Article

Experimental demonstration of quantum secret sharing

TITTEL, Wolfgang, ZBINDEN, Hugo, GISIN, Nicolas

Abstract

Secret sharing is a multiparty cryptographic task in which some secret information is splitted into several pieces which are distributed among the participants such that only an authorized set of participants can reconstruct the original secret. Similar to quantum key distribution, in quantum secret sharing, the secrecy of the shared information relies not on computational assumptions, but on laws of quantum physics. Here, we present an experimental demonstration of four-party quantum secret sharing via the resource of four-photon entanglement.

Reference

TITTEL, Wolfgang, ZBINDEN, Hugo, GISIN, Nicolas. Experimental demonstration of quantum secret sharing. *Physical review, A, Atomic, molecular, and optical physics*, 2001, vol. 63, no. 4

DOI : 10.1103/PhysRevA.63.042301

Experimental demonstration of quantum secret sharing

W. Tittel, H. Zbinden, and N. Gisin
Group of Applied Physics, University of Geneva, CH-1211, Geneva 4, Switzerland
(Received 23 June 2000; published 6 March 2001)

We present a setup for quantum secret sharing based on energy-time entanglement. In opposition to known implementations using three particle Greenberger-Horne-Zeilinger (GHZ) states, our idea takes advantage of only two entangled photons created via parametric down conversion. However, the system comprising the pump plus the two down-converted photons bare the same quantum correlation and can be used to mimic three entangled qubits. The relatively high coincidence count rates found in our setup enable for the first time an application of a quantum communication protocol based on more than two qubits.

DOI: 10.1103/PhysRevA.63.042301 PACS number(s): 03.67.Hk, 03.67.Dd

I. INTRODUCTION

Entangled particles play the major role both as candidates for tests of fundamental physics [1–4] as well as in the whole field of quantum communication [5]. Until recently, most work has been focused on two-particle correlations. For a couple of years, however, the interest in multi-particle entanglement—which we identify in this article with $n>2$—is growing rapidly. From the fundamental side, particles in so-called GHZ states enable new tests of nonlocality [6]. From the side of quantum communication, more and more ideas for applications [7] like quantum secret sharing (QSS) [8–11] emerge. However, a major problem still is the lack of multi-photon sources. Nonlinear effects that enable one to ''split'' a pump photon into more than two entangled photons have extremely low efficiency, and experiments still lie in the future. Recently Bouwmeester *et al.* could demonstrate a different approach where they started with two pairs of entangled photons and transformed them via a clever measurement into three photons in a GHZ state and a fourth independant trigger photon [12]. In this article we demonstrate the feasibility of QSS using what we term pseudo-GHZ states. In opposition to ''true'' GHZ states, our states do not consist of three down-converted photons but only of two down-converted ones plus the pump photon. However, and essential for QSS, they bare the necessary GHZ quantum correlation. Moreover, thanks to much higher coincidence count rates, they enable us for the first time to realize a multi-particle application of quantum communication.

The outline of this article is the following: After a short review of GHZ states (Sec. II A), we will explain the QSS protocol (Sec. II B)—first based on GHZ states and then using pseudo-GHZ states. Section III is dedicated to the experimental setup (Sec. III A) and to the results (Sec. III B). A brief discussion concerning some interesting security aspects and its relation to the maximum transmission distance is finally given in Sec. IV, followed by a short conclusion.

II. THEORETICAL PART

A. GHZ states

Entangled states of more than two qubits, so-called GHZ states, can be described in the form

$$|\psi\rangle_{GHZ}=\frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2|0\rangle_3+|1\rangle_1|1\rangle_2|1\rangle_3), \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are orthogonal states in an arbitrary Hilbert space and the indices label the particles (in this case three). As shown by Greenberger, Horne, and Zeilinger in 1989 [6], the attempt to find a local model able to reproduce the quantum correlations faces an inconsistency. In the multi-particle case, the contradiction occurs already when trying to describe the perfect correlations. Thus, demonstrating these correlations directly shows that nature cannot be described by local theories. However, since it will never be possible to experimentally demonstrate perfect correlations, the question arises whether there is some kind of threshold, similar to the one given by Bell inequalities for two-particle correlations [1], that enables one to separate the ''nonlocal'' from the ''local'' region. Indeed, the generalized Bell inequality for the three-particle case [13],

$$S_3^{\lambda}=|E(\alpha',\beta,\gamma)+E(\alpha,\beta',\gamma)+E(\alpha,\beta,\gamma') -E(\alpha',\beta',\gamma')|\leqslant 2 \tag{2}$$

with $E(\alpha,\beta,\gamma)$ the expectation value for a correlation measurement with analyzer settings α,β,γ, can be violated by quantum mechanics, the maximal value being

$$S_3^{qm}=4. \tag{3}$$

For instance, finding a correlation function of the form $E(\alpha,\beta,\gamma)=V\cos(\alpha+\beta+\gamma)$ with visibility V above 50% shows that the correlations under test cannot be described by a local theory. Note that this value is much lower than in the two-particle case where the threshold visibility is $\approx 71\%$.

B. Quantum secret sharing

Quantum secret sharing [8–10] is an expansion of the ''traditional'' quantum key distribution to more than two parties. In this new application of quantum communication, a sender, usually called Alice, distributes a secret key to two other parties, Bob and Charlie, in a way that neither Bob nor Charlie alone have any information about the key, but that together they have full information. Moreover, an eavesdrop-

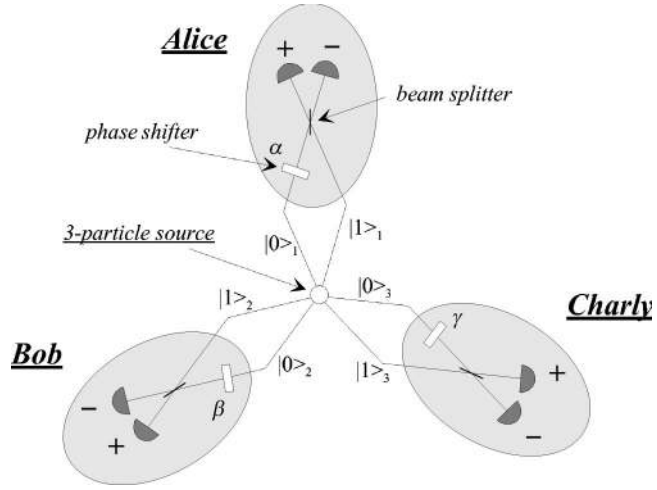

FIG. 1. Schematics for quantum secret sharing using GHZ states. Note that in a real implementation, the source would be part of Alice setup and not of a fourth, independent party.

per trying to get some information about the key creates errors in the transmission data and thus reveals her presence. The motivation for secret sharing is to guarantee that Bob and Charlie must cooperate—one of them might be dishonest—in order to do some task, one might think for instance of accessing classified information.

1. QSS using GHZ states

As pointed out by Żukowski *et al.* [8] and by Hillery *et al.* [9], this protocol can be realized using GHZ states. Assume three photons in a GHZ state of the form (1) with $|0\rangle$ and $|1\rangle$ being different modes of the particles (Fig. 1). After combining the modes at beamsplitters located at Alice's, Bob's and Charlie's, respectively, the probability to find the three photons in any combination of output ports depends on the settings α,β,γ of the phase shifters:

$$P_{i,j,k}=\tfrac{1}{8}(1+ijk\cos(\alpha+\beta+\gamma)) \tag{4}$$

with $i,j,k=\pm 1$ labeling the different output ports. Before every measurement, Alice, Bob and Charlie choose randomly one out of two phase values $(0,\pi/2)$. After a sufficient number of runs, they publicly identify the cases where all detected a photon. All three then announce the phases chosen and single out the cases where the sum adds up either to 0 or to π. Note that the probability function [Eq. (4)] yields 1/4 for these cases. Denoting $l=\cos(\alpha+\beta+\gamma)=\pm 1$ and using $P_{i,j,k}=1/4$, Eq. (4) leads to

$$ijkl=1. \tag{5}$$

At this point, each of them knows two out of the values i,j,k,l. If now Bob and Charlie get together and join their knowledge, they know three of the four parameters and can thus determine the last one, which is also known to Alice. Identifying ''-1'' with bit value ''0'' and ''$+1$'' with ''1,'' the correlated sequences of parameter values can then be turned into a secret key.

2. QSS using pseudo-GHZ states

We now explain how to implement quantum secret sharing using our source (see Fig. 2). The idea is based on a recently developed novel source for quantum communication, creating entangled photons in energy-time Bell states [14,15]. A short light pulse emitted at time t_0 enters an interferometer having a path length difference which is large compared to the duration of the pulse. The pulse is thus split

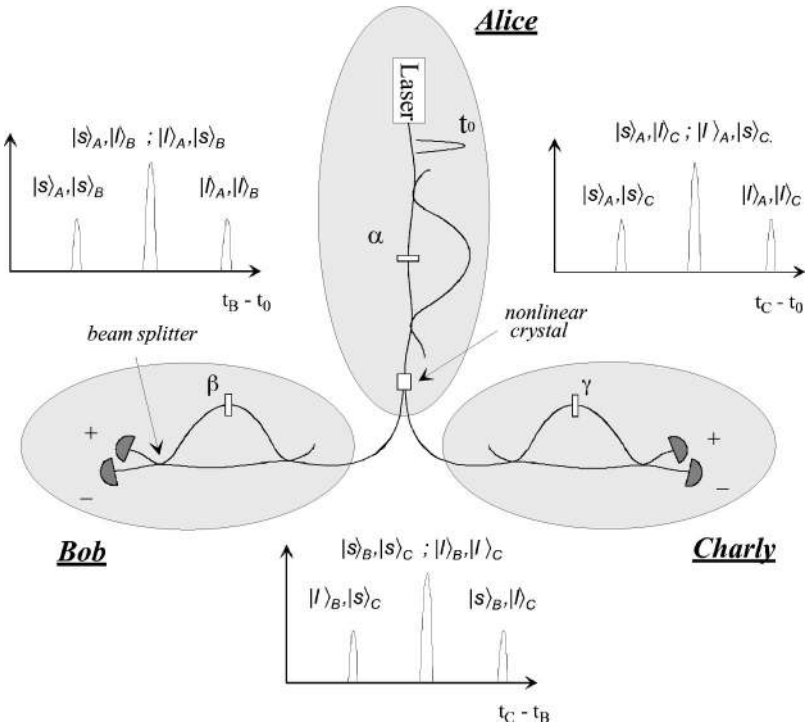

FIG. 2. Principle setup for quantum secret sharing using energy-time entangled pseudo-GHZ states. Here shown is a fiber optical realization.

into two pulses of smaller, equal amplitude, following each other with a fixed phase relation. The light is then focused into a nonlinear crystal where some of the pump photons are downconverted into photon pairs. The pump energy is assumed to be such that the possibility to create more than one pair from one initial pump pulse can be neglected. This first part of the setup is located at Alice's. The downconverted photons are then separated and sent to Bob and Charlie, respectively. Both of them are in possession of a similar interferometer as Alice, introducing exactly the same difference of travel times. The two possibilities for the photons to pass through any device lead to three time differences between emission of the pump pulse at Alice's and detection of the photons at Bob's and Charlie's, as well as between the detection of one downconverted photon at Bob's and the correlated one at Charlie's (Fig. 2). Looking for example at the possible time differences between detection at Bob's and emission of the pump pulse $(t_B - t_0)$, we find three different terms. The first one is due to ''pump pulse traveled via the short arm and Bob's photon traveled via the short arm'' to which we refer as $|s\rangle_A, |s\rangle_B$. Please note that this notation considers the pump pulse as being a single photon (now termed ''Alice's photon''), stressing the fact that only one pump photon is annihilated to create one photon pair. Moreover, the fact that this state is not a product state is taken into account by separating the two kets by '','' . The second time difference is either due to $|s\rangle_A, |l\rangle_B$, or to $|l\rangle_A, |s\rangle_B$, and the third one to $|l\rangle_A, |l\rangle_B$. Similar time spectra arise when looking at the time differences between emission at Alice's and detection at Charlie's $(t_C - t_0)$, as well as between the detections at Bob's and Charlie's $(t_C - t_B)$. Selecting now only processes leading to the central peaks [16], we find two possibilities. If both of them are indistinguishable, the process is described by

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|l\rangle_A, |s\rangle_B |s\rangle_C + e^{i(\alpha+\beta+\gamma)} |s\rangle_A, |l\rangle_B |l\rangle_C), \quad (6)$$

with phases α, β, γ in the different interferometers. The maximally entangled state (6) is similar to the GHZ state given in Eq. (1), the difference being that the three photons do not exist at the same time (remember the '',''). Therefore, our state is obviously of no significance concerning GHZ-type tests of nonlocality. To stress this difference, we call it pseudo-GHZ state. However, the probability function describing the triple coincidences [Eq. (4)]—in our case between emission of a pump pulse and detection at Bob's and Charlie's—is the same as the one originating from a true GHZ state, therefore allowing QSS. To avoid the complication of switching the pump laser randomly between one of the two input ports—equivalent to detecting a photon in one or the other output port—we let Alice choose between one of four phase values $\alpha'(0, \pi/2, \pi, 3\pi/2)$. To map the choice of phases on the initial scheme where the information of Alice, Bob, and Charlie is given by a phase setting *and* a detector label, we assign a different notation to characterize Alice phases (Table I). Using this convention, we can implement the same protocol as given above, the advantage being the fact that our setup circumvents creation and coincidence detection of triple photons. Indeed, the emission of the bright pump pulse can be considered as detection of a photon with 100% efficiency, and only photon-pair generation is necessary. This leads to much higher triple coincidence rates, enabling the demonstration of a multi-qubit application of quantum communication. Note as well that the same setup can also be used for two-party quantum key distribution based energy-time Bell states [15].

TABLE I. Mapping of the four possible phases α' at Alice's on two phase values α and the parameter i.

α'	0	$\pi/2$	π	$3\pi/2$
α	0	$\pi/2$	0	$\pi/2$
i	1	1	-1	-1

Like in two-party quantum cryptography, the security of quantum secret sharing using GHZ states is given by the fact that the measurements are made in noncommuting bases [9,10,17]. An eavesdropper, including a dishonest Alice, Bob or Charlie, is thus forced to guess about the bases that will be chosen. The fact that she will guess wrong in half of the cases then leads to detectable errors in the transmission data which reveal her presence. However, as discussed in [10], the order of releasing the public information to verify the security of the transmitted data is important in the three-party case, where one must face the situation of an internal eavesdropper.

One might question the security of our setup, the weak point being the channel leading from Alice's interferometer to the crystal. Here, the light is classical and the phase could be measured without modifying the system. However, since this part is controlled by Alice and the parts physically accessible to an eavesdropper carry only quantum systems, our realization does not incorporate any loophole. Note as well that in the schemes presented in Figs. 1 and 2, not only Alice but any of the three can force the two others to collaborate. However, it is not clear yet whether Alice's special position of having access to the source might give her an advantage concerning internal eavesdropping. In this case, the symmetry for key distribution might be broken. Being beyond the scope of this article, problems arising from external and internal eavesdropping are certainly worth further theoretical investigation.

III. EXPERIMENTAL REALIZATION

A. Experimental setup

To generate the short pump pulse, we use a pulsed diode laser (Pico-Quant PDL 800), emitting 600 ps (FWHM) pulses of 655 nm wavelength at a repetition frequency of 80 MHz. The small amount of also emitted infrared light is prevented from entering the subsequent setup by means of a dispersive prism. After passing a polarizing beamsplitter (PBS) serving as optical isolator, the pump is focused into a single mode fiber and guided into a fiber-optical Michelson interferometer made of a 3 dB fiber coupler and chemically deposited silver end mirrors. The path-length difference corresponds to a difference of travel time of ≈ 1.2 ns, splitting

the pump pulse into two well separated pulses. The temperature of the whole interferometer is maintained stable. To change the phase difference, we elongate the fiber of the long arm by means of a piezo-electric actuator. Three polarization controllers enable us to control the evolution of the polarization state within the different parts of the interferometer. By these means, we ensure that the evolutions of polarization in the long and the short arm are identical. Besides, the light being back-reflected is prevented from impinging onto the laser diode by means of the PBS. Finally, the horizontally polarized light leaving the interferometer by the second output fiber is focused into a $4\times3\times12$ mm $KNBO_3$ crystal, cut and oriented in order to ensure colinear, degenerate phasematching, hence creating photon pairs at 1310 nm wavelength. Behind the crystal, the red pump light is absorbed by a filter (RG1000), and the photon pairs are focused into a fiber coupler, separating them in half of the cases. The average pump power before the crystal is ≈ 1 mW, and the energy per pulse is—remember that each initial pump pulse is now split into two—≈ 6 pJ. To characterize the performance of our source, we connect the coupler's output fibers to single-photon counters—passively quenched germanium avalanche photodiodes, operated in Geiger-mode and cooled to 77 K. They feature quantum efficiencies of $\approx 5\%$ at dark count rates of 30 kHz. We find net single-photon rates of 20 and 27 KHz, respectively, leading to 420 coincidences per second in a 1 ns coincidence window.

The down-converted photons are finally guided into fiber optical Michelson interferometers, located at Bob's and Charlie's, respectively. The interferometers, consisting of a 3 dB fiber coupler and Faraday mirrors, have been described in detail in [18]. To access the second output port, usually coinciding with the input port for this kind of interferometer, we implement three-port optical circulators. The interferometers incorporate equal path length differences, and the travel time difference is the same as the one introduced by the interferometer acting on the pump pulse. To control their phases, the temperature of Alice and Bob's interferometers can be varied or can be maintained stable.

The output ports are connected to single-photon counters, operated as discussed before. Due to 6 dB additional losses in each interferometer, the single-photon detection rates drop to 4–7 kHz. The electrical output from each detector is fed into a fast AND gate, together with a signal, coincident with the emission of a pump pulse. We condition the detection at Bob's and Charlie's on the central peaks ($|s\rangle_P, |l\rangle_A$ and $|l\rangle_P, |s\rangle_A$, and $|s\rangle_P, |l\rangle_B$ and $|l\rangle_P, |s\rangle_B$, respectively). Looking at coincident detections between two AND gates—equivalent to triple coincidences—we finally select only the interfering processes for detection.

B. Results

To demonstrate the feasibility of quantum secret sharing, we verify whether the quantum correlations are correctly described by the sinusoidal function given in Eq. (4). Linearly changing the phase in Alice's (as well as in Bob's) interferometer we observe sinusoidal fringes in the triple coincidence rates (see Fig. 3). Maximum count rates are around

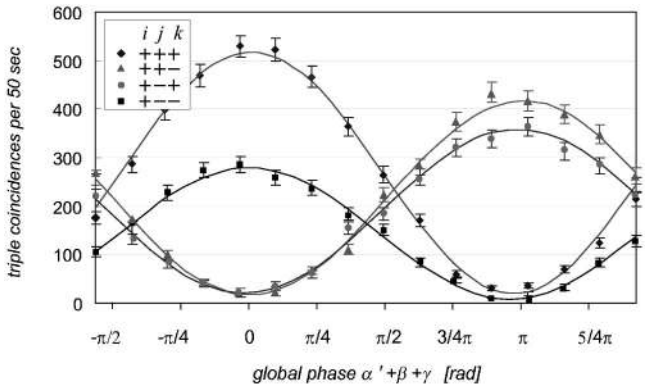

FIG. 3. Result of the measurement when changing the global phase ϕ' by varying the phase α' in Alice interferometer. The different mean values are due to nonequal quantum efficiencies of the single photon detectors.

800 in 50 s and minimum ones around 35. Visibilities are in between 89.3% and 94.5% for the different detector combinations, leading to a mean visibility of $92.2\pm0.8\%$ and a quantum bit error rate R_{QBER}—the ratio of errors to detected events—of $(3.9\pm0.4)\%$. The R_{QBER} can directly be obtained from the visibility: $R_{\mathrm{QBER}}=(1-V)/2$. Figure 4 shows the same results, now taking into account that Alice may have chosen a phase value larger than $\pi/2$ and that the mapping given in Table I applies. In these cases, the new global phase yields $\phi=\phi'-\pi/2$ and the value for i changes from $+1$ to -1. Figure 4 depicts the modified data around $\phi=0$ (i.e., $l=+1$); the (similar) figure for $\phi=\pi$ (i.e., $l=-1$) is not shown here. For better presentation, the data is divided into two graphs, one focusing on the detector combinations showing constructive interference, the other one on the combinations showing destructive interference. If, e.g., Bob and Charlie both detect a photon in the ''+''-labeled detectors in the case $\phi=0$ (i.e., $j,k,l=+1$), they know that Alice value i must be $+1$ as well since this is the only detector combination showing constructive interference.

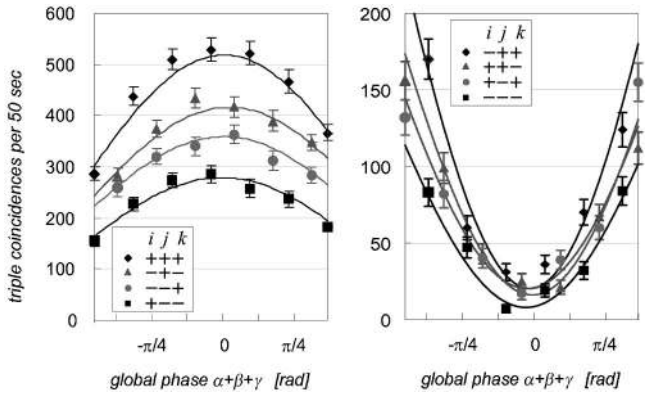

FIG. 4. Interpreting the obtained results for QSS (corresponding to Table I). The figure shows the data around $\phi=0$ (i.e., $l=+1$). If, e.g., Bob and Charlie both detect a photon in the ''+''-labeled detectors in this case, they know that Alice value i must be $+1$ as well.

IV. DISCUSSION AND CONCLUSION

Like in all experimental quantum key distribution, the R_{QBER} is nonzero, even in the absence of any eavesdropping. The observed 4% can be divided into two different parts. The first one—the so-called $R_{\mathrm{QBER}}^{\mathrm{opt}}$—originates from nonperfect localization of the pump pulse, limited resolution of the single-photon detectors and nonperfect interference. Note that the number of errors is due to wrongly arriving photons at Alice's and Bob's. Therefore, it decreases with transmission losses—at the same rate as does the number of transmitted photons. Hence, these errors do not engender an increase of the R_{QBER} with distance. The other part—the $R_{\mathrm{QBER}}^{\mathrm{acc}}$—is caused by wrong counts from accidentally correlated counts at the single-photon counters. In opposition to the errors mentioned before, these errors are independent of losses, since, in our experiment, they are mostly due to (constant) detector noise. Therefore, the $R_{\mathrm{QBER}}^{\mathrm{acc}}$ increases linearly with losses. However, since it causes only 10% of the total R_{QBER} in our laboratory demonstration, the R_{QBER} will increase only at a small rate. From our results we can estimate the R_{QBER} as a function of losses of the quantum channel:

$$R_{\mathrm{QBER}}(L) = R_{\mathrm{QBER}}^{\mathrm{opt}} + \frac{1}{1-L} R_{\mathrm{QBER}}^{\mathrm{acc}}(0) \tag{7}$$

with $R_{\mathrm{QBER}}^{\mathrm{opt}} = 3.6\%$, and $R_{\mathrm{QBER}}^{\mathrm{acc}}(0) = 0.4\%$ being the detector induced R_{QBER} as measured in the lab. L characterizes the additional losses during transmission, where $L=0$ denotes no losses and $L=1$ means that all photons have been absorbed.

Let us briefly elaborate on the obtained visibilities with respect to the critical visibility that can still be tolerated. Its value is given by the point where the information that might have been obtained by an eavesdropper cannot be made arbitrarily small using classical error correction and privacy amplification any more. In case of two-party quantum key distribution using the Bennett-Brassard 1984 (BB84) protocol [19], it corresponds exactly to a violation of two-particle Bell inequalities [17]. In the three-party case, the critical visibility in the context of external eavesdropping is not known yet. However, it is reasonable to assume a similar connection. Therefore, we compare our mean visibilitiy to the value given by generalized Bell inequality [Eq. (2)], even if our setup does not incorporate GHZ-type nonlocality [20]: The found visibility of $92.2 \pm 0.8\%$ is more than 50 standard deviations (σ) higher than the the threshold visibility of 50% for the three-particle case. Moreover, it is more than 25σ above 71%, the value given by standard (two-particle) Bell inequalities—possibly important in the context of internal eavesdroping by one of the legitimated users. Within this respect, it is also interesting to calculate S_{exp}: We find $S_{exp} = 3.69$, well above $S_3^{\lambda} = 2$ [Eq. (2)]. Therefore, the performance of our source is good enough to detect any eavesdropping and to ensure secure key distribution. Moreover, the bit-rate of ≈ 15 Hz underlines its potential for real applications. To compare our coincidence rate to an experiment using true GHZ states [12], Bouwmeester *et al.* found one GHZ state per 150 s. However, in order to really implement our setup for quantum secret sharing, an active phase stabilization compensating small interferometric drifts in Alice's interferometer as well as fast phase modulators still have to be incorporated [21].

Let us finally comment on the possibility to extend our experiment to longer distances. As discussed before, the maximum achievable distance is likely to be limited either by a minimum visibility of $V = 50\%$, hence a R_{QBER} of 25% (external eavesdropping), or by $V_{min} \approx 71\%$, hence a R_{QBER} of $\approx 15\%$ (internal eavesdropping). From Eq. (7), we find that losses of 96%, equivalent to 14 dB, or 98% (17 dB), respectively, can still be tolerated. Using the typical fiber attenuation of 0.35 dB/km at a wavelength of 1310 nm, this translates into a respective maximum transmission distance of 40 km in case of internal eavesdropping, or 50 km in case of external eavesdropping. Finally, taking into account that phase modulators, typically featuring losses of ≈ 3 dB, must still be implemented, we find a maximum span of 30–40 km.

In conclusion, we demonstrated the feasibility of quantum secret sharing using energy-time entangled pseudo-GHZ states in a laboratory experiment. We found bit-rates of around 15 Hz and quantum bit error rates of 4%, low enough to ensure secure key distribution. The advantage of our scheme is the fact that neither triple-photon generation nor coincidence detection of three photons is necessary, enabling for the first time an application of a multi-particle quantum communication protocol. Moreover, since energy time entanglement can be preserved over long distances [3], our results are very encouraging for realizations of quantum secret sharing over tens of kilometers.

ACKNOWLEDGMENTS

We would like to thank J.-D. Gautier for technical support and Picoquant for fast delivery of the laser. Support by the Swiss FNRS and the European QuCom (IST-1999-10033) project is gratefully acknowledged.

[1] J.S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[2] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **47**, 460 (1981).
[3] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998).
[4] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).
[5] Physics World, March 1998, special issue in quantum communication. *Introduction to Quantum Computation and Information*, edited by H.K. Lo, S. Popescu, and T. Spiller (World Scientific, Singapore, 1998).
[6] D.M. Greenberger, M.A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
[7] S. Bose, V. Vedral, and P.L. Knight, Phys. Rev. A **57**, 822 (1998).
[8] M. Żukowski, A. Zeilinger, M.A. Horne, and H. Weinfurter,

Acta Phys. Pol. A **93**, 187 (1998).
[9] M. Hillery, V. Buzek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[10] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
[11] R. Cleve, D. Gottesman, and H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
[12] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999).
[13] N.D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990); D.N. Klyshko, Phys. Lett. A **172**, 399 (1993); N. Gisin and H. Bechmann-Pasquinucci, *ibid.* **246**, 1 (1998).
[14] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).
[15] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[16] The desired processes are thus postselected, leading to a decrease of count rates. It is in principle possible to create only the events in the central peaks using switches instead of passive couplers [14].
[17] C. Fuchs, N. Gisin, R.B. Griffiths, C.S. Niu, and A. Perez, Phys. Rev. A **56**, 1163 (1997); I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).
[18] W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, Phys. Rev. A **59**, 4150 (1999).
[19] C.H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984), p. 175.
[20] Note that it is only important that the obtained *data* violates the Bell inequality and that this criterion applies even to crypto systems based on single photons. Nonlocality is not an issue in this context [17]!
[21] Stability is a common problem in all quantum key distribution schemes, the only exception being A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997); G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 517 (2000).