Quantum Cryptography Using Entangled Photons in Energy-Time Bell States

W. Tittel, J. Brendel, H. Zbinden, and N. Gisin
Group of Applied Physics, University of Geneva, CH-1211, Geneva 4, Switzerland
(Received 29 November 1999)

We present a setup for quantum cryptography based on photon pairs in energy-time Bell states and show its feasibility in a laboratory experiment. Our scheme combines the advantages of using photon pairs instead of faint laser pulses and the possibility to preserve energy-time entanglement over long distances. Moreover, using four-dimensional energy-time states, no fast random change of bases is required in our setup: Nature itself decides whether to measure in the energy or in the time base, thus rendering eavesdropper attacks based on "photon number splitting" less efficient.

PACS numbers: 03.67.Dd, 03.67.Hk

Quantum communication is probably one of the most rapidly growing and most exciting fields of physics within the last years [1]. Its most mature application is quantum cryptography [also called quantum key distribution (QKD)], ensuring the distribution of a secret key between two parties. This key can be used afterwards to encrypt and decrypt secret messages using the one time pad [2]. In opposition to the mostly used "public key" systems [2], the security of quantum cryptography is not based on mathematical complexity, but on an inherent property of single quanta. Roughly speaking, since it is not possible to measure an unknown quantum system without modifying it, an eavesdropper manifests herself by introducing errors in the transmitted data. During the past years, several prototypes based on faint laser pulses have been developed, demonstrating that quantum cryptography not only works inside the laboratory, but in the "real world" as well [1,3,4]. Besides, it has been shown that two-photon entanglement can be preserved over large distances [5], especially when being entangled in energy and time [6]. As pointed out by Ekert in 1991 [7], the nonlocal correlations engendered by such states can also be used to establish sequences of correlated bits at distant places.

Besides improvements in the domain of QKD, recent experimental progress in generating, manipulating, and measuring the so-called Bell states [8], has lead to fascinating applications like quantum teleportation [9], dense coding [10], and entanglement swapping [11]. In a recent paper, we proposed and tested a novel source for quantum communication generating a new kind of Bell states based on energy-time entanglement [12]. In this paper, we present a first application, exploiting this new source for quantum cryptography. Our scheme follows Ekert's initial idea concerning the use of photon-pair correlations. However, in opposition, it implements Bell states and can thus be seen in the broader context of quantum communication. Moreover, the fact that energy-time entanglement can be preserved over long distances renders our source particulary interesting for long-distance applications.

To understand the principle of our idea, we look at Fig. 1. 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 into two pulses of smaller amplitudes, following each other with a fixed phase relation. The light is then focused into a nonlinear crystal where some of the pump photons are down-converted into photon pairs. Working with pump energies low enough to ensure that generation of two photon pairs can be neglected, a created photon pair is described by

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|s\rangle_P|s\rangle_P + e^{i\phi}|l\rangle_P|l\rangle_P\right). \qquad (1)$$

$|s\rangle_P$ and $|l\rangle_P$ denote a down-converted photon created by a pump photon having traveled via the short or the long arm of the "pump" interferometer. The state (1) is composed of only two discrete emission times and not of a continuous spectrum. This contrasts with the energy-time entangled states used up to now [7,13]. Please note that, depending on the phase ϕ, Eq. (1) describes two of the four Bell states. Interchanging $|s\rangle$ and $|l\rangle$ for one of the two photons leads to generation of the remaining two Bell states. In general, the coefficients describing the amplitudes of the $|s\rangle|s\rangle$ and $|l\rangle|l\rangle$ states can be different, leading to nonmaximally entangled states. However, in this article, we will deal only with maximally entangled states. Behind the

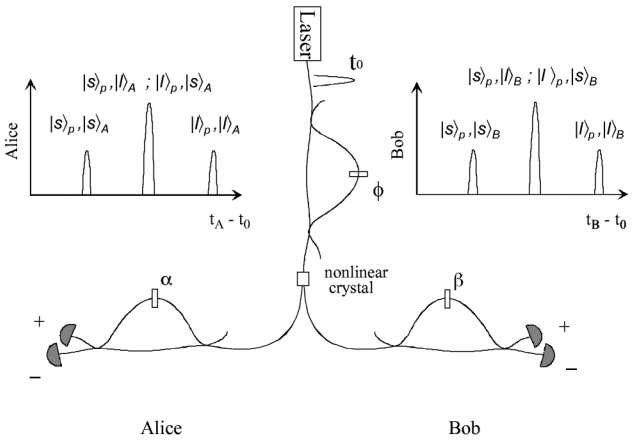

FIG. 1. Schematics of quantum key distribution using energy-time Bell states.

 © 2000 The American Physical Society

crystal, the photons are separated and are sent to Alice and Bob, respectively (see Fig. 1). There, each photon travels via another interferometer, introducing exactly the same difference of travel times through one or the other arm as did the previous interferometer, acting on the pump pulse. If Alice looks at the arrival times of the photons with respect to the emission time of the pump pulse t_0—note that she has two detectors to look at—, she will find the photons in one of three time slots. For instance, detection of a photon in the first slot corresponds to "pump photon having traveled via the short arm and down-converted photon via the short arm." To keep it short, we refer to this process as $|s\rangle_P, |s\rangle_A$, where P stands for the pump, and A for Alice's photon. However, the characterization of the complete photon pair is still ambiguous, since, at this point, the path of the photon having traveled to Bob (short or long in his interferometer) is unknown to Alice. Figure 1 illustrates all processes leading to a detection in the different time slots both at Alice's and at Bob's detector. Obviously, this reasoning holds for any combination of two detectors. In order to build up the secret key, Alice and Bob now publicly agree about the events where both detected a photon in one of the satellite peaks—without revealing in which one—or both in the central peak—without revealing the detector. The other 50% of events are discarded [14]. For instance, to come back to the above given example, if Bob tells Alice that he detected his photon in a satellite peak as well, she knows that the process must have been $|s\rangle_P, |s\rangle_A|s\rangle_B$. The same holds for Bob who now knows that Alice's photon traveled via the short arm in her interferometer. If both find the photons in the right peak, the process was $|l\rangle_P, |l\rangle_A|l\rangle_B$. In either case, Alice and Bob have correlated detection times. The cross terms where one of them detect a photon in the left and the other one in the right satellite peak do not occur. Assigning now bitvalues 0 (1) to the short (long) processes, Alice and Bob finally end up with a sequence of correlated bits.

Otherwise, if both find the photon in the central slot, the process must have been $|s\rangle_P, |l\rangle_A|l\rangle_B$ or $|l\rangle_P, |s\rangle_A|s\rangle_B$. If both possibilities are indistinguishable, we face the situation of interference and the probability for detection by a given combination of detectors (e.g., the "+"-labeled detector at Alice's and the "−" labeled one at Bob's) depends on the phases α, β, and ϕ in the three interferometers. The quantum mechanical treatment leads to $P_{i,j} = \frac{1}{4}[1 + ij\cos(\alpha + \beta - \phi)]$ with $i, j = \pm 1$ denoting the detector labels [12]. Hence, choosing appropriate phase settings, Alice and Bob will always find perfect correlations in the output ports. Either both detect the photons in detector "−" (bitvalue "0"), or both in detector "+" (bitvalue "1"). Since the correlations depend on the phases and thus on the energy of the pump and the down-converted photons, we refer to this base as the energy base (showing wavelike behavior), stressing the complementarity with the other, the time basis (showing particlelike behavior).

As in the BB84 protocol [14], it is the use of complementary bases that ensures the detection of an eavesdropper [15]. If we consider, for instance, the most intuitive intercept/resend strategy, the eavesdropper intercepts the photons, measures them in one of the two bases, and sends new, accordingly prepared photons instead. Since she never knows in which basis Bob's measurement will take place, she will in half of the cases eavesdrop and resend the photons in the "wrong basis" and therefore will statistically introduce errors in Bobs results, revealing in turn her presence. For a more general treatment of QKD and eavesdropping using energy-time complementarity, we refer the reader to [16]. Another eavesdropping strategy exploits the fact that photon pairs as well as faint pulses only mimic pure number states: there is always a small probability that there is actually more than one photon propagating to Bob [17,18]. This weakness is softened in our scheme thanks to the random choice of basis made by Nature independently for each photon. Hence, if two photons propagate towards Bob and Eve keeps one, she has only a 50% chance that hers has been prepared in the same basis as Bob's. This contrasts with schemes based on faint pulses where all photons in a pulse are prepared in the same state.

To generate the short pump pulses, we use a pulsed diode laser (PicoQuant PDL 800), emitting 600 ps (FWHM) pulses (coherence length $\approx$ 0.2 mm) of 655 nm wavelength at a repetition frequency of 80 MHz. The average power is of $\approx$10 mW, equivalent to an energy of 125 pJ per pulse. The light passes a dispersive prism, preventing the small quantity of also-emitted infrared light to enter the subsequent setup, and a polarizing beam splitter (PBS), serving as optical isolator. The pump is then focused into a singlemode fiber and is 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 times of $\approx$1.2 ns, splitting the pump pulse into two, well-seperated pulses. The arm-length difference of the whole interferometer can be controlled using a piezoelectric actuator in order to ensure any desired phase difference. Besides, the temperature is maintained stable. A fiber-optical polarization controller serves to equalize the evolution of the polarization states within the different arms of the interferometer. Another one controls the polarization state of the light that leaves the interferometer by the second output port. The horizontally polarized light is now focused into a $4 \times 3 \times 12$ mm $KNbO_3$ crystal, cut and oriented to ensure degenerate collinear phase matching, hence producing photon pairs at 1310 nm wavelength. Because of injection losses of the pump into the fiber and losses within the interferometer, the average power before the crystal drops to $\approx$1 mW, and the energy per pulse—remember that each initial pump pulse is now split into two—to $\approx$6 pJ. The probability for creation of more than one photon pair within the same or within two subsequent pulses is smaller than 1%, ensuring the assumption that leads to Eq. (1). Behind the crystal, the red pump light is absorbed by a filter (RG 1000). The

TABLE I. Results of the measurement in the time basis. The different coincidence count rates are due to different quantum efficiencies of the detectors, and the slight asymmetry in the correlated events can be explained by the nonequal transmission probabilities within the interferometers.

	++	+−	−+	−−
$s_P s_A$ AND $s_P s_B$	278 ± 6	197 ± 5	187 ± 5	147 ± 4
$l_P l_A$ AND $l_P l_B$	304 ± 7	201 ± 5	200 ± 5	148 ± 5
$s_P s_A$ AND $l_P l_B$	11 ± 0.8	10.4 ± 0.8	9.2 ± 0.7	9.4 ± 0.7
$l_P l_A$ AND $s_P s_B$	11.2 ± 0.4	8.6 ± 0.4	9.1 ± 0.4	8.5 ± 0.4
QBER [%]	3.7 ± 0.2	4.6 ± 0.2	4.5 ± 0.2	5.7 ± 0.3

down-converted photons are then focused into a fiber coupler, separating them in half of the cases, and are guided to Alice and Bob, respectively. The interferometers (type Michelson) located there have been described in detail in [6]. They consist of a 3-port optical circulator, providing access to the second output arm of the interferometer, a 3 dB fiber coupler, and Faraday mirrors in order to compensate any birefringence within the fiber arms. To control their phases, the temperature can be varied or can be maintained stable. Overall losses are about 6 dB. The path length differences of both interferometers are equal with respect to the coherence length of the down-converted photons—approximately 20 μm. In addition, the travel time difference is the same as the one introduced by the interferometer acting on the pump pulse. In this case, "the same" refers to the coherence time of the pump photons, around 800 fs or 0.23 mm, respectively.

To detect the photons, the output ports are connected to single-photon counters—passively quenched germanium avalanche photodiodes, operated in Geiger mode and cooled to 77 K [6]. We operate them at dark count rates of 30 kHz, leading to quantum efficiencies of $\approx$5%. The single-photon detection rates are of 4–7 kHz, the discrepancy being due to different detection efficiencies and losses in the circulators. The signals from the detectors as well as signals being coincident with the emission of a pump pulse are fed into fast AND gates.

To demonstrate our scheme, we first measure the correlated events in the time base. Conditioning the detection at Alice's and Bob's detectors both on the left satellite peaks, ($|s\rangle_P$,$|s\rangle_A$ and $|s\rangle_P$,$|s\rangle_B$) we count the number of coincident detections between both AND gates, that is the number of triple coincidences between emission of the pump pulse and detections at Alice's and Bob's. In subsequent runs, we measure these rates for the right-right ($|l\rangle_P$,$|l\rangle_A$ AND $|l\rangle_P$,$|l\rangle_B$) events, as well as for the right-left cross terms. We find values around 1700 coincidences per 100 sec for the correlated, and around 80 coincidences for the noncorrelated events (Table I). From the four times four rates—remember that we have four pairs of detectors—, we calculate the different quantum bit error rates QBER, which is the ratio of wrong to detected events. We find values in between 3.7% and 5.7%, leading to a mean value of QBER for the time base of (4.6 ± 0.1)%.

In order to evaluate the QBER in the energy basis, we condition the detection at Alice's and Bob's on the central peaks. Changing the phases in any of the three interferometers, we observe interference fringes in the triple coincidence count rates (Fig. 2). Fits yield visibilities of 89.3% to 94.5% for the different detector pairs (Table II). In the case of appropriately chosen phases, the number of correlated events is around 800 in 50 sec, and the number of errors is around 35. From these values, we calculate the QBERs for the four detector pairs. We find values in between 2.8% and 5.4%, leading to a mean QBER for the energy base of (3.9 ± 0.4)%. Note that this experiment can be seen as a Franson-type test of Bell inequalities as well [13,19]. From the mean visibility of (92.2 ± 0.8)%, we can infer to a violation of Bell inequalities by 27 standard deviations.

The measured QBER is small enough to guarantee the detection of an eavesdropper attack, allowing thus secure key distribution. The observed $\approx$4% are due to accidental coincidences from uncorrelated events at the single-photon detectors, a not perfectly localized pump pulse, nonperfect time resolution of the photon detectors, and, in the case of the energy basis, nonperfect interference. Note that these errors decrease at the same rate as the number of correlated events when increasing the distance between Alice and Bob (that is, when increasing the losses). In contrast to that, the number of errors due to the detector noise remain constant. Thus, the QBER slowly increases with distance. Experimental investigations show that introducing

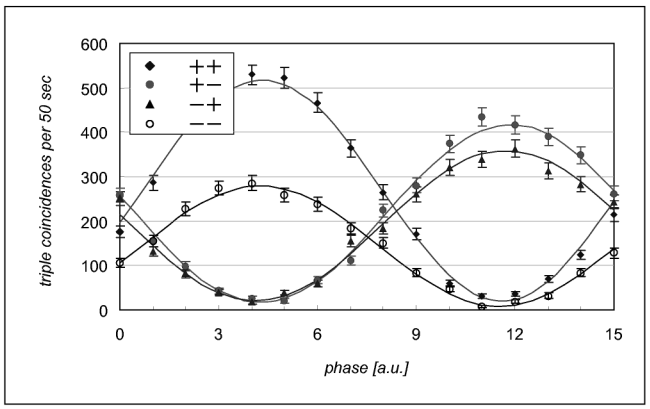

FIG. 2. Results of the measurement in the energy basis. The different mean values are due to different detector efficiencies.

TABLE II. Results of the measurement in the energy basis.

	++	+−	−+	−−
Visibility [%]	92.5 ± 1.8	92.6 ± 1.4	89.3 ± 1.9	94.5 ± 1.6
Max.	518 ± 13	416 ± 8	359 ± 9	279 ± 7
Min.	20 ± 5	16 ± 3	20 ± 4	8 ± 2
QBER [%]	3.7 ± 0.9	3.7 ± 0.7	5.3 ± 1	2.8 ± 0.8

6 dB overall losses—in the best case equivalent to 20 km of optical fiber—leads to an increment of only around 1%, hence to a QBER of 5%–6%. To improve the bit rate of our setup, there are several possibilities: simply increasing the repetition rate of the pump laser as well as the pulse energy would raise the bit rate of at least a factor of 5. However, the more serious obstacle is the low efficiency of single-photon detectors at telecomunication wavelength, and progress is expected to take place in the future. Besides detector performance, another problem of all QKD schemes developed up to now is stability, the only exception being [3]. In order to really implement our setup for quantum cryptography, the interferometers have to be actively stabilized, taking, for instance, advantage of the free ports.

To conclude, we presented a new setup for quantum cryptography using Bell states based on energy-time entanglement, and demonstrated its feasability in a laboratory experiment. We found bit rates of around 33 Hz and quantum bit error rates of around 4% which is low enough to ensure secure key distribution. Similar to all schemes based on photon pairs, our scheme has the advantage of starting the transmission with one photon and not with a weak pulse containing mostly zero photons. Furthermore, the use of discrete energy-time states, up to dimension 4, in our scheme, leads to the fact that no fast change between noncommuting bases is necessary. Nature itself chooses between the complementary properties energy and time, thus rendering eavesdropping strategies based on photon number splitting less efficient. Finally, the recent demonstration that energy-time entanglement can be preserved over long distances [6] shows that this scheme is perfectly adapted to long-distance quantum cryptography.

We would like to thank J. D. Gautier for technical support and PicoQuant for fast delivery of the laser. This work was supported by the Swiss NSF and the European QuCom (IST-1999-10033) projects.

Note added in proof.—See related work by Jennewein *et al.* [20] and Naik *et al.* [21].

[1] Special issue on quantum communication [Phys. World **11**, No. 3 (1998)]; W. Tittel, G. Ribordy, and N. Gisin, *ibid.* **11**, No. 3, 41 (1998).

[2] See, e.g., D. Welsh, *Codes and Cryptography* (Clarendon Press, New York, 1988).

[3] A. Muller *et al.*, Appl. Phys. Lett. **70**, 793 (1997); G. Ribordy *et al.*, J. Mod. Opt. **47**, 517 (2000).

[4] P. D. Townsend, Opt. Fiber Technol. **4**, 345 (1998); R. J. Hughes, G. L. Morgan, and C. G. Peterson, Report No. quant-ph/9904038; J.-M. Mérolla *et al.*, Phys. Rev. Lett. **82**, 1656 (1999).

[5] P. R. Tapster, J. G. Rarity, and P. C. M. Owens, Phys. Rev. Lett. **73**, 1923 (1994); W. Tittel *et al.*, Phys. Rev. A **57**, 3229 (1998); W. Tittel *et al.*, Phys. Rev. Lett. **81**, 3563 (1998); G. Weihs *et al.*, Phys. Rev. Lett. **81**, 5039 (1998).

[6] W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, Phys. Rev. A **59**, 4150 (1999).

[7] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[8] H. Weinfurter, Europhys. Lett **25,** 559 (1994); M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. **53,** R1209 (1996).

[9] D. Bouwmeester *et al.*, Nature (London) **390**, 575 (1997); D. Boschi *et al.*, Phys. Rev. Lett. **80**, 1121 (1998).

[10] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Phys. Rev. Lett. **76**, 4656 (1996).

[11] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).

[12] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).

[13] J. D. Franson, Phys. Rev. Lett. **62**, 2205 (1989).

[14] 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.

[15] C. Fuchs *et al.*, Phys. Rev. A **56**, 1163 (1997); I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).

[16] H. Bechmann-Pasquinucci and W. Tittel, Report No. quant-ph/9910095.

[17] An eavesdropper can take advantage of the occasional presence of (at least) two identical photons by simply measuring one and letting pass the other one unmeasured (photon number splitting attack). This security flaw can be softened using weaker pulses or lower pump energies. Still, the implementation of photon pairs features an important advantage: Bob's (noisy) detectors have to be activated only if Alice detected "her" photon—that is when *one* photon travels towards Bob. This contrasts with schemes based on faint pulses where the detecting electronics has to be activated whenever a weak pulse containing *mostly zero* photons was emitted. Therefore, for a given probability of generating two identically prepared photons, the error rate induced by the noisy detectors is much smaller.

[18] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Report No. quant-ph/9911054.

[19] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).

[20] T. Jennewein *et al.*, preceding Letter, Phys. Rev. Lett. **4,** 4729 (2000).

[21] D. S. Naik *et al.*, preceding Letter, Phys. Rev. Lett. **4,** 4733 (2000).