding the sister photon after detection of the trigger photon in the respective fiber is in practice less than 1. This means that the effective photon number is not 1 but rather $\mu\approx2/3$ (Ribordy *et al.*, 2001), still well above $\mu=0.02$.

Photon pairs generated by parametric downconversion offer a further major advantage if they are not merely used as a pseudo-single-photon source, but if their entanglement is exploited. Entanglement leads to quantum correlations that can be used for key generation (see Secs. II.D.3 and V). In this case, if two photon pairs are emitted within the same time window but their measurement basis is chosen independently, they produce completely uncorrelated results. Hence, depending on the realization, the problem of multiple photons can be avoided; see Sec. VI.J.

Figure 5 shows one of our sources creating entangled photon pairs at a wavelength of 1310 nm, as used in tests of Bell's inequalities over 10 kilometers (Tittel *et al.*, 1998). Although not as simple as faint laser sources, diode-pumped photon-pair sources emitting in the near infrared can be made compact, robust, and rather handy.

3. Photon guns

The ideal single-photon source is a device that, when one pulls the trigger, and only then, emits one and only one photon. Hence the name *photon gun*. Although photon antibunching was first demonstrated years ago (Kimble *et al.*, 1977), a practical and handy device is still awaited. At present, there are essentially three different experimental approaches that more or less come close to this ideal.

A first idea is to work with a single two-level quantum system that obviously cannot emit two photons at a time. The manipulation of single trapped atoms or ions requires a much too involved technical effort. Single organic dye molecules in solvents (Kitson *et al.*, 1998) or solids (Brunel *et al.*, 1999; Fleury *et al.*, 2000) are easier to handle but offer only limited stability at room temperature. A promising candidate, however, is the nitrogen-vacancy center in diamond, a substitutional nitrogen atom with a vacancy trapped at an adjacent lattice position (Brouri *et al.*, 2000; Kurtsiefer *et al.*, 2000). It is possible to excite individual nitrogen atoms with a 532-nm laser beam, which will subsequently emit a fluorescence photon around 700 nm (12-ns decay time). The fluorescence exhibits strong photon antibunching, and the samples are stable at room temperature. However, the big remaining experimental challenge is to increase the collection efficiency (currently about 0.1%) in order to obtain mean photon numbers close to 1. To obtain this efficiency, an optical cavity or a photonic band-gap structure must suppress emission in all spatial modes but one. In addition, the spectral bandwidth of this type of source is broad (on the order of 100 nm), enhancing the effect of perturbations in a quantum channel.

A second approach is to generate photons by single electrons in a mesoscopic *p-n* junction. The idea is to profit from the fact that thermal electrons show antibunching (the Pauli exclusion principle) in contrast to photons (Imamoglu and Yamamoto, 1994). The first experimental results have been presented (Kim *et al.*, 1999), but with extremely low efficiencies and only at a temperature of 50 mK!

Finally, another approach is to use the photon emission of electron-hole pairs in a semiconductor quantum dot. The frequency of the emitted photon depends on the number of electron-hole pairs present in the dot. After one creates several such pairs by optical pumping, they will sequentially recombine and hence emit photons at different frequencies. Therefore, a single-photon pulse can be obtained by spectral filtering (Gérard *et al.*, 1999; Michler *et al.*, 2000; Santori *et al.*, 2000). These dots can be integrated in solid-state microcavities with strong enhancements of spontaneous emission (Gérard *et al.*, 1998).

In summary, today's photon guns are still too complicated to be used in a QC prototype. Moreover, due to their low quantum efficiencies, they do not offer an advantage over faint laser pulses with extremely low mean photon numbers μ.

B. Quantum channels

The single-photon source and the detectors must be connected by a "quantum channel." Such a channel is not especially quantum, except that it is intended to carry information encoded in individual quantum systems. Here "individual" does not mean "nondecomposible," but only the opposite of "ensemble." The idea is that the information is coded in a physical system only once, in contrast to classical communication, in which many photons carry the same information. Note that the present-day limit for fiber-based classical optical communication is already down to a few tens of photons, although in practice one usually uses many more. With increasing bit rate and limited mean power—imposed to avoid nonlinear effects in silica fibers—these figures are likely to get closer and closer to the quantum domain.

Individual quantum systems are usually two-level systems, called qubits. During their propagation they must be protected from environmental noise. Here "environment" refers to everything outside the degree of freedom used for the encoding, which is not necessarily outside the physical system. If, for example, the information is encoded in the polarization state, then the optical frequencies of the photon are part of the environment. Hence coupling between the polarization and the optical frequency has to be mastered[18] (e.g., by avoiding wavelength-sensitive polarizers and birefringence). Moreover, the sender of the qubits should avoid any correlation between the polarization and the spectrum of the photons.

Another difficulty is that the bases used by Alice to code the qubits and the bases used by Bob for his measurements must be related by a known and stable unitary transformation. Once this unitary transformation is known, Alice and Bob can compensate for it and get the expected correlation between their preparations and measurements. If it changes with time, they need active feedback to track it, and if the changes are too fast, the communication must be interrupted.

1. Single-mode fibers

Light is guided in optical fibers thanks to the refractive index profile $n(x,y)$ across the section of the fibers (traditionally, the z axis is along the propagation direction). Over the last 25 years, a lot of effort has gone into reducing transmission losses—initially several dB per km—and today the attenuation is as low as 2 dB/km at 800-nm wavelength, 0.35 dB/km at 1310 nm, and 0.2 dB/km at 1550 nm (see Fig. 6). It is amusing to note that the dynamical equation describing optical pulse propagation (in the usual slowly varying envelope aproximation) is identical to the Schrödinger equation, with $V(x,y)=-n(x,y)$ (Snyder, 1983). Hence a positive bump in the refractive index corresponds to a potential well. The region of the well is called the fiber core. If the core is large, many bound modes exist, corresponding to many guided modes in the fiber. Such fibers are called multimode fibers, They usually have cores 50 μm in diameter. The modes couple easily, acting on the qubit like a nonisolated environment. Hence multimode fibers are not appropriate as quantum channels (see, however, Townsend, 1998a, 1998b). If, however, the core is small enough (diameter of the order of a few wavelengths), then a single spatial mode is guided. Such fibers are called single-mode fibers. For telecommunications wavelengths (i.e., 1.3 and 1.5 μm), their core is typically 8 μm in diameter. Single-mode fibers are very well suited to carry single quanta. For example, the optical phase at the output of a fiber is in a stable relation with the phase at the input, provided the fiber does not become elongated. Hence fiber interferometers are very stable, a fact exploited in many instruments and sensors (see, for example, Cancellieri, 1993).

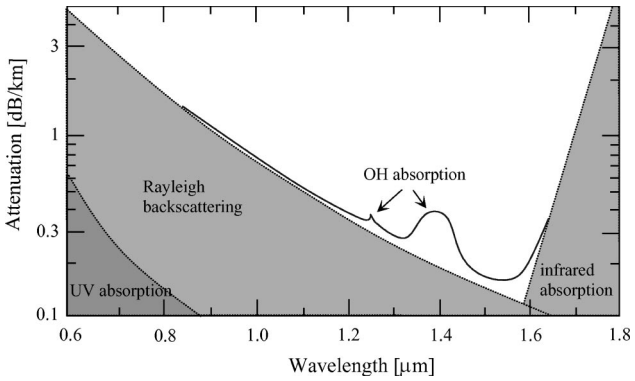

FIG. 6. Transmission losses vs wavelength in optical fibers. Electronic transitions in SiO_2 lead to absorption at lower wavelengths, and excitation of vibrational modes leads to losses at higher wavelengths. Superposed is the absorption due to Rayleigh backscattering and to transitions in OH groups. Modern telecommunications are based on wavelengths around 1.3 μm (the second telecommunications window) and 1.5 μm (the third telecommunications window).

Accordingly, a single-mode fiber with perfect cylindric symmetry would provide an ideal quantum channel. But all real fibers have some asymmetries, so that the two polarization modes are no longer degenerate, but rather each has its own propagation constant. A similar effect is caused by chromatic dispersion, in which the group delay depends on the wavelength. Both dispersion effects are the subject of the next subsections.

2. Polarization effects in single-mode fibers

Polarization effects in single-mode fibers are a common source of problems in all optical communication schemes, classical as well as quantum ones. In recent years these effects have been the subject of a major research effort in classical optical communication (Gisin *et al.*, 1995). As a result, today's fibers are much better than the fibers of a decade ago. Today, the remaining birefringence is small enough for the telecommunications industry, but for quantum communication any

[18]Note that, as we shall see in Sec. V, using entangled photons prevents such information leakage.

birefringence, even extremely small, will always remain a concern. All fiber-based implementations of QC have to face this problem. This is clearly true for polarization-based systems, but it is equally a concern for phase-based systems, since interference visibility depends on the polarization states. Hence, although polarization effects are not the only source of difficulties, we shall describe them in some detail, distinguishing among four effects: the geometric phase, birefringence, polarization mode dispersion, and polarization-dependent losses.

The *geometric phase* as encountered when guiding light in an optical fiber is a special case of the Berry phase,[19] which results when any parameter describing a property of the system under concern, here the k vector characterizing the propagation of the light field, undergoes an adiabatic change. Think first of a linear polarization state, let us say vertical at the input. Will it still be vertical at the output? Vertical with respect to what? Certainly not the gravitational field! One can follow that linear polarization by hand along the fiber and see how it may change even along a closed loop. If the loop stays in a plane, the state after a loop coincides with the input state, but if the loop explores the three dimensions of our space, then the final state will differ from the initial one by an angle. Similar reasoning holds for the axes of elliptical polarization states. The two circular polarization states are the eigenstates. During parallel transport they acquire opposite phases, called the Berry phases. The presence of a geometrical phase is not fatal for quantum communication. It simply means that initially Alice and Bob have to align their systems by defining, for instance, the vertical and diagonal directions (i.e., performing the unitary transformation mentioned before). If these vary slowly, they can be tracked, though this requires active feedback. However, if the variations are too fast, the communication might be interrupted. Hence aerial cables that swing in the wind are not appropriate (except with self-compensating configurations; see Sec. IV.C.2).

Birefringence is the presence of two different phase velocities for two orthogonal polarization states. It is caused by asymmetries in the fiber geometry and in the residual stress distribution inside and around the core. Some fibers are made birefringent on purpose. Such fibers are called polarization-maintaining fibers because the birefringence is large enough to effectively uncouple the two polarization eigenmodes. Note that only these two orthogonal polarization modes are maintained; all other modes, in contrast, evolve very quickly, making this kind of fiber completely unsuitable for polarization-based QC systems.[20] The global effect of the birefringence is equivalent to an arbitrary combination of two waveplates; that is, it corresponds to a unitary transformation. If this transformation is stable, Alice and Bob can compensate for it. The effect of birefringence is thus similar to the effect of the geometric phase, though, in addition to causing a rotation, it may also affect the ellipticity. Stability of birefringence requires slow thermal and mechanical variations.

Polarization mode dispersion (PMD) is the presence of two different group velocities for two orthogonal polarization modes. It is due to a delicate combination of two causes. First, birefringence produces locally two group velocities. For optical fibers, this local dispersion is in good approximation equal to the phase dispersion, of the order of a few picoseconds per kilometer. Hence, an optical pulse tends to split locally into a fast mode and a slow mode. But because the birefringence is small, the two modes couple easily. Hence any small imperfection along the fiber produces polarization mode coupling: some energy of the fast mode couples into the slow mode and vice versa. PMD is thus similar to a random walk[21] and grows only with the square root of the fiber length. It is expressed in $\mathrm{ps\,km^{-1/2}}$, with values as low as 0.1 $\mathrm{ps\,km^{-1/2}}$ for modern fibers and possibly as high as 0.5 or even $1\,\mathrm{ps\,km^{-1/2}}$ for older ones.

Typical lengths for polarization mode coupling vary from a few meters up to hundreds of meters. The stronger the coupling, the weaker the PMD (the two modes do not have time to move apart between the couplings). In modern fibers, the couplings are even artificially increased during the drawing process of the fibers (Hart *et al.*, 1994; Li and Nolan, 1998). Since the couplings are exceedingly sensitive, the only reasonable description is a statistical one, hence PMD is described as a statistical distribution of delays $\delta\tau$. For sufficiently long fibers, the statistics are Maxwellian, and PMD is related to the fiber length ℓ, the mean coupling length h, the mean modal birefringence B, and the rms delay as follows (Gisin *et al.*, 1995): $\mathrm{PMD} \equiv \sqrt{\langle\langle \delta\tau^2 \rangle\rangle} = Bh\sqrt{\ell/h}$. Polarization mode dispersion could cause depolarization, which would be devastating for quantum communication, similar to any decoherence in quantum information processing. Fortunately, for quantum communication the remedy is easy; it suffices to use a source with a coherence time longer than the largest delay $\delta\tau$. Hence, when laser pulses are used (with typical spectral widths $\Delta\lambda \leqslant 1$ nm, corresponding to a coherence time $\geqslant 3$ ps; see Sec. III.A.1), PMD is no real problem. For photons cre-

[19]The Berry phase was introduced by Michael Berry in 1984, and was then observed in optical fiber by Tomita and Chiao (1986) and on the single-photon level by Hariharan *et al.* (1993). It was studied in connection with photon pairs by Brendel *et al.* (1995).

[20]Polarization-maintaining fibers may be of use for phase-based QC systems. However, this requires that the whole setup—transmission lines as well as interferometers at each end—be made of polarization-maintaining fibers. While this is possible in principle, the need to install a completely new fiber network makes this solution not very practical.

[21]In contrast to Brownian motion, which describes particle diffusion in space as time passes, here photons diffuse over time as they propagate along the fiber.

ated by parametric downconversion, however, PMD can impose severe limitations, since $\Delta\lambda \geqslant 10$ nm (coherence time $\leqslant 300$ fs) is not unusual.

Polarization-dependent loss is a differential attenuation between two orthogonal polarization modes. This effect is negligible in fibers, but can be significant in components like phase modulators. In particular, some integrated optics waveguides actually guide only one mode and thus behave almost like polarizers (e.g., proton exchange waveguides in $LiNbO_3$). Polarization-dependent losses are usually stable, but if connected to a fiber with some birefringence, the relation between the polarization state and the loss may fluctuate, producing random outcomes (Elamari *et al.*, 1998). Polarization-dependent loss cannot be described by a unitary operator acting in the polarization state space (but it is of course unitary in a larger space (Huttner, Gautier, *et al.*, 1996). Thus it does not preserve the scalar product. In particular, it can turn nonorthogonal states into orthogonal ones, which can then be distinguished unambiguously (at the cost of some loss; Huttner, Gautier, *et al.*, 1996; Clarke *et al.*, 2000). Note that this attenuation could be used by Eve, especially to eavesdrop on the two-state protocol (Sec. II.D.1).

Let us conclude this section on polarization effects in fibers by mentioning that they can be passively compensated for, provided one uses a go-and-return configuration, with Faraday mirrors, as described in Sec. IV.C.2.

3. Chromatic dispersion effects in single-mode fibers

In addition to polarization effects, chromatic dispersion can also cause problems for quantum cryptography. For instance, as explained in Secs. IV.C and V.B, schemes implementing phase or phase-and-time coding rely on photons arriving at well-defined times, that is, on photons well localized in space. However, in dispersive media like optical fibers, different group velocities act as a noisy environment on the localization of the photon as well as on the phase acquired in an interferometer. Hence the broadening of photons featuring nonzero bandwidth, or, in other words, the coupling between frequency and position, must be circumvented or controlled. This implies working with photons of small bandwidth, or, as long as the bandwidth is not too large, operating close to the wavelength λ_0 at which chromatic dispersion is zero, i.e., for standard fibers around 1310 nm. Fortunately, fiber losses are relatively small at this wavelength and amount to ≈ 0.35 dB/km. This region is called the second telecommunications window.[22] There are also special fibers, called dispersion-shifted fibers, with a refractive index profile such that the chromatic dispersion goes to zero around 1550 nm, where the attenuation is minimal (Neumann, 1988).[23]

Chromatic dispersion does not constitute a problem in the case of faint laser pulses, for which the bandwidth is small. However, it becomes a serious issue when utilizing photon pairs created by parametric downconversion. For instance, sending photons of 70-nm bandwidth (as used in our long-distance tests of Bell's inequality; Tittel *et al.*, 1998) down 10 km of optical fibers leads to a temporal spread of around 500 ps (assuming photons centered at λ_0 and a typical dispersion slope of $0.086\ \mathrm{ps\,nm^{-2}\,km^{-1}}$). However, this can be compensated for when using energy-time-entangled photons (Franson, 1992; Steinberg *et al.*, 1992a, 1992b, Larchuk *et al.*, 1995). In contrast to polarization coding, in which frequency and the physical property used to implement the qubit are not conjugate variables, frequency and time (thus position) constitute a Fourier pair. The strict energy anticorrelation of signal and idler photons enables one to achieve a dispersion for one photon that is equal in magnitude but opposite in sign to that of the sister photon, thus corresponding to the same delay[24] (see Fig. 7). The effect of broadening of the two wave packets then cancels out, and two simultaneously emitted photons stay coincident. However, note that the arrival time of the pair varies with respect to its emission time. The frequency anticorrelation also provides the basis for avoiding a decrease in visibility due to different wave packet broadening in the two arms of an interferometer. Since the choromatic dispersion properties of optical fibers do not change with time—in contrast to birefringence—no active tracking and compensation are required. It thus turns out that phase and phase-time coding are particularly suited to transmission over long distances in optical fibers: nonlinear effects decohering the qubit "energy" are completely negligible, and chromatic dispersion effects acting on the localization can be avoided or compensated for in many cases.

4. Free-space links

Although today's telecommunications based on optical fibers are very advanced, such channels may not always be available. Hence there is also some effort in developing free-space line-of-sight communication sys-

[22]The first one, around 800 nm, is almost no longer used. It was motivated by the early existence of sources and detectors at this wavelength. The third window is around 1550 nm, where the attenuation reaches an absolute minimum (Thomas *et al.*, 2000) and where erbium-doped fibers provide convenient amplifiers (Desurvire, 1994).

[23]Chromatic dispersion in fibers is mainly due to the material, essentially silicon, but also to the refractive index profile. Indeed, longer wavelengths feel regions farther away from the core where the refractive index is lower. Dispersion-shifted fibers have, however, been abandoned by today's industry, because it has turned out to be simpler to compensate for the global chromatic dispersion by adding an extra fiber with high negative dispersion. The additional loss is then compensated for by an erbium-doped fiber amplifier.

[24]Here we assume a predominantly linear dependence of chromatic dispersion as a function of the optical frequency, a realistic assumption.

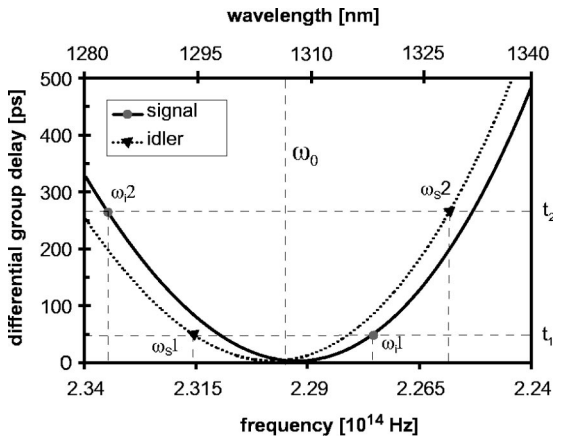

FIG. 7. Illustration of cancellation of chromatic dispersion effects in the fibers connecting an entangled-particle source and two detectors. The figure shows differential group delay curves for two slightly different fibers approximately 10 km long. Using frequency-correlated photons with central frequency ω_0—determined by the properties of the fibers—the difference in propagation times t_2-t_1 between the signal (at $\omega_s 1,\omega_s 2$) and idler (at $\omega_i 1,\omega_i 2$) photon is the same for all ω_s,ω_i. Note that this cancellation scheme is not restricted to signal and idler photons at nearly equal wavelengths. It also applies to asymmetrical setups in which the signal photon (generating the trigger to indicate the presence of the idler photon) is at a short wavelength of around 800 nm and travels only a short distance. Using a fiber with appropriate zero dispersion wavelength λ_0, it is still possible to achieve equal differential group delay with respect to the energy-correlated idler photon sent through a long fiber at a telecommunications wavelength.

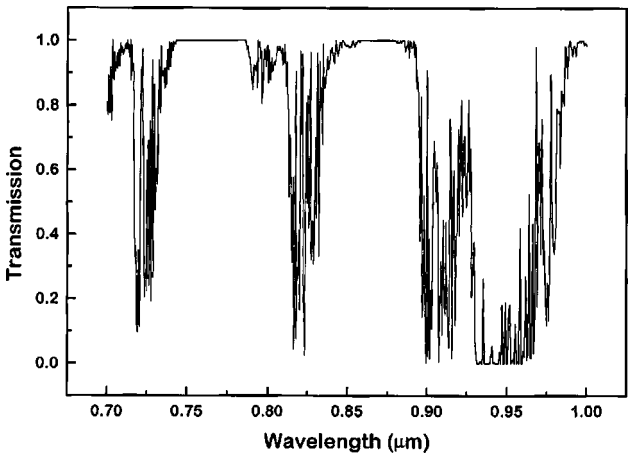

FIG. 8. Transmission losses in free space as calculated using the LOWTRAN code for earth-to-space transmission at the elevation and location of Los Alamos, USA. Note that there is a low-loss window at around 770 nm—a wavelength at which high-efficiency silicon APD's can be used for single-photon detection (see also Fig. 9 and compare to Fig. 6). Figure courtesy of Richard Hughes.

tems, not only for classical data transmission but also for quantum cryptography (see Hughes, Buttler, *et al.*, 2000 and Gorman *et al.*, 2000).

Transmission over free space features some advantages compared to the use of optical fibers. The atmosphere has a high transmission window at a wavelength of around 770 nm (see Fig. 8), where photons can easily be detected using commercial, high-efficiency photon-counting modules (see Sec. III.C.1). Furthermore, the atmosphere is only weakly dispersive and essentially nonbirefringent[25] at these wavelengths. It will thus not alter the polarization state of a photon.

However, there are some drawbacks concerning free-space links as well. In contrast to the signal transmitted in a guiding medium where the energy is "protected" and remains localized in a small region of space, the energy transmitted via a free-space link spreads out, leading to higher and varying transmission losses. In addition to loss of energy, ambient daylight, or even moonlight at night, can couple into the receiver, leading to a higher error rate. However, such errors can be kept to a reasonable level by using a combination of spectral filtering (interference filters $\leqslant 1$ nm), spatial filtering at the receiver, and timing discrimination using a coincidence window of typically a few nanoseconds. Finally, it is clear that the performance of free-space systems depends dramatically on atmospheric conditions and is possible only in clear weather.

Finally, let us briefly comment on the different sources leading to coupling losses. A first concern is the transmission of the signals through a turbulent medium, leading to *arrival-time jitter* and *beam wander* (hence problems with *beam pointing*). However, as the time scales for atmospheric turbulences involved are rather small—around 0.1–0.01 s—the time jitter due to a variation of the effective refractive index can be compensated for by sending a reference pulse at a different wavelength a short time (around 100 ns) before each signal pulse. Since this reference pulse experiences the same atmospheric conditions as the subsequent one, the signal will arrive essentially without jitter in the time window defined by the arrival of the reference pulse. In addition, the reference pulse can be reflected back to the transmitter and used to correct the direction of the laser beam by means of adaptive optics, hence compensating for beam wander and ensuring good beam pointing.

Another issue is beam divergence, hence increase of spot size at the receiver end caused by diffraction at the transmitter aperture. Using, for example, 20-cm-diameter optics, one obtains a diffraction-limited spot size after 300 km of ≈ 1 m. This effect can in principle be kept small by taking advantage of larger optics. However, it can also be advantageous to have a spot size that is large compared to the receiver's aperture in order to ensure constant coupling in case of remaining beam wander. In their 2000 paper, Gilbert and Hamrick provide a comprehensive discussion of free-space channels in the context of QC.

C. Single-photon detection

With the availability of pseudo-single-photon and photon-pair sources, the success of quantum cryptogra-

[25]In contrast to an optical fiber, air is not subject to stress and is hence isotropic.

phy essentially depends on the ability to detect single photons. In principle, this can be achieved using a variety of techniques, for instance, photomultipliers, avalanche photodiodes, multichannel plates, and superconducting Josephson junctions. The ideal detector should fulfill the following requirements:

- the quantum detection efficiency should be high over a large spectral range,
- the probability of generating noise, that is, a signal without an arriving photon, should be small,
- the time between detection of a photon and generation of an electrical signal should be as constant as possible, i.e., the time jitter should be small, to ensure good timing resolution,
- the recovery time (i.e., the dead time) should be short to allow high data rates.

In addition, it is important to keep the detectors practical. For instance, a detector that needs liquid helium or even nitrogen cooling would certainly render commercial development difficult.

Unfortunately, it turns out that it is impossible to fulfill all the above criteria at the same time. Today, the best choice is avalanche photodiodes (APD's). Three different semiconductor materials are used: either silicon, germanium, or indium gallium arsenide, depending on the wavelengths.

APDs are usually operated in the so-called *Geiger mode*. In this mode, the applied voltage exceeds the breakdown voltage, leading an absorbed photon to trigger an electron avalanche consisting of thousands of carriers. To reset the diode, this macroscopic current must be quenched—the emission of charges must be stopped and the diode recharged (Cova *et al.*, 1996). Three main possibilities exist:

- In *passive-quenching* circuits, a large (50–500 kΩ) resistor is connected in series with the APD (see, for example, Brown *et al.*, 1986). This causes a decrease in the voltage across the APD as soon as an avalanche starts. When it drops below breakdown voltage, the avalanche stops and the diode recharges. The recovery time of the diode is given by its capacitance and by the value of the quench resistor. The maximum count rate varies from a few hundred kilohertz to a few megahertz.
- In *active-quenching* circuits, the bias voltage is actively lowered below the breakdown voltage as soon as the leading edge of the avalanche current is detected (see, for example, Brown *et al.*, 1987). This mode makes possible higher count rates than those in passive quenching (up to tens of megahertz), since the dead time can be as short as tens of nanoseconds. However, the fast electronic feedback system makes active-quenching circuits much more complicated than passive ones.
- Finally, in *gated-mode* operation, the bias voltage is kept below the breakdown voltage and is raised above it only for a short time, typically a few nanosecods when a photon is expected to arrive. Maximum count rates similar to those in active-quenching circuits can be obtained using less complicated electronics. Gated-mode operation is commonly used in quantum cryptography based on faint laser pulses, for which the arrival times of the photons are well known. However, it only applies if prior timing information is available. For two-photon schemes, it is most often combined with a passive-quenched detector, generating the trigger signal for the gated detector.

In addition to Geiger mode, Brown and Daniels (1989) have investigated the performance of silicon APD's operated in *sub-Geiger mode*. In this mode, the bias voltage is kept slightly smaller than the breakdown voltage such that the multiplication factor—around 100—is sufficient to detect an avalanche, yet, is still small enough to prevent real breakdowns. Unfortunately, the single-photon counting performance in this mode is rather poor, and thus efforts have not been continued, the major problem being the need for extremely low-noise amplifiers.

An avalanche engendered by carriers created in the conduction band of the diode can be set off not only by an impinging photon, but also by unwanted causes. These might be thermal or band-to-band tunneling processes, or emissions from trapping levels populated while a current transits through the diode. The first two produce avalanches not due to photons and are referred to as *dark counts*. The third process depends on previous avalanches and its effects are called *afterpulses*. Since the number of trapped charges decreases exponentially with time, these afterpulses can be limited by applying large dead times. Thus there is a tradeoff between high count rates and low afterpulses. The time constant of the exponential decrease of afterpulses shortens for higher temperatures of the diode. Unfortunately, operating APD's at higher temperatures leads to a higher fraction of thermal noise, that is, higher dark counts. Thus there is again a tradeoff to be optimized. Finally, increasing the bias voltage leads to a higher quantum efficiency and a smaller time jitter, at the cost of an increase in noise.

We thus see that the optimal operating parameters—voltage, temperature, and dead time (i.e., maximum count rate)—depend on the specific application. Moreover, since the relative magnitudes of efficiency, thermal noise, and afterpulses vary with the type of semiconductor material used, no general solution exists. In the next two sections we briefly discuss the different types of APD's. The first section focuses on silicon APD's for the detection of photons at wavelengths below 1 μm; the second comments on germanium and on indium gallium arsenide APD's for photon counting at telecommunications wavelengths. The different behavior of the three types is shown in Fig. 9. Although the best figure of merit for quantum cryptography is the ratio of dark-count rate R to detection efficiency η, we show here the better-known noise equivalent power (NEP), which shows similar behavior. The noise equivalent power is defined as the optical power required to measure a unity signal-to-noise ratio and is given by

$$NEP = \frac{h\nu}{\eta}\sqrt{2R}. \tag{25}$$

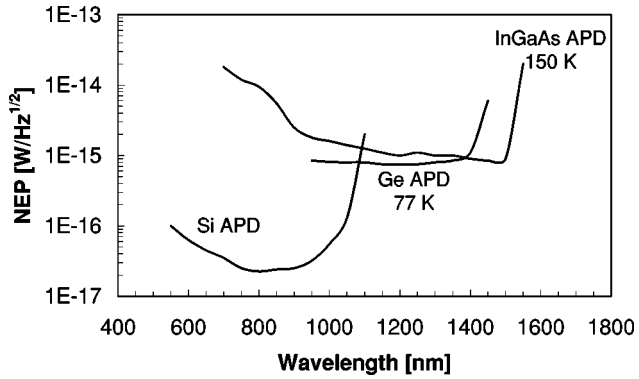

FIG. 9. Noise equivalent power as a function of wavelength for silicon, germanium, and InGaAs/InP APD's.

Here, h is Planck's constant and ν is the frequency of the impinging photons.

1. Photon counting at wavelengths below 1.1 μm

Since the beginning of the 1980s much work has been done to characterize silicon APD's for single-photon counting (Ingerson 1983; Brown *et al.*, 1986, 1987; Brown and Daniels, 1989; Spinelli, 1996), and the performance of Si APD's has continuously been improved. Since the first test of Bell's inequality using Si APD's by Shih and Alley in 1988, they have completely replaced the photomultipliers used until then in the domain of fundamental quantum optics, now known as quantum communication. Today, quantum efficiencies of up to 76% (Kwiat *et al.*, 1993) and time jitter as low as 28 ps (Cova *et al.*, 1989) have been reported. Commercial single-photon counting modules are available (for example, EG&G SPCM-AQ-151), featuring quantum efficiencies of 70% at a wavelength of 700 nm, a time jitter of around 300 ps, and maximum count rates higher than 5 MHz. Temperatures of $-20\,^{\circ}$C—sufficient to keep thermally generated dark counts as low as 50 Hz—can easily be achieved using Peltier cooling. Single-photon counters based on silicon APD's thus offer an almost perfect solution for all applications in which photons of wavelengths below 1 μm can be used. Apart from fundamental quantum optics, these applications include quantum cryptography in free space and in optical fibers; however, due to high losses, the latter works only over short distances.

2. Photon counting at telecommunications wavelengths

When working in the second telecommunications window (1.3 μm), one can take advantage of APD's made from germanium or InGaAs/InP semiconductor materials. In the third window (1.55 μm), the only option is InGaAs/InP.

Photon counting with germanium APD's, although known for 30 years (Haecker *et al.*, 1971), began to be used in quantum communication as the need arose to transmit single photons over long distances using optical fibers, which necessitated working at telecommunications wavelengths. In 1993, Townsend, Rarity, and Tapster (1993a) implemented a single-photon interference scheme for quantum cryptography over a distance of 10 km, and in 1994, Tapster, Rarity, and Owens demonstrated a violation of Bell's inequalities over 4 km. These experiments were the first to take advantage of Ge APD's operated in passively quenched Geiger mode. At a temperature of 77 K, which can be achieved using either liquid nitrogen or Stirling engine cooling, typical quantum efficiencies of about 15% at dark-count rates of 25 kHz can be achieved (Owens *et al.*, 1994), and time jitter down to 100 ps has been observed (Lacaita *et al.*, 1994) a normal value being 200–300 ps.

Traditionally, germanium APD's have been implemented in the domain of long-distance quantum communication. However, this type of diode is currently being replaced by InGaAs APD's, and it has become more and more difficult to find germanium APD's on the market. Motivated by pioneering research reported in 1985 (Levine *et al.*, 1985), the latest research focuses on InGaAs APD's, which allow single-photon detection in both telecommunications windows. Starting with work by Zappa *et al.* (1994), InGaAs APD's as single-photon counters have meanwhile been thoroughly characterized (Lacaita *et al.*, 1996; Ribordy *et al.*, 1998; Karlsson *et al.*, 1999; Hiskett *et al.*, 2000; Rarity *et al.*, 2000; Stucki *et al.*, 2001), and the first implementations for quantum cryptography have been reported (Ribordy, 1998; Bourennane *et al.*, 1999; Bethune and Risk, 2000; Hughes, Morgan, and Peterson, 2000; Ribordy *et al.*, 2000). However, if operating Ge APD's is already more inconvenient than using silicon APD's, the practicality of InGaAs APD's is even worse, the problem being an extremely high afterpulse fraction. Therefore operation in passive-quenching mode is impossible for applications in which low noise is crucial. In gated mode, InGaAs APD's are better for single-photon counting at 1.3 μm than Ge APD's. For instance, at a temperature of 77 K and a dark-count probability of 10^{-5} per 2.6-ns gate, quantum efficiencies of around 30% and 17% have been reported for InGaAs and Ge APD's, respectively (Ribordy *et al.*, 1998), while the time jitter of both devices is comparable. If working at a wavelength of 1.55 μm, the temperature has to be increased for single-photon detection. At 173 K and a dark-count rate of 10^{-4}, a quantum efficiency of 6% can still be observed using InGaAs/InP devices, while the same figure for germanium APD's is close to zero.

To date, no industrial effort has been made to optimize APD's operating at telecommunications wavelengths for photon counting, and their performance still lags far behind that one of silicon APD's.[26] However, there is no fundamental reason why photon counting at wavelengths above 1 μm should be more difficult than at wavelengths below 1 μm except that the high-

[26]The first commercial photon counter at telecommunications wavelengths came out only this year (the Hamamatsu photomultiplier R5509-72). However, its efficiency is not yet sufficient for use in quantum cryptography.

wavelength photons are less energetic. The real reasons for the lack of commercial products are, first, that silicon, the most common semiconductor material, is not sensitive enough (the band gap is too large), and second that the market for photon counting is not yet mature. But, without great risk, one can predict that good commercial photon counters will become available in the near future and that they will have a major impact on quantum cryptography.

D. Quantum random-number generators

The key used in the one-time pad must be secret and used only once. Consequently it must be as long as the message, and it must be perfectly random. The latter point proves to be a delicate and interesting one. Computers are deterministic systems that cannot create truly random numbers. However, all secure cryptosystems, both classical and quantum ones, require truly random numbers.[27] Hence the random numbers must be created by a random physical process. Moreover, to make sure that the process does not merely appear random while having some hidden deterministic pattern, the process needs to be completely understood. It is thus of interest to implement a simple process in order to gain confidence in the randomness of its proper operation.

A natural solution is to rely on the random choice of a single photon at a beamsplitter[28] (Rarity *et al.*, 1994). In this case the randomness is in principle guaranteed by the laws of quantum mechanics, though one still has to be very careful not to introduce any experimental artifact that could correlate adjacent bits. Different experimental realizations have been demonstrated (Jennewein, Achleitner, *et al.*, 2000; Stefanov *et al.*, 2000; Hildebrand, 2001), and prototypes are commercially available (www.gap-optique.unige.ch). One particular problem is the dead time of the detectors, which may introduce a strong anticorrelation between neighboring bits. Similarly, afterpulses may provoke a correlation. These detector-related effects increase with higher pulse rates, limiting the bit rate of a quantum number generator to a few megahertz.

In the BB84 protocol Alice has to choose randomly among four different states and Bob between two bases. The limited random-number generation rate may force Alice to produce her numbers in advance and store them, creating a security risk. On Bob's side the random-bit creation rate can be lower, since, in principle, the basis need be changed only after a photon has been detected, which normally happens at rates below 1 MHz. However, one must make sure that this does not give a spy an opportunity for a Trojan horse attack (see Sec. VI.K).

An elegant configuration integrating the random-number generator into the QC system consists in using a passive choice of bases, as discussed in Sec. V (Muller *et al.*, 1993). However, the problem of detector-induced correlation remains.

E. Quantum repeaters

Today's fiber-based QC systems are limited to operation over tens of kilometers due to the combination of fiber losses and detector noise. The losses by themselves only reduce the bit rate (exponentially with distance). With perfect detectors the distance would not be limited. However, because of the dark counts, each time a photon is lost there is a chance that a dark count produces an error. Hence, when the probability of a dark count becomes comparable to the probability that a photon is correctly detected, the signal-to-noise ratio tends to 0 [more precisely, the mutual information $I(\alpha,\beta)$ tends to a lower bound[29]]. In this section we briefly explain how the use of entangled photons and of entanglement swapping (Żukowski *et al.*, 1993) could offer ways to extend the achievable distances in the foreseeable future (some prior knowledge of entanglement swapping is assumed). Let t_{link} denote the transmission coefficient (i.e., the probability that a photon sent by Alice gets to one of Bob's detectors), η the detector efficiency, and p_{dark} the dark-count probability per time bin. With a perfect single-photon source, the probability P_{raw} of a correct qubit detection is $P_{raw}=t_{link}\eta$, while the probability P_{det} of an error is $P_{det}=(1-t_{link}\eta)p_{dark}$. Accordingly, the QBER$=P_{det}/(P_{raw}+P_{det})$, and the normalized net rate is $\rho_{net}=(P_{raw}+P_{det})\cdot fct(\mathrm{QBER})$, where the function fct denotes the fraction of bits remaining after error correction and privacy amplification. For the sake of illustration, we simply assume a linear dependence dropping to zero for QBER$\geqslant$15% (this simplification does not affect the qualitative results of this section; for a more precise calculation, see Lütkenhaus 2000): $fct(\mathrm{QBER})=1-\mathrm{QBER}/15\%$. The corresponding net rate ρ_{net} is displayed in Fig. 10. Note that it drops to zero near 90 km.

Let us now assume that instead of a perfect single-photon source, Alice and Bob use a perfect two-photon source set in the middle of their quantum channel. Each photon then has a probability $\sqrt{t_{link}}$ of reaching a detector. The probability of a correct joined detection is thus $P_{raw}=t_{link}\eta^2$, while an error occurs with probability $P_{det}=(1-\sqrt{t_{link}}\eta)^2p_{dark}^2+2\sqrt{t_{link}}\eta(1-\sqrt{t_{link}}\eta)p_{dark}$ (both photons lost and two dark counts, or one photon lost and one dark count). This can be conveniently rewritten as $P_{raw}=t_{link}\eta^n$ and $P_{det}=[t_{link}^{1/n}\eta+(1-t_{link}^{1/n}\eta)p_{dark}]^n-t_{link}\eta^n$, valid for any division of the

[27]The PIN number that the bank assigns to your ATM card must be random. If not, someone else knows it.

[28]Strictly speaking, the choice is made only once the photons are detected at one of the outports.

[29]The absolute lower bound is 0, but depending on the assumed eavesdropping strategy, Eve could take advantage of the losses. In the latter case, the lower bound is given by her mutual information $I(\alpha,\epsilon)$.

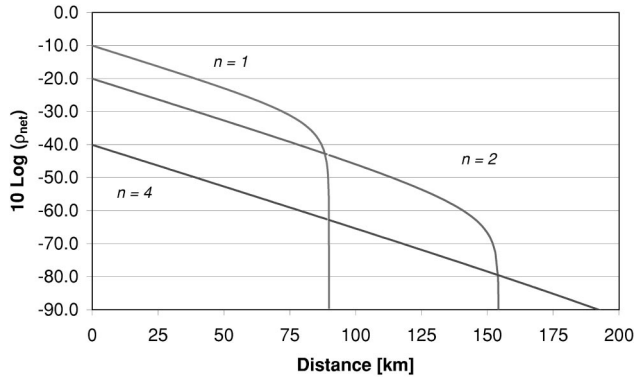

FIG. 10. Normalized net key creation rate ρ_{net} as a function of distance in optical fibers. For $n=1$, Alice uses a perfect single-photon source. For $n>1$, the link is divided into n equal-length sections, and $n/2$ two-photon sources are distributed between Alice and Bob. Parameters: detection efficiency $\eta=10\%$, dark-count probability $p_{dark}=10^{-4}$, and fiber attenuation $\alpha=0.25$ dB/km.

link into n equal-length sections and n detectors. Note that the measurements performed at the nodes between Alice and Bob transmit (swap) the entanglement to the twin photons without revealing any information about the qubit (these measurements are called Bell measurements and are at the core of entanglement swapping and of quantum teleportation). The corresponding net rates are displayed in Fig. 10. Clearly, the rates for short distances are smaller when several detectors are used, because of their limited efficiencies (here we assume $\eta=10\%$), but the distance before the net rate drops to zero is extended to longer distances! Intuitively, this can be understood as follows. Let us assume that a logical qubit propagates from Alice to Bob (although some photons propagate in the opposite direction). Then, each two-photon source and each Bell measurement acts on this logical qubit as a kind of quantum nondemolition measurement, testing whether the logical qubit is still there. In this way, Bob activates his detectors only when there is a large chance $t_{link}^{1/n}$ that the photon gets to his detectors.

Note that if in addition to detector noise there is noise due to decoherence, then the above idea can be extended, using entanglement purification. This is essentially the idea behind quantum repeaters (Briegel *et al.*, 1998; Dur *et al.*, 1999).

IV. EXPERIMENTAL QUANTUM CRYPTOGRAPHY WITH FAINT LASER PULSES

Experimental quantum key distribution was demonstrated for the first time in 1989 (the results were published only in 1992 by Bennett, Bessette, *et al.*). Since then, tremendous progress has been made. Today, several groups have shown that quantum key distribution is possible, even outside the laboratory. In principle, any two-level quantum system could be used to implement QC. In practice, all implementations have relied on photons. The reason is that their interaction with the environment, also called decoherence, can be controlled and moderated. In addition, researchers can benefit from all the tools developed in the past two decades for optical telecommunications. It is unlikely that other carriers will be employed in the foreseeable future.

Comparing different QC setups is a difficult task, since several criteria must be taken into account. What matters in the end, of course, is the rate of corrected secret bits (the distilled bit rate R_{dist}) that can be transmitted and the transmission distance. One can already note that with present and near-future technology it will probably not be possible to achieve rates of the order of gigahertz, which are now common with conventional optical communication systems (in their comprehensive paper published in 2000, Gilbert and Hamrick discuss practical methods for achieving high-bit-rate QC). This implies that encryption with a key exchanged through QC will be limited to highly confidential information. While the determination of the transmission distance and rate of detection (the raw bit rate R_{raw}) is straightforward, estimating the net rate is rather difficult. Although, in principle, errors in the bit sequence follow only from tampering by a malevolent eavesdropper, the situation is rather different in reality. Discrepancies between the keys of Alice and Bob also happen because of experimental imperfections. The error rate QBER can be easily determined. Similarly, the error correction procedure is rather simple. Error correction leads to a reduction of the key rate that depends strongly on the QBER. The real problem is to estimate the information obtained by Eve, a quantity necessary for privacy amplification. This depends not only on the QBER, but also on other factors, such as the photon number statistics of the source or the way the choice of the measurement basis is made. Moreover in a pragmatic approach, one might also accept restrictions on Eve's technology, limiting her strategies and therefore also the information she can obtain per error she introduces. Since the efficiency of privacy amplification rapidly decreases when the QBER increases, the distilled bit rate depends dramatically on Eve's information and hence on the assumptions made. One can define as the maximum transmission distance the distance at which the distilled rate reaches zero. This distance can give one an idea of the difficulty of evaluating a QC system from a physical point of view.

Technological aspects must also be taken into account. In this article we do not focus on all the published performances (in particular not on the key rates), which strongly depend on current technology and the financial resources of the research teams who carried out the experiments. Rather, we try to weigh the intrinsic technological difficulties associated with each setup and to anticipate certain technological advances. Last but not least, the cost of realizing a prototype should also be considered.

In this section, we first deduce a general formula for the QBER and consider its impact on the distilled rate. We then review faint-pulse implementations. We class them according to the property used to encode the qubits value and follow a rough chronological order. Fi-

nally, we assess the possibility of adopting the various setups for the realization of an industrial prototype. Systems based on entangled photon pairs are presented in the next section.

A. Quantum bit error rate

The QBER is defined as the ratio of wrong bits to the total number of bits received[30] and is normally on the order of a few percent. We can express it as a function of rates,

$$\mathrm{QBER}=\frac{N_{wrong}}{N_{right}+N_{wrong}}=\frac{R_{error}}{R_{sift}+R_{error}}\approx\frac{R_{error}}{R_{sift}}. \quad (26)$$

Here the sifted key corresponds to the cases in which Alice and Bob made compatible choices of bases, hence its rate is half that of the raw key.

The raw rate is essentially the product of the pulse rate f_{rep}, the mean number of photons per pulse μ, the probability t_{link} of a photons arriving at the analyzer, and the probability η of the photon's being detected:

$$R_{sift}=\frac{1}{2}R_{raw}=\frac{1}{2}qf_{rep}\mu t_{link}\eta. \quad (27)$$

The factor q ($q\leqslant 1$, typically 1 or $\frac{1}{2}$) must be introduced for some phase-coding setups in order to correct for noninterfering path combinations (see, for example, Secs. IV.C and V.B).

One can identify three different contributions to R_{error}. The first arises from photons that end up in the wrong detector due to imperfect interference or polarization contrast. The rate R_{opt} is given by the product of the sifted-key rate and the probability p_{opt} of a photon's going to the wrong detector:

$$R_{opt}=R_{sift}p_{opt}=\frac{1}{2}qf_{rep}\mu t_{link}p_{opt}\eta. \quad (28)$$

For a given setup, this contribution can be considered as an intrinsic error rate indicating its suitability for use in QC. We shall discuss it below in the case of each particular system.

The second contribution, R_{det}, arises from the detector dark counts (or from remaining environmental stray light in free-space setups). This rate is independent of the bit rate.[31] Of course, only dark counts falling within the short time window when a photon is expected give rise to errors,

$$R_{det}=\frac{1}{2}\frac{1}{2}f_{rep}p_{dark}n, \quad (29)$$

where p_{dark} is the probability of registering a dark count per time window and per detector, and n is the number of detectors. The two factors of $\frac{1}{2}$ are related to the fact that a dark count has a 50% chance of happening when Alice and Bob have chosen incompatible bases (and is thus eliminated during sifting) and a 50% chance of occurring in the correct detector.

Finally, error counts can arise from uncorrelated photons due to imperfect photon sources:

$$R_{acc}=\frac{1}{2}\frac{1}{2}p_{acc}f_{rep}t_{link}n\eta. \quad (30)$$

This factor appears only in systems based on entangled photons, where the photons belonging to different pairs but arriving in the same time window are not necessarily in the same state. The quantity p_{acc} is the probability of finding a second pair within the time window, knowing that a first one was created.[32]

The QBER can now be expressed as follows:

$$\mathrm{QBER}=\frac{R_{opt}+R_{det}+R_{acc}}{R_{sift}} \quad (31)$$

$$=p_{opt}+\frac{p_{dark}n}{t_{link}\eta 2q\mu}+\frac{p_{acc}}{2q\mu} \quad (32)$$

$$=\mathrm{QBER}_{opt}+\mathrm{QBER}_{det}+\mathrm{QBER}_{acc}. \quad (33)$$

We now analyze these three contributions. The first one, QBER_{opt}, is independent of the transmission distance (it is independent of t_{link}). It can be considered as a measure of the optical quality of the setup, depending only on the polarization or interference fringe contrast. The technical effort needed to obtain and, more importantly, to maintain a given QBER_{opt} is an important criterion for evaluating different QC setups. In polarization-based systems, it is rather simple to achieve a polarization contrast of 100:1, corresponding to a QBER_{opt} of 1%. In fiber-based QC, the problem is to maintain this value in spite of polarization fluctuations and depolarization in the fiber link. For phase-coding setups, QBER_{opt} and the interference visibility are related by

$$\mathrm{QBER}_{opt}=\frac{1-V}{2}. \quad (34)$$

A visibility of 98% thus translates into an optical error rate of 1%. Such a value implies the use of well-aligned and stable interferometers. In bulk optics, perfect mode overlap is difficult to achieve, but the polarization is stable. In single-mode fiber interferometers, on in contrast, perfect mode overlap is automatically achieved, but the polarization must be controlled, and chromatic dispersion can constitute a problem.

The second contribution, QBER_{det}, increases with distance, since the dark-count rate remains constant while the bit rate goes down like t_{link}. It depends en-

[30]In the following section we consider systems implementing the BB84 protocol. For other protocols, some of the formulas have to be slightly adapted.

[31]This is true provided that afterpulses (see Sec. III.C) do not contribute to the dark counts.

[32]Note that a passive choice of measurement basis implies that four detectors (or two detectors during two time windows) are activated for every pulse, thus leading to a doubling of R_{det} and R_{acc}.

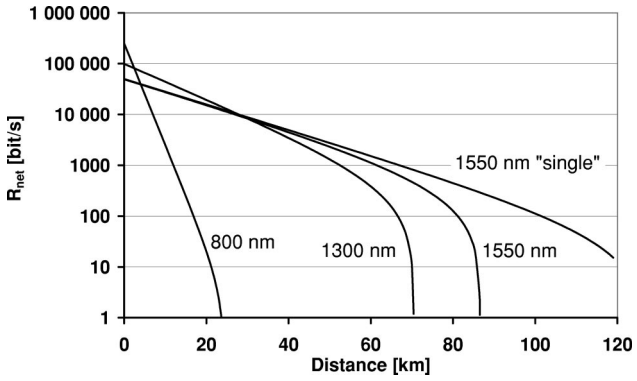

FIG. 11. Bit rate, after error correction and privacy amplification, vs fiber length. The chosen parameters are as follows: pulse rates of 10 MHz for faint laser pulses ($\mu=0.1$) and 1 MHz for the case of ideal single photons (1550-nm "single"); losses of 2, 0.35, and 0.25 dB/km; detector efficiencies of 50, 20, and 10; dark-count probabilities of 10^{-7}, and 10^{-5}, and 10^{-5} for 800, 1300, and 1550 nm, respectively. Losses at Bob's end and QBER_{opt} are neglected.

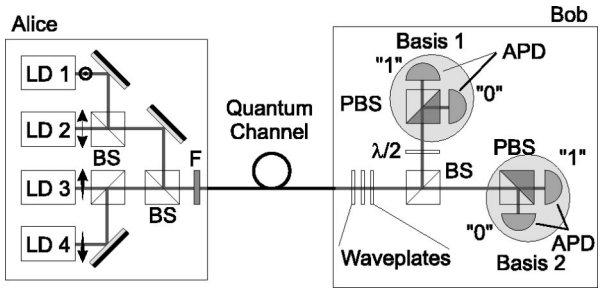

FIG. 12. Typical system for quantum cryptography using polarization coding: LD, laser diode; BS, beamsplitter; F, neutral density filter; PBS, polarizing beamsplitter; λ/2, half waveplate; APD, avalanche photodiode.

tirely on the ratio of the dark-count rate to the quantum efficiency. At present, good single-photon detectors are not commercially available for telecommunications wavelengths. The span of QC is not limited by decoherence. As QBER_{opt} is essentially independent of the fiber length, it is detector noise that limits the transmission distance.

Finally, the QBER_{acc} contribution is present only in some two-photon schemes in which multiphoton pulses are processed in such a way that they do not necessarily encode the same bit value (see, for example, Secs. V.B.1 and V.B.2). Although all systems have some probability of multiphoton pulses, in most these contribute only to the information available to Eve (see Sec. VI.H) and not to the QBER. However, for implementations featuring passive choice by each photon, the multiphoton pulses do not contribute to Eve's information but only to the error rate (see Sec. VI.J).

Now, let us calculate the useful bit rate as a function of the distance. R_{sift} and QBER are given as a function of t_{link} in Eqs. (27) and (32), respectively. The fiber link transmission decreases exponentially with length. The fraction of bits lost due to error correction and privacy amplification is a function of QBER and depends on Eve's strategy. The number of remaining bits R_{net} is given by the sifted-key rate multiplied by the difference between the Alice-Bob mutual Shannon information $I(\alpha,\beta)$ and Eve's maximal Shannon information $I^{\max}(\alpha,\epsilon)$:

$$R_{net}=R_{sift}[I(\alpha,\beta)-I^{\max}(\alpha,\epsilon)]. \tag{35}$$

The difference between $I(\alpha,\beta)$ and $I^{\max}(\alpha,\epsilon)$ is calculated here according to Eqs. (63) and (65) (Sec. VI.E), considering only individual attacks and no multiphoton pulses. We obtain R_{net} (the useful bit rate after error correction and privacy amplification) for different wavelengths as shown in Fig. 11. There is first an exponential decrease, then, due to error correction and privacy amplification, the bit rates fall rapidly down to zero. This is most evident when comparing the curves 1550 and 1550 nm "single," since the latter features a QBER that is 10 times lower. One can see that the maximum range is about 100 km. In practice it is closer to 50 km, due to nonideal error correction and privacy amplification, multiphoton pulses, and other optical losses not considered here. Finally, let us mention that typical key creation rates on the order of a thousand bits per second over distances of a few tens of kilometers have been demonstrated experimentally (see, for example, Townsend, 1998b or Ribordy *et al.*, 2000).

B. Polarization coding

Encoding the qubits in the polarization of photons is a natural solution. The first demonstration of QC by Bennett and co-workers (Bennett, Bessette, *et al.*, 1992) made use of this choice. They realized a system in which Alice and Bob exchanged faint light pulses produced by a light-emitting diode and containing less than one photon on average over a distance of 30 cm in air. In spite of the small scale of this experiment, it had an important impact on the community, as it showed that it was not unreasonable to use single photons instead of classical pulses for encoding bits.

A typical QC system with the BB84 four-state protocol using the polarization of photons is shown in Fig. 12. Alice's system consists of four laser diodes. They emit short classical photon pulses ($\approx$1 ns) polarized at $-45°$, $0°$, $+45°$, and $90°$. For a given qubit, a single diode is triggered. The pulses are then attenuated by a set of filters to reduce the average number of photons to well below 1, and sent along the quantum channel to Alice.

It is essential that the pulses remain polarized for Bob to be able to extract the information encoded by Alice. As discussed in Sec. III.B.2, polarization mode dispersion may depolarize the photons, provided the delay it introduces between polarization modes is longer than the coherence time. This sets a constraint on the type of lasers used by Alice.

Upon reaching Bob, the pulses are extracted from the fiber. They travel through a set of waveplates used to recover the initial polarization states by compensating for the transformation induced by the optical fiber (Sec. III.B.2). The pulses then reach a symmetric beamsplit-

ter, implementing the basis choice. Transmitted photons are analyzed in the vertical-horizontal basis with a polarizing beamsplitter and two photon-counting detectors. The polarization state of the reflected photons is first rotated with a waveplate by 45° ($-45° \rightarrow 0°$). The photons are then analyzed with a second set of polarizing beamsplitters and photon-counting detectors. This implements the diagonal basis. For illustration, let us follow a photon polarized at $+45°$. We see that its state of polarization is arbitrarily transformed in the optical fiber. At Bob's end, the polarization controller must be set to bring it back to $+45°$. If it chooses the output of the beamsplitter corresponding to the vertical-horizontal basis, it will experience an equal probability of reflection or transmission at the polarizing beamsplittter, yielding a random outcome. On the other hand, if it chooses the diagonal basis, its state will be rotated to 90°. The polarizing beamsplitter will then reflect it with unit probability, yielding a deterministic outcome.

Instead of having Alice use four lasers and Bob two polarizing beamsplitters, one can also implement this system with active polarization modulators such as Pockels cells. For emission, the modulator is randomly activated for each pulse to rotate the state of polarization to one of the four states, while, at the receiver, it randomly rotates half of the incoming pulses by 45°. It is also possible to realize the whole system with fiber optics components.

Antoine Muller and co-workers at the University of Geneva have used such a system to perform QC experiments over optical fibers (1993; see also Bréguet *et al.*, 1994). They created a key over a distance of 1100 meters with photons at 800 nm. In order to increase the transmission distance, they repeated the experiment with photons at 1300 nm (Muller *et al.*, 1995, 1996) and created a key over a distance of 23 km. An interesting feature of this experiment is that the quantum channel connecting Alice and Bob consisted of an optical fiber part of an installed cable used by the telecommunications company Swisscom for carrying phone conversations. It runs between the Swiss cities of Geneva and Nyon, under Lake Geneva (Fig. 13). This was the first time QC was performed outside of a physics laboratory. These experiments had a strong impact on the interest of the wider public in the new field of quantum communication.

These two experiments highlighted the fact that the polarization transformation induced by a long optical fiber was unstable over time. Indeed, when monitoring the QBER of their system, Muller noticed that, although it remained stable and low for some time (on the order of several minutes), it would suddenly increase after a while, indicating a modification of the polarization transformation in the fiber. This implies that a real fiber-based QC system would require active alignment to compensate for this evolution. Although not impossible, such a procedure is certainly difficult. James Franson did indeed implement an active-feedback alignment system (Franson and Jacobs, 1995), but did not pursue this line of research. It is interesting to note that replacing standard fibers with polarization-maintaining fibers does not solve the problem. The reason is that, in spite of their name, these fibers do not maintain polarization, as explained in Sec. III.B.2.

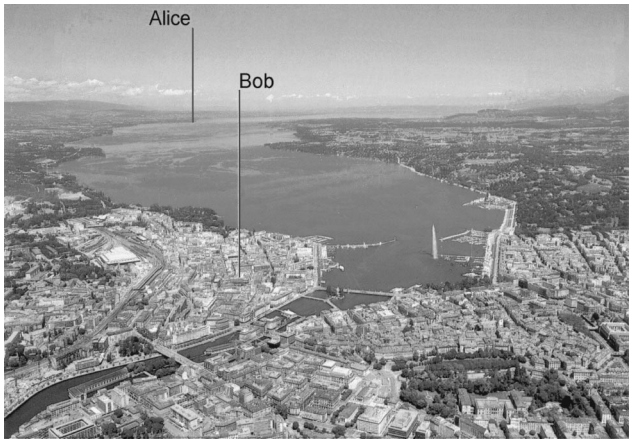

FIG. 13. Geneva and Lake Geneva. The Swisscom optical fiber cable used for quantum cryptography experiments runs under the lake between the town of Nyon, about 23 km north of Geneva, and the center of the city.

Recently, Townsend has also investigated such polarization-encoding systems for QC on short-span links up to 10 kilometers (1998a, 1998b) with photons at 800 nm. It is interesting to note that, although he used standard telecommunications fibers which could support more than one spatial mode at this wavelength, he was able to ensure single-mode propagation by carefully controlling the launching conditions. Because of the problem discussed above, polarization coding does not seem to be the best choice for QC in optical fibers. Nevertheless, this problem is drastically reduced when considering free-space key exchange, as air has essentially no birefringence at all (see Sec. IV.E).

C. Phase coding

The idea of encoding the value of qubits in the phase of photons was first mentioned by Bennett in the paper in which he introduced the two-state protocol (1992). It is indeed a very natural choice for optics specialists. State preparation and analysis are then performed with interferometers, which can be realized with single-mode optical fiber components.

Figure 14 presents an optical fiber version of a Mach-Zehnder interferometer. It is made out of two symmetric couplers—the equivalent of beamsplitters—connected to each other, with one phase modulator in each arm. One can inject light into the setup, using a continuous and classical source, and monitor the intensity at the output ports. Provided that the coherence length of the light used is larger than the path mismatch in the interferometers, interference fringes can be recorded. Taking into account the $\pi/2$ phase shift experienced upon reflection at a beamsplitter, the effect of the phase modu-

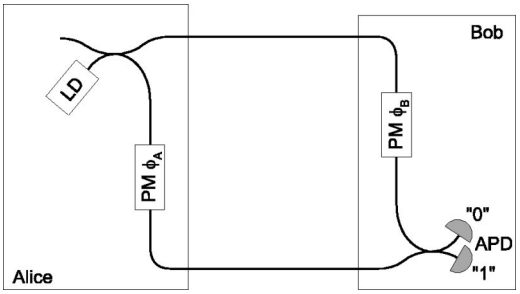

FIG. 14. Conceptual interferometric setup for quantum cryptography using an optical fiber Mach-Zehnder interferometer: LD, laser diode; PM, phase modulator; APD, avalanche photodiode.

lators (ϕ_A and ϕ_B), and the path-length difference (ΔL), the intensity in the output port labeled "0" is given by

$$I_0=\overline{I}\cdot\cos^2\left(\frac{\phi_A-\phi_B+k\Delta L}{2}\right), \tag{36}$$

where k is the wave number and $\overline{I}$ the intensity of the source. If the phase term is equal to $\pi/2+n\pi$, where n is an integer, destructive interference is obtained. Therefore the intensity registered in port 0 reaches a minimum, and all the light exits from port 1. When the phase term is equal to $n\pi$, the situation is reversed: constructive interference is obtained in port 0, while the intensity in port 1 goes to a minimum. With intermediate phase settings, light can be recorded in both ports. This device acts like an optical switch. It is essential to keep the path difference stable in order to record stationary interferences.

Although we have discussed the behavior of this interferometer for classical light, it works exactly the same when a single photon is injected. The probability of detecting the photon in one output port can be varied by changing the phase. It is the fiber optic version of Young's double-slit experiment, in which the arms of the interferometer replace the apertures.

This interferometer combined with a single-photon source and photon-counting detectors can be used for QC. Alice's setup consists of the source, the first coupler, and the first phase modulator, while Bob takes the second modulator and coupler, as well as the detectors. Let us consider the implementation of the four-state BB84 protocol. On the one hand, Alice can apply one of four phase shifts $(0,\pi/2,\pi,3\pi/2)$ to encode a bit value. She associates 0 and $\pi/2$ with bit 0, and π and $3\pi/2$ with bit 1. On the other hand, Bob performs a basis choice by randomly applying a phase shift of either 0 or $\pi/2$. He associates the detector connected to the output port 0 with a bit value of 0, and the detector connected to port 1 with bit 1. When the difference of their phase is equal to 0 or π, Alice and Bob are using compatible bases and they obtain deterministic results. In such cases, Alice can infer from the phase shift she applied the output port chosen by the photon at Bob's end and hence the bit value he registered. Bob, on his side, deduces from the output port chosen by the photon the phase that Alice selected. When the phase difference equals $\pi/2$ or $3\pi/2$, the bases are incompatible and the photon randomly chooses which port it takes at Bob's coupler. This scheme is summarized in Table I. We must stress that it is essential with this scheme to keep the path difference stable during a key exchange session. It should not change by more than a fraction of a wavelength of the photons. A drift of the length of one arm would indeed change the phase relation between Alice and Bob and induce errors in their bit sequence.

TABLE I. Implementation of the BB84 four-state protocol with phase encoding.

Alice			Bob	
Bit value	ϕ_A	ϕ_B	$\phi_A-\phi_B$	Bit value
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	π	1

It is interesting to note that encoding qubits with two-path interferometers is formally isomorphic to polarization encoding. The two arms correspond to a natural basis, and the weights c_j of each qubit state $\psi=(c_1e^{-i\phi/2},c_2e^{i\phi/2})$ are determined by the coupling ratio of the first beamsplitter, while the relative phase ϕ is introduced in the interferometer. The Poincaré sphere representation, which applies to all two-level quantum systems, can also be used to represent phase-coding states. In this case, the azimuth angle represents the relative phase between the light that has propagated along the two arms. The elevation corresponds to the coupling ratio of the first beamsplitter. States produced by a switch are on the poles, while those resulting from the use of a 50/50 beamsplitter lie on the equator. Figure 15 illustrates this analogy. Consequently, all polarization schemes can also be implemented using phase coding.

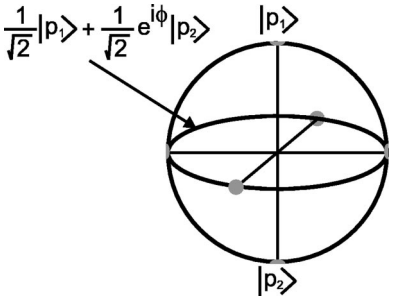

FIG. 15. Poincaré sphere representation of two-level quantum states generated by two-path interferometers. The poles correspond to the states generated by an interferometer in which the first coupler is replaced by a switch. The states generated with a symmetrical beamsplitter are on the equator. The azimuth indicates the phase between the two paths.

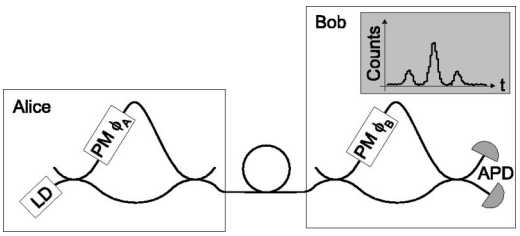

FIG. 16. Double Mach-Zehnder implementation of an interferometric system for quantum cryptography: LD, laser diode; PM, phase modulator; APD, avalanche photodiode. The inset represents the temporal count distribution recorded as a function of the time passed since the emission of the pulse by Alice. Interference is observed in the central peak.

Similarly, every coding using two-path interferometers can be realized using polarization. However, in practice one choice is often more convenient than the other, depending on circumstances like the nature of the quantum channel.[33]

1. The double Mach-Zehnder implementation

Although the scheme presented in the previous section works perfectly well on an optical table, it is impossible to keep the path difference stable when Alice and Bob are separated by more than a few meters. As mentioned above, the relative length of the arms should not change by more than a fraction of a wavelength. If Alice and Bob are separated by 1 kilometer, for example, it is clearly impossible to prevent path difference changes smaller than 1 μm caused by environmental variations. In his 1992 letter, Bennett also showed how to circumvent this problem. He suggested using two unbalanced Mach-Zehnder interferometers, one for Alice and one for Bob, connected in series by a single optical fiber (see Fig. 16). When monitoring counts as a function of the time since the emission of the photons, Bob obtains three peaks (see the inset in Fig. 16). The first one corresponds to the photons that chose the short path in both Alice's and Bob's interferometers, while the last one corresponds to photons that chose both the long paths. Finally, the central peak corresponds to photons that chose the short path in Alice's interferometer and the long one in Bob's, and vice versa. If these two processes are indistinguishable, they produce interference. A timing window can be used to discriminate between interfering and noninterfering events. If the latter are disregarded, it is then possible for Alice and Bob to exchange a key.

The advantage of this setup is that both "halves" of the photon travel in the same optical fiber. They thus experience the same optical length in the environmentally sensitive part of the system, provided that the variations in the fiber are slower than their temporal separations, determined by the interferometer's imbalance ($\approx$5 ns). This condition is much less difficult to fulfill. In order to obtain good fringe visibility, and hence a low error rate, the imbalances of the interferometers must be equal to within a fraction of the coherence time of the photons. This implies that the path differences must be matched to within a few millimeters, which does not constitute a problem. The imbalance must be chosen so that it is possible to distinguish the three temporal peaks clearly and thus discriminate interfering from noninterfering events. It must typically be larger than the pulse length and the timing jitter of the photon-counting detectors. In practice, the second condition is the more stringent one. Assuming a time jitter of the order of 500 ps, an imbalance of at least 1.5 ns keeps the overlap between the peaks low.

The main difficulty associated with this QC scheme is that the imbalances of Alice's and Bob's interferometers must be kept stable to within a fraction of the wavelength of the photons during a key exchange to maintain correct phase relations. This implies that the interferometers must lie in containers whose temperature is stabilized. In addition, for long key exchanges an active system is necessary to compensate for drift.[34] Finally, in order to ensure the indistinguishability of both interfering processes, one must make sure that in each interferometer the polarization transformation induced by the short path is the same as that induced by the long path. Both Alice and Bob must then use a polarization controller to fulfill this condition. However, the polarization transformation is rather stable in short optical fibers whose temperature is kept stable and which do not experience strains. Thus this adjustment does not need to be repeated frequently.

Paul Tapster and John Rarity of DERA, the Defence Evalution and Research Agency (Malvern, England), working with Paul Townsend, were the first to test this system over a fiber optic spool of 10 km (Townsend *et al.*, 1993a, 1993b). Townsend later improved the interferometer by replacing Bob's input coupler with a polarization splitter to suppress the lateral noninterfering peaks (1994). In this case, it is again unfortunately necessary to align the polarization state of the photons at Bob's end, in addition to stabilizing the imbalance in the interferometers. He later thoroughly investigated key exchange with phase coding and improved the transmission distance (Marand and Townsend, 1995; Townsend, 1998b). He also tested the possibility of multiplexing a

[33]Note, in addition, that using many-path interferometers opens up the possibility of coding quantum systems of dimensions larger than 2, like qutrits, ququarts, etc. (Bechmann-Pasquinucci and Peres, 2000; Bechmann-Pasquinucci and Tittel, 2000; Bourennane, Karlsson, and Bjorn, 2001).

[34]Polarization coding requires the optimization of three parameters (three parameters are necessary for unitary polarization control). In comparison, phase coding requires optimization of only one parameter. This is possible because the coupling ratios of the beamsplitters are fixed. Both solutions would be equivalent if one could limit the polarization evolution to rotations of the elliptic states without changes in the ellipticity.

quantum channel using two different wavelengths with conventional data transmission over a single optical fiber (Townsend, 1997a). Richard Hughes and co-workers from Los Alamos National Laboratory have also extensively tested such an interferometer (1996; Hughes, Morgan, and Peterson, 2000) up to distances of 48 km of installed optical fiber.[35]

2. "Plug-and-play" systems

As discussed in the two previous sections, both polarization and phase coding require active compensation of optical path fluctuations. A simple approach would be to alternate between adjustment periods—when pulses containing large numbers of photons are exchanged between Alice and Bob to adjust the compensating system correcting for slow drifts in phase or polarization—and qubits transmission periods, when the number of photons is reduced to a quantum level.

An approach invented in 1989 by Martinelli, then at CISE Tecnologie Innovative in Milano, allows one to automatically and passively compensate for all polarization fluctuations in an optical fiber (see also Martinelli, 1992). Let us first consider what happens to the polarization state of a light pulse traveling through an optical fiber, before being reflected by a Faraday mirror—a mirror with a $\lambda/4$ Faraday rotator[36] in front. We must first define a convenient description of the change in polarization of light reflected by a mirror at normal incidence. Let the mirror be in the x-y plane and z be the optical axis. Clearly, all linear polarization states are unchanged by a reflection. However, right-handed circular polarization is changed into left-handed and vice versa. Actually, after a reflection the rotation continues in the same sense, but since the propagation direction is reversed, right-handed and left-handed polarizations are swapped. The same holds for elliptic polarization states: the axes of the ellipse are unchanged, but right and left are exchanged. Accordingly, on a Poincaré sphere the polarization transformation upon reflection is described by a symmetry through the equatorial plane: the north and south hemispheres are exchanged $[\vec{m}\rightarrow(m_1,m_2,-m_3)]$, or in terms of the qubit state vector,

$$T:\ \begin{pmatrix}\psi_1\\ \psi_2\end{pmatrix}\rightarrow\begin{pmatrix}\psi_2^*\\ \psi_1^*\end{pmatrix}. \tag{37}$$

This is a simple representation, but some attention has to be paid. This transformation is not unitary. Indeed, the above description switches from a right-handed reference frame XYZ to a left-handed one $XY\tilde{Z}$, where $\tilde{Z}=-Z$. There is nothing wrong in doing this, and this explains the nonunitary polarization transformation.[37] Note that other descriptions are possible, but they require artificially breaking the XY symmetry. The main reason for choosing this particular transformation is that the description of the polarization evolution in the optical fiber before and after the reflection is then straightforward. Indeed, let $U=e^{-i\omega\vec{B}\vec{\sigma}\ell/2}$ describe this evolution under the effect of some modal birefringence $\vec{B}$ in a fiber section of length ℓ (where $\vec{\sigma}$ is the vector whose components are the Pauli matrices). Then the evolution after reflection is simply described by the inverse operator $U^{-1}=e^{i\omega\vec{B}\vec{\sigma}\ell/2}$. Now that we have a description of the mirror, let us add the Faraday rotator. It produces a $\pi/2$ rotation of the Poincaré sphere around the north-south axis: $F=e^{-i\pi\sigma_z/4}$ (see Fig. 17). Because the Faraday effect is nonreciprocal (remember that it is due to a magnetic field, which can be thought of as produced by a spiraling electric current), the direction of rotation around the north-south axis is independent of the light propagation direction. Accordingly, after reflection on the mirror, the second passage through the Faraday rotator rotates the polarization in the same direction (see again Fig. 17) and is described by the same operator F. Consequently, the total effect of a Faraday mirror is to

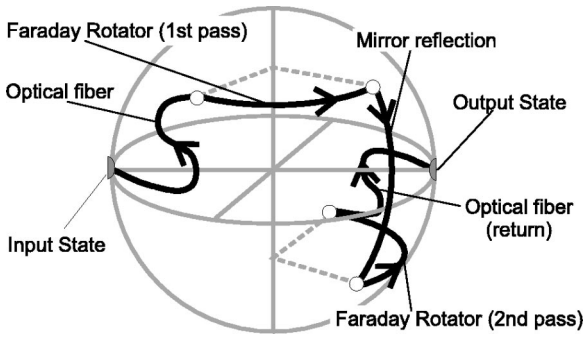

FIG. 17. Evolution of the polarization state of a light pulse represented on the Poincaré sphere over a round-trip propagation along an optical fiber terminated by a Faraday mirror.

[35]Note that in this experiment, Hughes and co-workers used an unusually high mean number of photons per pulse. They used a mean photon number of approximately 0.6 in the central interference peak, corresponding to a $\mu\approx1.2$ in the pulses leaving Alice. The latter value is the relevant one for eavesdropping analysis, since Eve could use an interferometer—conceivable with present technology—in which the first coupler was replaced by an optical switch and that allowed her to exploit all the photons sent by Alice. In light of this high μ and optical losses (22.8 dB), one may argue that this implementation was not secure, even when taking into account only so-called realistic eavesdropping strategies (see Sec. VI.I). Finally, it is possible to estimate the results that other groups would have obtained if they had used a similar value of μ. One then finds that key distribution distances of the same order could have been achieved. This illustrates that the distance is a somewhat arbitrary figure of merit for a QC system.

[36]These commercially available components are extremely compact and convenient when using telecommunications wavelengths, which is not true for other wavelengths.

[37]Note that this transformation is positive, but not completely positive. It is thus closely connected to the partial transposition map (Peres, 1996). If several photons are entangled, then it is crucial to describe all of them in frames with the same chirality. Actually that this is necessary is the content of the Peres-Horodecki entanglement witness (Horodecki *et al.*, 1996).

change any incoming polarization state into its orthogonal state: $\vec{m} \rightarrow -\vec{m}$. This is best seen in Fig. 17 but can also be expressed mathematically:

$$FTF: \begin{pmatrix} \psi_1 \\ \psi_2 \end{pmatrix} \rightarrow \begin{pmatrix} \psi_2^* \\ -\psi_1^* \end{pmatrix}. \tag{38}$$

Finally, the whole optical fiber can be modeled as consisting of a discrete number of birefringent elements. If there are N such elements in front of the Faraday mirror, the change in polarization during a round trip can be expressed (recall that the operator FTF only changes the sign of the corresponding Bloch vector $\vec{m} = \langle \psi | \vec{\sigma} | \psi \rangle$) as

$$U_1^{-1} \cdots U_N^{-1} FTF U_N \cdots U_1 = FTF. \tag{39}$$

The output polarization state is thus orthogonal to the input one, regardless of any birefringence in the fibers. This approach can thus correct for time-varying birefringence changes, provided that they are slow compared to the time required for the light to make a round trip (a few hundred microseconds).

By combining this approach with time multiplexing in a long-path interferometer, it is possible to implement a quantum cryptography system based on phase coding in which all optical and mechanical fluctuations are automatically and passively compensated for (Muller *et al.*, 1997). We performed the first experiment on such a system in early 1997 (Zbinden *et al.*, 1997), and a key was exchanged over a 23-km installed optical fiber cable (the same one as was used in the polarization coding experiments mentioned above). This setup featured a high interference contrast (fringe visibility of 99.8%) and excellent long-term stability and clearly established the value of the approach for QC. The fact that no optical adjustments were necessary earned it the nickname of "plug-and-play" setup. It is interesting to note that the idea of combining time multiplexing with Faraday mirrors was first used to implement an "optical microphone" (Bréguet and Gisin, 1995).[38]

However, our first realization still suffered from certain optical inefficiencies, and it has been improved since then. Like the setup tested in 1997, the new system is based on time multiplexing, in which the interfering pulses travel along the same optical path, but now, in different time ordering. A schematic is shown in Fig. 18. Briefly, the general idea is that pulses emitted at Bob's end can travel along one of two paths: they can go via the short arm, be reflected at the Faraday mirror (FM) at Alice's end, and finally, back at Bob's, setup travel via the long arm. Or, they travel first via the long arm at Bob's end, get reflected at Alice's end, and return via the short arm of Bob's setup. These two possibilities then superpose on beamsplitter C_1. We shall now explain the

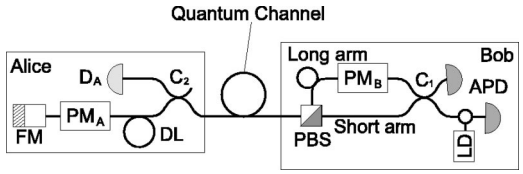

FIG. 18. Self-aligned plug-and-play system: LD, laser diode; APD, avalanche photodiode; C_i, fiber coupler; PM_j, phase modulator; PBS, polarizing beamsplitter; DL, optical delay line; FM, Faraday mirror; D_A, classical detector.

realization of this scheme in greater detail: A short and bright laser pulse is injected into the system through a circulator. It splits at a coupler. One of the half pulses, labeled P_1, propagates through the short arm of Bob's setup directly to a polarizing beamsplitter. The polarization transformation in this arm is set so that it is fully transmitted. P_1 is then sent through the fiber optic link. The second half pulse, labeled P_2, takes the long arm to the polarizing beamsplitter. The polarization evolution is such that P_2 is reflected. A phase modulator present in this long arm is left inactive so that it imparts no phase shift to the outgoing pulse. P_2 is also sent through the link, with a delay on the order of 200 ns. Both half pulses travel to Alice. P_1 goes through a coupler. The diverted light is detected with a classical detector to provide a timing signal. This detector is also important in preventing so-called Trojan horse attacks, which are discussed in Sec. VI.K. The nondiverted light then propagates through an attenuator and an optical delay line—consisting simply of an optical fiber spool—whose role will be explained later. Finally, it passes a phase modulator before being reflected by the Faraday mirror. P_2 follows the same path. Alice briefly activates her modulator to apply a phase shift on P_1 only, in order to encode a bit value exactly as in the traditional phase-coding scheme. The attenuator is set so that when the pulses leave Alice, they contain no more than a fraction of a photon. When they reach the polarizing beamsplitter after their return trip through the link, the polarization state of the pulses is exactly orthogonal to what it was when they left, thanks to the effect of the Faraday mirror. P_1 is then reflected instead of being transmitted. It takes the long arm to the coupler. When it passes, Bob activates his modulator to apply a phase shift used to implement his basis choice. Similarly, P_2 is transmitted and takes the short arm. Both pulses reach the coupler at the same time and they interfere. Single-photon detectors are then used to record the output port chosen by the photon.

We implemented the four full-state BB84 protocol with this setup. The system was tested once again on the same installed optical fiber cable linking Geneva and Nyon (23 km; see Fig. 13) at 1300 nm, and we observed a very low $\mathrm{QBER}_{opt} \approx 1.4\%$ (Ribordy *et al.*, 1998, 2000). Proprietary electronics and software were developed to allow for fully automated and user-friendly operation of the system. Because of the intrinsically bidirectional nature of this system, great attention had to be paid to Rayleigh backscattering. Light traveling in an optical fi-

[38]Note that since then, we have used this interferometer for various other applications: a nonlinear index-of-refraction measurement in fibers (Vinegoni, Wegmuller, and Gisin, 2000) and an optical switch (Vinegoni, Wegmuller, Huttner, and Gisin, 2000).

ber undergoes scattering by inhomogeneities. A small fraction ($\approx 1\,\%$) of this light is recaptured by the fiber in the backward direction. When the repetition rate is high enough, pulses traveling to and from Alice must intersect at some point along the line. Their intensity, however, is strongly different. The pulses are more than a thousand times brighter before than after reflection from Alice. Backscattered photons can accompany a quantum pulse propagating back to Bob and induce false counts. We avoided this problem by making sure that pulses traveling to and from Bob are not present in the line simultaneously. They are emitted by Bob in the form of trains. Alice stores these trains in her optical delay line, which consists of an optical fiber spool. Bob waits until all the pulses of a train have reached him before sending the next one. Although it completely solves the problem of Rayleigh backscattering-induced errors, this configuration has the disadvantage of reducing the effective repetition frequency. A storage line half as long as the transmission line amounts to a reduction of the bit rate by a factor of approximately 3.

Researchers at IBM simultaneously and independently developed a similar system at 1300 nm (Bethune and Risk, 2000). However, they avoided the problems associated with Rayleigh backscattering by reducing the intensity of the pulses emitted by Bob. Since these could not be used for synchronization purposes any longer, they added a wavelength-multiplexed classical channel (1550 nm) in the line to allow Bob and Alice to synchronize their systems. They tested their setup on a 10-km optical fiber spool. Both of these systems are equivalent and exhibit similar performances. In addition, the group of Anders Karlsson at the Royal Institute of Technology in Stockholm verified in 1999 that this technique also works at a wavelength of 1550 nm (Bourennane *et al.*, 1999, 2000). These experiments demonstrate the potential of plug-and-play-like systems for real-world quantum key distribution. They certainly constitute a good candidate for the realization of prototypes.

Their main disadvantage with respect to the other systems discussed in this section is that they are more sensitive to Trojan horse strategies (see Sec. VI.K). Indeed, Eve could send a probe beam and recover it through the strong reflection by the mirror at the end of Alice's system. To prevent such an attack, Alice adds an attenuator to reduce the amount of light propagating through her system. In addition, she must monitor the incoming intensity using a classical linear detector. Systems based on this approach cannot be operated with a true single-photon source and thus will not benefit from the progress in this field.[39]

D. Frequency coding

Phase-based systems for QC require phase synchronization and stabilization. Because of the high frequency of optical waves (approximately 200 THz at 1550 nm), this condition is difficult to fulfill. One solution is to use self-aligned systems like the plug-and-play setups discussed in the previous section. Goedgebuer and his team from the University of Besançon, in France, introduced an alternative solution (Sun *et al.*, 1995; Mazurenko *et al.*, 1997; Mérolla *et al.*, 1999; see also Molotkov, 1998). Note that the title of this section is not completely accurate, since the value of the qubits is coded not in the frequency of the light, but in the relative phase between sidebands of a central optical frequency.

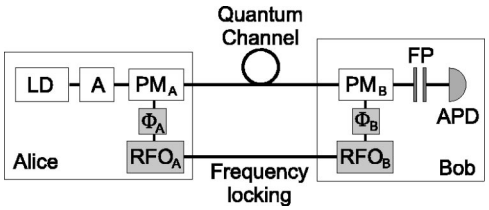

FIG. 19. Implementation of sideband modulation: LD, laser diode; A, attenuator; PM_i, optical phase modulator; Φ_j, electronic phase controller; RFO_k, radio frequency oscillator; FP, Fabry-Perot filter; APD, avalanche photodiode.

Their system is depicted in Fig. 19. A source emits short pulses of classical monochromatic light with angular frequency ω_S. A first phase modulator PM_A modulates the phase of this beam with a frequency $\Omega \ll \omega_S$ and a small modulation depth. Two sidebands are thus generated at frequencies $\omega_S \pm \Omega$. The phase modulator is driven by a radio-frequency oscillator RFO_A whose phase Φ_A can be varied. Finally, the beam is attenuated so that the sidebands contain much less than one photon per pulse, while the central peak remains classical. After the transmission link, the beam experiences a second phase modulation applied by PM_B. This phase modulator is driven by a second radio-frequency oscillator RFO_B with the same frequency Ω and phase Φ_B. These oscillators must be synchronized. After passing through this device, the beam contains the original central frequency ω_S, the sidebands created by Alice, and the sidebands created by Bob. The sidebands at frequencies $\omega_S \pm \Omega$ are mutually coherent and thus yield interference. Bob can then record the interference pattern in these sidebands after removal of the central frequency and the higher-order sidebands with a spectral filter.

To implement the B92 protocol (see Sec. II.D.1), Alice randomly chooses the value of the phase Φ_A for each pulse. She associates a bit value of 0 with phase 0 and a bit value of 1 with phase π. Bob also randomly chooses whether to apply a phase Φ_B of 0 or π. One can see that if $|\Phi_A - \Phi_B| = 0$, the interference is constructive and Bob's single-photon detector has a nonzero probability of recording a count. This probability depends on the number of photons initially present in the sideband, as well as on the losses induced by the channel. On the other hand, if $|\Phi_A - \Phi_B| = \pi$, interference is destructive, and no count will ever be recorded. Consequently, Bob can infer, every time he records a count, that he applied the same phase as Alice. When a given pulse does not yield a detection, the reason can be that the phases ap-

[39]The fact that the pulses make a round trip implies that losses are doubled, yielding a reduced counting rate.

plied were different and destructive interference took place. It can also mean that the phases were actually equal, but the pulse was empty or the photon got lost. Bob cannot decide between these two possibilities. From a conceptual point of view, Alice sends one of two nonorthogonal states. There is then no way for Bob to distinguish between them deterministically. However, he can perform a generalized measurement, also known as a *positive operator value measurement*, which will sometimes fail to give an answer, but at all other times gives the correct one.

Eve could perform the same measurement as Bob. When she obtains an inconclusive result, she could just block both the sideband and the central frequency so that she does not have to guess a value and does not risk introducing an error. To prevent her from doing that, Bob verifies the presence of this central frequency. Now if Eve tries to conceal her presence by blocking only the sideband, the reference central frequency will still have a certain probability of introducing an error. It is thus possible to catch Eve in both cases. The monitoring of the reference beam is essential in all two-state protocols to reveal eavesdropping. In addition, it was shown that this reference-beam monitoring can be extended to the four-state protocol (Huttner *et al.*, 1995).

The advantage of this setup is that the interference is controlled by the phase of the radio-frequency oscillators. Their frequency is six orders of magnitude smaller than the optical frequency and thus considerably easier to stabilize and synchronize. It is indeed a relatively simple task, which can be achieved by electronic means. The Besançon group performed key distribution with such a system. The source they used was a distributed Bragg reflector (DBR) laser diode at a wavelength of 1540 nm and a bandwidth of 1 MHz. It was externally modulated to obtain 50-ns pulses, thus increasing the bandwidth to about 20 MHz. They used two identical $LiNbO_3$ phase modulators operating at a frequency $\Omega/2\pi=300$ MHz. Their spectral filter was a Fabry-Perot cavity with a finesse of 55. Its resolution was 36 MHz. They performed key distribution over a 20-km single-mode optical fiber spool, recording a $QBER_{opt}$ contribution of approximately 4%. They estimated that 2% could be attributed to the transmission of the central frequency by the Fabry-Perot cavity. Note also that the detector noise was relatively high due to the long pulse durations. Both these errors could be lowered by increasing the separation between the central peak and the sidebands, allowing reduced pulse widths and hence shorter detection times and lower dark counts. Nevertheless, a compromise must be found since, in addition to the technical drawbacks of high-speed modulation, the polarization transformation in an optical fiber depends on the wavelength. The remaining 2% of the $QBER_{opt}$ is due to polarization effects in the setup.

This system is another possible candidate. Its main advantage is that it could be used with a true single-photon source if it existed. On the other hand, the contribution of imperfect interference visibility to the error rate is significantly higher than that measured with plug-and-play systems. In addition, if this system is to be truly independent of polarization, it is essential to ensure that the phase modulators have very low polarization dependency. In addition, the stability of the frequency filter may constitute a practical difficulty.

E. Free-space line-of-sight applications

Since optical fiber channels may not always be available, several groups are trying to develop free-space line-of-sight QC systems capable, for example, of distributing a key between building rooftops in an urban setting.

Of course it may sound difficult to detect single photons amidst background light, but the first experiments have already demonstrated the feasibility of free-space QC. Sending photons through the atmosphere also has advantages, since this medium is essentially nonbirefringent (see Sec. III.B.4). It is then possible to use plain polarization coding. In addition, one can ensure very high channel transmission over long distances by carefully choosing the wavelength of the photons (see again Sec. III.B.4). The atmosphere has, for example, a high transmission "window" in the vicinity of 770 nm (transmission as high as 80% can occur between a ground station and a satellite), which happens to be compatible with commercial silicon APD photon-counting modules (detection efficiency can be as high as 65% with low noise).

The systems developed for free-space applications are actually very similar to that shown in Fig. 12. The main difference is that the emitter and receiver are connected by telescopes pointing at each other, instead of by an optical fiber. The contribution of background light to errors can be maintained at a reasonable level by using a combination of timing discrimination (coincidence windows of typically a few nanoseconds), spectral filtering (interference filters $\leqslant 1$ nm), and spatial filtering (coupling into an optical fiber). This can be illustrated by the following simple calculation. Let us suppose that the isotropic spectral background radiance is $10^{-2}\ \mathrm{W\,m^{-2}\,nm^{-1}\,sr^{-1}}$ at 800 nm. This corresponds to the spectral radiance of a clear zenith sky with a sun elevation of 77° (Zissis and Larocca, 1978). The divergence θ of a Gaussian beam with radius w_0 is given by $\theta=\lambda/w_0\pi$. The product of beam (telescope) cross section and solid angle, which is a constant, is therefore $\pi w_0^2\pi\theta^2=\lambda^2$. By multiplying the radiance by λ^2, one obtains the spectral power density. With an interference filter of 1-nm width, the power incident on the detector is 6×10^{-15} W, corresponding to 2×10^4 photons per second or 2×10^{-5} photons per nanosecond. This quantity is approximately two orders of magnitude larger than the dark-count probability of Si APD's, but still compatible with the requirements of QC. The performance of free-space QC systems depends dramatically on atmospheric conditions and air quality. This is problematic for urban applications where pollution and aerosols degrade the transparency of air.

The first free-space QC experiment over a distance of more than a few centimeters[40] was performed by Jacobs and Franson in 1996. They exchanged a key over a distance of 150 m in a hallway illuminated with standard fluorescent lighting and over 75 m outdoors in bright daylight without excessive QBER. Hughes and his team were the first to exchange a key over more than one kilometer under outdoor nighttime conditions (Buttler *et al.*, 1998; Hughes, Buttler, *et al.*, 2000). More recently, they even improved their system to reach a distance of 1.6 km under daylight conditions (Buttler *et al.*, 2000). Finally, Rarity and co-workers performed a similar experiment, in which they exchanged a key over a distance of 1.9 km under nighttime conditions (Gorman *et al.*, 2001).

Until quantum repeaters become available and allow us to overcome the distance limitation of fiber-based QC, free-space systems seem to offer the only possibility for QC over distances of more than a few dozen kilometers. A QC link could be established between ground-based stations and a low-orbit (300–1200 km) satellite. The idea is for Alice and Bob to each exchange a key (k_A and k_B, respectively) with the same satellite, using QC. Then the satellite publicly announces the value $K = k_A \oplus k_B$, where $\oplus$ represents the XOR operator or, equivalently, the binary addition modulo 2 without carry. Bob subtracts his key from this value to recover Alice's key ($k_A = K \ominus k_B$).[41] The fact that the key is known to the satellite operator may at first be seen as a disadvantage. But this point might actually be conducive to the development of QC, since governments always like to control communications. Although it has not yet been demonstrated, Hughes as well as Rarity have estimated—in view of their free-space experiments—that the difficulty can be overcome. The main difficulty would come from beam pointing—do not forget that the satellites will move with respect to the ground—and wandering induced by turbulence. In order to minimize the latter problem, the photons would in practice probably be sent down from the satellite. Atmospheric turbulence is concentrated almost entirely in the first kilometer above the earth's surface. Another possibile way to compensate for beam wander is to use adaptative optics. Free-space QC experiments over distances of about 2 km constitute a major step towards key exchange with a satellite. According to Buttler *et al.* (2000), the optical depth is indeed similar to the effective atmospheric thickness that would be encountered in a surface-to-satellite application.

F. Multi-user implementations

Paul Townsend and colleagues have investigated the application of QC over multi-user optical fiber networks (Townsend *et al.*, 1994; Phoenix *et al.*, 1995; Townsend, 1997b). They used a passive optical fiber network architecture in which one Alice, the network manager, is connected to multiple network users (i.e., many Bobs; see Fig. 20). The goal is for Alice to establish a verifiably secure and unique key with each Bob. In the classical limit, the information transmitted by Alice is gathered by all Bobs. However, because of their quantum behavior, the photons are effectively routed at the beamsplitter to one, and only one, of the users. Using the double Mach-Zehnder configuration discussed above, they tested such an arrangement with three Bobs. Nevertheless, because of the fact that QC requires a direct and low-attenuation optical channel between Alice and Bob, the ability to implement it over large and complex networks appears limited.

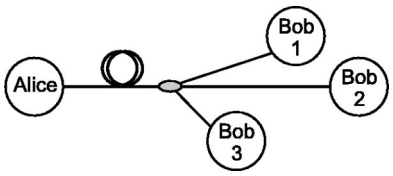

FIG. 20. Multi-user implementation of quantum cryptography with one Alice connected to three Bobs by optical fibers. The photons sent by Alice randomly choose to go to one or the other Bob at a coupler.

V. EXPERIMENTAL QUANTUM CRYPTOGRAPHY WITH PHOTON PAIRS

The possibility of using entangled photon pairs for quantum cryptography was first proposed by Ekert in 1991. In a subsequent paper, he investigated, with other researchers, the feasibility of a practical system (Ekert *et al.*, 1992). Although all tests of Bell's inequalities (for a review see, for example, Zeilinger, 1999) can be seen as experiments in quantum cryptography, systems specifically designed to meet the special requirements of QC, like quick changes of basis, have been implemented only recently.[42] In 1999, three groups demonstrated quantum cryptography based on the properties of entangled photons. Their results were reported in the same issue of Phys. Rev. Lett. (Jennewein, Simon, *et al.*, 2000; Naik *et al.*, 2000; Tittel *et al.*, 2000), illustrating the rapid progress in the still new field of quantum communication.

One advantage of using photon pairs for QC is the fact that one can remove empty pulses, since the detec-

[40]Remember that Bennett and co-workers performed the first demonstration of QC over 30 cm in air (Bennett, Bessette, *et al.*, 1992).

[41]This scheme could also be used with optical fiber implementation provided that secure nodes existed. In the case of a satellite, one tacitly assumes that it constitutes such a secure node.

[42]This definition of quantum cryptography applies to the famous experiment by Aspect and co-workers testing Bell's inequalities with time-varying analyzers (Aspect *et al.*, 1982). QC had, however, not yet been invented. It also applies to the more recent experiments closing *locality loopholes*, like the one performed in Innsbruck using fast polarization modulators (Weihs *et al.*, 1998) or the one performed in Geneva using two analyzers on each side (Tittel *et al.*, 1999; Gisin and Zbinden, 1999).

tion of one photon of a pair reveals the presence of a companion. In principle, it is thus possible to have a probability of emitting a nonempty pulse equal to one.[43] It is beneficial only because currently available single-photon detectors feature a high dark-count probability. The difficulty of always collecting both photons of a pair somewhat reduces this advantage. One frequently hears that photon pairs have the advantage of avoiding multiphoton pulses, but this is not correct. For a given mean photon number, the probability that a nonempty pulse contains more than one photon is essentially the same for weak pulses as for photon pairs (see Sec. III.A.2).

A second advantage is that using entangled photons pair prevents unintended information leakage in unused degrees of freedom (Mayers and Yao, 1998). Observing a QBER lower than approximately 15%, or equivalently observing that Bell's inequality is violated, indeed guarantees that the photons are entangled, so that the different states are not fully distinguishable through other degrees of freedom. A third advantage was indicated recently by new and elaborate eavesdropping analyses. The fact that passive state preparation can be implemented prevents multiphoton splitting attacks (see Sec. VI.J).

The coupling between the optical frequency and the property used to encode the qubit, i.e., decoherence, is rather easy to master when using faint laser pulses. However, this issue is more serious when using photon pairs, because of the larger spectral width. For example, for a spectral width of 5 nm full width at half maximum (FWHM)—a typical value, equivalent to a coherence time of 1 ps—and a fiber with a typical polarization mode dispersion of 0.2 ps/$\sqrt{\text{km}}$, transmission over a few kilometers induces significant depolarization, as discussed in Sec. III.B.2. In the case of polarization-entangled photons, this effect gradually destroys their correlation. Although it is in principle possible to compensate for this effect, the statistical nature of the polarization mode dispersion makes this impractical.[44] Although perfectly fine for free-space QC (see Sec. IV.E), polarization entanglement is thus not adequate for QC over long optical fibers. A similar effect arises when dealing with energy-time-entangled photons. Here, the chromatic dispersion destroys the strong time correlations between the photons forming a pair. However, as discussed in Sec. III.B.3, it is possible to compensate passively for this effect either using additional fibers with opposite dispersion, or exploiting the inherent energy correlation of photon pairs.

[43]Photon-pair sources are often, though not always, pumped continuously. In these cases, the time window determined by a trigger detector and electronics defines an effective pulse.

[44]In the case of weak pulses, we saw that a full round trip together with the use of Faraday mirrors circumvents the problem (see Sec. IV.C.2). However, since the channel loss on the way from the source to the Faraday mirror inevitably increases the fraction of empty pulses, the main advantage of photon pairs vanishes in such a configuration.

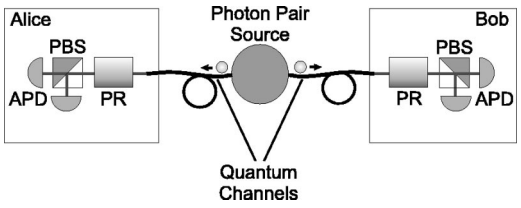

FIG. 21. Typical system for quantum cryptography exploiting photon pairs entangled in polarization: PR, active polarization rotator; PBS, polarizing beamsplitter; APD, avalanche photodiode.

Generally speaking, entanglement-based systems are far more complex than setups based on faint laser pulses. They will most certainly not be used in the near future for the realization of industrial prototypes. In addition, the current experimental key creation rates obtained with these systems are at least two orders of magnitude smaller than those obtained with faint laser pulse setups (net rate on the order of a few tens of bits per second, in contrast to a few thousand bits per second for a 10-km distance). Nevertheless, they offer interesting possibilities in the context of cryptographic optical networks. The photon-pair source can indeed be operated by a key provider and situated somewhere in between potential QC customers. In this case, the operator of the source has no way of getting any information about the key obtained by Alice and Bob.

It is interesting to emphasize the close analogy between one- and two-photon schemes, which was first noted by Bennett, Brassard, and Mermin (1992). In a two-photon scheme, when Alice detects her photon, she effectively prepares Bob's photon in a given state. In the one-photon analog, Alice's detectors are replaced by sources, while the photon-pair source between Alice and Bob is bypassed. The difference between these schemes lies only in practical issues, like the spectral widths of the light. Alternatively, one can look at this analogy from a different point of view: in two-photon schemes, it is as if Alice's photon propagates backwards in time from Alice to the source and then forward in time from the source to Bob.

A. Polarization entanglement

A first class of experiments takes advantage of polarization-entangled photon pairs. The setup, depicted in Fig. 21, is similar to the scheme used for polarization coding based on faint pulses. A two-photon source emits pairs of entangled photons flying back to back towards Alice and Bob. Each photon is analyzed with a polarizing beamsplitter whose orientation with respect to a common reference system can be changed rapidly. The results of two experiments were reported in the spring of 2000 (Jennewein, Simon, *et al.*, 2000; Naik *et al.*, 2000). Both used photon pairs at a wavelength of 700 nm, which were detected with commercial single-photon detectors based on silicon APD's. To create the photon pairs, both groups took advantage of parametric down-conversion in one or two β-BaB_2O_4 (BBO) crystals

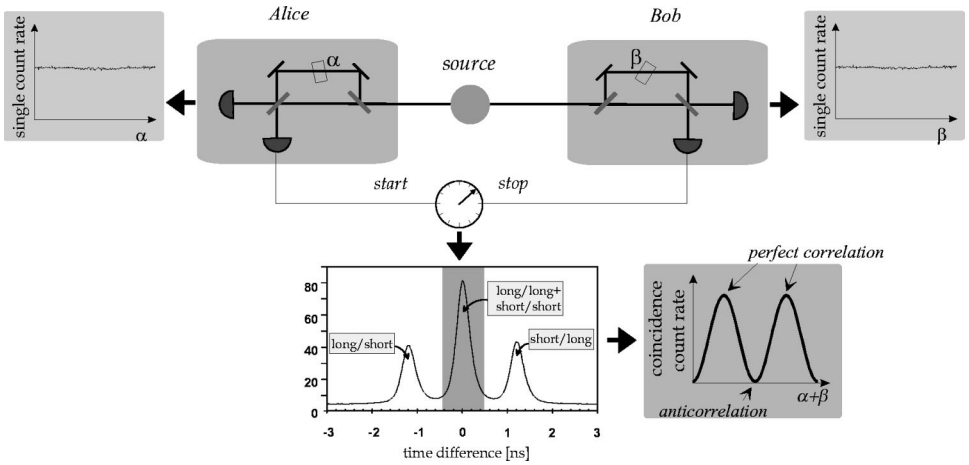

FIG. 22. Principle of phase-coding quantum cryptography using energy-time-entangled photon pairs.

pumped by an argon-ion laser. The analyzers consisted of fast modulators that were used to rotate the polarization state of the photons, in front of polarizing beam-splitters.

The group of Anton Zeilinger, then at the University of Innsbruck, demonstrated such a cryptosystem, including error correction, over a distance of 360 m (Jennewein, Simon, *et al.*, 2000). Inspired by a test of Bell's inequalities performed with the same setup a year earlier (Weihs *et al.*, 1998), they positioned the two-photon source near the center between the two analyzers. Special optical fibers, designed for guiding only a single mode at 700 nm, were used to transmit the photons to the two analyzers. The results of the remote measurements were recorded locally, and the processes of key sifting and error correction were implemented at a later stage, long after the distribution of the qubits. Two different protocols were implemented: one based on Wigner's inequality (a special form of Bell's inequalities) and the other based on BB84.

The group of Paul Kwiat, then at Los Alamos National Laboratory, demonstrated the Ekert protocol (Naik *et al.*, 2000). This experiment was a table-top realization in which the source and the analyzers were separated by only a few meters. The quantum channel consisted of a short free-space distance. In addition to performing QC, the researchers simulated different eavesdropping strategies. As predicted by theory, they observed a rise in the QBER with an increase of the information obtained by the eavesdropper. Moreover, they have also recently implemented the six-state protocol described in Sec. II.D.2 and observed the predicted QBER increase to 33% (Enzer *et al.*, 2001).

The main advantage of polarization entanglement is that analyzers are simple and efficient. It is therefore relatively easy to obtain high contrast. Naik and coworkers, for example, measured a polarization extinction of 97%, mainly limited by electronic imperfections of the fast modulators. This amounts to a QBER_{opt} contribution of only 1.5%. In addition, the constraint on the coherence length of the pump laser is not very stringent (note that, if it is shorter than the length of the crystal, some difficulties can arise, but we will not go into these here).

In spite of their qualities, it would be difficult to reproduce these experiments over distances of more than a few kilometers of optical fiber. As mentioned in the introduction to this section, polarization is indeed not robust enough to avoid decoherence in optical fibers. In addition, the polarization state transformation induced by an installed fiber frequently fluctuates, making an active alignment system absolutely necessary. Nevertheless, these experiments are very interesting in the context of free-space QC.

B. Energy-time entanglement

1. Phase coding

Another class of experiments takes advantage of energy-time-entangled photon pairs. The idea originates from an arrangement proposed by Franson in 1989 to test Bell's inequalities. As we shall see below, it is comparable to the double Mach-Zehnder configuration discussed in Sec. IV.C.1. A source emits pairs of energy-correlated photons, that were created at exactly the same (unknown) time (see Fig. 22). This can be achieved by pumping a nonlinear crystal with a pump of long coherence time. The pairs of downconverted photons are then split, and one photon is sent to each party down quantum channels. Both Alice and Bob possess a widely but identically unbalanced Mach-Zehnder interferometer, with photon-counting detectors connected to the outputs. Locally, if Alice or Bob change the phase of their interferometer, no effect on the count rates is observed, since the imbalance prevents any single-photon interference. Looking at the detection time at Bob's end with respect to the arrival time at Alice's end, three different values are possible for each combination of detectors. The different possibilities in a time spectrum are shown in Fig. 22. First, both photons can propagate through the short arms of the interferometers. Second, one can take the long arm at Alice's end, while the other one takes the short one at Bob's, or vice versa. Finally, both photons can propagate through the long arms. When the path differences of the interferometers are matched to within a fraction of the coherence length of the downconverted photons, the short-short and the

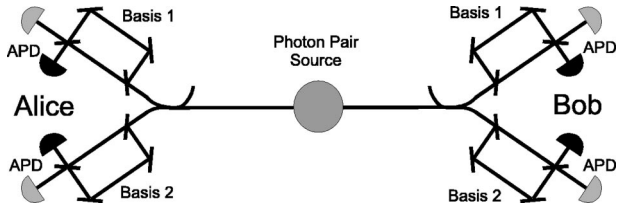

FIG. 23. System for quantum cryptography based on phase-coding entanglement: APD, avalanche photodiode. The photons choose their bases randomly at Alice and Bob's couplers.

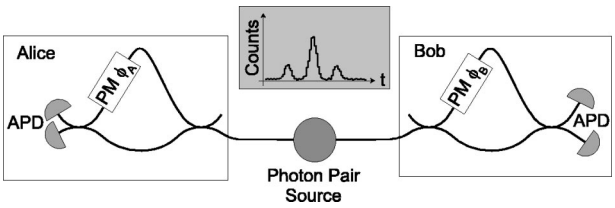

FIG. 24. Quantum cryptography system exploiting photons entangled in energy-time and active basis choice. Note the similarity to the faint-laser double Mach-Zehnder implementation depicted in Fig. 16.

long-long processes are indistinguishable, provided that the coherence length of the pump photon is larger than the path-length difference. Conditioning detection only on the central time peak, one observes two-photon interferences—nonlocal quantum correlations (Franson, 1989)[45]—that depend on the sum of the relative phases in Alice's and Bob's interferometers (see Fig. 22). The phases of Alice's and Bob's interferometers can, for example, be adjusted so that both photons always emerge from the same output port. It is then possible to exchange bits by associating values with the two ports. This, however, is insufficient. A second measurement basis must be implemented to ensure security against eavesdropping attempts. This measurement can be made, for example, by adding a second interferometer to the systems (see Fig. 23). In this case, when reaching an analyzer, a photon chooses randomly to go to one or the other interferometer. The second set of interferometers can also be adjusted to yield perfect correlations between output ports. The relative phases between their arms should, however, be chosen so that when the photons go to interferometers that are not associated with each other, the outcomes are completely uncorrelated.

Such a system features passive state preparation by Alice, yielding security against multiphoton splitting attacks (see Sec. VI.J). In addition, it also features a passive basis choice by Bob, which constitutes an elegant solution: neither a random-number generator nor an active modulator are necessary. It is nevertheless clear that QBER_{det} and QBER_{acc} [defined in Eq. (33)] are doubled, since the number of activated detectors is twice as high. This disadvantage is not as important as it first appears, since the alternative, a fast modulator, introduces losses close to 3 dB, also resulting in an increase of these error contributions. The striking similarity between this scheme and the double Mach-Zehnder arrangement discussed in the context of faint laser pulses in Sec. IV.C.1 is obvious when one compares Figs. 24 and 16.

This scheme was realized in the first half of 2000 by our group at the University of Geneva (Ribordy *et al.*, 2001). It was the first experiment in which an asymmetric setup optimized for QC was used instead of a system designed for tests of Bell's inequality, with a source located midway between Alice and Bob (see Fig. 25). The two-photon source (a $KNbO_3$ crystal pumped by a doubled Nd-YAG laser) provided energy-time-entangled photons at nondegenerate wavelengths—one at around 810 nm, the other centered at 1550 nm. This choice allowed the use of high-efficiency silicon-based single-photon counters featuring low noise to detect the photons of the lower wavelength. To avoid the high transmission losses at this wavelength in optical fibers, the distance between the source and the corresponding analyzer was very short, of the order of a few meters. The other photon, at the wavelength where fiber losses are minimal, was sent via an optical fiber to Bob's interferometer and then detected by InGaAs APD's. The decoherence induced by chromatic dispersion was limited by the use of dispersion-shifted optical fibers (see Sec. III.B.3).

Implementing the BB84 protocol in the manner discussed above, with a total of four interferometers, is difficult. Indeed, they must be aligned and their relative phase kept accurately stable during the whole key distribution session. To simplify this problem, we devised birefringent interferometers with polarization multiplexing of the two bases. Consequently the constraint on the stability of the interferometers was equivalent to that encountered in the faint-pulse double Mach-Zehnder system. We obtained interference visibilities typically of 92%, yielding in turn a QBER_{opt} contribution of about 4%. We demonstrated QC over a transmission distance of 8.5 km in a laboratory setting using a fiber on a spool and generated several megabits of key in hour-long ses-

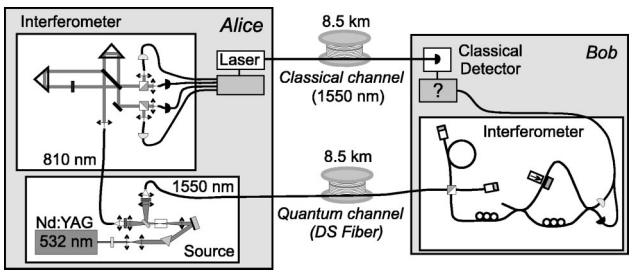

FIG. 25. Schematic diagram of the first system designed and optimized for long-distance quantum cryptography and exploiting phase coding of entangled photons.

[45]The imbalance of the interferometers must be large enough so that the middle peak can easily be distinguished from the satellite ones. This minimal imbalance is determined by the convolution of the detector's jitter (tens of picoseconds), the electronic jitter (from tens to hundreds of picoseconds), and the single-photon coherence time (<1 ps).

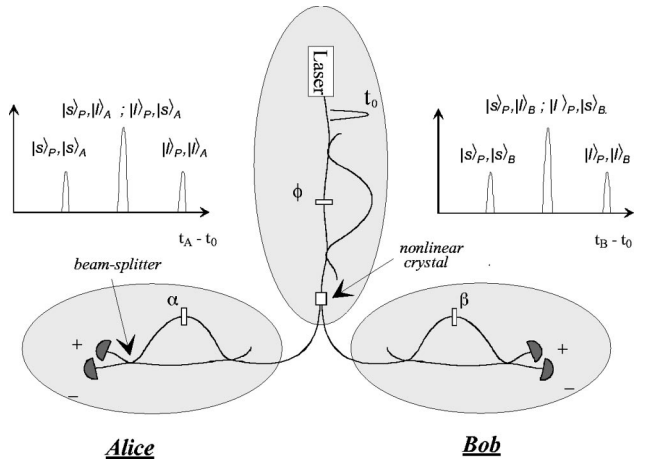

FIG. 26. Schematics of quantum cryptography using entangled-photon phase-time coding.

sions. This is the longest span realized to date for QC with photon pairs.

As already mentioned, it is essential for this scheme to have a pump laser whose coherence length is longer than the path imbalance of the interferometers. In addition, its wavelength must remain stable during a key exchange session. These requirements imply that the pump laser must be somewhat more elaborate than in the case of polarization entanglement.

2. Phase-time coding

We have mentioned in Sec. IV.C that states generated by two-path interferometers are two-level quantum systems. They can also be represented on a Poincaré sphere. The four states used for phase coding in the previous section would lie equally distributed on the equator of the sphere. The coupling ratio of the beamsplitter is 50%, and a phase difference is introduced between the components propagating through either arm. In principle, the four-state protocol can be equally well implemented with only two states on the equator and two others on the poles. In this section, we present a system exploiting such a set of states. Proposed by our group in 1999 (Brendel *et al.*, 1999), the scheme follows in principle the Franson configuration described in the context of phase coding. However, it is based on a pulsed source emitting entangled photons in so-called energy-time Bell states (Tittel *et al.*, 2000). The emission time of the photon pair is therefore given by a superposition of only two discrete terms, instead of by a wide and continuous range bounded only by the long coherence length of the pump laser (see Sec. V.B.1).

Consider Fig. 26. If Alice registers the arrival times of the photons with respect to the emission time of the pump pulse t_0, she finds the photons in one of three time slots (note that she has two detectors to take into account). For instance, detection of a photon in the first slot corresponds to the pump photon's having traveled via the short arm and the downconverted photon's having traveled via the short arm. To keep it simple, we refer to this process as $|s\rangle_P,|s\rangle_A$, where P stands for the pump and A for Alice's photon.[46] However, the characterization of the complete photon pair is still ambiguous, since, at this point, the path of the photon that has traveled to Bob (short or long in his interferometer) is unknown to Alice. Figure 26 illustrates all processes leading to a detection in the different time slots both at Alice's and at Bob's detector. Obviously, this reasoning holds for any combination of two detectors. In order to build up the secret key, Alice and Bob now publicly agree about the events when both detected a photon in one of the satellite peaks—without revealing in which one—or both in the central peak—without revealing in which detector. This procedure corresponds to key sifting. For instance, in the example discussed above, if Bob tells Alice that he has detected his photon in a satellite peak, she knows that it must have been the left peak. This is because the pump photon has traveled via the short arm, hence Bob can detect his photon either in the left satellite or in the central peak. The same holds for Bob, who now knows that Alice's photon traveled via the short arm in her interferometer. Therefore, in the case of joint detection in a satellite peak, Alice and Bob must have correlated detection times. Assigning a bit value to each side peak, Alice and Bob can exchange a sequence of correlated bits.

The cases where both find the photon in the central time slot are used to implement the second basis. They correspond to the $|s\rangle_P,|l\rangle_A|l\rangle_B$ and $|l\rangle_P,|s\rangle_A|s\rangle_B$ possibilities. If these are indistinguishable, one obtains two-photon interferences, exactly as in the case discussed in the previous section on phase coding. Adjusting the phases and keeping them stable, one can use the perfect correlations between output ports chosen by the photons at Alice's and Bob's interferometers to establish the key bits in this second basis.

Phase-time coding has recently been implemented in a laboratory experiment by our group (Tittel *et al.*, 2000) and was reported at the same time as the two polarization entanglement-based schemes mentioned above. A contrast of approximately 93% was obtained, yielding a QBER_{opt} contribution of 3.5%, similar to that obtained with the phase-coding scheme. This experiment will be repeated over long distances, since losses in optical fibers are low at the downconverted photon wavelength (1300 nm).

An advantage of this setup is that coding in the time basis is particularly stable. In addition, the coherence length of the pump laser is no longer critical. However, it is necessary to use relatively short pulses ($\approx$500 ps) powerful enough to induce a significant downconversion probability.

Phase-time coding, as discussed in this section, can also be realized with faint laser pulses (Bechmann-Pasquinucci and Tittel, 2000). The one-photon configuration has so far never been realized. It would be similar to the double Mach-Zehnder setup discussed in Sec. IV.C.1, but with the first coupler replaced by an active

[46]Note that it does not constitute a product state.

switch. For the time basis, Alice would set the switch either to full transmission or to full reflection, while for the energy basis she would set it at 50%. This illustrates how research on photon pairs can yield advances on faint-pulse systems.

3. Quantum secret sharing

In addition to QC using phase-time coding, we used the setup depicted in Fig. 26 for the first proof-of-principle demonstration of quantum secret sharing—the generalization of quantum key distribution to more than two parties (Tittel *et al.*, 2001). In this new application of quantum communication, Alice distributes a secret key to two other users, Bob and Charlie, in such a way that neither Bob nor Charlie alone has any information about the key, but together they have full information. As in traditional QC, an eavesdropper trying to get some information about the key creates errors in the transmission data and thus reveals her presence. The motivation behind quantum secret sharing is to guarantee that Bob and Charlie cooperate—one of them might be dishonest—in order to obtain a given piece of information. In contrast with previous proposals using three-particle Greenberger-Horne-Zeilinger states (Żukowski *et al.*, 1998; Hillery *et al.*, 1999), pairs of entangled photons in so-called energy-time Bell states were used to mimic the necessary quantum correlation of three entangled qubits, although only two photons exist at the same time. This is possible because of the symmetry between the preparation device acting on the pump pulse and the devices analyzing the downconverted photons. Therefore the emission of a pump pulse can be considered as the detection of a photon with 100% efficiency, and the scheme features a much higher coincidence rate than that expected with the initially proposed "triple-photon" schemes.

VI. EAVESDROPPING

A. Problems and objectives

After the qubit exchange and basis reconciliation, Alice and Bob each have a sifted key. Ideally, these keys are identical. But in real life, there are always some errors, and Alice and Bob must apply some classical information processing protocols, like error correction and privacy amplification to their data (see Sec. II.C.4). The first protocol is necessary to obtain identical keys and the second to obtain a secret key. Essentially, the problem of eavesdropping is to find protocols which, given that Alice and Bob can only measure the QBER, either provide Alice and Bob with a verifiably secure key or stop the protocol and inform the users that the key distribution has failed. This is a delicate problem at the intersection of quantum physics and information theory. Actually, it comprises several eavesdropping problems, depending on the precise protocol, the degree of idealization one admits, the technological power one assumes Eve has, and the assumed fidelity of Alice and Bob's equipment. Let us immediately stress that a complete analysis of eavesdropping on a quantum channel has yet to be achieved. In this section we review some of the problems and solutions, without any claim for mathematical rigor or complete coverage of the huge and rapidly evolving literature.

The general objective of eavesdropping analysis is to find ultimate and practical proofs of security for some quantum cryptosystems. "Ultimate proofs" guarantee security against entire classes of eavesdropping attacks, even if Eve uses not only the best of today's technology, but any conceivable future technology. These proofs take the form of theorems, with clearly stated assumptions expressed in mathematical terms. In contrast, practical proofs deal with some actual pieces of hardware and software. There is thus a tension between "ultimate" and "practical" proofs. Indeed, the former favor general abstract assumptions, whereas the latter concentrate on physical implementations. Nevertheless, it is worth finding such proofs. In addition to the security issue, they provide illuminating lessons for our general understanding of quantum information.

In the ideal game Eve has perfect technology: she is limited only by the laws of quantum mechanics, but not at all by current technology.[47] In particular, Eve cannot clone qubits, as this is incompatible with quantum dynamics (see Sec. II.C.2), but she is free to use any unitary interaction between one or several qubits and an auxiliary system of her choice. Moreover, after the interaction, Eve may keep her auxiliary system unperturbed, in complete isolation from the environment, for an arbitrarily long time. Finally, after listening to all the public discussion between Alice and Bob, she can perform the measurement of her choice on her system, being again limited only by the laws of quantum mechanics. One assumes further that all errors are due to Eve. It is tempting to assume that some errors are due to Alice's and Bob's instruments, and this probably makes sense in practice. However, there is the danger of Eve's replacing them with higher-quality instruments (see the next section).

In the next section we elaborate on the most relevant differences between the above ideal game (ideal especially from Eve's point of view) and real systems. Next, we return to the idealized situation and present several eavesdropping strategies, starting from the simplest, in which explicit formulas can be written down, and ending with a general abstract security proof. Finally, we discuss practical eavesdropping attacks and comment on the complexity of a real system's security.

B. Idealized versus real implementation

Alice and Bob use the technology available today. This trivial remark has several implications. First, all

[47]The question of whether QC would survive the discovery of the currently unknown validity limits of quantum mechanics is interesting. Let us argue that it is likely that quantum mechanics will always adequately describe photons at telecommunications and visible wavelengths, just as classical mechanics will always adequately describe the fall of apples, whatever the future of physics may be.

real components are imperfect, so that the qubits are not prepared and detected in the exact basis described by the theory. Moreover, a real source always has a finite probability of producing more than one photon. Depending on the details of the encoding device, all photons carry the same qubit (see Sec. VI.J). Hence, in principle, Eve could measure the photon number without perturbing the qubit. This scenario is discussed in Sec. VI.H. Recall that, ideally, Alice should emit single-qubit photons, i.e., each logical qubit should be encoded in a single degree of freedom of a single photon.

On Bob's side the efficiency of his detectors is quite limited and the dark counts (spontaneous counts not produced by photons) are non-negligible. The limited efficiency is analogous to the losses in the quantum channel. The analysis of the dark counts is more delicate, and no complete solution is known. Conservatively, Lütkenhaus (2000) assumes in his analysis that all dark counts provide information to Eve. He also advises that, whenever two detectors fire simultaneously (generally due to a real photon and a dark count), Bob should not disregard such events but should choose a value at random. Note also that the different contributions of dark counts to the total QBER depend on whether Bob's choice of basis is implemented using an active or a passive switch (see Sec. IV.A).

Next, one usually assumes that Alice and Bob have thoroughly checked their equipment and that it is functioning according to specifications. This assumption is not unique to quantum cryptography but is critical, as Eve could be the actual manufacturer of the equipment. Classical cryptosystems must also be carefully tested, like any commercial apparatus. Testing a cryptosystem is tricky, however, because in cryptography the client buys confidence and security, two qualities difficult to quantify. Mayers and Yao (1998) proposed using Bell's inequality to test whether the equipment really obeys quantum mechanics, but even this is not entirely satisfactory. Interestingly, one of the most subtle loopholes in all present-day tests of Bell's inequality, the detection loophole, can be exploited to produce purely classical software mimicking all quantum correlations (Gisin and Gisin, 1999). This illustrates once again the close connection between practical issues in QC and philosophical debates about the foundations of quantum physics.

Finally, one must assume that Alice and Bob are perfectly isolated from Eve. Without such an assumption the entire game would be meaningless: clearly, Eve is not allowed to look over Alice's shoulder. However, this elementary assumption is again nontrivial. What if Eve uses the quantum channel connecting Alice to the outside world? Ideally, the channel should incorporate an isolator[48] to keep Eve from shining light into Alice's output port to examine the interior of her laboratory. Since all isolators operate only on a finite bandwidth, there should also be a filter, but filters have only a finite efficiency, and so on. Except for Sec. VI.K, in which this assumption is discussed, we shall henceforth assume that Alice and Bob are isolated from Eve.

C. Individual, joint, and collective attacks

In order to simplify the problem, several eavesdropping strategies of limited generality have been defined (Lütkenhaus, 1996; Biham and Mor, 1997a, 1997b) and analyzed. Of particular interest is the assumption that Eve attaches independent probes to each qubit and measures her probes one after the other. This class of attack is called the *individual attack*, or *incoherent attack*. This important class is analyzed in Secs. VI.D and VI.E. Two other classes of eavesdropping strategies let Eve process several qubits coherently, hence the name *coherent attacks*. The most general coherent attacks are called *joint attacks*, while an intermediate class assumes that Eve attaches one probe per qubit, as in individual attacks, but can measure several probes coherently, as in coherent attacks. This intermediate class is called the *collective attack*. It is not known whether this class is less efficient than the most general class, that of joint attacks. It is also not known whether it is more efficient than the simpler individual attacks. Actually, it is not even known whether joint attacks are more efficient than individual ones.

For joint and collective attacks, the usual assumption is that Eve measures her probe only after Alice and Bob have completed all public discussion about basis reconciliation, error correction, and privacy amplification. For the more realistic individual attacks, one assumes that Eve waits only until the basis reconciliation phase of the public discussion.[49] The motivation for this assumption is that one hardly sees what Eve could gain by waiting until after the public discussion on error correction and privacy amplification before measuring her probes, since she is going to measure them independently anyway.

Individual attacks have the nice feature that the problem can be entirely translated into a classical one: Alice, Bob, and Eve all have classical information in the form of random variables α, β, and ϵ, respectively, and the laws of quantum mechanics impose constraints on the joint probability distribution $P(\alpha,\beta,\epsilon)$. Such classical scenarios have been widely studied by the classical cryptology community, and many of their results can thus be directly applied.

D. Simple individual attacks: Intercept-resend and measurement in the intermediate basis

The simplest attack for Eve consists in intercepting all photons individually, measuring them in a basis chosen randomly between the two bases used by Alice, and sending new photons to Bob prepared according to her

[48]Optical isolators, based on the Faraday effect, let light pass through in only one direction.

[49]With today's technology, it might even be fair to assume that in individual attacks Eve must measure her probe before the basis reconciliation.

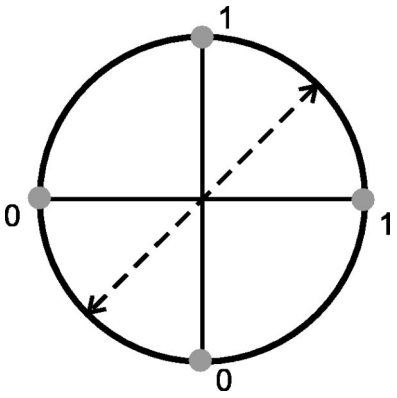

FIG. 27. Poincaré representation of the BB84 states and the intermediate basis, also known as the Breidbart basis, that can be used by Eve.

result. As presented in Sec. II.C.3 and assuming that the BB84 protocol is used, Eve thus gets 0.5 bits of information per bit in the sifted key, for an induced QBER of 25%. Let us illustrate the general formalism with this simple example. Eve's mean information gain on Alice's bit, $I(\alpha,\epsilon)$, equals their relative entropy decrease:

$$I(\alpha,\epsilon)=H_{a\ priori}-H_{a\ posteriori}, \tag{40}$$

i.e., $I(\alpha,\beta)$ is the number of bits one can save by writing α when knowing β. Since the *a priori* probability for Alice's bit is uniform, $H_{a\ priori}=1$. The *a posteriori* entropy has to be averaged over all possible results r that Eve might get:

$$H_{a\ posteriori}=\sum_r P(r)H(i|r), \tag{41}$$

$$H(i|r)=-\sum_i P(i|r)\log_2[P(i|r)], \tag{42}$$

where the *a posteriori* probability of bit i, given Eve's result r, is given by Bayes's theorem:

$$P(i|r)=\frac{P(r|i)P(i)}{P(r)}, \tag{43}$$

with $P(r)=\Sigma_i P(r|i)P(i)$. In the case of intercept resend, Eve gets one out of four possible results: $r\in\{\uparrow,\downarrow,\leftarrow,\rightarrow\}$. After the basis has been revealed, Alice's input assumes one of two values: $i\in\{\uparrow,\downarrow\}$ (assuming the $\uparrow\downarrow$ basis was used, the other case is completely analogous). One gets $P(i=\uparrow|r=\uparrow)=1$, $P(i=\uparrow|r=\rightarrow)=\frac{1}{2}$, and $P(r)=\frac{1}{2}$. Hence, $I(\alpha,\epsilon)=1-\frac{1}{2}h(1)-\frac{1}{2}h(\frac{1}{2})=1-\frac{1}{2}=\frac{1}{2}$ [with $h(p)=p\log_2(p)+(1-p)\log_2(1-p)$].

Another strategy for Eve, no more difficult to implement, consists in measuring the photons in the intermediate basis (see Fig. 27), also known as the Breidbart basis (Bennett, Bessette, *et al.*, 1992). In this case the probability that Eve guesses the correct bit value is $p=\cos(\pi/8)^2=\frac{1}{2}+\sqrt{2}/4\approx 0.854$, corresponding to a QBER$=2p(1-p)=25\%$ and a Shannon information gain per bit of

$$I=1-H(p)\approx 0.399. \tag{44}$$

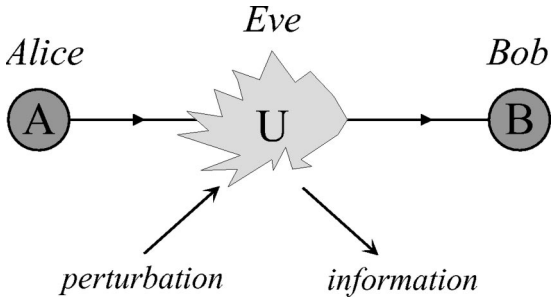

FIG. 28. Eavesdropping on a quantum channel. Eve extracts information from the quantum channel between Alice and Bob at the cost of introducing noise into that channel.

Consequently, this strategy is less advantageous for Eve than the intercept-resend strategy. Note however, that with this strategy Eve's probability of guessing the correct bit value is 85%, compared to only 75% in the intercept-resend case. This is possible because in the latter case, Eve's information is deterministic in half the cases, while in the former Eve's information is always probabilistic (formally, this results from the convexity of the entropy function).

E. Symmetric individual attacks

In this section we present in some detail how Eve could get the maximum Shannon information for a fixed QBER, assuming a perfect single-qubit source and restricting Eve to attacks on one qubit after the other (i.e., individual attacks). The motivation is that this idealized situation is rather simple to treat and nicely illustrates several of the subtleties of the subject. Here we concentrate on the BB84 four-state protocol; for related results on the two-state and six-state protocols, see Fuchs and Peres (1996) and Bechmann-Pasquinucci and Gisin (1999), respectively.

The general idea of eavesdropping on a quantum channel is as follows. When a qubit propagates from Alice to Bob, Eve can let a system of her choice, called a probe, interact with the qubit (see Fig. 28). She can freely choose the probe and its initial state, but the system must obey the rules of quantum mechanics (i.e., be described in some Hilbert space). Eve can also choose the interaction, but it should be independent of the qubit state, and she should obey the laws of quantum mechanics; i.e., her interaction must be described by a unitary operator. After the interaction a qubit has to go to Bob (in Sec. VI.H we consider lossy channels, so that Bob does not always expect a qubit, a fact that Eve can take advantage of). It makes no difference whether this qubit is the original one (possibly in a modified state). Indeed, the question does not even make sense, since a qubit is nothing but a qubit. However, in the formalism it is convenient to use the same Hilbert space for the qubit sent by Alice as for the qubit received by Bob (this is no loss of generality, since the swap operator—defined by $\psi\otimes\phi\rightarrow\phi\otimes\psi$ for all ψ,ϕ—is unitary and could be appended to Eve's interaction).

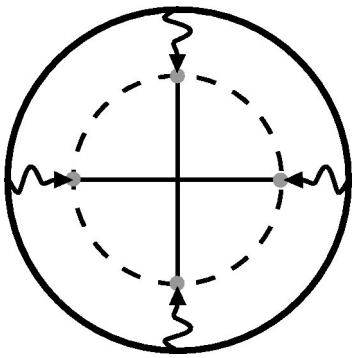

FIG. 29. Poincaré representation of BB84 states in the event of a symmetrical attack. The state received by Bob after the interaction of Eve's probe is related to the one sent by Alice by a simple shrinking factor. When the unitary operator U entangles the qubit and Eve's probe, Bob's state [Eq. (46)] is mixed and is represented by a point inside the Poincaré sphere.

Let $\mathcal{H}_{Eve}$ and $\mathbf{C}^2\otimes\mathcal{H}_{Eve}$ be the Hilbert spaces of Eve's probe and of the total qubit+probe system, respectively. If $|\vec{m}\rangle$, $|0\rangle$, and U denote the qubit's and the probe's initial states and the unitary interaction, respectively, then the state of the qubit received by Bob is given by the density matrix obtained by tracing out Eve's probe:

$$\rho_{Bob}(\vec{m})=\mathrm{Tr}_{\mathcal{H}_{Eve}}(U|\vec{m},0\rangle\langle\vec{m},0|U^{\dagger}). \tag{45}$$

The symmetry of the BB84 protocol makes it very natural to assume that Bob's state is related to Alice's $|\vec{m}\rangle$ by a simple shrinking factor[50] $\eta\in[0,1]$ (see Fig. 29):

$$\rho_{Bob}(\vec{m})=\frac{1+\eta\vec{m}\vec{\sigma}}{2}. \tag{46}$$

Eavesdropping attacks that satisfy the above condition are called *symmetric-attacks*.

Since the qubit state space is two dimensional, the unitary operator is entirely determined by its action on two states, for example, the $|\uparrow\rangle$ and $|\downarrow\rangle$ states (in this section we use spin-$\frac{1}{2}$ notation for the qubits). After the unitary interaction, it is convenient to write the states in the Schmidt form (Peres, 1997):

$$U|\uparrow,0\rangle=|\uparrow\rangle\otimes\phi_{\uparrow}+|\downarrow\rangle\otimes\theta_{\uparrow}, \tag{47}$$

$$U|\downarrow,0\rangle=|\downarrow\rangle\otimes\phi_{\downarrow}+|\uparrow\rangle\otimes\theta_{\downarrow}, \tag{48}$$

where the four states $\phi_{\uparrow}$, $\phi_{\downarrow}$, $\theta_{\uparrow}$, and $\theta_{\downarrow}$ belong to the Hilbert space of Eve's probe $\mathcal{H}_{Eve}$ and satisfy $\phi_{\uparrow}\perp\theta_{\uparrow}$ and $\phi_{\downarrow}\perp\theta_{\downarrow}$. By symmetry $|\phi_{\uparrow}|^2=|\phi_{\downarrow}|^2\equiv\mathcal{F}$ and $|\theta_{\uparrow}|^2=|\theta_{\downarrow}|^2\equiv\mathcal{D}$. Unitarity imposes $\mathcal{F}+\mathcal{D}=1$ and

$$\langle\phi_{\uparrow}|\theta_{\downarrow}\rangle+\langle\theta_{\uparrow}|\phi_{\downarrow}\rangle=0. \tag{49}$$

The ϕ's correspond to Eve's state when Bob receives the qubit undisturbed, while the θ's are Eve's state when the qubit is disturbed.

Let us emphasize that this is the most general unitary interaction satisfying Eq. (46). One finds that the shrinking factor is given by $\eta=\mathcal{F}-\mathcal{D}$. Accordingly, if Alice sends $|\uparrow\rangle$ and Bob measures it in the compatible basis, then $\langle\uparrow|\rho_{Bob}(\vec{m})|\uparrow\rangle=\mathcal{F}$ is the probability that Bob gets the correct result. Hence $\mathcal{F}$ is the fidelity and $\mathcal{D}$ the QBER.

Note that only four states span Eve's relevant state space. Hence Eve's effective Hilbert space is at most four dimensional, no matter how subtle she might be.[51] This greatly simplifies the analysis.

Symmetry requires that the attack on the other basis satisfy

$$U|\rightarrow,0\rangle=U\frac{|\uparrow,0\rangle+|\downarrow,0\rangle}{\sqrt{2}} \tag{50}$$

$$=\frac{1}{\sqrt{2}}(|\uparrow\rangle\otimes\phi_{\uparrow}+|\downarrow\rangle\otimes\theta_{\uparrow} \tag{51}$$

$$+|\downarrow\rangle\otimes\phi_{\downarrow}+|\uparrow\rangle\otimes\theta_{\downarrow}) \tag{52}$$

$$=|\rightarrow\rangle\otimes\phi_{\rightarrow}+|\leftarrow\rangle\otimes\theta_{\rightarrow}, \tag{53}$$

where

$$\phi_{\rightarrow}=\frac{1}{2}(\phi_{\uparrow}+\theta_{\uparrow}+\phi_{\downarrow}+\theta_{\downarrow}), \tag{54}$$

$$\theta_{\rightarrow}=\frac{1}{2}(\phi_{\uparrow}-\theta_{\uparrow}-\phi_{\downarrow}+\theta_{\downarrow}). \tag{55}$$

Similarly,

$$\phi_{\leftarrow}=\frac{1}{2}(\phi_{\uparrow}-\theta_{\uparrow}+\phi_{\downarrow}-\theta_{\downarrow}), \tag{56}$$

$$\theta_{\leftarrow}=\frac{1}{2}(\phi_{\uparrow}+\theta_{\uparrow}-\phi_{\downarrow}-\theta_{\downarrow}). \tag{57}$$

Condition (46) for the $\{|\rightarrow\rangle,|\leftarrow\rangle\}$ basis implies that $\theta_{\rightarrow}\perp\phi_{\rightarrow}$ and $\theta_{\leftarrow}\perp\phi_{\leftarrow}$. By proper choice of the phases, $\langle\phi_{\uparrow}|\theta_{\downarrow}\rangle$ can be made real. By condition (49), $\langle\theta_{\uparrow}|\phi_{\downarrow}\rangle$ is then also real. Symmetry implies that $\langle\theta_{\rightarrow}|\phi_{\leftarrow}\rangle\in\mathrm{Re}$. A straightforward computation concludes that all scalar products among Eve's states are real and that the ϕ's generate a subspace orthogonal to the θ's:

$$\langle\phi_{\uparrow}|\theta_{\downarrow}\rangle=\langle\phi_{\downarrow}|\theta_{\uparrow}\rangle=0. \tag{58}$$

Finally, using $|\phi_{\rightarrow}|^2=\mathcal{F}$, i.e., that the shrinking is the same for all states, one obtains a relation between the probe states' overlap and the fidelity:

[50]Fuchs and Peres were the first to derive the result presented in this section, using numerical optimization. Almost simultaneously, it was derived by Robert Griffiths and his student Chi-Sheng Niu under very general conditions, and by Nicolas Gisin using the symmetry argument presented here. These five authors joined forces to produce a single paper (Fuchs *et al.*, 1997). The result of this section is thus also valid without this symmetry assumption.

[51]Actually, Niu and Griffiths (1999) showed that two-dimensional probes suffice for Eve to get as much information as with the strategy presented here, though in their case the attack is not symmetric (one basis is more disturbed than the other).

$$\mathcal{F}=\frac{1+\langle\hat{\theta}_{\uparrow}|\hat{\theta}_{\downarrow}\rangle}{2-\langle\hat{\phi}_{\uparrow}|\hat{\phi}_{\downarrow}\rangle+\langle\hat{\theta}_{\uparrow}|\hat{\theta}_{\downarrow}\rangle}, \tag{59}$$

where the hats denote normalized states, e.g., $\hat{\phi}_{\uparrow}=\phi_{\uparrow}\mathcal{D}^{-1/2}$.

Consequently the entire class of symmetric individual attacks depends only on two real parameters:[52] $\cos(x)\equiv\langle\hat{\phi}_{\uparrow}|\hat{\phi}_{\downarrow}\rangle$ and $\cos(y)\equiv\langle\hat{\theta}_{\uparrow}|\hat{\theta}_{\downarrow}\rangle$.

Thanks to symmetry, it suffices to analyze this scenario for the case when Alice sends the $|\uparrow\rangle$ state and Bob measures in the $\{\uparrow,\downarrow\}$ basis (if not, Alice, Bob, and Eve disregard the data). Since Eve knows the basis, she knows that her probe is in one of the following two mixed states:

$$\rho_{Eve}(\uparrow)=\mathcal{F}P(\phi_{\uparrow})+\mathcal{D}P(\theta_{\uparrow}), \tag{60}$$

$$\rho_{Eve}(\downarrow)=\mathcal{F}P(\phi_{\downarrow})+\mathcal{D}P(\theta_{\downarrow}). \tag{61}$$

An optimum measurement strategy for Eve to distinguish between $\rho_{Eve}(\uparrow)$ and $\rho_{Eve}(\downarrow)$ consists in first determining whether her state is in the subspace generated by $\phi_{\uparrow}$ and $\phi_{\downarrow}$ or the one generated by $\theta_{\uparrow}$ and $\theta_{\downarrow}$. This is possible, since the two subspaces are mutually orthogonal. Eve must then distinguish between two pure states with an overlap of either $\cos x$ or $\cos y$. The first alternative occurs with probability $\mathcal{F}$, the second with probability $\mathcal{D}$. The optimal measurement distinguishing two states with overlap $\cos x$ is known to provide Eve with the correct guess with probability $[1+\sin(x)]/2$ (Peres, 1997). Eve's maximal Shannon information, attained when she performs the optimal measurements, is thus given by

$$I(\alpha,\epsilon)=\mathcal{F}\cdot\left[1-h\left(\frac{1+\sin x}{2}\right)\right]+\mathcal{D}\cdot\left[1-h\left(\frac{1+\sin y}{2}\right)\right], \tag{62}$$

where $h(p)=-p\log_2(p)-(1-p)\log_2(1-p)$. For a given error rate $\mathcal{D}$, this information is maximal when $x=y$. Consequently, for $\mathcal{D}=[1-\cos(x)]/2$, one obtains:

$$I^{\max}(\alpha,\epsilon)=1-h\left(\frac{1+\sin x}{2}\right). \tag{63}$$

This provides the explicit and analytic optimum eavesdropping strategy. For $x=0$ the QBER (i.e., $\mathcal{D}$) and the information gain are both zero. For $x=\pi/2$ the QBER is $\frac{1}{2}$ and the information gain 1. For small QBER's, the information gain grows linearly:

$$I^{\max}(\alpha,\epsilon)=\frac{2}{\ln 2}\mathcal{D}+O(\mathcal{D})^2\approx 2.9\mathcal{D}. \tag{64}$$

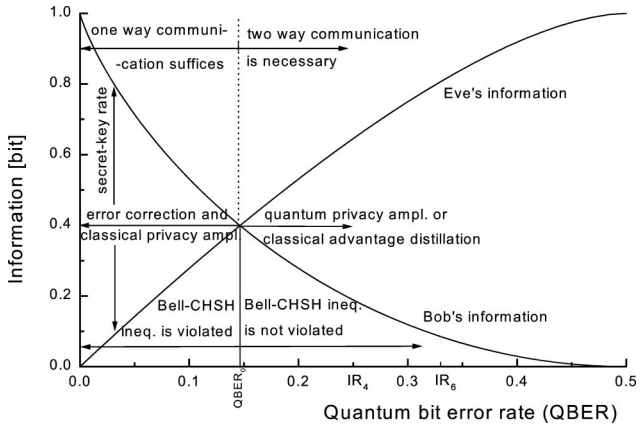

FIG. 30. Eve's and Bob's information vs the QBER, here plotted for incoherent eavesdropping on the four-state protocol. For QBER's below QBER_0, Bob has more information than Eve, and secret-key agreement can be achieved using classical error correction and privacy amplification, which can, in principle, be implemented using only one-way communication. The secret-key rate can be as large as the information differences. For QBER's above QBER_0 ($\equiv\mathcal{D}_0$), Bob has a disadvantage with respect to Eve. Nevertheless, Alice and Bob can apply quantum privacy amplification up to the QBER corresponding to the intercept-resend eavesdropping strategies (IR_4 and IR_6 for the four-state and six-state protocols, respectively). Alternatively, they can apply a classical protocol called advantage distillation, which is effective up to precisely the same maximal QBER IR_4 and IR_6. Both the quantum and the classical protocols require two-way communication. Note that for the eavesdropping strategy that will be optimal, from Eve Shannon point of view, on the four-state protocol, QBER_0 should correspond precisely to the noise threshold above which a Bell's inequality can no longer be violated.

Once Alice, Bob, and Eve have measured their quantum systems, they are left with classical random variables α, β, and ϵ, respectively. Secret-key agreement between Alice and Bob is then possible using only error correction and privacy amplification if and only if the Alice-Bob mutual Shannon information $I(\alpha,\beta)$ is greater than the Alice-Eve or the Bob-Eve mutual information,[53] $I(\alpha,\beta)>I(\alpha,\epsilon)$ or $I(\alpha,\beta)>I(\beta,\epsilon)$. It is thus interesting to compare Eve's maximal information [Eq. (64)] with Bob's Shannon information. The latter depends only on the error rate $\mathcal{D}$:

$$I(\alpha,\beta)=1-h(\mathcal{D}) \tag{65}$$

$$=1+\mathcal{D}\log_2(\mathcal{D})+(1-\mathcal{D})\log_2(1-\mathcal{D}). \tag{66}$$

Bob's and Eve's information are plotted in Fig. 30. As expected, for low error rates $\mathcal{D}$, Bob's information is greater. But, more errors provide Eve with more infor-

[52]Interestingly, when the symmetry is extended to a third maximally conjugated basis, as is natural in the six-state protocol of Sec. II.D.2, the number of parameters reduces to one. This parameter measures the relative quality of Bob's and Eve's "copy" of the qubit sent by Alice. When both copies are of equal quality, one recovers the optimal cloning presented in Sec. II.F (Bechmann-Pasquinucci and Gisin, 1999).

[53]Note, however, that if this condition is not satisfied, other protocols might sometimes be used; see Sec. II.C.5. These protocols are significantly less efficient and are usually not considered as part of "standard" QC. Note also that, in the scenario analyzed in this section, $I(\beta,\epsilon)=I(\alpha,\epsilon)$.

mation, while decreasing Bob's information. Hence both information curves cross at a specific error rate $\mathcal{D}_0$:

$$I(\alpha,\beta)=I^{\max}(\alpha,\epsilon)\Leftrightarrow\mathcal{D}=\mathcal{D}_0\equiv\frac{1-1/\sqrt{2}}{2}\approx 15\%. \quad (67)$$

Consequently the security criterion against individual attacks for the BB84 protocol is

$$\text{BB84 secure}\Leftrightarrow\mathcal{D}<\mathcal{D}_0\equiv\frac{1-1/\sqrt{2}}{2}. \quad (68)$$

For QBER's greater than $\mathcal{D}_0$, no (one-way communication) error correction and privacy amplification protocol can provide Alice and Bob with a secret key that is immune to any individual attacks.

Let us mention that there exists a class of more general classical protocols, called *advantage distillation* (Sec. II.C.5), which uses two-way communication. These protocols can guarantee secrecy if and only if Eve's intervention does not disentangle Alice and Bob's qubits (assuming they use the Ekert version of the BB84 protocol; Gisin and Wolf, 2000). If Eve optimizes her Shannon information as discussed in this section, this disentanglement limit corresponds to a QBER$=1-1/\sqrt{2}\approx 30\%$ (Gisin and Wolf, 1999). However, using more brutal strategies, Eve can disentangle Alice and Bob's qubits for a QBER of 25%; see Fig. 30. The latter is thus the absolute upper limit, taking into account the most general secret-key protocols. In practice, the limit (67) is more realistic, since advantage distillation algorithms are much less efficient than classical privacy amplification algorithms.

F. Connection to Bell's inequality

There is an intriguing connection between the tight-bound [Eq. (68)] and the Clauser-Horne-Shimony-Holt (CHSH) form of Bell's inequality (Bell, 1964; Clauser *et al.*, 1969; Clauser and Shimony, 1978; Zeilinger, 1999):

$$S\equiv E(a)+E(a,b')+E(a',b)-E(a',b')\leqslant 2. \quad (69)$$

Here $E(a,b)$ is the correlation between Alice and Bob's data when measuring $\sigma_a\otimes\mathbb{1}$ and $\mathbb{1}\otimes\sigma_b$, where σ_a denotes an observable with eigenvalues ± 1 parametrized by the label a. Recall that Bell's inequalities are necessarily satisfied by all local models but are violated by quantum mechanics.[54] To establish this connection, assume that the same quantum channel is used to test Bell's inequality. It is well known that, for error-free channels, a maximal violation by a factor $\sqrt{2}$ is achievable: $S_{\max}=2\sqrt{2}>2$. However, if the channel is imperfect, or equivalently if some perturbing Eve acts on the channel, then the quantum correlation $E(a,b|\mathcal{D})$ is reduced:

$$E(a,b|\mathcal{D})=\mathcal{F}\cdot E(a,b)-\mathcal{D}\cdot E(a,b) \quad (70)$$

$$=(1-2\mathcal{D})\cdot E(a,b), \quad (71)$$

where $E(a,b)$ denotes the correlation for the unperturbed channel. The achievable amount of violation is then reduced to $S_{\max}(\mathcal{D})=(1-2\mathcal{D})2\sqrt{2}$, and for large perturbations no violation at all can be achieved. Interestingly, the critical perturbation $\mathcal{D}$ up to which a violation can be observed is precisely the same $\mathcal{D}_0$ as the limit derived in the previous section for the security of the BB84 protocol:

$$S_{\max}(\mathcal{D})>2\Leftrightarrow\mathcal{D}<\mathcal{D}_0\equiv\frac{1-1/\sqrt{2}}{2}. \quad (72)$$

This is a surprising and appealing connection between the security of QC and tests of quantum nonlocality. One could argue that this connection is quite natural, since, if Bell's inequality were not violated, then quantum mechanics would be incomplete, and no secure communication could be based on such an incomplete theory. In some sense, Eve's information is like probabilistic local hidden variables. However, the connection between Eqs. (68) and (72) has not been generalized to other protocols. A complete picture of these connections is thus not yet available.

Let us emphasize that nonlocality plays no direct role in QC. Indeed, Alice is generally in Bob's absolute past. Nevertheless, Bell's inequality can be violated by spacelike separated events as well as by timelike separated events. However, the independence assumption necessary to derive Bell's inequality is justified by locality considerations only for spacelike separated events.

G. Ultimate security proofs

The security proof of QC with a perfect apparatus and a noise-free channel is straightforward. However, the fact that security can still be proven for an imperfect apparatus and noisy channels is far from obvious. Clearly, something has to be assumed about the apparatus. In this section we simply make the hypothesis that they are perfect. For the channel that is not under Alice and Bob's control, however, nothing is assumed. The question is then Up to what QBER can Alice and Bob apply error correction and privacy amplification to their classical bits? In the previous sections we found that the threshold is close to a QBER of 15%, assuming individual attacks. In principle Eve could manipulate several qubits coherently. How much help to Eve this possibility provides is still unknown, though some bounds are known. In 1996, Dominic Mayers (1996b) presented the

[54]Let us stress that the CHSH-Bell's inequality is the strongest possible for two qubits. Indeed, this inequality is violated if and only if the correlation cannot be reproduced by a local hidden-variable model (Pitowski, 1989).

main ideas on how to prove security.[55] In 1998, two major papers were made public on the Los Alamos archives (Mayers, 1998, and Lo and Chau, 1999). Today, these proofs are generally considered valid, thanks to the work of—among others—Shor and Preskill (2000), Inamori *et al.* (2001), and Biham *et al.* (1999). However, it is worth noting that during the first few years after the initial disclosure of these proofs, hardly anyone in the community understood them.

Here we shall present the argument in a form quite different from the original proofs. Our presentation aims at being transparent in the sense that it rests on two theorems. The proofs of the theorems are difficult and will be omitted. However, their claims are easy to understand and rather intuitive. Once one accepts the theorems, the security proof is straightforward.

The general idea is that at some point Alice, Bob, and Eve perform measurements on their quantum systems. The outcomes provide them with classical random variables α, β, and ϵ, respectively, with $P(\alpha,\beta,\epsilon)$ the joint probability distribution. The first theorem, a standard of classical information-based cryptography, states the necessary and sufficient condition on $P(\alpha,\beta,\epsilon)$ for Alice and Bob to extract a secret key from $P(\alpha,\beta,\epsilon)$ (Csiszár and Körner, 1978). The second theorem is a clever version of Heisenberg's uncertainty relation expressed in terms of available information (Hall, 1995): it sets a bound on the sum of the information about Alice's key available to Bob and to Eve.

Theorem 1. For a given $P(\alpha,\beta,\epsilon)$, Alice and Bob can establish a secret key (using only error correction and classical privacy amplification) if and only if $I(\alpha,\beta) \geqslant I(\alpha,\epsilon)$ or $I(\alpha,\beta) \geqslant I(\beta,\epsilon)$, where $I(\alpha,\beta)=H(\alpha)-H(\alpha|\beta)$ denotes the mutual information and H is the Shannon entropy.

Theorem 2. Let E and B be two observables in an N-dimensional Hilbert space. Let ϵ, β, $|\epsilon\rangle$, and $|\beta\rangle$ be the corresponding eigenvalues and eigenvectors, respectively, and let $c=\max_{\epsilon,\beta}\{|\langle\epsilon|\beta\rangle|\}$. Then

$$I(\alpha,\epsilon)+I(\alpha,\beta)\leqslant 2\log_2(Nc), \tag{73}$$

where $I(\alpha,\epsilon)=H(\alpha)-H(\alpha|\epsilon)$ and $I(\alpha,\beta)=H(\alpha)-H(\alpha|\beta)$ are the entropy differences corresponding to the probability distribution of the eigenvalues α prior to and deduced from any measurement by Eve and Bob, respectively.

The first theorem states that Bob must have more information about Alice's bits than does Eve (see Fig. 31).

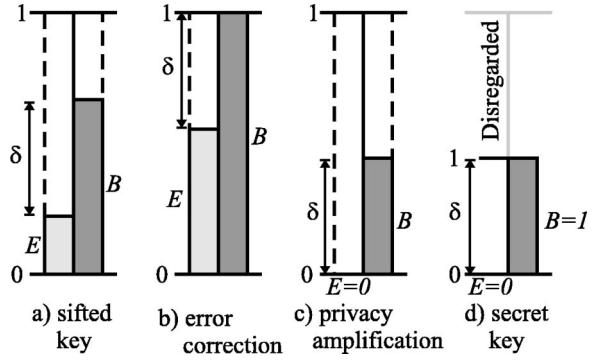

FIG. 31. Intuitive illustration of Theorem 1. The initial situation is depicted in (a). During the one-way public discussion phase of the protocol, Eve receives as much information as Bob; the initial information difference δ thus remains. After error correction, Bob's information equals 1, as illustrated in (b). After privacy amplification Eve's information is zero. In (c) Bob has replaced with random bits all bits to be disregarded. Hence the key still has its original length, but his information has decreased. Finally, in (d) removal of the random bits shortens the key to the initial information difference. Bob has full information on this final key, while Eve has none.

Since error correction and privacy amplification can be implemented using only one-way communication, Theorem 1 can be understood intuitively as follows. The initial situation is depicted in Fig. 31(a). During the public phase of the protocol, because of the one-way communication, Eve receives as much information as Bob. The initial information difference δ thus remains. After error correction, Bob's information equals 1, as illustrated in Fig. 31(b). After privacy amplification Eve's information is zero. In Fig. 31(c) Bob has replaced all bits to be disregarded by random bits. Hence the key still has its original length, but his information has decreased. Finally, upon removal of the random bits, the key is shortened to the initial information difference δ; see Fig. 31(d). Bob has full information about this final key, while Eve has none.

The second theorem states that if Eve performs a measurement providing her with some information $I(\alpha,\epsilon)$, then, because of the perturbation, Bob's information is necessarily limited. Using these two theorems, the argument now runs as follows. Suppose Alice sends out a large number of qubits and that n are received by Bob in the correct basis. The relevant Hilbert space's dimension is thus $N=2^n$. Let us relabel the bases used for each of the n qubits such that Alice uses n times the x basis. Hence Bob's observable is the n-time tensor product $\sigma_x\otimes\cdots\otimes\sigma_x$. By symmetry, Eve's optimal information about the correct bases is precisely the same as her optimal information about the incorrect ones (Mayers, 1998). Hence one can bound her information, assuming she measures $\sigma_z\otimes\cdots\otimes\sigma_z$. Accordingly, $c=2^{-n/2}$, and Theorem 2 implies

$$I(\alpha,\epsilon)+I(\alpha,\beta)\leqslant 2\log_2(2^n 2^{-n/2})=n. \tag{74}$$

That is, the sum of Eve's and Bob's information per qubit is less than or equal to 1. This result is quite intuitive:

[55] One of the authors (N.G.) vividly remembers the 1996 Institute for Scientific Interchange workshop in Torino, Italy, sponsored by Elsag Bailey, where he ended his talk by stressing the importance of security proofs. Dominic Mayers stood up, gave some explanation, and wrote a formula on a transparency, claiming that this was the result of his proof. We think it is fair to say that no one in the audience understood Mayers' explanation. However, N.G. kept the transparency, and it contains the basic Eq. (75) (up to a factor of 2, which corresponds to an improvement of Mayer's result obtained in 2000 by Shor and Preskill, using ideas from Lo and Chau).

together, Eve and Bob cannot receive more information than is sent out by Alice! Next, combining the bound (74) with Theorem 1, one deduces that a secret key is achievable whenever $I(\alpha,\beta)\geqslant n/2$. Using $I(\alpha,\beta)=n[1-\mathcal{D}\log_2(\mathcal{D})-(1-\mathcal{D})\log_2(1-\mathcal{D})]$, one obtains the sufficient condition on the error rate $\mathcal{D}$ (i.e., the QBER):

$$\mathcal{D}\log_2(\mathcal{D})+(1-\mathcal{D})\log_2(1-\mathcal{D})\leqslant\frac{1}{2}, \tag{75}$$

i.e., $\mathcal{D}\leqslant 11\%$.

This bound, QBER$\leqslant 11\%$, is precisely that obtained in Mayers's proof (after improvement by Shor and Preskill, 2000). The above proof is, strictly speaking, only valid if the key is much longer than the number of qubits that Eve attacks coherently, so that the Shannon information we used represents averages over many independent realizations of classical random variables. In other words, assuming that Eve can coherently attack a large but finite number n_0 of qubits, Alice and Bob can use the above proof to secure keys much longer than n_0 bits. If one assumes that Eve has unlimited power and is able to attack coherently any number of qubits, then the above proof does not apply, but Mayers's proof can still be used and provides precisely the same bound.

This 11% bound for coherent attacks is clearly compatible with the 15% bound found for individual attacks. The 15% bound is also necessary, since an explicit eavesdropping strategy reaching this bound is presented in Sec. VI.E. It is not known what happens in the intermediate range $11\%<\text{QBER}<15\%$, but the following scenario is plausible. If Eve is limited to coherent attacks on a finite number of qubits, then in the limit of arbitrarily long keys, she has a negligibly small probability that the bits combined by Alice and Bob during the error correction and privacy amplification protocols originate from qubits attacked coherently. Consequently, the 15% bound would still be valid (partial results in favor of this conjecture can be found in Cirac and Gisin, 1997 and Bechmann-Pasquinucci and Gisin, 1999). However, if Eve has unlimited power, in particular, if she can coherently attack an unlimited number of qubits, then the 11% bound might be required.

To conclude this section, let us stress that the above security proof applies equally to the six-state protocol (Sec. II.D.2). It also extends in a straightforward fashion to protocols using larger alphabets (Bechmann-Pasquinucci and Peres, 2000; Bechmann-Pasquinucci and Tittel, 2000; Bourennane, Karlsson, and Björn, 2001; Bourennane, Karlsson, Björn, Gisin, and Cerf, 2001).

H. Photon number measurements and lossless channels

In Sec. III.A we saw that all real photon sources have a finite probability of emittting more than one photon. If all emitted photons encode the same qubit, Eve can take advantage of this. In principle, she can first measure the number of photons in each pulse without disturbing the degree of freedom encoding the qubits.[56] Such measurements are sometimes called quantum nondemolition measurements, because they do not perturb the qubit; in particular they do not destroy the photons. This is possible because Eve knows in advance that Alice sends a mixture of states with well-defined photon numbers[57] (see Sec. II.F). Next, if Eve finds more than one photon, she keeps one and sends the other(s) to Bob. In order to prevent Bob from detecting a lower qubit rate, Eve must use a channel with lower losses. Using an ideally lossless quantum channel, Eve can even, under certain conditions, keep one photon and increase the probability that pulses with more than one photon get to Bob! Finally, when Eve finds one photon, she may destroy it with some probability that she does not affect the total number of qubits received by Bob. Consequently, if the probability that a nonempty pulse has more than one photon (on Alice's side) is greater than the probability that a nonempty pulse is detected by Bob, then Eve can get full information without introducing any perturbation. This is possible only when the QC protocol is not perfectly implemented, but it is a realistic situation (Huttner *et al.*, 1995; Yuen, 1997).

Quantum nondemolition atacks have recently received a lot of attention (Brassard *et al.*, 2000; Lütkenhaus, 2000). The debate is not yet settled. We would like to argue that it might be unrealistic, or even unphysical, to assume that Eve can perform ideal quantum nondemolition attacks. Indeed, she first needs the capacity to perform quantum nondemolition photon-number measurements. Although impossible with today's technology, this is a reasonable assumption (Nogues *et al.*, 1999). Next, she should be able to keep her photon until Alice and Bob reveal the basis. In principle, this could be achieved using a lossless channel in a loop. We discuss this eventuality below. Another possibility would be for Eve to map her photon to a quantum memory. This does not exist today but might well exist in the future. Note that the quantum memory should have essentially unlimited decoherence time, since Alice and Bob could easily wait for minutes before revealing the bases.[58] Finally, Eve must access a lossless channel, or at least a channel with lower losses than that used by Alice and

[56]For polarization coding, this is quite clear, but for phase coding one may think (incorrectly) that phase and photon number are incompatible. However, the phase used for encoding is a relative phase between two modes. Whether these modes are polarization modes or correspond to different times (determined, for example, by the relative length of interferometers), does not matter.

[57]Recall that a mixture of coherent states $|e^{i\phi}\alpha\rangle$ with a random phase ϕ, as produced by lasers when no phase reference is available, is equal to a mixture of photon number states $|n\rangle$ with Poisson statistics: $\int_0^{2\pi}|e^{i\phi}\alpha\rangle\langle e^{i\phi}\alpha|\,(d\phi/2\pi)=\Sigma_{n\geqslant 0}\,(\mu^n/n!)\,e^{-\mu}|n\rangle\langle n|$, where $\mu=|\alpha|^2$.

[58]The quantum part of the protocol could run continuously, storing large amounts of raw classical data, but the classical part of the protocol, which processes these raw data, could take place just seconds before the key is used.

Bob. This might be the trickiest point. Indeed, besides using a shorter channel, what can Eve do? Telecommunications fibers are already at the physical limits of what can be achieved (Thomas *et al.*, 2000). The loss is almost entirely due to Rayleigh scattering, which is unavoidable: solve the Schrödinger equation in a medium with inhomogeneities and you get scattering. When the inhomogeneities are due to the molecular stucture of the medium, it is difficult to imagine lossless fibers. The 0.18-dB/km attenuation in silica fibers at 1550 nm is a lower bound imposed by physics rather then technology.[59] Note that using air is not a viable solution, since attenuation at telecommunications wavelengths is rather high. Vacuum, the only way to avoid Rayleigh scattering, also has limitations, due to diffraction, again an unavoidable physical phenomenon. In the end, it seems that Eve has only two possibilities left. Either she uses teleportation (with extremely high success probability and fidelity) or she converts the photons to another wavelength (without perturbing the qubit). Both of these "solutions" seem unrealistic in the foreseeable future.

Consequently, when considering the type of attacks discussed in this section, it is essential to distinguish the ultimate proofs from the practical ones. Indeed, the assumptions about the defects of Alice and Bob's apparatuses must be very specific and might thus be of limited interest, while for practical considerations these assumptions must be very general and might thus be excessive.

I. A realistic beamsplitter attack

The attack presented in the previous section takes advantage of pulses containing more than one photon. However, as discussed, it uses unrealistic assumptions. In this section, following Dusek *et al.* (2000) and Lütkenhaus (2000), we briefly comment on a realistic attack that, also exploits multiphoton pulses (for details, see Felix *et al.*, 2001, where this and other examples are presented). Assume that Eve splits all pulses in two, analyzing each half in one of the two bases, using photon counting devices able to distinguish between pulses with 0, 1, and 2 photons (see Fig. 32). In practice this could be realized using many single-photon counters in parallel. This requires nearly perfect detectors, but at least one does not need to assume technology completely out of today's realm. Whenever Eve detects two photons in the same output, she sends a photon in the corresponding

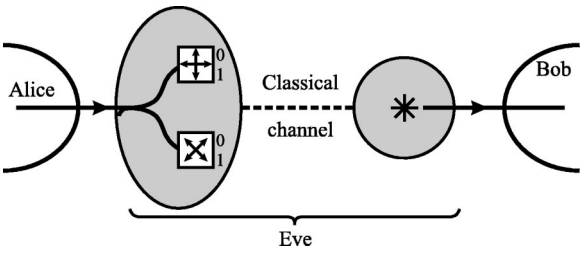

FIG. 32. Realistic beamsplitter attack. Eve stops all pulses. The two photon pulses have a 50% probability of being analyzed by the same analyzer. If this analyzer is compatible with the state prepared by Alice, then both photons are detected with the same outcome; if not, there is a 50% chance that they are detected with the same outcome. Hence there is a probability of $\frac{3}{8}$ that Eve detects both photons with the same outcome. In such a case, and only in such a case, she resends a photon to Bob. In $\frac{2}{3}$ of these cases she introduces no errors, since she has identified the correct state and gets full information; in the remaining cases she has a 50% probability of introducing an error and gains no information. The total QBER is thus $\frac{1}{6}$, and Eve's information gain is $\frac{2}{3}$.

state into Bob's apparatus. Since Eve's information is classical, she can overcome all the losses of the quantum channel. In all other cases, Eve sends nothing to Bob. In this way, Eve sends a fraction ($\frac{3}{8}$) of the pulses containing at least two photons to Bob. She introduces a QBER of $\frac{1}{6}$ and gets information $I(A,E)=\frac{2}{3}=4\cdot\mathrm{QBER}$. Bob does not see any reduction in the number of detected photons, provided that the transmission coefficient of the quantum channel t satisfies

$$t \leqslant \frac{3}{8}\mathrm{Prob}(n\geqslant 2|n\geqslant 1)\approx\frac{3\mu}{16}, \tag{76}$$

where the last expression assumes Poissonian photon distribution. Accordingly, for a fixed QBER, this attack provides Eve with twice the information she would get from using the intercept-resend strategy. To counter such an attack, Alice should use a mean photon number μ such that Eve can use this attack on only a fraction of the pulses. For example, Alice could use pulses weak enough that Eve's mean information gain is identical to what she would obtain with the simple intercept-resend strategy (see Sec. II.C.3). For 10-, 14-, and 20-dB attenuation, this corresponds to $\mu=0.25, 0.1$, and 0.025, respectively.

J. Multiphoton pulses and passive choice of states

Multiphoton pulses do not necessarily constitute a threat to key security, but they limit the key creation rate because they imply that more bits must be discarded during key distillation. This fact is based on the assumption that all photons in a pulse carry the same qubit, so that Eve does not need to copy the qubit going to Bob, but merely keeps the copy that Alice inadvertently provides. When using weak pulses, it seems unavoidable that all the photons in a pulse carry the same qubit. However, in two-photon implementations, each

[59]Photonics crystal fibers have the potential to overcome the Rayleigh scattering limit. There are two kinds of such fibers. The first kind guides light by total internal reflection, as in ordinary fibers. In these fibers most of the light also propagates in silica, and thus the loss limit is similar. In the second kind, most of the light propagates in air. Thus the theoretical loss limit is lower. However, today the losses are extremely high, in the range of hundreds of dB/km. The best reported result that we are aware of is 11 dB/km, and it was obtained with the first kind of fiber (Canning *et al.*, 2000).

photon on Alice's side independently chooses a state [in the experiments of Ribordy *et al.* (2001) and Tittel *et al.* (2000), each photon randomly chooses both its basis and its bit value; in the experiments of Naik *et al.* (2000) and Jennewein, Simon, *et al.* (2000), only the bit value choice is random]. Hence, when two photon pairs are simultaneously produced, the two twins carry independent qubits by accident. Consequently, Eve cannot take advantage of such multiphoton twin pulses. This might be one of the main advantages of two-photon schemes over the much simpler weak-pulse schemes. But the multiphoton problem is then on Bob's side, which gets a noisy signal, consisting partly of photons not in Alice's state.

K. Trojan horse attacks

All eavesdropping strategies discussed up to this point have consisted of Eve's attempt to get a maximum information from the qubits exchanged by Alice and Bob. However, Eve can also pursue a completely different strategy: she can herself send signals that enter Alice and Bob's offices through the quantum channel. This kind of strategy is called a Trojan horse attack. For example, Eve can send light pulses into the fiber entering Alice's or Bob's apparatus and analyze the backreflected light. In this way, it is in principle possible to detect which laser just flashed, which detector just fired, or the settings of phase and polarization modulators. This cannot be prevented by simply using a shutter, since Alice and Bob must leave the "door open" for the photons to exit and enter, respectively.

In most QC setups the amount of backreflected light can be made very small, and sensing the apparatus with light pulses through the quantum channel is difficult. Nevertheless, this attack is especially threatening in the plug-and-play scheme on Alice's side (Sec. IV.C.2), since a mirror is used to send the light pulses back to Bob. Thus, in principle, Eve can send strong light pulses to Alice and sense the applied phase shift. However, by applying the phase shift only during a short time $\Delta t_{\mathrm{phase}}$ (a few nanoseconds), Alice can oblige Eve to send the spying pulse at the same time as Bob. Remember that in the plug-and-play scheme, pulses coming from Bob are macroscopic and an attenuator at Alice's end reduces them to below the one-photon level, say, 0.1 photons per pulse. Hence, if Eve wants to get, say, one photon per pulse, she has to send ten times Bob's pulse energy. Since Alice is detecting Bob's pulses for triggering her apparatus, she must be able to detect an increase in energy of these pulses in order to reveal the presence of a spying pulse. This is a relatively easy task, provided that Eve's pulses look the same as Bob's. However, Eve could of course use another wavelength or ultrashort pulses (or very long pulses with low intensity, hence the importance of Δt_{phase}); therefore Alice must introduce an optical bandpass filter with a transmission spectrum corresponding to the sensitivity spectrum of her detector and choose a Δt_{phase} that fits the bandwidth of her detector.

There is no doubt that Trojan horse attacks can be prevented by technical measures. However, the fact that this class of attacks exists illustrates that the security of QC can never be guaranteed by the principles of quantum mechanics only, but must necessarily rely on technical measures that are subject to discussion.[60]

L. Real security: Technology, cost, and complexity

Despite the elegance and generality of security proofs, the ideal of a QC system whose security relies entirely on quantum principles is unrealistic. The technological implementation of abstract principles will always be questionable. It is likely that they will remain the weakest point in all systems. Moreover, one should remember the obvious relation:

$$\text{Infinite security} \Rightarrow \text{Infinite cost} \Rightarrow \text{Zero practical interest}. \tag{77}$$

On the other hand, however, one should not underestimate the following two advantages of QC. First, it is much easier to forecast progress in technology than in mathematics: the danger that QC will break down overnight is negligible, in contrast to public-key cryptosystems. Next, the security of QC depends on the technological level of the adversary *at the time of the key exchange*, in contrast to complexity-based systems whose coded message can be registered and broken thanks to future progress. The latter point is relevant for secrets whose value lasts many years.

One often points to low bit rate as one of the current limitations of QC. However, it is important to stress that QC need not be used in conjunction with one-time-pad encryption. It can also be used to provide a key for a symmetrical cipher such as AES, whose security is greatly enhanced by frequent key changes.

To conclude this section, let us briefly elaborate on the differences and similarities between technological and mathematical complexity and on their possible connections and implications. Mathematical complexity means that the number of steps needed to run complex algorithms increases exponentially as the size of the input grows linearly. Similarly, one can define the technological complexity of a quantum computer as an exponentially increasing difficulty to process coherently all the qubits necessary to run a (noncomplex) algorithm on a linearly growing number of input data. It might be interesting to consider the possibility that the relationship between these two concepts of complexity is deeper. It could be that the solution of a problem requires either a complex classical algorithm or a quantum algorithm that itself requires a complex quantum computer.[61]

---

[60] Another technological loophole, recently pointed out by Kurtsiefer *et al.* (2001), is the possible information leakage caused by light emitted by APD's during their breakdown.

[61] Penrose (1994) pushes these speculations even further, suggesting that spontaneous collapses stop quantum computers whenever they try to compute beyond a certain complexity.

VII. CONCLUSIONS

Quantum cryptography is a fascinating illustration of the dialog between basic and applied physics. It is based on a beautiful combination of concepts from quantum physics and information theory and made possible by the tremendous progress in quantum optics and the technology of optical fibers and free-space optical communication. Its security principle relies on deep theorems in classical information theory and on a profound understanding of Heisenberg's uncertainty principle, as illustrated by Theorems 1 and 2 in Sec. VI.G (the only mathematically involved theorems in this review). Let us also emphasize the important contributions of QC to classical cryptography: privacy amplification and classical bound information (Secs. II.C.4 and II.C.5) are examples of concepts in classical information whose discovery were much inspired by QC. Moreover, the fascinating tension between quantum physics and relativity, as illustrated by Bell's inequality, is not far away, as discussed in Sec. VI.F. Now, despite significant progress in recent years, many open questions and technological challenges remain.

One technological challenge at present concerns improved detectors compatible with telecommunications fibers. Two other issues concern free-space QC and quantum repeaters. The former is currently the only way to realize QC over thousands of kilometers using the technology of the near future (see Sec. IV.E). The idea of quantum repeaters (Sec. III.E) is to encode the qubits in such a way that if the error rate is low, then errors can be detected and corrected entirely in the quantum domain. The hope is that such techniques could extend the range of quantum communication to essentially unlimited distances. Indeed, Hans Briegel, then at the University of Innsbruck, and co-workers (1998) showed that the number of additional qubits needed for quantum repeaters can be made smaller than the numbers of qubits needed to improve the fidelity of the quantum channel (Dur *et al.*, 1999). One could thus overcome the decoherence problem. However, the main practical limitation is not decoherence but loss (most photons never get to Bob, but those that do get there exhibit high fidelity).

As for open questions, let us emphasize three main concerns. First, complete and realistic analyses of the security issues are still missing. Next, figures of merit for comparing QC schemes based on different quantum systems (with different dimensions, for example) are still awaited. Finally, the delicate question of how to test the apparatuses has not yet received enough attention. Indeed, a potential customer of quantum cryptography buys confidence and secrecy, two qualities hard to quantify. Interestingly, both of these issues are connected to Bell's inequality (see Secs. VI.F and VI.B). Clearly, this connection cannot be phrased in the old context of local hidden variables, but rather in the context of the security of tomorrow's communications. Here, as in the entire field of quantum information, old concepts are renewed by looking at them from a fresh perspective: let us exploit quantum weirdness.

QC could well be the first application of quantum mechanics at the single-quantum level. Experiments have demonstrated that keys can be exchanged over distances of a few tens of kilometers at rates on the order of at least a thousand bits per second. There is no doubt that the technology can be mastered and the question is not whether QC will find commercial applications, but when. At present QC is still very limited in distance and in secret bit rate. Moreover, public-key systems dominate the market and, being pure software, are tremendously easier to manage. Every so often, we hear in the news that some classical cryptosystem has been broken. This would be impossible with properly implemented QC. But this apparent strength of QC might turn out to be its weak point: security agencies would be equally unable to break quantum cryptograms!

ACKNOWLEDGMENTS

This work was supported by the Swiss Fonds National de la Recherche Scientifique (FNRS) and the European Union projects European Quantum Cryptography and Single-Photon Optical Technologies (EQCSPOT) and Long-Distance Photonic Quantum Communication (QUCOMM) financed by the Swiss Office Fédéral de l'Education et de la Science (OFES). The authors would also like to thank Richard Hughes for providing Fig. 8, and acknowledge Charles H. Bennett and Paul G. Kwiat for their very careful reading of the manuscript and their helpful remarks.

REFERENCES

Ardehali, M., H. F. Chau, and H.-K. Lo, 1998, "Efficient quantum key distribution," preprint quant-ph/9803007.

Aspect, A., J. Dalibard, and G. Roger, 1982, "Experimental test of Bell's inequalities using time-varying analyzers," Phys. Rev. Lett. **49**, 1804–1807.

Bechmann-Pasquinucci, H., and N. Gisin, 1999, "Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography," Phys. Rev. A **59**, 4238–4248.

Bechmann-Pasquinucci, H., and A. Peres, 2000, "Quantum cryptography with 3-state systems," Phys. Rev. Lett. **85**, 3313–3316.

Bechmann-Pasquinucci, H., and W. Tittel, 2000, "Quantum cryptography using larger alphabets," Phys. Rev. A **61**, 062308.

Bell, J. S., 1964, "On the problem of hidden variables in quantum mechanics," Rev. Mod. Phys. **38**, 447–452 [reprinted in Bell, J. S., 1987, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University, Cambridge, England)].

Bennett, C. H., 1992, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett. **68**, 3121–3124.

Bennett, C. H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, 1992, "Experimental quantum cryptography," J. Cryptology **5**, 3–28.

Bennett, C. H., and G. Brassard, 1984, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, (IEEE, New York), pp. 175–179.

Bennett, C. H., and G. Brassard, 1985, "Quantum public key distribution system," IBM Tech. Discl. Bull. **28**, 3153–3163.
Bennett, C. H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, 1993, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Phys. Rev. Lett. **70**, 1895–1899.
Bennett, C. H., G. Brassard, C. Crépeau, and U. M. Maurer, 1995, "Generalized privacy amplification," IEEE Trans. Inf. Theory **41**, 1915–1923.
Bennett, C. H., G. Brassard, and A. Ekert, 1992, "Quantum cryptography," Sci. Am. **267**, 50–57.
Bennett, C. H., G. Brassard, and N. D. Mermin, 1992, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. **68**, 557–559.
Bennett, C. H., G. Brassard, and J.-M. Robert, 1988, "Privacy amplification by public discussion," SIAM J. Comput. **17**, 210–229.
Berry, M. V., 1984, "Quantal phase factors accompanying adiabatic changes," Proc. R. Soc. London, Ser. A **392**, 45–57.
Bethune, D., and W. Risk, 2000, "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light," IEEE J. Quantum Electron. **36**, 340–347.
Biham, E., M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, 1999, "A proof of the security of quantum key distribution," preprint quant-ph/9912053.
Biham, E., and T. Mor, 1997a, "Security of quantum cryptography against collective attacks," Phys. Rev. Lett. **78**, 2256–1159.
Biham, E., and T. Mor, 1997b, "Bounds on information and the security of quantum cryptography," Phys. Rev. Lett. **79**, 4034–4037.
Bourennane, M., F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, 1999, "Experiments on long wavelength (1550 nm) 'plug and play' quantum cryptography system," Opt. Express **4**, 383–387.
Bourennane, M., A. Karlsson, and G. Björn, 2001, "Quantum key distribution using multilevel encoding," Phys. Rev. A **64**, 012306.
Bourennane, M., A. Karlsson, G. Björn, N. Gisin, and N. Cerf, 2001, "Quantum key distribution using multilevel encoding: security analysis," preprint quant-ph/0106049.
Bourennane, M., D. Ljunggren, A. Karlsson, P. Jonsson, A. Hening, and J. P. Ciscar, 2000, "Experimental long wavelength quantum cryptography: from single photon transmission to key extraction protocols," J. Mod. Opt. **47**, 563–579.
Braginsky, V. B., and F. Y. Khalili, 1992, *Quantum Measurement* (Cambridge University, Cambridge, England).
Brassard, G., 1988, *Modern Cryptology: A Tutorial*, Lecture Notes in Computer Science, Vol. 325 (Springer, New York).
Brassard, G., C. Crépeau, D. Mayers, and L. Salvail, 1998, in *Proceedings of Randomized Algorithms, Satellite Workshop of the 23rd International Symposium on Mathematical Foundations of Computer Science*, Brno, Czech Republic, edited by R. Freivalds (Aachen University, Aachen, Germany), pp. 13–15.
Brassard, G., N. Lütkenhaus, T. Mor, and B. C. Sanders, 2000, "Limitations on practical quantum cryptography," Phys. Rev. Lett. **85**, 1330–1333.
Brassard, G., and L. Salvail, 1994, in *Advances in Cryptology—EUROCRYPT '93 Proceedings*, Lecture Notes in Computer Science, Vol. 765, edited by T. Helleseth (Springer, New York), p. 410.
Bréguet, J., and N. Gisin, 1995, "New interferometer using a 3×3 coupler and Faraday mirrors," Opt. Lett. **20**, 1447–1449.
Bréguet, J., A. Muller, and N. Gisin, 1994, "Quantum cryptography with polarized photons in optical fibers: experimental and practical limits," J. Mod. Opt. **41**, 2405–2412.
Brendel, J., W. Dultz, and W. Martienssen, 1995, "Geometric phase in 2-photon interference experiments," Phys. Rev. A **52**, 2551–2556.
Brendel, J., N. Gisin, W. Tittel, and H. Zbinden, 1999, "Pulsed energy-time entangled twin-photon source for quantum communication," Phys. Rev. Lett. **82**, 2594–2597.
Briegel, H.-J., W. Dur, J. I. Cirac, and P. Zoller, 1998, "Quantum repeaters: the role of imperfect local operations in quantum communication," Phys. Rev. Lett. **81**, 5932–5935.
Brouri, R., A. Beveratios, J.-P. Poizat, and P. Grangier, 2000, "Photon antibunching in the fluorescence of individual colored centers in diamond," Opt. Lett. **25**, 1294–1296.
Brown, R. G. W., and M. Daniels, 1989, "Characterization of silicon avalanche photodiodes for photon correlation measurements. 3: Sub-Geiger operation," Appl. Opt. **28**, 4616–4621.
Brown, R. G. W., R. Jones, J. G. Rarity, and K. D. Ridley, 1987, "Characterization of silicon avalanche photodiodes for photon correlation measurements. 2: Active quenching," Appl. Opt. **26**, 2383–2389.
Brown, R. G. W., K. D. Ridley, and J. G. Rarity, 1986, "Characterization of silicon avalanche photodiodes for photon correlation measurements. 1: Passive quenching," Appl. Opt. **25**, 4122–4126.
Brunel, C., B. Lounis, P. Tamarat, and M. Orrit, 1999, "Triggered source of single photons based on controlled single molecule fluorescence," Phys. Rev. Lett. **83**, 2722–2725.
Bruss, D., 1998, "Optimal eavesdropping in quantum cryptography with six states," Phys. Rev. Lett. **81**, 3018–3021.
Bruss, D., A. Ekert, and C. Macchiavello, 1998, "Optimal universal quantum cloning and state estimation," Phys. Rev. Lett. **81**, 2598–2601.
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. Simmons, 1998, "Practical free-space quantum key distribution over 1 km," Phys. Rev. Lett. **81**, 3283–3286.
Buttler, W. T., R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, 2000, "Daylight quantum key distribution over 1.6 km," Phys. Rev. Lett. **84**, 5652–5655.
Bužek, V., and M. Hillery, 1996, "Quantum copying: beyond the no-cloning theorem," Phys. Rev. A **54**, 1844–1852.
Cancellieri, G., 1993, Ed., *Single-Mode Optical Fiber Measurement: Characterization and Sensing* (Artech House, Boston).
Canning, J., M. A. van Eijkelenborg, T. Ryan, M. Kristensen, and K. Lyytikainen, 2000, "Complex mode coupling within air-silica structured optical fibers and applications," Opt. Commun. **185**, 321–324.
Cirac, J. I., and N. Gisin, 1997, "Coherent eavesdropping strategies for the 4-state quantum cryptography protocol," Phys. Lett. A **229**, 1–7.
Clarke, R. B. M., A. Chefles, S. M. Barnett, and E. Riis, 2000, "Experimental demonstration of optimal unambiguous state discrimination," Phys. Rev. A **63**, 040305.
Clauser, J. F., M. A. Horne, A. Shimony, and R. A. Holt, 1969, "Proposed experiment to test local hidden variable theories," Phys. Rev. Lett. **23**, 880–884.

Clauser, J. F., and A. Shimony, 1978, "Bell's theorem: experimental tests and implications," Rep. Prog. Phys. **41**, 1881–1927.

Cova, S., M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, 1996, "Avalanche photodiodes and quenching circuits for single-photon detection," Appl. Opt. **35**, 1956–1976.

Cova, S., A. Lacaita, M. Ghioni, and G. Ripamonti, 1989, "High-accuracy picosecond characterization of gain-switched laser diodes," Opt. Lett. **14**, 1341–1343.

Csiszár, I., and J. Körner, 1978, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory **IT-24**, 339–348.

De Martini, F., V. Mussi, and F. Bovino, 2000, "Schroedinger cat states and optimum universal quantum cloning by entangled parametric amplification," Opt. Commun. **179**, 581–589.

Desurvire, E., 1994, "The golden age of optical fiber amplifiers," Phys. Today **47** (1), 20–27.

Deutsch, D., 1985, "Quantum theory, the Church-Turing principle and the universal quantum computer," Proc. R. Soc. London, Ser. A **400**, 97–105.

Deutsch, D., A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, 1996, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," Phys. Rev. Lett. **77**, 2818–2821; **80**, 2022(E) (1996).

Dieks, D., 1982, "Communication by EPR devices," Phys. Lett. **92A**, 271–272.

Diffie, W., and M. E. Hellman, 1976, "New directions in cryptography," IEEE Trans. Inf. Theory **IT-22**, 644–654.

Dur, W., H.-J. Briegel, J. I. Cirac, and P. Zoller, 1999, "Quantum repeaters based on entanglement purification," Phys. Rev. A **59**, 169–181; **60**, 725(E).

Dusek, M., M. Jahma, and N. Lütkenhaus, 2000, "Unambiguous state discrimination in quantum cryptography with weak coherent states," Phys. Rev. A **62**, 022306.

Einstein, A., B. Podolsky, and N. Rosen, 1935, "Can quantum-mechanical description of physical reality be considered complete?," Phys. Rev. **47**, 777–780.

Ekert, A. K., 1991, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661–663.

Ekert, A. K., 2000, "Coded secrets cracked open," Phys. World **13** (2), 39–40.

Ekert, A. K., and B. Huttner, 1994, "Eavesdropping techniques in quantum cryptosystems," J. Mod. Opt. **41**, 2455–2466.

Ekert, A. K., J. G. Rarity, P. R. Tapster, and G. M. Palma, 1992, "Practical quantum cryptography based on two-photon interferometry," Phys. Rev. Lett. **69**, 1293–1296.

Elamari, A., H. Zbinden, B. Perny, and C. Zimmer, 1998, "Statistical prediction and experimental verification of concatenations of fiber optic components with polarization dependent loss," J. Lightwave Technol. **16**, 332–339.

Enzer, D., P. Hadley, R. Hughes, G. Peterson, and P. Kwiat, 2001, private communication.

Felix, S., A. Stefanov, H. Zbinden, and N. Gisin, 2001, "Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses," J. Mod. Opt. **48**, 2009–2021.

Fleury, L., J.-M. Segura, G. Zumofen, B. Hecht, and U. P. Wild, 2000, "Nonclassical photon statistics in single-molecule fluorescence at room temperature," Phys. Rev. Lett. **84**, 1148–1151.

Franson, J. D., 1989, "Bell inequality for position and time," Phys. Rev. Lett. **62**, 2205–2208.

Franson, J. D., 1992, "Nonlocal cancellation of dispersion," Phys. Rev. A **45**, 3126–3132.

Franson, J. D., and B. C. Jacobs, 1995, "Operational system for quantum cryptography," Electron. Lett. **31**, 232–234.

Freedmann, S. J., and J. F. Clauser, 1972, "Experimental test of local hidden variable theories," Phys. Rev. Lett. **28**, 938–941.

Fry, E. S., and R. C. Thompson, 1976, "Experimental test of local hidden variable theories," Phys. Rev. Lett. **37**, 465–468.

Fuchs, C. A., N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, 1997, "Optimal eavesdropping in quantum cryptography. I: Information bound and optimal strategy," Phys. Rev. A **56**, 1163–1172.

Fuchs, C. A., and A. Peres, 1996, "Quantum state disturbance vs. information gain: uncertainty relations for quantum information," Phys. Rev. A **53**, 2038–2045.

Gérard, J.-M., and B. Gayral, 1999, "Strong Purcell effect for InAs quantum boxes in three-dimensional solid-state microcavities," J. Lightwave Technol. **17**, 2089–2095.

Gérard, J.-M., B. Sermage, B. Gayral, B. Legrand, E. Costard, and V. Thierry-Mieg, 1998, "Enhanced spontaneous emission by quantum boxes in a monolithic optical microcavity," Phys. Rev. Lett. **81**, 1110–1113.

Gilbert, G., and M. Hamrick, 2000, "Practical quantum cryptography: a comprehensive analysis (part one)," internal report (MITRE, McLean, USA), preprint quant-ph/0009027.

Gisin, B., and N. Gisin, 1999, "A local hidden variable model of quantum correlation exploiting the detection loophole," Phys. Lett. A **260**, 323–327.

Gisin, N., 1998, "Quantum cloning without signaling," Phys. Lett. A **242**, 1–3.

Gisin, N., *et al.*, 1995, "Definition of polarization mode dispersion and first results of the COST 241 round-robin measurements," Pure Appl. Opt. **4**, 511–522.

Gisin, N., and S. Massar, 1997, "Optimal quantum cloning machines," Phys. Rev. Lett. **79**, 2153–2156.

Gisin, N., R. Renner, and S. Wolf, 2000, *Proceedings of the Third European Congress of Mathematics*, Barcelona (Birkhäuser, Basel) (in press).

Gisin, N., and S. Wolf, 1999, "Quantum cryptography on noisy channels: quantum versus classical key-agreement protocols," Phys. Rev. Lett. **83**, 4200–4203.

Gisin, N., and S. Wolf, 2000, *Advances in Cryptology—Proceedings of Crypto 2000*, Lecture Notes in Computer Science, Vol. 1880, edited by M. Bellare (Springer, New York), pp. 482–500.

Gisin, N., and H. Zbinden, 1999, "Bell inequality and the locality loophole: active versus passive switches," Phys. Lett. A **264**, 103–107.

Goldenberg, L., and L. Vaidman, 1995, "Quantum cryptography based on orthogonal states," Phys. Rev. Lett. **75**, 1239–1243.

Gorman, P. M., P. R. Tapster, and J. G. Rarity, 2001, "Secure free-space key exchange to 1.9 km and beyond," J. Mod. Opt. **48**, 1887–1901.

Haecker, W., O. Groezinger, and M. H. Pilkuhn, 1971, "Infrared photon counting by Ge avalanche diodes," Appl. Phys. Lett. **19**, 113–115.

Hall, M. J. W., 1995, "Information exclusion principle for complementary observables," Phys. Rev. Lett. **74**, 3307–3310.

Hariharan, P., M. Roy, P. A. Robinson, and J. W. O'Byrne, 1993, "The geometric phase observation at the single photon level," J. Mod. Opt. **40**, 871–877.

Hart, A. C., R. G. Huff, and K. L. Walker, 1994, "Method of making a fiber having low polarization mode dispersion due to a permanent spin," U.S. Patent No. 5,298,047.

Hildebrand, E., 2001, Ph.D. thesis (Johann Wolfgang Goethe-Universität, Frankfurt am Main).

Hillery, M., V. Buzek, and A. Berthiaume, 1999, "Quantum secret sharing," Phys. Rev. A **59**, 1829–1834.

Hiskett, P. A., G. S. Buller, A. Y. Loudon, J. M. Smith, I. Gontijo, A. C. Walker, P. D. Townsend, and M. J. Robertson, 2000, "Performance and design of InGaAs/InP photodiodes for single-photon counting at 1.55 μm," Appl. Opt. **39**, 6818–6829.

Hong, C. K., and L. Mandel, 1985, "Theory of parametric frequency down conversion of light," Phys. Rev. A **31**, 2409–2418.

Hong, C. K., and L. Mandel, 1986, "Experimental realization of a localized one-photon state," Phys. Rev. Lett. **56**, 58–60.

Horodecki, M., R. Horodecki, and P. Horodecki, 1996, "Separability of mixed states: necessary and sufficient conditions," Phys. Lett. A **223**, 1–8.

Hughes, R., W. Buttler, P. Kwiat, S. Lamoreaux, G. Morgan, J. Nordhold, and G. Peterson, 2000, "Free-space quantum key distribution in daylight," J. Mod. Opt. **47**, 549–562.

Hughes, R., G. G. Luther, G. L. Morgan, and C. Simmons, 1996, in *Advances in Cryptology—CRYPTO '96 Proceedings*, Lecture Notes in Computer Science, Vol. 1109, edited by N. Koblitz (Springer, New York), pp. 329–342.

Hughes, R., G. Morgan, and C. Peterson, 2000, "Quantum key distribution over a 48-km optical fiber network," J. Mod. Opt. **47**, 533–547.

Huttner, B., J. D. Gautier, A. Muller, H. Zbinden, and N. Gisin, 1996, "Unambiguous quantum measurement of nonorthogonal states," Phys. Rev. A **54**, 3783–3789.

Huttner, B., N. Imoto, and S. M. Barnett, 1996, "Short distance applications of quantum cryptography," J. Nonlinear Opt. Phys. Mater. **5**, 823–832.

Huttner, B., N. Imoto, N. Gisin, and T. Mor, 1995, "Quantum cryptography with coherent states," Phys. Rev. A **51**, 1863–1869.

Imamoglu, A., and Y. Yamamoto, 1994, "Turnstile device for heralded single photons: Coulomb blockade of electron and hole tunneling in quantum confined p-i-n heterojunctions," Phys. Rev. Lett. **72**, 210–213.

Inamori, H., L. Rallan, and V. Vedral, 2000, "Security of EPR-based quantum cryptography against incoherent symmetric attacks," preprint quant-ph/0103058.

Ingerson, T. E., R. J. Kearney, and R. L. Coulter, 1983, "Photon counting with photodiodes," Appl. Opt. **22**, 2013–2018.

Ivanovic, I. D., 1987, "How to differentiate between nonorthogonal states," Phys. Lett. A **123**, 257–259.

Jacobs, B., and J. Franson, 1996, "Quantum cryptography in free space," Opt. Lett. **21**, 1854–1856.

Jennewein, T., U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, 2000, "A fast and compact quantum random number generator," Rev. Sci. Instrum. **71**, 1675–1680.

Jennewein, T., C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, 2000, "Quantum cryptography with entangled photons," Phys. Rev. Lett. **84**, 4729–4732.

Karlsson, A., M. Bourennane, G. Ribordy, H. Zbinden, J. Brendel, J. Rarity, and P. Tapster, 1999, "A single-photon counter for long-haul telecom," IEEE Circuits Devices Mag. **15**, 34–40.

Kempe, J., C. Simon, G. Weihs, and A. Zeilinger, 2000, "Optimal photon cloning," Phys. Rev. A **62**, 032302.

Kim, J., O. Benson, H. Kan, and Y. Yamamoto, 1999, "A single-photon turnstile device," Nature (London) **397**, 500–503.

Kimble, H. J., M. Dagenais, and L. Mandel, 1977, "Photon antibunching in resonance fluorescence," Phys. Rev. Lett. **39**, 691–694.

Kitson, S. C., P. Jonsson, J. G. Rarity, and P. R. Tapster, 1998, "Intensity fluctuation spectroscopy of small numbers of dye molecules in a microcavity," Phys. Rev. A **58**, 620–627.

Kolmogorov, A. N., 1956, *Foundations of the Theory of Probability* (Chelsea, New York).

Kurtsiefer, C., S. Mayer, P. Zarda, and H. Weinfurter, 2000, "Stable solid-state source of single photons," Phys. Rev. Lett. **85**, 290–293.

Kurtsiefer, C., P. Zarda, S. Mayer, and H. Weinfurter, 2001, "The breakdown flash of Silicon Avalanche Photodiodes—backdoor for eavesdropper attacks?," J. Mod. Opt. **48**, 2039–2047.

Kwiat, P. G., A. M. Steinberg, R. Y. Chiao, P. H. Eberhard, and M. D. Petroff, 1993, "High-efficiency single-photon detectors," Phys. Rev. A **48**, R867–870.

Kwiat, P. G., E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, 1999, "Ultrabright source of polarization-entangled photons," Phys. Rev. A **60**, R773–776.

Lacaita, A., P. A. Francese, F. Zappa, and S. Cova, 1994, "Single-photon detection beyond 1 μm: performance of commercially available germanium photodiodes," Appl. Opt. **33**, 6902–6918.

Lacaita, A., F. Zappa, S. Cova, and P. Lovati, 1996, "Single-photon detection beyond 1 μm: performance of commercially available InGaAs/InP detectors," Appl. Opt. **35**, 2986–2996.

Larchuk, T. S., M. V. Teich, and B. E. A. Saleh, 1995, "Nonlocal cancellation of dispersive broadening in Mach-Zehnder interferometers," Phys. Rev. A **52**, 4145–4154.

Levine, B. F., C. G. Bethea, and J. C. Campbell, 1985, "Room-temperature 1.3-μm optical time domain reflectometer using a photon counting InGaAs/InP avalanche detector," Appl. Phys. Lett. **45**, 333–335.

Li, M. J., and D. A. Nolan, 1998, "Fiber spin-profile designs for producing fibers with low PMD," Opt. Lett. **23**, 1659–1661.

Lo, H.-K., and H. F. Chau, 1998, "Why quantum bit commitment and ideal quantum coin tossing are impossible," Physica D **120**, 177–187.

Lo, H.-K., and H. F. Chau, 1999, "Unconditional security of quantum key distribution over arbitrary long distances," Science **283**, 2050–2056.

Lütkenhaus, N., 1996, "Security against eavesdropping in quantum cryptography," Phys. Rev. A **54**, 97–111.

Lütkenhaus, N., 2000, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61**, 052304.

Marand, C., and P. D. Townsend, 1995, "Quantum key distribution over distances as long as 30 km," Opt. Lett. **20**, 1695–1697.

Martinelli, M., 1989, "A universal compensator for polarization changes induced by birefringence on a retracing beam," Opt. Commun. **72**, 341–344.

Martinelli, M., 1992, "Time reversal for the polarization state in optical systems," J. Mod. Opt. **39**, 451–455.

Maurer, U. M., 1993, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory **39**, 733–742.

Maurer, U. M., and S. Wolf, 1999, "Unconditionally secure key agreement and intrinsic information," IEEE Trans. Inf. Theory **45**, 499–514.

Mayers, D., 1996a, "The trouble with quantum bit commitment," quant-ph/9603015.

Mayers, D., 1996b, *Advances in Cryptology—Proceedings of Crypto'96*, Lecture Notes in Computer Science, Vol. 1109, edited by N. Koblitz (Springer, New York), pp. 343–357.

Mayers, D., 1997, "Unconditionally secure Q bit commitment is impossible," Phys. Rev. Lett. **78**, 3414–3417.

Mayers, D., 1998, "Unconditional security in quantum cryptography," J. Assn. Comput. Mac. (in press).

Mayers, D., and A. Yao, 1998, *Proceedings of the 39th Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Los Alamitos, California), p. 503.

Mazurenko, Y., R. Giust, and J. P. Goedgebuer, 1997, "Spectral coding for secure optical communications using refractive index dispersion," Opt. Commun. **133**, 87–92.

Mérolla, J-M., Y. Mazurenko, J. P. Goedgebuer, and W. T. Rhodes, 1999, "Single-photon interference in sidebands of phase-modulated light for quantum cryptography," Phys. Rev. Lett. **82**, 1656–1659.

Michler, P., A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. Zhang, E. Hu, and A. Imamoglu, 2000, "A quantum dot single photon turnstile device," Science **290**, 2282–2285.

Milonni, P. W., and M. L. Hardies, 1982, "Photons cannot always be replicated," Phys. Lett. A **92**, 321–322.

Molotkov, S. N., 1998, "Quantum cryptography based on photon 'frequency' states: example of a possible realization," Sov. Phys. JETP **87**, 288–293.

Muller, A., J. Breguet, and N. Gisin, 1993, "Experimental demonstration of quantum cryptography using polarized photons in optical fiber over more than 1 km," Europhys. Lett. **23**, 383–388.

Muller, A., T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, 1997, " 'Plug and play' systems for quantum cryptography," Appl. Phys. Lett. **70**, 793–795.

Muller, A., H. Zbinden, and N. Gisin, 1995, "Underwater quantum coding," Nature (London) **378**, 449–449.

Muller, A., H. Zbinden, and N. Gisin, 1996, "Quantum cryptography over 23 km in installed under-lake telecom fibre," Europhys. Lett. **33**, 335–339.

Naik, D., C. Peterson, A. White, A. Berglund, and P. Kwiat, 2000, "Entangled state quantum cryptography: eavesdropping on the Ekert protocol," Phys. Rev. Lett. **84**, 4733–4736.

Neumann, E.-G., 1988, *Single-Mode Fibers: Fundamentals*, Springer Series in Optical Sciences, Vol. 57 (Springer, Berlin).

Niu, C. S., and R. B. Griffiths, 1999, "Two-qubit copying machine for economical quantum eavesdropping," Phys. Rev. A **60**, 2764–2776.

Nogues, G., A. Rauschenbeutel, S. Osnaghi, M. Brune, J. M. Raimond, and S. Haroche, 1999, "Seeing a single photon without destroying it," Nature (London) **400**, 239–242.

Owens, P. C. M., J. G. Rarity, P. R. Tapster, D. Knight, and P. D. Townsend, 1994, "Photon counting with passively quenched germanium avalanche," Appl. Opt. **33**, 6895–6901.

Penrose, R., 1994, *Shadows of the Mind* (Oxford University, Oxford, England).

Peres, A., 1988, "How to differentiate between two nonorthogonal states," Phys. Lett. A **128**, 19.

Peres, A., 1996, "Separability criteria for density matrices," Phys. Rev. Lett. **76**, 1413–1415.

Peres, A., 1997, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, The Netherlands).

Phoenix, S. J. D., S. M. Barnett, P. D. Townsend, and K. J. Blow, 1995, "Multi-user quantum cryptography on optical networks," J. Mod. Opt. **6**, 1155–1163.

Piron, C., 1990, *Mécanique quantique, bases et applications* (Presses Polytechniques et Universitaires Romandes, Lausanne, Switzerland).

Pitowsky, I., 1989, Ed. *Quantum Probability—Quantum Logic*, Lecture Notes in Physics, Vol. 321 (Springer, Berlin).

Rarity, J. G., P. C. M. Owens, and P. R. Tapster, 1994, "Quantum random-number generation and key sharing," J. Mod. Opt. **41**, 2435–2444.

Rarity, J. G., and P. R. Tapster, 1988, in *Photons and Quantum Fluctuations*, edited by E. R. Pike and H. Walther (Hilger, Bristol, England), pp. 122–150.

Rarity, J. G., T. E. Wall, K. D. Ridley, P. C. M. Owens, and P. R. Tapster, 2000, "Single-photon counting for the 1300–1600-nm range by use of Peltier-cooled and passively quenched InGaAs avalanche photodiodes," Appl. Opt. **39**, 6746–6753.

Ribordy, G., J. Brendel, J. D. Gautier, N. Gisin, and H. Zbinden, 2001, "Long distance entanglement based quantum key distribution," Phys. Rev. A **63**, 012309.

Ribordy, G., J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, 2000, "Fast and user-friendly quantum key distribution," J. Mod. Opt. **47**, 517–531.

Ribordy, G., J. D. Gautier, H. Zbinden, and N. Gisin, 1998, "Performance of InGaAsInP avalanche photodiodes as gated-mode photon counters," Appl. Opt. **37**, 2272–2277.

Rivest, R. L., A. Shamir, and L. M. Adleman, 1978, "A method of obtaining digital signatures and public-key cryptosystems," Commun. ACM **21**, 120–126.

Santori, C., M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, 2000, "Triggered single photons from a quantum dot," Phys. Rev. Lett. **86**, 1502–1505.

Shannon, C. E., 1949, "Communication theory of secrecy systems," Bell Syst. Tech. J. **28**, 656–715.

Shih, Y. H., and C. O. Alley, 1988, "New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion," Phys. Rev. Lett. **61**, 2921–2924.

Shor, P. W., 1994, *Proceedings of the 35th Symposium on Foundations of Computer Science*, edited by S. Goldwasser (IEEE Computer Society, Los Alamitos, California), pp. 124–134.

Shor, P. W., and J. Preskill, 2000, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444.

Simon, C., G. Weihs, and A. Zeilinger, 1999, "Quantum cloning and signaling," Acta Phys. Slov. **49**, 755–760.

Simon, C., G. Weihs, and A. Zeilinger, 2000, "Optimum quantum cloning via stimulated emission," Phys. Rev. Lett. **84**, 2993–2996.

Singh, S., 1999, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Fourth Estate, London).

Snyder, A. W., and J. D. Love, 1983, *Optical Waveguide Theory* (Chapman & Hall, London).

Spinelli, A., L. M. Davis, and H. Dauted, 1996, "Actively quenched single-photon avalanche diode for high repetition rate time-gated photon counting," Rev. Sci. Instrum. **67**, 55–61.

Stallings, W., 1999, *Cryptography and Network Security: Principles and Practices* (Prentice Hall, Upper Saddle River, New Jersey).

Stefanov, A., O. Guinnard, L. Guinnard, H. Zbinden, and N. Gisin, 2000, "Optical quantum random number generator," J. Mod. Opt. **47**, 595–598.

Steinberg, A. M., P. Kwiat, and R. Y. Chiao, 1992a, "Dispersion cancellation and high-resolution time measurements in a fourth-order optical interferometer," Phys. Rev. A **45**, 6659–6665.

Steinberg, A. M., P. Kwiat, and R. Y. Chiao, 1992b, "Dispersion cancellation in a measurement of the single-photon propagation velocity in glass," Phys. Rev. Lett. **68**, 2421–2424.

Stucki, D., G. Ribordy, A. Stefanov, H. Zbinden, J. Rarity, and T. Wall, 2001, "Photon counting for quantum key distribution with Peltier-cooled InGaAs/InP APD's," J. Mod. Opt. **48**, 1967–1981.

Sun, P. C., Y. Mazurenko, and Y. Fainman, 1995, "Long-distance frequency-division interferometer for communication and quantum cryptography," Opt. Lett. **20**, 1062–1063.

Tanzilli, S., H. De Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D. B. Ostrowsky, and N. Gisin, 2001, "Highly efficient photon-pair source using a periodically poled lithium niobate waveguide," Electron. Lett. **37**, 26–28.

Tapster, P. R., J. G. Rarity, and P. C. M. Owens, 1994, "Violation of Bell's inequality over 4 km of optical fiber," Phys. Rev. Lett. **73**, 1923–1926.

Thomas, G. A., B. I. Shraiman, P. F. Glodis, and M. J. Stephen, 2000, "Towards the clarity limit in optical fiber," Nature (London) **404**, 262–264.

Tittel, W., J. Brendel, H. Zbinden, and N. Gisin, 1998, "Violation of Bell inequalities by photons more than 10 km apart," Phys. Rev. Lett. **81**, 3563–3566.

Tittel, W., J. Brendel, H. Zbinden, and N. Gisin, 1999, "Long-distance Bell-type tests using energy-time entangled photons," Phys. Rev. A **59**, 4150–4163.

Tittel, W., J. Brendel, H. Zbinden, and N. Gisin, 2000, "Quantum cryptography using entangled photons in energy-time bell states," Phys. Rev. Lett. **84**, 4737–4740.

Tittel, W., H. Zbinden, and N. Gisin, 2001, "Experimental demonstration of quantum secret sharing," Phys. Rev. A **63**, 042301.

Tomita, A., and R. Y. Chiao, 1986, "Observation of Berry's topological phase by use of an optical fiber," Phys. Rev. Lett. **57**, 937–940.

Townsend, P., 1994, "Secure key distribution system based on quantum cryptography," Electron. Lett. **30**, 809–811.

Townsend, P., 1997a, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using WDM," Electron. Lett. **33**, 188–190.

Townsend, P., 1997b, "Quantum cryptography on multiuser optical fiber networks," Nature (London) **385**, 47–49.

Townsend, P., 1998a, "Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems," IEEE Photonics Technol. Lett. **10**, 1048–1050.

Townsend, P., 1998b, "Quantum cryptography on optical fiber networks," Opt. Fiber Technol.: Mater., Devices Syst. **4**, 345–370.

Townsend, P. D., S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, 1994, "Design of QC systems for passive optical networks," Electron. Lett. **30**, 1875–1876.

Townsend, P., J. G. Rarity, and P. R. Tapster, 1993a, "Single photon interference in a 10 km long optical fiber interferometer," Electron. Lett. **29**, 634–639.

Townsend, P., J. Rarity, and P. Tapster, 1993b, "Enhanced single photon fringe visibility in a 10 km-long prototype quantum cryptography channel," Electron. Lett. **29**, 1291–1293.

Vernam, G., 1926, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," J. Am. Inst. Electr. Eng. **45**, 109–115.

Vinegoni, C., M. Wegmuller, and N. Gisin, 2000, "Determination of nonlinear coefficient n^2/A_{eff} using a self-aligned interferometer and a Faraday mirror," Electron. Lett. **36**, 886–888.

Vinegoni, C., M. Wegmuller, B. Huttner, and N. Gisin, 2000, "Measurement of nonlinear polarization rotation in a highly birefringent optical fiber using a Faraday mirror," J. Opt. A, Pure Appl. Opt. **2**, 314–318.

Walls, D. F., and G. J. Milburn, 1995, Eds., *Quantum Optics* (Springer, Berlin).

Weihs, G., T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, 1998, "Violation of Bell's inequality under strict Einstein locality conditions," Phys. Rev. Lett. **81**, 5039–5043.

Wiesner, S., 1983, "Conjugate coding," SIGACT News **15**, 78–88.

Wigner, E. P., 1961, *The Logic of Personal Knowledge: Essays Presented to Michael Polanyi on his Seventieth Birthday, 11 March 1961* (Routledge & Kegan Paul, London), pp. 231–238.

Wootters, W. K., and W. H. Zurek, 1982, "A single quantum cannot be cloned," Nature (London) **299**, 802–803.

Yuen, H. P., 1997, "Quantum amplifiers, quantum duplicators and quantum cryptography," Quantum Semiclassic. Opt. **8**, 939.

Zappa, F., A. Lacaita, S. Cova, and P. Webb, 1994, "Nanosecond single-photon timing with InGaAs/InP photodiodes," Opt. Lett. **19**, 846–848.

Zbinden, H., J.-D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, 1997, "Interferometry with Faraday mirrors for quantum cryptography," Electron. Lett. **33**, 586–588.

Zeilinger, A., 1999, "Experiment and the foundations of quantum physics," Rev. Mod. Phys. **71**, S288–S297.

Zissis, G., and A. Larocca, 1978, in *Handbook of Optics*, edited by W. G. Driscoll (McGraw-Hill, New York), Sec. 3.

Żukowski, M., A. Zeilinger, M. A. Horne, and A. Ekert, 1993, " 'Event-ready-detectors' Bell experiment via entanglement swapping," Phys. Rev. Lett. **71**, 4287–4290.

Żukowski, M., A. Zeilinger, M. Horne, and H. Weinfurter, 1998, "Quest for GHZ states," Acta Phys. Pol. A **93**, 187–195.