

Long-distance entanglement-based quantum key distribution

Grégoire Ribordy,* Jürgen Brendel,† Jean-Daniel Gautier, Nicolas Gisin, and Hugo Zbinden
Gap-Optique, Université de Genève, 20 rue de l'Ecole-de-Médecine, 1211 Genève 4, Switzerland

(Received 7 August 2000; published 13 December 2000)

A detailed analysis of quantum key distribution employing entangled states is presented. We tested a system based on photon pairs entangled in energy-time optimized for long-distance transmission. It is based on a Franson-type setup for monitoring quantum correlations, and uses a protocol analogous to the Bennett-Brassard 1984 protocol. Passive-state preparation is implemented by polarization multiplexing in the interferometers. We distributed a sifted key of 0.4 Mbit at a raw rate of 134 Hz and with an error rate of 8.6% over a distance of 8.5 km. We thoroughly discuss the noise sources and practical difficulties associated with entangled-state systems. Finally, the level of security offered by this system is assessed and compared with that of faint-laser-pulse systems.

DOI: 10.1103/PhysRevA.63.012309

PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD), the most advanced application of the new field of quantum information theory, offers the possibility for two remote parties—Alice and Bob—to exchange a secret key without meeting or resorting to the services of a courier. This key can in turn be used to implement a secure encryption algorithm, such as the “one-time pad,” in order to establish a confidential communication link. In principle, the security of QKD relies on the laws of quantum physics, although this claim must be somewhat softened because of the lack of ideal components—in particular, the photon source and the detectors.

After the first proposal by Bennett and Brassard [1], various systems of QKD have been introduced and tested by groups around the world (see [2–5] for recent experiments). Until recently, all QKD experiments relied on strongly attenuated laser pulses, as an approximation to single photons, because of the lack of appropriate sources for such states. Although this solution is the simplest from an experimental point of view, it suffers from two important drawbacks. First, the fact that a fraction of the pulses contains more than one photon constitutes a vulnerability to certain eavesdropping strategies. Second, the maximum transmission distance is reduced, because of the fact that most of the pulses are actually empty. Both points are discussed in more detail below.

Ekert proposed in 1991 a protocol utilizing entangled states for QKD [6]. Photon-pair sources making use of parametric down-conversion are relatively simple and flexible. They have been used for several years and were exploited, for example, for tests of Bell inequalities [7–9]. These experiments demonstrated that entanglement of photon pairs can be preserved over long distances in optical fibers, and could thus allow the implementation of QKD.

Recently, the first entangled photon-pairs QKD experiments were performed [10–12]. Both Naik *et al.* [11] and Jennewein *et al.* [12] chose to use photons at a wavelength of

702 nm, entangled in polarization, for their investigations. Although this choice is appropriate for free-space QKD, it prevents any transmission over a distance of more than a few kilometers in optical fibers. Polarization entanglement is indeed not very robust to decoherence, and attenuation at this wavelength is rather high in optical fibers. Tittel *et al.* used photon pairs correlated in energy and time and with a wavelength where the attenuation in fibers is low, but their actual implementation was not optimized for long-distance transmission [10].

In this paper, we present a system for QKD with entangled photon pairs exploiting a source optimized for long-distance distribution and not Bell inequalities testing, like previous experiments. In addition, we believe that it offers a particularly high level of security. We introduce first the principle of our system, then discuss experimental results obtained under laboratory conditions. Finally, we compare it with other experiments and evaluate its advantages and drawbacks, before concluding.

II. PRINCIPLE OF THE QKD SYSTEM

When designing a QKD system where photons are exchanged between Alice and Bob, one must first choose on which property to encode the qubit values. Although polarization is a straightforward choice, it is not the most appropriate one when transmitting photon pairs over optical fibers. The intrinsic birefringence of these fibers, also known as polarization mode dispersion, associated with the large spectral width [typically 5 nm full width at half maximum (FWHM) at 800 nm] of the down-converted photons yields rapid depolarization. Considering that such photons typically have a coherence time of the order of 1 ps, and that standard telecommunications fibers exhibit a polarization mode dispersion of 0.2 ps/km^{1/2}, one sees that the polarization mode separation is already substantial after a few kilometers. This fact indicates that polarization is not robust enough for long-distance QKD in fibers when using photon pairs. A solution is therefore to encode the values of the qubits on the phase of the photons. In addition, previous experiments demonstrated that the polarization transformation induced by an installed optical fiber sometimes changes abruptly. An active polariza-

*Email address: gregoire.ribordy@physics.unige.ch

†Present address: Luciol Instruments SA, 31 Chemin de la Vuarpillière, 1260 Nyon, Switzerland.

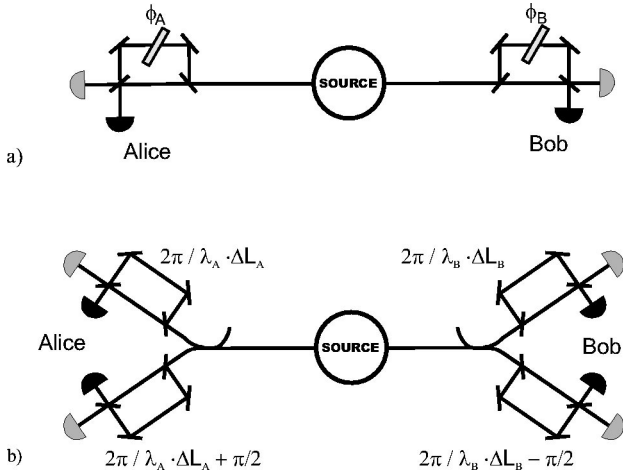


FIG. 1. (a) Franson-type arrangement for generating nonlocal quantum correlations with photon pairs entangled in energy-time. (b) Implementation of the double measurement basis with four interferometers.

tion alignment system is consequently necessary to compensate these fluctuations.

A second important parameter for a QKD system is the wavelength of the photons. Two opposite factors influence this choice. On the one hand, the attenuation in optical fibers decreases with an increase of the wavelength from 2 dB/km at 800 nm to a local minimum of 0.35 dB/km at 1300 nm and an absolute minimum of 0.25 dB/km at 1550 nm. On the other hand, photons with lower energy—or longer wavelength—tend to be more difficult to detect. Below 900 nm, one typically uses commercial modules built around a silicon avalanche photodiode (Si APD) biased above breakdown. They offer good quantum detection efficiency (typically 50%), low-noise count rate (100 Hz), and easy operation. In the so-called second telecom window, germanium avalanche photodiodes (Ge APD's) can be used. Their performance is not as good as that of Si APD's and they require liquid-nitrogen cooling. Finally, only indium gallium arsenide avalanche photodiodes (InGaAs APD's) exhibit sufficient detection efficiency in the third telecom window around 1550 nm. They have the same drawbacks as Ge APD's, but also require gated operation to yield low enough dark counting rates. Taking into account these factors, one can conclude that, up to a few kilometers, 800 nm is a good choice. In addition, beyond 30–40 km, the only real possibility is to operate the system at 1550 nm, because fiber attenuation becomes really critical.

A. QKD protocol

Our system is based on a Franson arrangement [13]. It exploits photon pairs entangled in energy-time, where the sums of both the energy and the momenta of the down-converted photons equal those of the pump photon. A source located between Alice and Bob generates such pairs, which are split at its output [see Fig. 1(a)]. One photon is sent to each party down quantum channels. Both Alice and Bob possess an unbalanced Mach-Zehnder interferometer, with

photon-counting detectors connected at its outputs. When considering a given photon pair, four events can yield coincidences between one detector at Alice's and one at Bob's. First, the photons can both propagate through the short arms of the interferometers. Then, one can take the long arm at Alice's, while the other takes the short one at Bob's. The opposite is also possible. Finally, both photons can propagate through the long arms. When the path differences of the interferometers are matched within a fraction of the coherence length of the down-converted photons, the short-short and the long-long processes are indistinguishable and thus yield two-photon interference, provided that the coherence length of the pump photons is longer than the path difference. If one monitors these coincidences as a function of time, three peaks appear. The central one is constituted by the interfering short-short and long-long events. It can be separated from noninterfering ones by placing a window discriminator. Only interfering processes will be considered below.

We implemented a protocol analogous to that of Bennett and Brassard (BB84). Ekert *et al.* showed in [14] that the probabilities for Alice and Bob to get correlated counts (the photons choose the same port at Alice's and Bob's) and anticorrelated counts (they choose different ports) are given by

$$P_{\text{correlation}} = P(A=0;B=0) + P(A=1;B=1) \\ = \frac{1}{2}[1 + \cos(\phi_A + \phi_B)], \quad (1)$$

$$P_{\text{anticorrelation}} = P(A=0;B=1) + P(A=1;B=0) \\ = \frac{1}{2}[1 - \cos(\phi_A + \phi_B)], \quad (2)$$

where Alice's phase ϕ_A and Bob's phase ϕ_B can be set independently in each interferometer. The results of Alice's and Bob's measurements are represented by A and B . They can take values of 0 or 1 depending on the detector that registered the count. One sees that, if the sum of the phases is equal to 0, $P_{\text{correlation}}=1$ and $P_{\text{anticorrelation}}=0$. In this case, Alice can deduce that, whenever she gets a count in one detector, Bob will also get one in the associated detector. If both Alice and Bob set their phases to 0, they can exchange a key by associating a bit value with each detector. However, if they want their system to be secure against eavesdropping attempts, they must implement a second measurement basis. This can be done, for example, by adding a second interferometer to their systems [see Fig. 1(b)]. Now, when reaching an analyzer, a photon chooses randomly to go to one or the other interferometer. The phase difference between Alice's interferometers is set to $\pi/2$, whereas that between Bob's is $-\pi/2$. If both photons of a pair go to associated interferometers, the sum of the phase they experience is 0. We obtain again the correlated outcomes discussed above. On the contrary, if they go to different interferometers, the sum is $\pm\pi/2$. In this case, one finds that $P_{\text{correlation}}=\frac{1}{2}$ and $P_{\text{anticorrelation}}=\frac{1}{2}$. Alice's and Bob's outcomes are then not correlated at all. They perform incompatible measurements. After exchanging a sequence of pairs, the parties must of

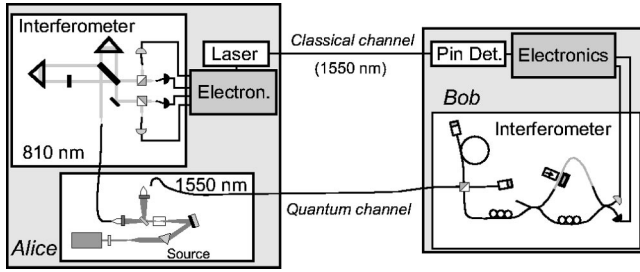


FIG. 2. Asymmetric system for quantum key distribution utilizing photon pairs.

course go through the conventional steps of key distillation, as in any QKD system: key sifting, error correction, and privacy amplification [15].

B. Photon-pair configuration

Let us now discuss the choice of wavelength for the photons of the pairs. As mentioned earlier, when transmitting photons over long distances, one should select a wavelength of 1550 nm to minimize fiber attenuation. However, detectors sensitive to such photons require gated operations in order to keep the dark counting rates low. Therefore, we selected an asymmetrical configuration where only the photon traveling to Bob has this wavelength, while the one traveling to Alice has a wavelength below 900 nm. She can consequently use free-running Si APD detectors. Whenever she gets a click, she sends a classical signal to Bob to warn him to gate his detectors. The source is located very close to Alice's interferometers, to keep fiber attenuation negligible (see Fig. 2). One should note that in such an asymmetrical configuration the losses in Alice's apparatus seem to be unimportant. When a photon gets lost in Alice's analyzer, she does not send a classical signal to Bob, who in turn does not gate his detectors. Such an event can thus not yield a false count through detector noise. A second possibility is to utilize one photon of the pair simply to generate a trigger signal, indicating the presence of the other one. This solution is not optimal. The second photon must indeed be sent through a preparation device featuring attenuation, which will reduce its probability to be detected by Bob.

Systems using pairs of photons entangled in energy-time are more sensitive to chromatic dispersion spreading in the transmission line than faint-pulse setups, because of the relatively large spectral width of the pairs. Indeed, interfering events are discriminated from noninterfering ones by timing information. Spreading of the photons between Alice and Bob induced by chromatic dispersion must thus be kept to a minimum. For example, assuming a spectral width of 6 nm, an impulsion launched in a standard single-mode fiber featuring a typical dispersion coefficient of $18 \text{ ps nm}^{-1} \text{ km}^{-1}$ at 1550 nm would spread to 1 ns after 10 km of fiber. This effect can be avoided by using dispersion-shifted (DS) fibers with their dispersion minimum close to the down-converted wavelength. It is also possible to compensate dispersion (see [16]), although this implies additional attenuation.

C. Characterizing the system

In order to characterize our system and assess its advantages over other setups, we introduce in this section the equations expressing the quantum bit error rate \mathcal{D} and the sifted key distribution rate.

In principle, when an eavesdropper—Eve—performs a measurement on a qubit exchanged between Alice and Bob, she induces a perturbation with nonzero probability, yielding errors in the bit sequence. These discrepancies reveal her presence. Nevertheless, in practical systems, errors also happen because of experimental imperfections. One can quantify the frequency of these errors as the probability of getting a false count over the total probability of getting a count [see Eq. (3)]. In the limit of low error probability, this ratio can be approximated by the probability of getting an incorrect count over the probability of getting a correct one. As discussed above, Bob's detectors are operated in gated mode and these probabilities must thus be calculated per gate. In addition, we will consider only the cases where compatible bases are selected by Alice and Bob.

$$\mathcal{D} = \frac{\text{Prob}(\text{incorrect count})}{\text{Prob}(\text{incorrect} + \text{correct counts})} \approx \frac{\text{Prob}(\text{incorrect count})}{\text{Prob}(\text{correct count})} \quad (3)$$

The correct count probability is expressed as the product of several terms. The first one is μ , the probability of having a photon leaving the source in the direction of Bob whenever Alice detects a photon and sends a classical pulse. Then come the probabilities T_L and T_B for this photon to be transmitted, respectively, by the fiber link and by Bob's apparatus. The next factor q_{interf} is equal to $\frac{1}{2}$ in our system and takes into account the fact that only half of the photons will actually yield interfering events that can be used to generate the key. The factor η_D represents the quantum detection efficiency of Bob's detectors. Finally, the term q_{basis} accounts for the cases where Alice and Bob perform incompatible measurements. It is equal to $\frac{1}{2}$ for a symmetrical basis choice:

$$P_{\text{correct}} = \mu T_L T_B q_{\text{interf}} \eta_D q_{\text{basis}} \quad (4)$$

The probability of getting a false count per gate can be thought of as the sum of three terms. It can arise first through a detector error. Each one of our four detectors can register a noise count. It will yield an error in 25% of the cases, a correct bit also in 25% of the cases, and an incompatible measurement in the remaining 50%. It is thus accounted for by the probability $p_{\text{cs}} (= 4 \times p_{\text{cs}} \times 1/4)$:

$$P_{\text{incorrect}} = p_{\text{cs}} = \mu T_L T_B q_{\text{interf}} \eta_D q_{\text{basis}} p_{\text{opt}} + \nu T_L T_B q_{\text{interf}} \eta_D q_{\text{basis}} q_{\text{acc}} \quad (5)$$

The second term corresponds to the cases where, because of imperfect phase alignment of the interferometers, a photon chooses the wrong output port of the interferometer. It is given by the product of the probability of getting a correct count multiplied by the probability p_{opt} for the photon to

choose the wrong port. In an interferometric system, it stems from nonunity visibility V , and is given by

$$p_{\text{opt}} = \frac{1 - V}{2}. \quad (6)$$

Finally, the last term takes into account the probability of getting a count from an accidental coincidence. It is given by the product of the probability ν of having an uncorrelated photon within a gate with the probability for this photon to reach Bob's system and be detected in the compatible basis. Because of the fact that it is not correlated with Alice's, this photon will choose the output randomly and yield a false count in 50% of the cases, and a correct one also in 50%. This is accounted for by the factor q_{acc} , which is equal to $\frac{1}{2}$.

These three components can be separated into three \mathcal{D} contributions as in Eq. (7). These formulas are general and thus still valid for other systems:

$$\mathcal{D} = \mathcal{D}_{\text{det}} + \mathcal{D}_{\text{opt}} + \mathcal{D}_{\text{acc}}, \quad (7)$$

$$\mathcal{D}_{\text{det}} = \frac{p_{\text{cs}}}{\mu T_L T_B q_{\text{interf}} \eta_D q_{\text{basis}}}, \quad (8)$$

$$\mathcal{D}_{\text{opt}} = \frac{\mu T_L T_B q_{\text{interf}} \eta_D q_{\text{basis}} p_{\text{opt}}}{\mu T_L T_B q_{\text{interf}} \eta_D q_{\text{basis}}} = p_{\text{opt}}, \quad (9)$$

$$\mathcal{D}_{\text{acc}} = \frac{\nu T_L T_B q_{\text{interf}} \eta_D q_{\text{basis}} q_{\text{acc}}}{\mu T_L T_B q_{\text{interf}} \eta_D q_{\text{basis}}} = q_{\text{acc}} \frac{\nu}{\mu}. \quad (10)$$

One should note that, if the basis choice was implemented actively, only two out of the four detectors at Bob's would be gated for a given bit. This implies that both \mathcal{D}_{det} and \mathcal{D}_{acc} would be reduced by a factor of 2. In principle, active switching thus ensures a gain of factor 2 in \mathcal{D}_{det} corresponding to approximately 10 km of transmission distance at 1550 nm. In practice, this is not true because of the additional losses induced by devices used to perform active base choices (Pockel cells or LiNbO₃ phase modulators, for example).

When the length of the fiber link is increased, T_L decreases. The probability of getting a right count is reduced, while the probability of registering a dark count remains constant and \mathcal{D}_{det} thus increases. On the other hand, as they do not depend on T_L , both \mathcal{D}_{opt} and \mathcal{D}_{acc} remain unchanged. When exchanging key material over long distances, \mathcal{D}_{det} becomes consequently the main contribution and sets an ultimate limit on the span. In order to maximize the distance, one should clearly choose the best detectors available, and maximize the correct count probability. In systems exploiting faint laser pulses, it is essential that the multiphoton pulse probability be low to ensure security. In this case, one selects for μ a value well below unity, which reduces the correct count probability. A given \mathcal{D} is thus reached for a shorter transmission distance. Setting this parameter to 0.1—a typical value—instead of 1 has the same effect on \mathcal{D}_{det} as adding fiber attenuation of 10 dB, corresponding to a distance of about 40 km at 1550 nm. One sees clearly a first

advantage of using photon pairs instead of faint laser pulses. This issue is discussed in more detail in Sec. V.

Unfortunately, additional factors reduce this advantage. Comparing the predicted performance of our photon-pair system with that of a well-tested faint-pulse system like our ‘‘plug and play’’ setup [5], we see that the ratio of \mathcal{D}_{det} for a given transmission distance is in theory equal to

$$\frac{\mathcal{D}_{\text{det}}^{\text{PP}}}{\mathcal{D}_{\text{det}}} = \frac{\mu q_{\text{interf}}}{2 \mu^{\text{PP}} q_{\text{interf}}^{\text{PP}}} = \frac{5}{2}. \quad (11)$$

This result is obtained by setting $q_{\text{interf}}^{\text{PP}} = 1$ and $\mu^{\text{PP}} = 0.1$ for the plug and play system and $q_{\text{interf}} = 1/2$ and $\mu = 1$ for our photon-pair system. The factor 2 in the denominator comes from the fact that active basis selection is performed with the plug and play system. The other factors are assumed to be identical and they just cancel out. This means that our new system should be able to handle 4 dB of additional fiber attenuation, corresponding to approximately 16 km at 1550 nm. However, one should note that photon-pair systems suffer from an additional contribution to their error rate— \mathcal{D}_{acc} —which somewhat reduces this advantage. Although it is important, this span increase would not revolutionize the potential applications of QKD over optical fibers.

Finally, it is possible to estimate the actual raw key creation rate (after sifting, but before distillation) by multiplying the probability of getting a right count by the counting rate registered by Alice:

$$R_{\text{raw}} = f_{\text{Alice}} P_{\text{correct}}. \quad (12)$$

The quantity f_{Alice} represents the repetition frequency and P_{correct} is given by Eq. (4). One can then apply correction factors to estimate the distilled key rate [17].

III. IMPLEMENTATION OF THE SYSTEM

Now that the principles of QKD using photon pairs entangled in energy-time have been discussed, we can consider the actual implementation of the system. It consists of four basic subsystems: the photon-pair source, Alice's interferometer, Bob's interferometer, and the classical channel (Fig. 2). We also discuss the procedure used to measure and adjust the path differences of the interferometers.

A. The photon pair source

The source is basically made up of a pump laser, a beam shaping and delivery optical system, a nonlinear crystal, and two optical collection systems (see Fig. 3). It is built with bulk optics. The pump laser is a GCL-100-S frequency-doubled yttrium aluminum garnet (YAG) laser manufactured by Crystalaser. It emits 100 mW of single-mode light at 532 nm. Its spectral width is narrower than 10 kHz. This corresponds to a coherence length of about 30 km for the pump photons, and yields in turn a high visibility for the two-photon interference. Its frequency stability was verified to be better than 50 MHz per 10 min. This is an important parameter since the wavelength of the pump photons controls the wavelengths of the down-converted photons. These must re-

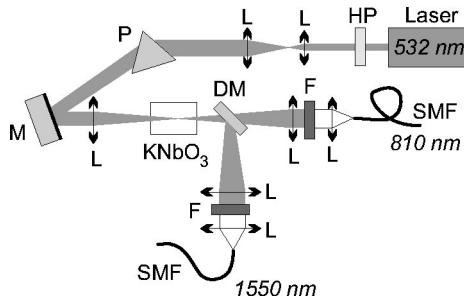


FIG. 3. Schematic diagram of the photon pair source (HW, half-wave plate; L, lens; P, dispersive prism; M, metallic mirror; DM, dichroic mirror; F, filter; SMF, single-mode fiber).

main stable during a key distribution session, because they determine the relative phases the photons experience in the interferometers.

The collimated beam passes first through a half-wave plate, which rotates its linear polarization state to horizontal. It goes then through a Keplerian beam expander ($\times 2$). It then passes a dispersive prism and a Schott BG39 band-pass filter ($T=98\%$ at 532 nm and $T=10^{-4}$ at 1064 nm), in order to remove any infrared light that might mask actual photon pairs. Both of these components are aligned so that the angle between their surfaces and the incident beam is close to the Brewster angle, in order to minimize pump-power loss by partial reflection. The beam is then reflected by a metallic mirror before going through a pinhole, which complements our simple monochromator. It is then focused on the KNbO_3 nonlinear crystal through a biconvex achromat with 100-mm focal length. The crystal measures $3(\phi\text{plane}) \times 4(\theta\text{plane}) \times 10\text{mm}^3$. It is cut with a θ angle of 22.95° and allows collinear down-conversion at 810 and 1550 nm when kept at room temperature and illuminated normally with a pump at 532 nm. Its first face is covered with antireflection (AR) coating for 532 nm, while the second one has AR coating for 810 and 1550 nm. The crystal can be slightly rotated ($\pm 5^\circ$) to tune the pump incidence angle. This parameter is used to adjust the down-converted wavelengths. The down-converted beams are then split by a dichroic mirror aligned at 45° incidence. The photons at 810 nm experience a transmission coefficient of approximately 80%, while the 1550 nm photons experience a reflection coefficient of more than 98%. The short-wavelength beam is then collimated by a biconvex achromat with a focal length of 150 mm. A set of two uncoated filters is used to block off the pump light. One should avoid fluorescence in this process, in order to minimize the probability of recording coincidences from uncorrelated photons. This is achieved by using first a low-fluorescence Schott KV550 long-pass filter ($T=20\%$ at 532 nm) to reduce the pump intensity, before blocking it with a Schott RG715 long-pass filter. The 810 nm photons are then focused onto the core of a single-mode fiber (cutoff wavelength less than 780 nm, mode field diameter $5.5 \mu\text{m}$) by a collimator (focal length 11 mm) with a receptacle for fiber optic connectors.

After being reflected by the dichroic mirror, the 1550-nm beam is collimated by a biconvex achromat with focal length of 75 mm. The pump beam is then removed by a coated

silicon long-wave-pass filter (5% cut on at 1050 nm), offering a transmission coefficient at 1550 nm close to 100%. The down-converted beam is then focused onto the core of a single-mode fiber (cutoff wavelength less than 1260 nm, mode field diameter $10.5 \mu\text{m}$), through an identical fiber collimator as for the 810 nm beam.

As discussed above, the probability μ of having one photon at 1550 nm leaving the source, knowing that there was one at 810 nm, must be maximized, if one wants to gain an advantage with respect to faint-laser-pulse systems. This implies that the collection efficiency of the long-wavelength photons must in particular be optimized through careful alignment of the optical system and appropriate selection of the optical components (coating, numerical aperture). The focal lengths of the lenses located in the three beams were selected to match the size of their Gaussian waists inside the crystal. We followed the collecting beams in the reverse direction, starting from the mode field diameter of the fibers, and calculating their transformation through the various components up to the crystal. This mode matching is essential to obtain a high μ .

To characterize this source, we connect the short-wavelength output port to a Si photon-counting detector and the long-wavelength one to a gated InGaAs detector. We obtained a value of approximately 1.1 MHz for the single counting rate on the Si detector. When monitoring the coincidences in a 2 ns window using the single-channel analyzer of a time-to-amplitude converter, and taking into account the fact that the quantum detection efficiency of the InGaAs detector is only 8.5%, the best value of μ we obtained was 70%. Such a performance required extremely careful alignment. As far as we know, it is the best reported. However, a more typical and easily reproducible value of μ is 64%. It will be used in the rest of the paper. In order to evaluate the probability of registering an accidental coincidence caused by noncorrelated photons, we delayed the coincidence window by a few nanoseconds. Subtracting the value of the thermal noise of the InGaAs detector, we measured a value of ν of 1%. We measured the spectral width of the down-converted photons at 810 nm, and found it to be smaller than 5 nm FWHM.

B. Alice's interferometer

In the description of the key distribution principle, it was explained that Alice and Bob each needed two unbalanced interferometers in order to switch between two incompatible measurement bases. The path differences of these interferometers must be matched within a fraction of a wavelength, plus or minus a phase shift of $\pi/2$. They must then be kept stable during the QKD process. As this condition is very difficult to fulfill, it is beneficial to devise a system where Alice and Bob have only one interferometer each. This can, for example, be achieved by simply inserting in the interferometers fast phase modulators. However, these devices are costly, and they introduce significant attenuation in the setup. In addition, passive-state preparation offers superior security, as will be discussed in Sec. V.

We devised an elegant alternative. The two interferometers can be multiplexed in polarization. We add in the long

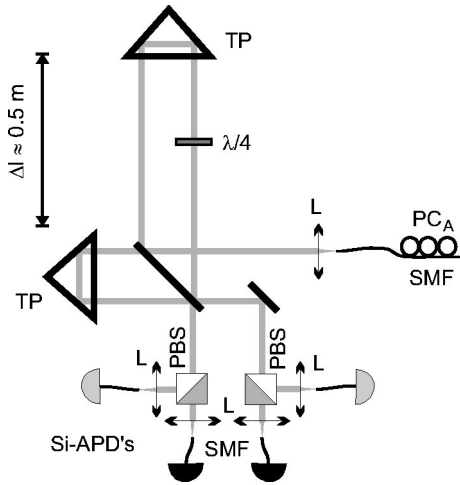


FIG. 4. Schematic diagram of Alice's interferometer (PC_A , polarization controller; SMF, single-mode fiber; L , lens; TP, trombone prism; PBS, polarizing beam splitter).

arm of both Mach-Zehnder interferometers a birefringent element inducing a phase shift of $\pi/2$ between the horizontal and vertical polarization modes. Assuming constructive interference in one port for vertically polarized light, we will then observe an equal probability for choosing each output port for horizontally polarized light. In order to distinguish between the two measurement bases, we also add polarizing beam splitters (PBS's) separating vertical and horizontal polarizations between the output ports and the detectors. When a circularly or 45° -linearly-polarized photon enters such a device, it decides upon incidence on the PBS whether it experienced a phase difference of $(2\pi/\lambda_A)\Delta L_A$ or $(2\pi/\lambda_A)\Delta L_A + \pi/2$. Determination of the output port of the PBS reveals the phase experienced. This principle, offering passive-state preparation, is implemented in Alice's interferometer. Please note that this polarization multiplexing can also be used with the phase-encoding faint-laser-pulse scheme introduced by Townsend [18]. When realizing the interferometers, care has to be taken to keep the interfering events ($short_A$ - $short_B$, and $long_A$ - $long_B$) as indistinguishable as possible to maintain high fringe visibility. Because of the relatively wide spectrum of the down-converted photons, chromatic dispersion may constitute a problem. It should be kept as low as possible in order to maximize the overlap between the two processes. As dispersion in optical fibers is rather high around 810 nm, we chose to implement Alice's analyzer with bulk optics, in the form of a folded Mach-Zehnder interferometer (see Fig. 4). Before launching the photons into the interferometers, their polarization state is adjusted with a fiber loop controller. The input port consists of a fiber collimator ($f=11$ mm), generating a beam with a diameter of 3 mm. The photons are then split at a 50-50 hybrid beam-splitting cube (side 25.4 mm). We used trombone prisms (right-angle accuracy of $\pm 5''$) as reflectors, in order to simplify alignment. A zero-order quarter-wave plate ($\lambda_0=800$ nm) is inserted in the long arm and vertically aligned to apply the phase shift on vertical states. A polarizing beam splitter (side 11 mm, extinction greater than 40 dB) is inserted in each output port. Each beam is then focused on

the core of a single-mode fiber (cutoff wavelength less than 780 nm, mode field diameter $5.5 \mu\text{m}$) using a collimator (NA 0.25, $f=11$ mm). The fibers serve as mode filters to yield high fringe visibility. They are then connected to Si APD photon-counting detectors. Although four such devices are required for complete implementation of the setup, we had only two available. When testing the QKD process, we exchanged the fibers to test all four ports. Both detectors are actively quenched (EG & G SPCM-AQR-15FC and SPCM-AQ-141-FC). They both have a quantum detection efficiency of about 50%, and noise counting rates of the order of 100 Hz. Whenever a count is registered, the detectors are electronically inhibited for 500 ns.

The path difference in the interferometers must be larger than the coherence length of the down-converted photons ($l_c \approx 3 \times 10^{-4}$ m), to prevent single-photon interference. Unfortunately the events are broadened by the detector's time jitter (of the order of 800 ps FWHM for a coincidence detection between the first Si APD and an InGaAs APD, and 360 ps FWHM for a coincidence between the second Si detector and an InGaAs detector, while the jitter of the InGaAs APD was measured to be 250 ps). The minimum path difference is thus not limited by the coherence length, but by the width of the coincidences. In order to keep the overlap between adjacent events below a few percent, we set the time difference to approximately 3 ns, corresponding to a round-trip path difference of $2 \times 0.5 = 1$ m in air. This distance should be kept stable within a fraction of a wavelength during a QKD session. In order to reduce the phase drifts induced by temperature fluctuations, the interferometer is placed in an insulated box. Moreover, the temperature is regulated with an accuracy of 0.01°C . Finally, the mount holding the reflection prism of the long arm is fixed to the beam splitter by a glass rod (pure silica), featuring a low linear expansion coefficient of $5 \times 10^{-7} \text{ m}^{-1} \text{ K}^{-1}$ (approximately 50 times smaller than that of the aluminum base plate). The length of the long arm can be varied coarsely by a translation stage with a precision of approximately $5 \mu\text{m}$. Fine adjustment is then performed with a piezoelectric element, featuring a displacement coefficient of about $0.05 \mu\text{m}/\text{V}$.

The transmission loss of the interferometer was approximately 9 dB. This value was very sensitive to the alignment of the reflecting prisms and the fiber collimators.

C. Bob's interferometer

Bob's interferometer is similar to Alice's analyzer, except that it is implemented with optical fibers (see Fig. 5). It is realized with two 3-dB couplers connected to each other. The long arm consists of DS fiber with λ_0 close to 1550 nm, in order to avoid spreading of the photons and maximize the visibility. The path difference is about 70 cm, corresponding to an optical length of approximately 1 m. A fiber loop polarization controller is also inserted in this long arm to ensure identical polarization-state transformation for both paths. The birefringent element used to implement polarization multiplexing consists of a piezoelectric element applying a variable strain on a 5-mm-long uncoated section of the long

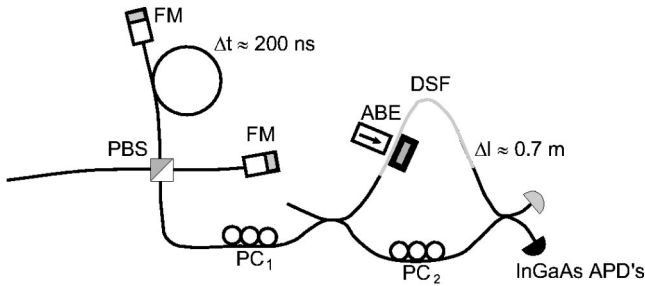


FIG. 5. Schematic diagram of Bob's interferometer (PBS, polarizing beam splitter; FM, Faraday mirror; PC, polarization controllers; ABE, adjustable birefringent element; DSP, dispersion-shifted fiber).

arm. This allows tuning the phase difference by adjusting a continuous voltage. One typically introduces a birefringence of 2π with a voltage of about 50 V, which implies that the adjustment is not very critical. The exact value depends on the initial strain applied on the element. In the case of Bob, we separate the two polarizations corresponding to the measurement bases before injecting the photons in the interferometer. This information is then transformed into a detection time information. This is achieved by placing a fiber optic polarizing beam splitter (extinction of 20 dB) between the line and the interferometer. The photons are split according to their polarization and reflected by two Faraday mirrors, which transform their polarization states into orthogonal states upon reflection. This ensures that they exit by the port connected to the interferometer with orthogonal polarizations. While the first arm of this device measures only 1 m, the second one is 20 m longer, so that a delay of 200 ns is introduced between the two polarization states. The photon-counting detectors are gated twice, and one can infer the measurement basis, from the detection time bin. As discussed above, after traveling through the optical fiber line connecting Alice and Bob, the photons are depolarized. This ensures that each photon will choose randomly with 50% probability the basis at the PBS. For example, the degree of polarization of Bob's photons drops from a value close to 100% at the output of the source to only 25% after an 8.5-km-long fiber. However, as Eve could devise a strategy where she could benefit from forcing detection of a given qubit in a particular basis, we must introduce a polarizer aligned at 45° or a polarization scrambler in front of the PBS. As the photons cross the PBS twice polarized orthogonally, we expect that the imperfections of this device will only reduce the counting rate, but not introduce errors. The photons then go through a fiber loop polarization controller (PC_1) to align these states with the axes of the variable phase plate. The overall attenuation of Bob's apparatus is -5.2 dB. It was measured by connecting a 1550-nm light-emitting diode (LED) to the input port of the PBS and by adding the powers measured at each output port. This attenuation comes from the insertion losses of the PBS (1.5 dB), the Faraday mirrors (1 dB), and the couplers (0.5 dB), as well as the FC/PC connectors. The interferometer is also placed in an insulated box, where the temperature is kept stable within 0.01 °C.

The two detectors connected to the output ports of the interferometer are EPM 239 AA InGaAs APD's manufactured by Epitaxx. They are mounted on a measurement stick that is immersed into liquid nitrogen and heated by a resistor to adjust their temperature to -60 °C. The voltage across them is kept below breakdown, except when they are gated by the application of a 2-ns-long and 7.5-V-high voltage step [19]. The detectors' quantum detection efficiencies are 9.3% and 9.4%, respectively, for a thermal noise probability per gate of 2.8×10^{-5} and 2×10^{-5} (please note that these detectors are different from the one used to characterize the photon-pair source). Although cooling the detectors to a lower temperature could still further reduce the thermal noise probability, the lifetime of the trapped charges yielding afterpulses would increase, so that the overall noise would actually rise. We checked at -60 °C the dependence of the noise probability on the gate repetition frequency. At 1 MHz, the maximum frequency of our signal generator, a slight increase was observed. As the minimum time between two subsequent gates is of the order of 200 ns, and the repetition frequency does not rise much above 100 kHz, we deduce from this measurement that afterpulses should cause only limited noise increase in our system.

We discuss the polarization alignment of Bob's interferometer in Sec. IV.

D. Aligning the interferometers

The optical path differences of Alice and Bob's interferometers must be adjusted to be equal within a few wavelengths. This is achieved by connecting them in series with a scannable Michelson interferometer. Light from a 1300-nm polarized LED is then injected in this setup. Because of the extremely low transmission of the bulk optics interferometer at this wavelength, the signal is recorded with a passively quenched germanium photon-counting APD. When scanning the path difference of the Michelson interferometer, one can register interference fringes when the discrepancy between the path differences in Alice's and Bob's interferometers is compensated. This allows measuring $|\Delta L_A - \Delta L_B|$ with micrometer accuracy. Because of the chromatic dispersion, this difference depends on the measurement wavelength. One can compute that at 1550 nm ΔL_B is approximately 400 μ m smaller in the case of an interferometer made of DS fiber than at 1300 nm. The translation stage in Alice's interferometer can then be used to adjust ΔL_A and reduce $|\Delta L_A - \Delta L_B|$ to below a few tens of micrometers. At this point, two-photon interference patterns can be observed when connecting the photon-pair source to the interferometers. Finally, the piezoelectric element can be used to tune the path difference with an accuracy smaller than the wavelength.

E. The classical channel

In all QKD systems, a classical channel must be available to perform key distillation. The experiment reported in this paper features full implementation of the physical components necessary for QKD. However, we did not realize the software generating the key from the raw bit sequence. The classical channel is thus simply used to transport timing in-

formation about the down-converted photons, in order to inform Bob to gate his detectors at the right time. It consists of a second optical fiber, a 1550-nm distributed feedback (DFB) laser diode at Alice's and a PIN InGaAs photodiode followed by an amplifier and a discriminator at Bob's. It features a time jitter of 200 ps and works with an attenuation of up to 30 dB. Eve should not be able to gain any information on the event registered by Alice from the time difference between the passing photon and the classical pulse. The time between the detection of a single photon and the emission of the classical pulse must then be equal for the four ports within the time jitter of the photon-counting detectors. This is achieved by adjusting the length of the cables between the detectors and the electronics. In addition to this timing signal, we also send on the classical channel information about which detector registered the count at Alice's. A second pulse, in one of four time bins, thus follows the synchronization one. Upon detection of a timing pulse, Bob triggers his detectors and feeds the result he registers along the decoded information about Alice's detection into a processing unit that generates several transistor-transistor logic (TTL) signals. Bob can thus keep track of correct and incorrect events, as well as cases where incompatible bases were used. For verification purposes, the system also provides false counts in each of the separate bases. These data are stored on a computer with a digital counter board (National Instruments PC-TIO-10). In order to implement an actual key distribution, one must simply remove Alice's information from the classical channel, by disconnecting one cable. The events are then just stored by Alice and Bob until key distillation.

IV. EXPERIMENTAL RESULTS

A. System adjustment

Now that the principle of our system and its implementation have been described, we can present a QKD session. One must first adjust and characterize the setup. We assume below that Alice's interferometer is ready.

The first step is to align the polarization states in Bob's interferometer with the axes of the birefringent plate. One Faraday mirror is replaced by a reflectionless termination, so that only one polarization state is sent into Bob's system. In addition, the short arm of the interferometer, which does not contain the birefringent element, is opened. A polarized LED at 1550 nm is injected in the system. One then uses the controller PC_1 to adjust the state of polarization, while monitoring it with a polarimeter. The idea is to find a setting such that applying a voltage on the variable birefringent element does not modify this state. Once this is done, the polarization is recorded with the polarimeter and the short arm is connected. The controller PC_2 is then used to adjust the transformation in this arm to bring back the state to the position recorded on the polarimeter.

The next step is to measure and maximize the visibility of the two-photon interference fringes. The photon-pair source is connected to both interferometers. One Faraday mirror only is connected at Bob's, so that only one measurement basis is implemented. It is sufficient to consider one detector at each side. Alice's detector 1 registers a counting rate of

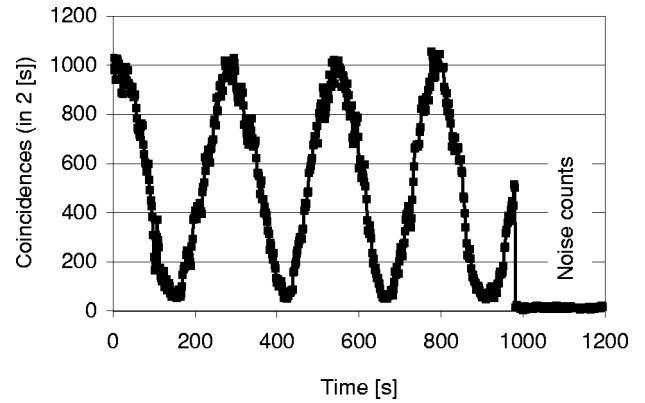


FIG. 6. Typical two-photon interference visibility measurement. Coincidences between a Si APD at Alice's and an InGaAs APD at Bob's.

approximately 100 kHz, with the polarization controller PC_A adjusted to maximize it. In addition, a variable voltage is applied on the piezoelectric element, varying the length of the long arm in Alice's interferometer. We used an SRS DS 345 function generator and a piezoelectric controller. The phase experienced by Alice's photon is thus modulated and two-photon interference fringes in the coincidences between the detectors can be recorded (see Fig. 6). The period is of the order of 4 min. At the end, the delay was modified to measure the noise counts. In the results presented, we obtained a visibility of $91.8\% \pm 0.8\%$ when subtracting these noise counts. This value is the same in both bases. Please note that this measurement essentially amounts to performing a Bell inequality test.

One must then adjust the birefringence in Bob's interferometer, so that the global phase introduced in both bases equals zero. The second Faraday mirror is connected, to implement the second basis. The voltage applied on the birefringent element is slowly tuned until the interference patterns obtained in each basis are brought in phase. This setting remains stable for hours.

The last step is to measure the probability for Bob's detectors to produce a thermal count per gate. We obtain a value of 3.3×10^{-5} and 4.4×10^{-5} , respectively. The fact that these probabilities are superior to the figures obtained during the characterization of the detectors probably comes from the fact that the time between two subsequent gates is not constant anymore but statistically distributed. Afterpulses may thus account for this increase. In addition, we have already noticed significant variations in the performance of InGaAs APD's between measurements, indicating limited repeatability.

B. Key distribution

Now that the system has been tuned and characterized, it is ready for QKD. Both of Alice's detectors are connected and the polarization controller PC_A is set so that they each yield the same counting rate. The total counting rate is approximately 100 kHz. The voltage applied on the piezoelectric element varying the length of the long arm of Alice's interferometer is adjusted manually to minimize \mathcal{D} . The key

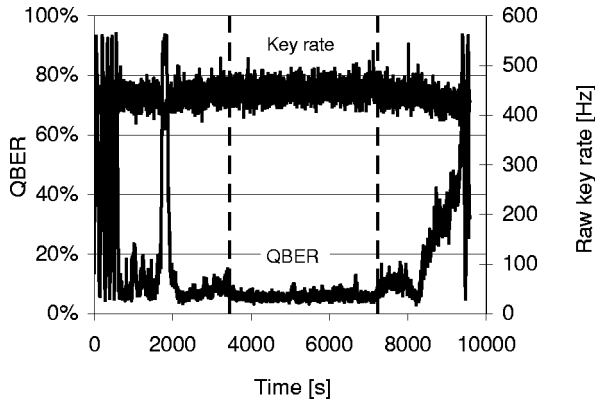


FIG. 7. Key distribution session. The vertical broken lines indicate the region used to calculate the average quantum-bit error rate \mathcal{D} (QBER). The acquisition time for one data point was 2 s.

distribution session can then start and last until the interferometers have drifted so that the error rate becomes too large. One must then readjust the voltage on the piezoelectric element. We observed that waiting for two hours after closing the boxes containing the interferometers ensures higher stability. We first connected Alice's and Bob's apparatus by a short fiber of 20 m with essentially no attenuation. Nevertheless, they were located in two different rooms in order to simulate remote operation.

We obtained a raw key distribution rate (after sifting, but before distillation) of 450 Hz, and a minimum \mathcal{D} of $4.7\% \pm 0.3\%$. The whole key distribution session was defined, somewhat arbitrarily, as the period of time during which the error rate remained below 10%. It lasted 63 min and allowed the distribution of 1.7 Mbit (see Fig. 7). The average error rate, calculated between the vertical dashed lines, was 5.9%. It is higher than the minimum because of slight variations in the relative phase difference in the interferometers induced by temperature drift. Before and after the key distribution region, fringes were recorded to verify the interference visibility. It is also possible to estimate the net rate (after distillation) using the formula presented in [5]. The fractions lost during error correction and privacy amplification increase with \mathcal{D} . A value of 178 Hz, readily usable for encryption, can be inferred.

We can apply the formula (8) to Eqs. (10) and (12) to verify that these values are consistent with the predictions and to evaluate the various contributions to the error rate. If we first consider the equation for the transmission rate, and solve for the detection efficiency—the quantity exhibiting the most significant uncertainty—we obtain by setting $\mu = 0.64$, $T_L = 0$ dB, and $T_B = -5.2$ dB an average quantum

detector efficiency η_D of 8.4%. This value is reasonably close to the expected value of 9.3%. Considering next the contribution of the detector noise to the error rate, we can calculate a value of 1% for \mathcal{D}_{det} , by setting p_{cs} to an average value of 3.9×10^{-5} obtained in the last step of the adjustment procedure. From the measured visibility of 91.8%, we can infer the contribution \mathcal{D}_{opt} to be equal to 4.1%. Finally, the accidental coincidence contribution to the error rate can be evaluated to 0.8% when setting ν to 1.1%. These contributions sum up to a total \mathcal{D} of 5.9%, slightly above the minimum value of \mathcal{D} measured ($4.7\% \pm 0.3\%$). These results are summarized in Table I.

We then connected an 8.45-km-long optical fiber spool between Alice and Bob to verify the behavior of our system. In order to avoid a reduction of the interference visibility caused by chromatic dispersion spreading, we selected DS fiber ($\lambda_0 = 1545$ nm). It featured an overall attenuation of 4.7 dB. The mode field diameter of this fiber being smaller than that of the standard fiber used in the source and Bob's interferometer (6 μm instead of 10.5 μm), rather high junction losses of 1.3 dB were obtained at each connection. In addition, the attenuation was 0.25 dB/km at 1550 nm (measured with an optical time-domain reflectometer). The classical channel was also implemented with an optical fiber spool whose length was adjusted within 7 cm (360 ps) of that of the quantum channel.

We first verified that the visibility remained unchanged and obtained a value of $91.7\% \pm 3.4\%$. This indicates that the use of the DS fiber clearly maintains high visibility interference. Measurement of the width of the coincidence peak between Alice and Bob separated by this DS fiber confirms this finding. It is essentially unchanged at 800 ps FWHM, while the peak broadens to 1.4 ns, yielding substantial overlap of interfering and noninterfering events (14% of the noninterfering events within 2 ns of the center of the interference peak), if the standard and DS fibers are exchanged.

Second, we performed key distribution during 51 min at a raw rate of 134 Hz, exchanging 0.41 Mbit. The average \mathcal{D} was 8.6% and the minimum \mathcal{D} $6.6\% \pm 0.6\%$. In this case, the net rate is estimated at 32 Hz. On the one hand, the values of \mathcal{D}_{opt} (4.1%) and \mathcal{D}_{acc} (1.0%) are essentially unchanged, as expected. On the other hand, \mathcal{D}_{det} increased to 3%. These contributions sum up to 8.1%, again slightly above the measured minimum value.

One can see in Fig. 8 a graph showing the quantum-bit error rate as a function of the attenuation of the link between Alice and Bob. It shows the experimental minimum (circles) and average (diamonds) values obtained with and without

TABLE I. Summary of the performance obtained.

Line length (m)	Attenuation (dB)	Minimum \mathcal{D}	Average \mathcal{D}	Raw rate (Hz)	Duration (min)	Raw key length (bits)	Estimated net rate (Hz)
20	≈ 0	4.7%	5.9%	450	63	1 704 118	178
8450	4.7	6.6%	8.6%	133	51	407 930	32

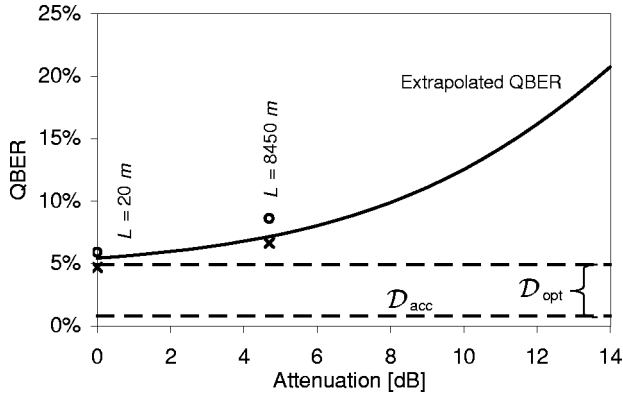


FIG. 8. Experimental values of \mathcal{D}_{\min} (circles) and $\mathcal{D}_{\text{average}}$ (crosses), and extrapolation of the QBER (continuous line). The two contributions (\mathcal{D}_{acc} and \mathcal{D}_{opt}) that do not depend on the distance are also shown (broken lines).

the spool connected. The solid line shows simulated values, with current InGaAs APD's. The contributions \mathcal{D}_{acc} and \mathcal{D}_{opt} , independent of the attenuation, are represented by the dashed lines.

V. DISCUSSION

A. Simulation of the performance with higher attenuation

We shall now evaluate the potential of this system for application over long fiber links and compare its performance with two other systems. It is a straightforward task to extrapolate the results obtained to take into account the effect of different transmission lines. As discussed above, the \mathcal{D}_{opt} and \mathcal{D}_{acc} contributions remain unchanged, while \mathcal{D}_{det} increases with the attenuation. Considering Fig. 8, one can see that, assuming an attenuation coefficient of 0.25 dB/km, an \mathcal{D} of 10% would be obtained with an attenuation of approximately 8.5 dB, corresponding to a fiber length of 24 km (0.25 dB/km and two connections with 1.3 dB). Although these performances may not seem very good compared, for example, with the results we reported in [5], one should remember that the distance is ultimately limited by the noise performance of the detector. The Epitaxy detectors used for this experiment show approximately a dark count probability four times higher than those available at the time of the last experiment (Fujitsu FPD5W1KS). In addition, the additional losses induced by the junctions could be reduced by using transition fibers with a slow variation of core diameter between the values of standard and DS fibers. Alternatively, the system could be completely realized with DS fiber. The 8.5-dB attenuation would hence translate into a distance of 34 km.

The accidental coincidence contribution to the error rate could be lowered in two ways. First, one could reduce the effective width of the gate window used for the InGaAs APD's. This could be done by feeding the coincidence signal into a time-to-amplitude converter with a single-channel analyzer. One can estimate that setting the width of this window to one standard deviation of the coincidence peak (800 ps FWHM) would reduce the accidental coincidences by a factor of 2, while suppressing only one-third of the real coinci-

dences. The ratio of real over accidental coincidences increases monotonically with a reduction of the width of the window. The limit is set by the reduction of the effective detection efficiency. The dark count probability would also be reduced by the same factor. The second solution to reduce this \mathcal{D} contribution is to decrease the pump power, at the expense of a reduction of the pair creation rate though. The probability of finding an uncorrelated photon indeed increases with the pump power. This illustrates why the attenuation in Alice's interferometer does matter after all. If it is too high, a very high pump power becomes necessary to obtain a given single-counting rate. Nevertheless, \mathcal{D}_{acc} does not really constitute an important contribution to the error rate, since it is about 1% and does not grow with distance.

The error contribution of about 4% due to nonunity visibility is more serious. This nonideal visibility probably stems from imperfect polarization alignment in the fiber interferometer, as well as residual chromatic dispersion. It may also come from a slight difference in the path differences of Alice's and Bob's interferometers. The two-photon interference fringes are indeed modulated by a Gaussian envelope, whose width is determined by the coherence length of the down-converted photons. It is essential to adjust the path differences to be as close as possible to the maximum of this envelope. However, as the coherence length is rather large, the top of this envelope is flat and difficult to find. Higher visibilities (up to 95%) were indeed obtained but not in a systematically reproducible way. In practice, we actually observed that it was difficult to tell whether the visibility improved or not when adjusting the piezoelectric element. Finally, one should also remember that an important feature of \mathcal{D}_{opt} is that it does not increase with the distance. However, it would clearly be valuable to try to improve this visibility.

B. Photon pairs rather than faint laser pulses?

It is essential for security reasons when working with faint-pulse systems to keep the fraction of pulses containing more than one photon smaller than the transmission probability $T_L T_B$. If this is not the case, the spy can use a so-called photon-number-splitting attack to obtain substantial information about the key material exchanged (see [20–22] for a discussion of this strategy). She could indeed measure the number of photons per pulse, and stop all those that do not contain more than one photon. In turn, when a pulse contains two or more photons, she splits it and stores one photon, while she dispatches the other photon to Bob through a lossless medium. Finally, she waits until Alice and Bob reveal the bases they used to perform her own measurements, and obtains full information. This potential attack implies that μ must be reduced when the distance is increased. It amplifies the effect of fiber attenuation on \mathcal{D}_{det} , which limits transmission to even shorter distances.

Our setup using photon pairs is not vulnerable to this attack. Indeed, even in the case where two (or more) photon pairs are created within a gate time of each other, the fact that the state preparation, amounting to the basis and bit value choices, is made in a passive way ensures that one photon is not correlated in any way with a photon belonging

to another pair. However, for this to be true, Alice must treat double detections cautiously [23]. She cannot simply discard these events, but must assign them a random value. This increases the error rate, without revealing information to Eve. When observing two photons in the quantum channel and a pulse in the classical one, Eve could otherwise deduce that their conjugates took the same output port at Alice's, yielding a single detection, and are thus correlated. In practice, because of limited detection efficiency, double detections are extremely rare. Like the experiment of Tittel *et al.* [10], our experiment thus offers a superior level of security, which represents its main advantage over faint-laser-pulse systems. The two other QKD experiments performed with photon pairs [11,12] used active-basis switching. Two photons of different pairs are thus invariably prepared in the same basis. Nevertheless, the actual bit value is selected randomly. In this case, when two photon pairs are emitted simultaneously, Eve can obtain probabilistic information about the bit value.

To summarize this security issue, we suggest distinguishing three levels. First, a system could be immune to all attacks, including multiphoton splitting, like the one presented in this article. In this case, the level of security is extremely high. Such a system resists attacks with existing as well as future technology. Its cost and complexity may, however, be too high for real applications. Second, one can consider systems based on faint pulses. They are immune to existing technology, but would not always resist multiphoton-splitting attacks. However, it is essential here to realize that, although in principle possible, such an attack would be in practice incredibly difficult. A natural idea for realizing a lossless channel—one of the components necessary for these attacks—is to use free-space propagation. However, attenuation in air at 1550 nm is higher than in fibers (0.64 dB/km under good visibility [24]). Moreover, it depends critically on the atmospheric conditions (in particular, humidity). Diffraction- and turbulence-induced beam wandering also reduce the transmission. On the other hand, faint-pulse systems offer the advantage of being reasonably easy to operate and automate. In addition, they could actually be ready for real applications quickly. Finally, one can look at classical public key cryptography, which is considered to offer sufficient security, when implemented with suitable key length. In addition, it is convenient to apply, as it does not require any dedicated channel, and has been in use for many years. It suffers from a major disadvantage, however. Its security could indeed be jeopardized overnight by some theoretical advance. In this event, QKD with faint pulses would constitute the only realistic replacement technology. In addition, when using public key cryptography, it is essential to assess the level of computer power that will become available to a potential eavesdropper during the time the encrypted information bears some importance. It is indeed also threatened by future developments, while both types of QKD system are vulnerable only to technology existing at the time of the key exchange. QKD with faint pulses may well constitute a compromise between complexity and security.

A second advantage is that, when Alice detects one photon of a pair, she knows that a twin photon was also created.

This means that we remove the vacuum component of the faint laser pulses. In principle the probability μ then approaches 1. The correct count probability for a given value of the attenuation is increased and the contribution \mathcal{D}_{det} lowered. A certain \mathcal{D} will be obtained after a longer distance. It is important to note that this is beneficial only because detectors are imperfect and feature noise. If they did not, it would always be possible to compensate the lower count probability by a larger repetition frequency.

C. Comparison with previous QKD experiments

We can now compare the performance of the system presented in this paper with two other setups. We first look at the plug and play QKD system presented in [5]. It features self-alignment and highly stable operation, and was tested by our group over a 22-km-long installed optical fiber. The system described here in principle allows distribution over a longer distance. If we now take into account the fact that our source yields a μ of only 0.6, we see that the ratio of the detector contributions to the error rates of both systems is reduced to $\mathcal{D}_{\text{det}}^{\text{PP}}/\mathcal{D}_{\text{det}}=3/2$, instead of $5/2$ when setting μ to 1. This factor corresponds to an attenuation of about 1.8 dB, which translates into 7 km of fiber at 1550 nm. This difference is not really significant. In addition, the plug and play system featured an excellent \mathcal{D}_{opt} of 0.14%, and no errors by accidental coincidences. However, the most important advantage of the system presented in this paper is clearly the fact that it relies on photon pairs and passive-state preparation, benefitting thus from high security. It does not offer to Eve any possibility to exploit multiphoton pulses for her attack. We must admit, however, that the operation of the plug and play system is definitely simpler than our system, thanks to its self-alignment feature. This would also constitute an important parameter when realizing a prototype to be used by nonphysicists. The main difficulty in the manipulation of our system comes from the fact that two interferometers must be aligned and kept stable. The stability problem is, of course, also encountered with all the other conventional phase-encoding QKD systems [2,3].

We can also compare it with the system presented by Tittel *et al.* in [10], who were the first ones to implement QKD with photon pairs beyond 1 μm . They used a pulsed pump laser, whose light passes through an interferometer, before impinging onto the nonlinear crystal and generating photon pairs. The first measurement basis is implemented exactly as in the continuous pump system presented in this paper. No phase change in the interferometers is required, since the second basis is implemented on noninterfering events. This implies that the factor q_{interf} has a value of 1, while the other parameters can in principle have the same value as in the continuous pump setup. This yields a reduction of \mathcal{D}_{det} by a factor 2. On the other hand, the two detectors must be opened during three time windows, because of the passive basis choice. The central window corresponds to the first measurement basis using interfering events, while the two others correspond to the second basis (noninterfering events). In the system presented here, the detectors are opened only twice. This implies an \mathcal{D}_{det} contribution $\frac{3}{2}$ times

higher in the pulsed source system, assuming identical detectors and transmission attenuation. Overall, this system features a \mathcal{D}_{det} contribution $0.75 (= \frac{3}{2} \times \frac{1}{2})$ times lower. This factor can be translated into a gain in distance of about 5 km. Finally, however, the fact that this pulsed source system requires alignment and stabilization of three interferometers (Alice, Bob, and the source) constitutes an additional practical difficulty.

VI. CONCLUSION

In this article, we presented a detailed analysis of quantum key distribution with entangled states, discussing in particular the noise sources and practical difficulties associated with these systems. A QKD system exploiting photon pairs optimized for long-distance operation was tested. We implemented an asymmetrical Franson-type experiment for photons entangled in energy-time and used a key distribution

protocol analogous to BB84. Passive-state preparation, realized by polarization multiplexing of the interferometers, offers superior security. With Alice and Bob directly connected, a shifted bit sequence of 1.7 Mbit was distributed at a raw rate of 450 Hz, and exhibited a quantum-bit error rate of 5.9%. With an 8.45-km-long fiber between them, we distributed a sequence of 0.41 Mbit at a raw rate of 134 Hz, and with an error rate of 8.6%. We also discussed the level of security offered by such a system. Finally, we compared the performance obtained with that of a faint-pulse scheme, as well as an alternate one based on entangled photon pairs.

ACKNOWLEDGMENTS

The Swiss FNRS and OFES as well as the European QuCom Project (No. IST-1999-10033) have supported this work. The authors would also like to thank Bruno Huttner for stimulating discussions.

-
- [1] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore* (IEEE, New York, 1984), p. 175.
 - [2] P. Townsend, *Opt. Fiber Technol.: Mater., Devices Syst.* **4**, 345 (1998).
 - [3] R. Hughes, G. Morgan, and C. Peterson, *J. Mod. Opt.* **47**, 533 (2000).
 - [4] J.-M. Mérolla, Y. Mazurenko, J.-P. Goedgebuer, and W. Rhodes, *Phys. Rev. Lett.* **82**, 1656 (1999).
 - [5] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, *J. Mod. Opt.* **47**, 517 (2000).
 - [6] A. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [7] P. Tapster, J. Rarity, and P. Owens, *Phys. Rev. Lett.* **73**, 1923 (1994).
 - [8] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Phys. Rev. Lett.* **81**, 3563 (1998).
 - [9] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, *Phys. Rev. Lett.* **81**, 5039 (1998).
 - [10] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Phys. Rev. Lett.* **84**, 4737 (2000).
 - [11] D. Naik, C. Peterson, A. White, A. Berglund, and P. Kwiat, *Phys. Rev. Lett.* **84**, 4733 (2000).
 - [12] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, *Phys. Rev. Lett.* **84**, 4729 (2000).
 - [13] J. D. Franson, *Phys. Rev. Lett.* **62**, 2205 (1989).
 - [14] A. Ekert, J. Rarity, P. Tapster, and M. Palma, *Phys. Rev. Lett.* **69**, 1293 (1992).
 - [15] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Cryptology* **5**, 3 (1992).
 - [16] *IEEE J. Lightwave Technol.* **12**, 1705 (1994); special issue edited by D. Hall.
 - [17] N. Lütkenhaus, *Phys. Rev. A* **61**, 052304 (1999).
 - [18] P. Townsend, *Electron. Lett.* **30**, 809 (1994).
 - [19] G. Ribordy, J.-D. Gautier, H. Zbinden, and N. Gisin, *Appl. Opt.* **37**, 2272 (1998).
 - [20] B. Huttner, N. Imoto, N. Gisin, and T. Mor, *Phys. Rev. A* **51**, 1863 (1995).
 - [21] H. Yuen, *Quantum Semiclassic. Opt.* **8**, 939 (1996).
 - [22] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, *Phys. Rev. Lett.* **85**, 1330 (2000).
 - [23] N. Lütkenhaus, *Phys. Rev. A* **59**, 3301 (1999).
 - [24] H. Gebbie, W. Harding, C. Hilsum, A. Pryce, and V. Roberts, *Proc. R. Soc. London, Ser. A* **206**, 87 (1951).