# Experimental quantum-cryptography scheme based on orthogonal states

Alessio Avella, Giorgio Brida, Ivo Pietro Degiovanni, Marco Genovese, Marco Gramegna, and Paolo Traina*
*INRIM, Strada delle cacce 91, I-10135 Turin, Italy*
(Received 13 July 2010; published 10 December 2010)

Since, in general, nonorthogonal states cannot be cloned, any eavesdropping attempt in a quantum-communication scheme using nonorthogonal states as carriers of information introduces some errors in the transmission, leading to the possibility of detecting the spy. Usually, orthogonal states are not used in quantum-cryptography schemes since they can be faithfully cloned without altering the transmitted data. Nevertheless, L. Goldberg and L. Vaidman [Phys. Rev. Lett. **75**, 1239 (1995)] proposed a protocol in which, even if the data exchange is realized using two orthogonal states, any attempt to eavesdrop is detectable by the legal users. In this scheme the orthogonal states are superpositions of two localized wave packets traveling along separate channels. Here we present an experiment realizing this scheme.

DOI: 10.1103/PhysRevA.82.062309 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Ex, 42.50.St

## I. INTRODUCTION

Quantum key distribution (QKD) is a method for transmitting a secret key between two partners (usually named Alice and Bob) by exploiting quantum properties of light. The most important characteristic of this idea is that the secrecy of the generated key is guaranteed by the very laws of nature, that is, by the properties of quantum states [1–3]. In the last decade, on one hand, QKD has kept its conceptual interest as a paradigmatic example of quantum technology [4–13], and on the other hand, it has abandoned the laboratories [14–19], becoming a mature technology for commercialization [20], with communications over more than 100 km having been achieved in both fiber [21–29] and open air [4,13,15,30–34].

Various protocols for realizing QKD have been suggested [1], such as the Bennett-Brassard 1984 (BB84) [35], Bennett 1992 (B92) [36], and Ekert [1991] (E91) [37] protocols. All of them are based on the use of nonorthogonal states, a condition that was considered necessary for guaranteeing security, up until a paper by Goldenberg and Vaidman (GV) [38]. That work presented, for the first time, a scheme for realizing a QKD protocol based on orthogonal states, whose security was based on two ingredients. First, the orthogonal states sent by Alice were superpositions of two localized wave packets that were not sent simultaneously to Bob. Second, the transmission time of the photons was random.

This scheme, beyond its interest for application, also has a large conceptual interest for understanding the quantum resources or properties needed for QKD. Nevertheless, up to now, no experimental realization has been done. The purpose of this paper is to present its first experimental implementation.

## II. THE PROPOSED SCHEME

In the theoretical proposal in Refs. [38] and [39], the orthogonal states sent by Alice are the superpositions of two localized wave packets, which are not sent simultaneously to Bob, but separated by a fixed delay. One has a direct correspondence between the state prepared by Alice and the bit received by Bob; for instance,

$$0 \rightarrow |\Psi_0\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle),$$
$$1 \rightarrow |\Psi_1\rangle = \frac{1}{\sqrt{2}}(|a\rangle - |b\rangle),$$

where $|a\rangle$ and $|b\rangle$ are two localized wave packets and the states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are orthogonal. The states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ are emitted randomly in time, and the presence of an eventual eavesdropper can be detected by legitimate users exploiting the information on the detection times [38,39]. The scheme works as follows: Alice sends Bob either $|\Psi_0\rangle$ or $|\Psi_1\rangle$. The launch on the quantum channel of wave packet $|b\rangle$ is delayed for some amount of time $\tau$ with respect to the launch of wave packet $|a\rangle$. $\tau$ is chosen larger than the traveling time $T$ of photons between Alice's and Bob's locations. As $|b\rangle$ will travel through the quantum channel only after wave packet $|a\rangle$ has already reached Bob's location, both packets are never simultaneously present in the quantum channels. Nonetheless, as pointed out in Ref. [38], the requirement for $\tau$ to be greater than the traveling time $T$ is not strictly necessary. Indeed the security of the protocol is ensured even if $\tau$ is only greater than the overall uncertainty in the measurement of the transmission and detection times $t_s$ and $t_r$ [38].

In our proof-of-principle experiment this is obtained by exploiting a balanced Mach-Zehnder interferometer (MZI) with two equal optical delays OD1 and OD2. According to Fig. 1, sources of single photon S0 and S1 at the two input ports of the beam splitter on Alice's side provide single photons propagating in the transmission channel in state $|\Psi_0\rangle$ and $|\Psi_1\rangle$, respectively. The emission time for the single photon in one of the two states is random, but it is registered by Alice.

As packet $|b\rangle$ is stored in OD1, wave packet $|a\rangle$ travels from Alice's to Bob's site and enters OD2, where it is delayed until $|b\rangle$ also reaches Bob's site. In this way the two packets interfere as they simultaneously arrive at the second beam splitter. Thus, the click of detector $D_i$ deterministically implies that the single-photon state was in state $|\Psi_i\rangle$; that is, it was sent by source $S_i$. Two security tests are performed by Alice and Bob to highlight the possible presence of an eavesdropper. The first is a public comparison between the sending times $t_s$ and

*p.traina@inrim.it

 

the receiving times $t_r$ for each photon. If we assume that the traveling time between the two parties is $T$, only the events detected at time $t_r = t_s + \tau + T$ are considered as part of the message, while all other events highlight the presence of Eve. The second test is the comparison of corresponding portions of the legitimate users' bit strings to estimate the quantum bit error rate (QBER). We emphasize that, in the ideal case, discrepancies in the transmission or detection times or in the bit strings can only be induced by an eavesdropper.

For the sake of completeness, let us mention that it was argued by Peres [40] that this protocol introduced no novelty with respect to the BB84 protocol. To this claim, GV replied that while in other protocols, such as the BB84 protocol, the security is guaranteed by nonorthogonality, in the GV protocol it is based on causality, since they proved that a successful eavesdropping would require superluminal signaling [39]. Furthermore, while all cryptographic schemes require two steps for sending information (sending the quantum object and then some classical information), in the GV protocol, only the first step is needed for communication; the second step is used only for assuring security against eavesdropping. These differences are very significant, since they contribute to understanding the quantum resources to be exploited for overcoming the limits imposed on classical systems.

## III. EXPERIMENTAL SETUP

Figure 1 shows the setup of the experiment representing the first realization of the GV protocol. Single-photon states are obtained by exploiting a heralded single-photon source based on parametric down-conversion (PDC) [41]. A cw 100-mW, Coherent CUBE diode laser system at 406 nm is used to pump a BBO type I crystal. PDC photon pairs at degeneracy (812 nm) are emitted in a slightly noncollinear regime (3° with respect to the pump direction). The heralding photons are selected by means of 1-nm-bandwidth interference filters, collected in a multimode optical fiber and detected by single-photon avalanche photodiode (SPAD) detectors. The heralded single photon, the carrier of the information to be exchanged between the legitimate parties, is collected in a single-mode optical fiber (a 10-nm interference filter is placed on the heralding arm only for background suppression). The cw laser operation ensures the generation of photon pairs at random times, and the detection of one photon of the pair in the heralding arm provides the temporal information on the emission of the single photon, as requested by the GV protocol. With the aim of realizing the proof-of-principle QKD scheme proposed by GV, Alice sends bit 0 or 1 by addressing the encoding photon to the proper input port of the MZI (S0 or S1, respectively). In our proof-of-principle experiment, this is achieved by just switching the optical fiber from one input port to another. Bob detects the single photons at the output of the interferometer. The balanced MZI contains

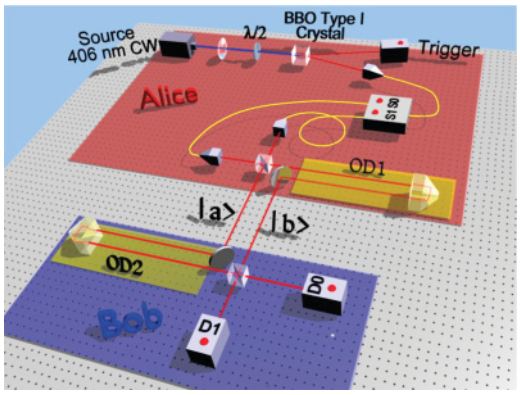


FIG. 1. (Color online) Experimental setup. A single-photon source (realized by exploiting a heralded single-photon source based on parametric down-conversion obtained by pumping with a 406-nm cw laser beam a type I BBO crystal) can be injected deterministically in either of the two input ports of the MZI (S0, S1), encoding (respectively) bit 0 or bit 1. Alice's site is composed of the two single-photon sources and the first optical delay (OD1). Bob's site is composed of the second optical delay (OD2; identical to OD1) and the two single-photon detectors (D0, D1).

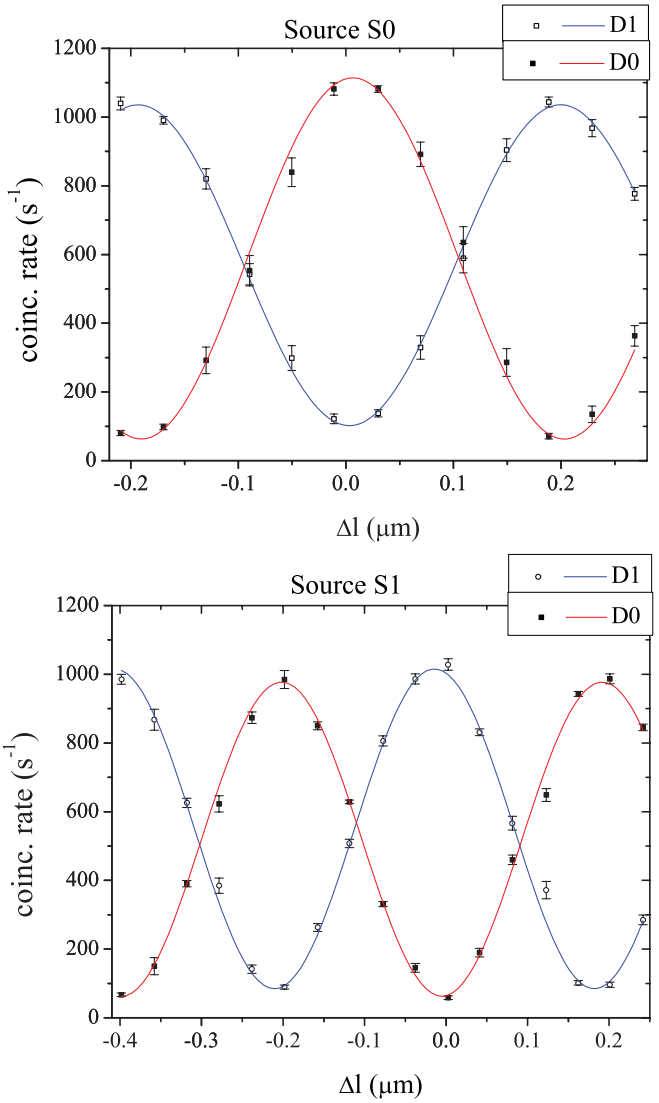


FIG. 2. (Color online) Number of detected events per second at detector D0 and D1 as a function of the path length difference $\Delta l$ between the two arms of the interferometer for source S0 (top) and S1 (bottom). As expected, the phase shifts between D0 and D1 sine fits of the coincidence counts are consistent with $\pi$.

both the optical delays and the transmission channel from Alice to Bob. In particular, after the input BS on Alice's side, one arm of the interferometer contains a delay line (realized through a trombone prism), while on the other arm the delay line (again, based on a trombone prism) is located at Bob's side. The positions of the trombones in the optical delays are adjusted via a closed-loop piezo movement system with nanometric resolution. Detection events after the output BS of the interferometer are obtained by SPAD detectors operating in Geiger mode. The electronics highlighting the presence of coincident detections is based, as usual, on a time-to-amplitude converter and multichannel analyzer. Specifically, in our case the temporal condition for the security of the QKD scheme is satisfied as the jitter of our detectors (corresponding to the uncertainty in the determination of the transmission or detection times) is about 300 ps, while the length of the delay lines is 60 cm, corresponding to a storage time of ∼2 ns. Let us also mention that, since the signal corresponding to the detection events on the heralding channel (containing the information on the sending times $t_s$) is properly delayed prior to exit from site A, an eavesdropper can never access the timing information before the transmission of each photon is concluded.

The stability of the interferometer has been tested by scanning the position of Alice's trombone prism with Bob's prism kept at a fixed position. Figure 2 shows the interference fringes of heralded counts. The visibilities ($V$) are well above 80%, irrespective of which port of the input beam splitter is used to inject the single photon into the interferometer. Even though, in recent years, very high visibilities have been achieved in similar setups [42,43], the results we obtain are absolutely comparable with those of several important works [44–47]. Furthermore, they are absolutely sufficient for a meaningful proof of principle of the GV protocol.

## IV. RESULTS AND DISCUSSION

The quality of the transmission is quantified by the QBER [QBER $= \frac{P_{\text{wrong}}}{P_{\text{right}}+P_{\text{wrong}}}$, where $P_{\text{right}}$ ($P_{\text{wrong}}$) is the probability of Bob's receiving a bit value which is equal to (different from) the one sent by Alice], measured to be 7%. This result has been proven to be stable for hundreds of seconds as shown in Fig. 3. The main results of our transmission are summarized in Table I.

Finally, we make some observations regarding the security of this QKD system. Despite the fact that an unconditional security proof of the GV protocol is still not available, we note that an efficient eavesdropping strategy against its ideal realization has not been found yet. In contrast, it can be shown that if a multiphoton component is present in the signal, an eavesdropper (Eve) can gain information on the key by performing a beam-splitter attack. For example, Eve can insert a beam splitter in both paths in such a way that the transmitted photons continue traveling toward Bob while measuring the outputs in the reflected modes with a duplicated Bob's detection apparatus. To do this successfully, Eve should be present from the initial tuning of the interferometer. The

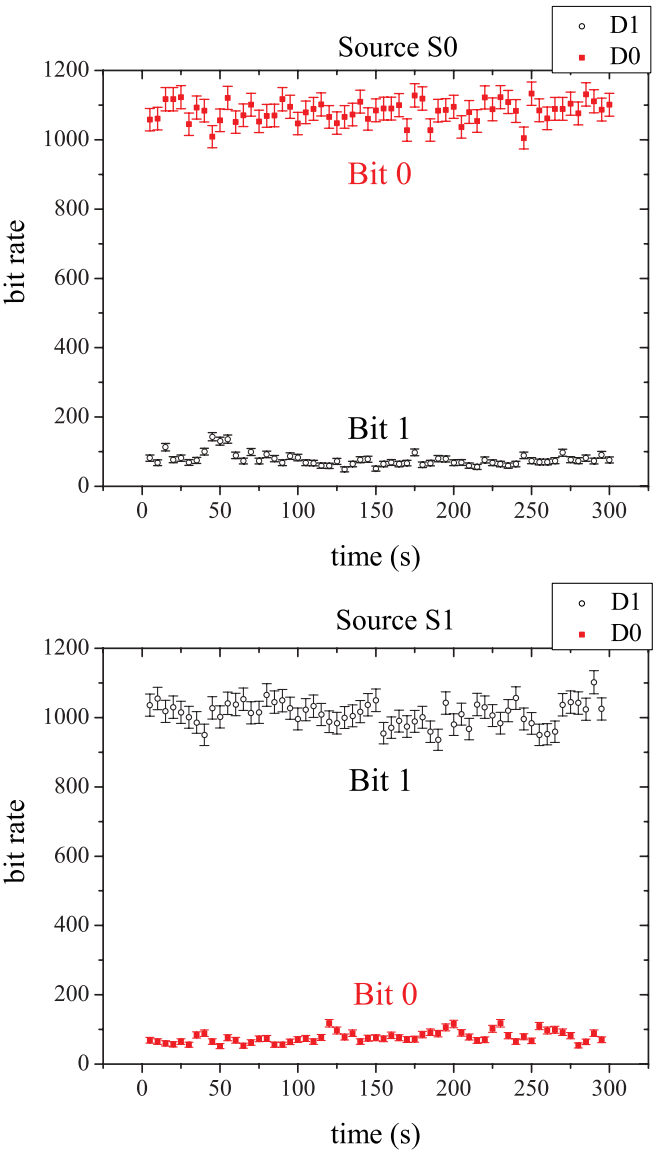


FIG. 3. (Color online) Detection events at both detectors, D1 and D0. Top: Source S0 is active, corresponding to the transmission of a string of bit 0. Bottom: Source S1 is active, corresponding to the transmission of a string of bit 1. The evaluated quantum bit error rates (QBERs) in the two cases are $\text{QBER}_{\text{S1}} = 0.071 \pm 0.014$ and $\text{QBER}_{\text{S0}} = 0.070 \pm 0.016$ in a series of 60 measurements 5 s long, showing the remarkable phase stability of the interferometer.

TABLE I. Main results obtained in our implementation of the QKD protocol proposed in Ref. [38]. $V_{\text{D0}}$ and $V_{\text{D1}}$ are the visibilities of the interference fringes observed at the two outputs of the interferometer by scanning the path-length difference. QBER is the estimated quantum bit error rate for the transmission.

| | $V_{\text{D0}}$ | $V_{\text{D1}}$ | QBER |
|---|---|---|---|
| S0 | $(89 \pm 1)\%$ | $(82 \pm 1)\%$ | $(7.0 \pm 1.6)\%$ |
| S1 | $(88 \pm 1)\%$ | $(85 \pm 1)\%$ | $(7.1 \pm 1.4)\%$ |

security issue in QKD protocols based on single photons, due to the presence of multiphoton components, is a very thoroughly investigated subject [1,2], which ultimately demands the use of efficient single-photon sources. In particular, our heralded single-photon source, presenting $g^{(2)}(0) = 0.06 \pm 0.01$, is a good approximation of an ideal single-photon source; thus, the information obtained by an eventual eavesdropper exploiting the presence of multiphoton components is negligible. In fact, if we attribute the measured QBER value due to experimental imperfections to an attack performed by an eavesdropper, the amount of information on the key obtained by this attack will be much greater than the amount obtained from a beam-splitting attack on our "almost-ideal single photons."

## V. CONCLUSIONS

In conclusion, we have realized the first proof-of-principle experimental implementation of QKD based on orthogonal states (the GV protocol) [38]. Our results demonstrate the possibility of achieving a secure QKD transmission with an orthogonal state and, therefore, provides a significant hint in the discussion of the minimal quantum resources.

## ACKNOWLEDGMENTS

This work was supported by CCQOTS Grant No. PRIN 2007FYETBY and NATO Grant No. CBP.NR.NRCL 983251. We thank L. Vaidman for bring his theoretical work to our attention.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002), and references therein.
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009), and references therein.
[3] M. Genovese, Phys. Rep. **413**, 319 (2005), and references therein.
[4] C. Erven, C. Couteau, R. Laflamme, and G. Weihs, Opt. Express **16**, 16840 (2008).
[5] A. P. Shurupov and S. Kulik, JETP Lett. **88**, 636 (2008).
[6] R. Kumar, M. Lucamarini, G. Di Giuseppe, R. Natali, G. Mancini, and P. Tombesi, Phys. Rev. A **77**, 022304 (2008).
[7] L. Zhang, C. Silberhorn, and I. A. Walmsley, Phys. Rev. Lett. **100**, 110504 (2008).
[8] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).
[9] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. **98**, 060503 (2007).
[10] T. G. Noh, Phys. Rev. Lett. **103**, 230501 (2009).
[11] A. H. Werner, T. Franz, and R. F. Werner, Phys. Rev. Lett. **103**, 220504 (2009).
[12] M. Boyer, D. Kenigsberg, and T. Mor, Phys. Rev. Lett. **99**, 140501 (2007).
[13] R. Ursin *et al.*, Nat. Phys. **3**, 481 (2007).
[14] G. Brida, N. Antonietti, M. Gramegna, L. Krivitsky, F. Piacentini, M. L. Rastello, I. Ruo Berchera, P. Traina, M. Genovese, and E. Predazzi, Int. J. Quantum Inf. **7**, 213 (2009).
[15] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, Appl. Phys. Lett. **89**, 101122 (2006).
[16] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
[17] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[18] Z. Walton, A. V. Sergienko, M. Atatüre, B. E. A. Saleh, and M. C. Teich, J. Mod. Opt. **48**, 2055 (2001).
[19] F. A. Bovino, P. Varisco, A. Martinoli, P. De Nicolo, S. Bruzzo, A. M. Colla, G. Castagnoli, G. Di Giuseppe, and A. V. Sergienko, Int. J. Quantum Inf. **3**, 141 (2005).
[20] T. Langer and G. Lenhart, New J. Phys. **11**, 055051 (2009).
[21] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, Opt. Express **14**, 13073 (2006).
[22] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, New J. Phys. **8**, 193 (2006).
[23] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, Phys. Rev. Lett. **93**, 180502 (2004).
[24] A. Tanaka *et al.*, Opt. Express **16**, 11354 (2008).
[25] C. Peng, J. Zhang, D. Yang, W. B. Gao, H. X. Ma, H. Yin, H. P. Zeng, T. Yang, X. B. Wang, and J. W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).
[26] H. Hübel, M. R. Vanner, T. Lederer, B. Blauensteiner, T. Lorünser, A. Poppe, and A. Zeilinger, Opt. Express **15**, 7853 (2007).
[27] T. Honjo *et al.*, Opt. Express **16**, 19118 (2008).
[28] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).
[29] D. Rosenberg *et al.*, New J. Phys. **11**, 045009 (2009).
[30] A. A. Semenov and W. Vogel, Phys. Rev. A **80**, 021802 (2009).
[31] T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).
[32] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi, New J. Phys. **11**, 045017 (2009).
[33] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, Nature **419**, 450 (2002).
[34] A. Poppe *et al.*, Opt. Express **12**, 3865 (2004).
[35] 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.
[36] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. **5**, 3 (1992).
[37] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[38] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **75**, 1239 (1995).
[39] L. Goldenberg and L. Vaidman, Phys. Rev. Lett. **77**, 3265 (1996).
[40] A. Peres, Phys. Rev. Lett. **77**, 3264 (1996).
[41] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, Cambridge, 1985).
[42] V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J. F. Roch, Phys. Rev. Lett. **100**, 220402 (2008).
[43] M. Ericsson, D. Achilles, J. T. Barreiro, D. Branning, N. A. Peters, and P. G. Kwiat, Phys. Rev. Lett. **94**, 050401 (2005).

[44] T. Wilk, S. C. Webster, H. P. Specht, G. Rempe, and A. Kuhn, Phys. Rev. Lett. **98**, 063601 (2007).

[45] K. Edamatsu, R. Shimizu, and T. Itoh, Phys. Rev. Lett. **89**, 213601 (2002).

[46] R. Kaltenbaek, B. Blauensteiner, M. Zukowski, M. Aspelmeyer, and A. Zeilinger, Phys. Rev. Lett. **96**, 240502 (2006).

[47] M. J. Pysher, E. J. Galvez, K. Misra, K. R. Wilson, B. C. Melius, and M. Malik, Phys. Rev. A **72**, 052327 (2005).