Deterministic and efficient quantum cryptography based on Bell's theorem

Zeng-Bing Chen,[1,2] Qiang Zhang,[1] Xiao-Hui Bao,[1] Jörg Schmiedmayer,[2] and Jian-Wei Pan[1,2]

[1]*Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[2]*Physikalisches Institut, Universität Heidelberg, Philosophenweg 12, 69120 Heidelberg, Germany*

(Received 28 January 2005; published 5 May 2006)

We propose a double-entanglement-based quantum cryptography protocol that is both efficient and deterministic. The proposal uses photon pairs with entanglement both in polarization and in time degrees of freedom; each measurement in which both of the two communicating parties register a photon can establish one and only one perfect correlation, and thus deterministically create a key bit. Eavesdropping can be detected by violation of local realism. A variation of the protocol shows a higher security, similar to the six-state protocol, under individual attacks. Our scheme allows a robust implementation under the current technology.

DOI: 10.1103/PhysRevA.73.050302 PACS number(s): 03.67.Dd, 03.65.Ud, 42.50.Dv

Entanglement and nonlocality lie at the heart of modern understanding of quantum foundations. One of the most striking aspects of entanglement is that certain *statistical* correlations derived for entangled states can be in conflict with local realism [1], as quantitatively shown by Bell's inequalities (BI) [2]. These fundamental issues were originally considered at the very boundary of physics and philosophy. Yet, they have found practical applications in quantum information science. In a remarkable paper by Ekert [3], BI have a profound utility in quantum cryptography (QC) (or, quantum key distribution, QKD) [4–7]. Actually, there is a fascinating link [3,7–9] between the security of certain quantum communication protocols and BI. However, quantum violations of the local realism also occur in an "all-vs-nothing" (AVN) form [10–13], which is more striking in the sense that the contradiction between quantum mechanics and local realism arises even for *definite* correlations. It, thus, remains to be seen if such an AVN nonlocality can have any application in quantum information, particularly, in QC. Most of the QC protocols [4–7] proposed so far are nondeterministic as only less than 50% qubits detected can be further used as key bits. This may be a practical problem, e.g., in the one-time-pad secret-key cryptosystem [7]. Such a problem may be eliminated by, deterministic QC protocol and secret direct communication, which attracted some recent interest [14,15].

For QC experiments realized with faint laser pulses, they may be insecure under the so-called beam splitter (BS) attack [7]. This is because the currently available photon sources have a finite probability of emitting more than one photon (or more than one entangled photon pair for entangled photon sources). An eavesdropper (usually called Eve) could, in principle, use a channel with lower photon loss or without loss and only allow those attenuated pulses containing n ($n \leqslant 2$) photons to reach the receiver. For these pulses, she can use a BS to steal at least one photon, thus getting full information without being detected. However, the entanglement-based QC protocols (such as Ekert's [3] and ours to be described below) exploit entanglement as a certain "security resource" and do not suffer from this kind of problem as the security therein is guaranteed by the violations of BI.

In this paper, based on the previously proved two-party AVN nonlocality (or inseparability) for two doubly entangled photon pairs [13], we propose a QC protocol, which is efficient and deterministic: *Each detected photon pair can establish a key bit* with the help of classical communications. This deterministic feature of our protocol stems from the very nature of the two-party AVN nonlocality: The two communicating parties always have perfect quantum correlations for whatever measurement bases they choose. An eavesdropper can be detected by observing the violation of local realism for the quantum channel. A variation of the present protocol is similar to the six-state protocol [16] and shows a higher security under simple individual attacks. A remarkable advantage of the present scheme is that all required measurements can be done with linear optical elements and as such, the experimental realization of the protocol is within the reach of current technology.

In our protocol (see Fig. 1), "doubly entangled" photon pairs (photon-1 and photon-2) in the state

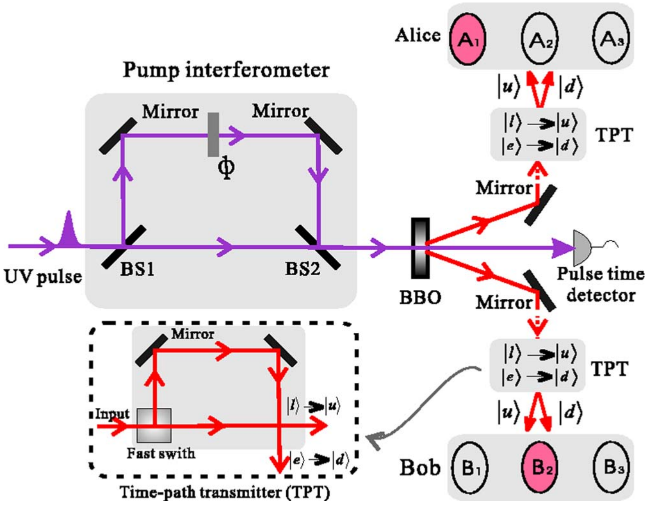

FIG. 1. (Color online) A proposed implementation of our QKD protocol.

$$|\Psi\rangle_{12}=\frac{1}{2}(|H\rangle_1|H\rangle_2+|V\rangle_1|V\rangle_2)(|\uparrow\rangle_1|\uparrow\rangle_2+|\downarrow\rangle_1|\downarrow\rangle_2) \qquad (1)$$

are generated via spontaneous parametric down conversion (SPDC) and sent, respectively, to two communicators, Alice and Bob. $|H\rangle$ ($|V\rangle$) stands for photons with horizontal (vertical) polarization; $|\uparrow\rangle$ and $|\downarrow\rangle$ span an orthonormal basis for either time or path states of photons. $|\Psi\rangle_{12}$ is maximally entangled both in polarization and in time path degrees of freedom of photons. The creation of the polarization-path entanglement was discussed in [13,17]. With a pump interferometer in Fig. 1, one can generate the polarization-time double entanglement. (More details are given at the end of this paper.)

To create secure keys, each party needs to measure observables involving the spin-type operators $x=|H\rangle\langle V|+|V\rangle\times\langle H|$, $z=|H\rangle\langle H|-|V\rangle\langle V|$ (for polarization) and $x'=|\uparrow\rangle\langle\downarrow|+|\downarrow\rangle\langle\uparrow|$, $z'=|\uparrow\rangle\langle\uparrow|-|\downarrow\rangle\langle\downarrow|$ (for time path). Particularly, the two parties should measure nine observables:

$$A_1\begin{cases} z_1 \\ x_1' \\ z_1\cdot x_1' \end{cases}, \quad A_2\begin{cases} z_1' \\ x_1 \\ x_1\cdot z_1' \end{cases}, \quad A_3\begin{cases} z_1z_1' \\ x_1x_1' \\ z_1z_1'\cdot x_1x_1' \end{cases};$$

$$B_1\begin{cases} x_2' \\ x_2 \\ x_2\cdot x_2' \end{cases}, \quad B_2\begin{cases} z_2 \\ z_2' \\ z_2\cdot z_2' \end{cases}, \quad B_3\begin{cases} z_2x_2' \\ x_2z_2' \\ z_2x_2'\cdot x_2z_2' \end{cases}. \qquad (2)$$

Alice (Bob) arranges her (his) local observables into three groups A_1, A_2, and A_3 (B_1, B_2, and B_3), each of which has three operators. As in Ref. [13], the three operators of each group can be measured by one and the same apparatus (to be described below). This is crucial in the AVN argument of nonlocality without the necessity of an additional assumption of noncontextuality [13,18]. When measuring the three operators of each group, e.g., A_1 (other groups are similar), we measure z_1 and x_1' simultaneously with the apparatus (also labeled as A_1), thus, also giving the measurement result of $z_1\cdot x_1'$, which is just the product of the readouts of z_1 and x_1'. To denote this fact, we then use $(\cdot)$ to separate the operators (as in $z_1\cdot x_1'$, $x_1\cdot z_1'$, $x_2\cdot x_2'$ and $z_2\cdot z_2'$) or operator products (as in $z_1z_1'\cdot x_1x_1'$ and $z_2x_2'\cdot x_2z_2'$), which can be identified as local "elements of reality" in the nonlocality argument [13]. In this way, the three operators in each group are comeasurable and are measured simultaneously by the same apparatus. Totally, we thus require six apparatuses (A_1, A_2, and A_3 for Alice; B_1, B_2, and B_3 for Bob), which can be realized without any mutual conflict only by linear optical elements [13].

Now, we are ready to describe the present QC protocol. For each of the emitted pairs, photon-1 (photon-2) goes to Alice (Bob) who then measures an operator group, which is chosen *randomly and independently* from the three groups A_1, A_2, and A_3 (B_1, B_2, and B_3). Any local outcome of the above measurements is completely random and can of course be either -1 or $+1$, representing, thus, one bit of information.

Now, one immediately has the following: For each pair of operator groups chosen by Alice and Bob, there is one and only one pair of outcomes of the local operators (or operator products) that possesses perfect correlation; totally Alice and Bob can establish nine pairs of perfectly correlated local outcomes as each of the two parties has three operator groups. For instance, if Alice (Bob) measures the three operators in A_1 (B_2), then only the outcomes of z_1 and z_2 will show perfect correlation, i.e., their product will certainly be 1. The above result stems from the fact that for the photon pairs in $|\Psi\rangle_{12}$, one has the following nine eigenequations [13]:

$$z_1\cdot z_2\big|_{|\Psi\rangle_{12}}=1, \quad z_1'\cdot z_2'\big|_{|\Psi\rangle_{12}}=1, \qquad (3)$$

$$x_1\cdot x_2\big|_{|\Psi\rangle_{12}}=1, \quad x_1'\cdot x_2'\big|_{|\Psi\rangle_{12}}=1, \qquad (4)$$

$$z_1z_1'\cdot z_2\cdot z_2'\big|_{|\Psi\rangle_{12}}=1, \quad x_1x_1'\cdot x_2\cdot x_2'\big|_{|\Psi\rangle_{12}}=1, \qquad (5)$$

$$z_1\cdot x_1'\cdot z_2x_2'\big|_{|\Psi\rangle_{12}}=1, \quad x_1\cdot z_1'\cdot x_2z_2'\big|_{|\Psi\rangle_{12}}=1, \qquad (6)$$

$$z_1z_1'\cdot x_1x_1'\cdot z_2x_2'\cdot x_2z_2'\big|_{|\Psi\rangle_{12}}=-1. \qquad (7)$$

We have used a simplification in the notations, e.g., $z_1\cdot z_2\big|_{|\Psi\rangle_{12}}=1$ means $z_1\cdot z_2|\Psi\rangle_{12}=|\Psi\rangle_{12}$.

After the above measurements have taken place on a photon pair, Alice and Bob can announce in public by classical communications, which of the three operator groups they have measured. They discard all measurements in which either or both of them fail to register a photon at all. In the case where Alice and Bob have detected a photon simultaneously from the emitted photon pairs, they can *deterministically* establish a secure key as they can know from the classical communications, which pair of their outcomes has the perfect correlation. For example, let us again assume that Alice (Bob) has chosen the apparatus A_1 (B_2). In this case, the two parties will certainly obtain $z_1\cdot z_2\big|_{|\Psi\rangle_{12}}=1$, from which Alice using her own outcome of z_1 can predict with certainty Bob's outcome of z_2, and *vise versa*. Any one of these types of perfect correlations can then be used to deterministically create a secure key bit. The deterministic feature of our QC protocol is thus demonstrated. As a comparison, Ekert's protocol is nondeterministic in the sense that successful detection of a photon by both Alice and Bob can establish at most a 2/9 raw key.

All QKD protocols consist of two parts: the quantum part producing the raw keys and the classical part (e.g., reconciliation and privacy amplification) [7]. The latter is not considered, as it is the same for all cryptographic protocols [19]. Now, it is ready to see that our protocol is more effective than the traditional protocols (e.g., Ekert's protocol) in the quantum part. For comparison, in Ekert's protocol 7/9 of the detected photon pairs is of no use for establishing raw keys and will be sacrificed to detect eavesdropping. Thus, in the quantum part, our protocol is $1/(1-7/9)=4.5$ times more efficient than the original Ekert protocol.

A complete security analysis of our QKD protocol is very difficult and beyond the scope of this paper. We consider the security issue by first following Ekert's security analysis [3]. In Ekert's protocol, the presence of an eavesdropper can be detected in conjunction with BI. This is because a possible intervention (interception, detection, and substitution of photons) by the eavesdropper is equivalent to introducing the local elements of physical reality into the system. Following this line of thought, Eve's intervention would acquire information, e.g., by randomly measuring observables like $A \in \{A_1,A_2,A_3\}$ and $B \in \{B_1,B_2,B_3\}$ with certain results (denoted by λ); afterwards she sends the replacement of the detected photons to Alice and Bob. Now, what Alice and Bob do is just to measure certain predetermined values of these operators (i.e., elements of physical reality) as already measured by Eve. In this case, Alice and Bob would obtain the correlation $E_{A\cdot B}=\int d\lambda \rho(\lambda)E_A(\lambda)E_B(\lambda)$, where the integration may also be a summation if the number of λ is finite and $\rho(\lambda)$ is the probability for Eve's result λ. Thus, in the presence of Eve, one has [12,13]:

$$\langle \mathcal{O}\rangle_{Eve} \equiv \int d\lambda \rho(\lambda)(-E_{z_1z_1'\cdot x_1x_1'\cdot z_2x_2'\cdot x_2z_2'} + E_{z_1z_1'\cdot z_2\cdot z_2'} + E_{x_1x_1'\cdot x_2\cdot x_2'} + E_{z_1\cdot x_1'\cdot z_2x_2'} + E_{x_1\cdot z_1'\cdot x_2z_2'} + E_{z_1\cdot z_2} + E_{z_1'\cdot z_2'} + E_{x_1\cdot x_2} + E_{x_1'\cdot x_2'}) \leqslant 7. \tag{8}$$

$E_{A\cdot B}=[C(A\cdot B = +1) - C(A\cdot B=-1)]/[C(A\cdot B=+1)+C(A\cdot B=-1)]$, where $C(A\cdot B=\pm 1)$ are the counting numbers when the measured variable $A\cdot B=\pm 1$. The measured nine sets of perfect correlations allow Alice and Bob to infer $E_{A\cdot B}$ in (8) and, then, $\langle \mathcal{O}\rangle_{Eve}$. The observed violation of (8) can, thus, detect Eve's eavesdropping by randomly choosing a small portion ("fair sample") of the generated key bits. Note that quantum prediction of the upper bound of (8) can be 9 [12,13], as can be seen from Eqs. (3)–(7).

The present scheme for detecting the eavesdropper is conceptually striking in the following sense. In Ekert's protocol, perfect correlations are used to establish secure keys, while statistical correlations are used to detect eavesdropping in terms of BI. However, in our protocol, *perfect correlations play the dual role of both establishing secure keys and detecting eavesdroppers*. Thus, we have demonstrated the link for the security against the eavesdropping of our protocol and a two-party version of Bell's theorem, and the definite quantum predictions used in a two-party AVN nonlocality argument may have a fascinating application in the deterministic QKD protocol.

Note that $|\Psi\rangle_{12}$ is a maximally entangled state in a $4\otimes 4$-dimensional Hilbert space [13]. To achieve higher security in QKD protocols, one may use either high-dimensional systems [19] or more alternative settings (e.g., three-base protocol [16]). Thus, one might expect that our QKD protocol using three measurement bases per party and high-dimensional entanglement has a bonus of higher security. To show that this is indeed the case, recall that Ekert's protocol can be regarded as a variation [5] of the BB84 protocol [4], and as such, the security of the former can be guaranteed by the security of the latter. Similarly, let us consider the case where Alice prepares the doubly entangled pair herself, measures one of her three operator groups in (2), and sends photon-2 to Bob, which might be subject to Eve's intercept-resend attacks. This modified protocol is then, in some sense, similar to the six-state (three-base) protocol [16], which is more secure than the original BB84 protocol. For instance, when Alice measures A_1, she will collapse her state onto the basis vectors $|H\rangle_1|\bar{\uparrow}\rangle_1$ $(z_1=1,x_1'=1)$ or $|V\rangle_1|\bar{\downarrow}\rangle_1$ $(z_1=-1,x_1'=-1)$ for which $z_1\cdot x_1'=1$, or $|H\rangle_1|\bar{\downarrow}\rangle_1$ $(z_1=1,x_1'=-1)$ or $|V\rangle_1|\bar{\uparrow}\rangle_1$ $(z_1=-1,x_1'=1)$ for which $z_1\cdot x_1'=-1$. $|\bar{\uparrow}\rangle=2^{-1/2}(|\uparrow\rangle+|\downarrow\rangle)$ and $|\bar{\downarrow}\rangle=2^{-1/2}(|\uparrow\rangle-|\downarrow\rangle)$. If Alice gets $|H\rangle_1|\bar{\uparrow}\rangle_1$ (with the probability of 1/4), Bob's state will be equivalently prepared as $|H\rangle_2|\bar{\uparrow}\rangle_2$, which is exactly the equal-amplitude superposition of the basis vectors for any of $\{B_1,B_2,B_3\}$. Note that any two basis vectors $|e_\alpha\rangle$ and $|e_\beta\rangle$ belonging to different bases in $\{B_1,B_2,B_3\}$ satisfy $|\langle e_\beta|e_\alpha\rangle|^2=1/4$, i.e., the three bases $\{B_1,B_2,B_3\}$ are mutually unbiased. If Eve, with the probability of 2/3, uses the wrong bases, she gets the wrong perfect correlations with Alice, and thus, no information. Explicit calculation shows that Eve can be detected with the probability of 1/2 in this case. Thus, Bob's error rate under the simple individual attacks is 1/3, implying that our protocol might be more secure, similar to the six-state protocol, but eliminates the latter's disadvantage of low efficiency.

A recent experiment [20] (see also [21]) has successfully created the path-polarization-entangled two-photon states. Note that the two photons experience two different paths from the source to the detectors. Then, the coherence of the path entanglement will be sensitive to the relative phase that a photon would acquire as it propagates along the two paths. The unavoidable fluctuations in the relative phase may destroy the path entanglement. To maintain the path coherence, especially in the long-distance case, the long-distance interferometric stability is required, which is extremely difficult in practice.

Fortunately, one can overcome the above problem by using the pulsed entanglement source where the two photons are entangled both in time (i.e., time-bin entanglement [22,23]) and in polarization. To create the required entanglement, a short, ultraviolet (UV) laser pulse is sent first through an unbalanced Mach-Zehnder interferometer (the pump interferometer) and then through a barium borate (BBO) crystal (see Fig. 1). The pump pulse is split by the first (50%–50%) BS (BS1) into two pulses, one propagating along the short path and another along the long path. If the pulse duration is shorter than the arm length difference, the output from (50%–50%) BS2 is two pulses well separated in time. For the case where there is one and only one polarization-entangled pair [assumed to be in $2^{-1/2}(|H\rangle_1|H\rangle_2+|V\rangle_1|V\rangle_2)$ for definiteness] production after the "early" and "late" pulses pass through the BBO crystal, the polarization-time-entangled two-photon state $|\Psi\rangle_{12}=\frac{1}{2}(|H\rangle_1|H\rangle_2+|V\rangle_1|V\rangle_2)(|e\rangle_1|e\rangle_2+|l\rangle_1|l\rangle_2)$ is then created by adjusting the phase ϕ. $|\uparrow\rangle\equiv|e\rangle$ (early time) and $|\downarrow\rangle\equiv|l\rangle$ (late time) are two orthonormal time states of photons. In Fig. 1, the pulse time detector can determine the emission time of the pump laser, giving a time fiducial signal.

Now, each photon held by Alice or Bob propagates along the same path. In this way, the time entanglement is much more robust than the path entanglement. Indeed, time-bin entanglement has been experimentally distributed over 50 km in optical fibers [23]. However, time-bin measurement is nondeterministic [22,23] and may, thus, reduce the efficiency of the key production.

We propose a measurement scheme with simple linear optical elements and fast switches. The setup in Fig. 1 can measure all local observables in (2) by using two " time-path transmitters" (TPT) with optical paths identical to the pump interferometer. In the TPT, a fast switch will reflect an incident photon into the long path of the TPT only for photons in $|e\rangle$; otherwise, it is switched off so that the $|l\rangle$ photons simply propagate along the short path of the TPT. The fast switch is controlled according to the timing of the pulsed photons by noting that $|e\rangle$ and $|l\rangle$ are two time states distinguishable with respect to the time-fiducial signal (see Fig. 1). In this way, the TPT transforms *coherently* $|e\rangle$ ($|l\rangle$) to $|d\rangle$ ($|u\rangle$), with $|d\rangle$ and $|u\rangle$ being two distinguishable paths of photons. Afterwards, all measurements in (2) can be done by the linear optics setups in Ref. [13].

The function of a fast switch can be accomplished by an acousto-optic modulator (AOM). Due to bulk acousto-optic interaction, an incident laser beam can be either diffracted ("first order") by or directly transmitted ("zero order") through an acousto-optic medium, depending on whether the acoustic wave is present or not. Thus, if $|e\rangle$ ($|l\rangle$) is subject to the first-order (zero-order) process, $|e\rangle$ and $|l\rangle$ will be separated in path, acting exactly as a TPT. The intensity change (the wavelength change can be safely neglected) between the zero-order and first-order beams may be compensated by an attenuator. The current commercial AOM [24] can reach a rising time of about several nanoseconds, which is sufficient enough for our proposal. Moreover, it was already used as a fast optic switch (On/Off), e.g., by Kuzmich *et al.* [24] for generating nonclassical photon pairs.

To summarize, we have proposed a double-entanglement-based QC protocol that is both efficient and deterministic. The deterministic feature and high efficiency of our protocol have obvious advantages in a practical utility. Importantly, our protocol is within the reach of the current technology and even allows for a robust intermediate-distance realization.

Note added in proof. Recently, M. Genovese kindly informed us their related work (Ref. [25]) using path-time double entanglement in nondeterministic QKD.

We thank Y.-A. Chen, X.-B. Wang, and Z. Zhao for useful discussions. This work was supported by the Fok Ying Tung Education Foundation, the NNSFC, and the CAS. We also acknowledge funding by the European Commission under Contract No. 509487 and the Alexander von Humboldt Stiftung.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

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

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

[4] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Proceeding, Bangalore, India (IEEE, New York, 1984), p. 175.

[5] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[6] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002); and references therein.

[8] B. Huttner and N. Gisin, Phys. Lett. A **228**, 13 (1997); C. Fuchs N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997); J. I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).

[9] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001); Phys. Rev. A **65**, 012311 (2001).

[10] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[11] J.-W. Pan *et al.*, Nature (London) **403**, 515 (2000).

[12] A. Cabello, Phys. Rev. Lett. **86**, 1911 (2001); *ibid.* **87**, 010403 (2001).

[13] Z.-B. Chen, J. W. Pan, Y. D. Zhang, C. Brukner, and A. Zeilinger, Phys. Rev. Lett. **90**, 160408 (2003).

[14] A. Beige *et al.*, J. Phys. A **35**, L407 (2002).

[15] Z. Zhao *et al.*, e-print quant-ph/0211098.

[16] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998); H. Bechmann-Pasquinucci, and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[17] C. Simon and J.-W. Pan, Phys. Rev. Lett. **89**, 257901 (2002).

[18] A. I. Lvovsky, Phys. Rev. Lett. **88**, 098901 (2002).

[19] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000); N. J. Cerf, M. Bourennane, A. Karlsson, and A. Gisins, *ibid.* **88**, 127902 (2002).

[20] T. Yang *et al.*, Phys. Rev. Lett. **95**, 240406 (2005).

[21] J.-W. Pan *et al.*, Nature (London) **423**, 417 (2003).

[22] J. Brendel N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999); I. Marcikic *et al.*, Phys. Rev. A **66**, 062308 (2002).

[23] I. Marcikic *et al.*, Phys. Rev. Lett. **93**, 180502 (2004).

[24] See, e.g., http://www.a-a.fr/Acousto_optic_products/; A. Kuzmich *et al.*, Nature (London) **423**, 731 (2003).

[25] M. Genovese and C. Novero, Eur. Phys. J. D **21**, 109 (2002).