Quantum key distribution without a shared reference frame

C. E. R. Souza, C. V. S. Borges, and A. Z. Khoury
Instituto de Física, Universidade Federal Fluminense, Niteroi, RJ 24210-346, Brazil

J. A. O. Huguenin
Departamento de Ciências Exatas, Polo Universitário de Volta Redonda-UFF, Avenida dos Trabalhadores 420, Vila Santa Cecília, Volta Redonda, RJ 27250-125, Brazil

L. Aolita and S. P. Walborn*
Instituto de Física, Universidade Federal do Rio de Janeiro, Caixa Postal 68528, Rio de Janeiro, RJ 21941-972, Brazil
(Received 12 September 2007; published 27 March 2008)

We report a simple quantum-key-distribution experiment in which Alice and Bob do not need to share a common polarization direction in order to send information. Logical qubits are encoded into nonseparable states of polarization and first-order transverse spatial modes of the same photon.

DOI: 10.1103/PhysRevA.77.032345 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

It has been shown that the transmission of quantum information generally requires a shared reference frame (SRF) and that this presents a considerable amount of overhead; an infinite amount of information must be exchanged in order to establish a perfect SRF [1,2]. The type of reference frame required depends not only on the physical system used, but also on how information is encoded.

There exist protocols for quantum communication without SRFs [3–8]. Generally, they follow the same idea as decoherence-free subspaces [9]: encode rotation-invariant "logical" qubit states into composite states of two or more physical qubits. For example, the states

$$|0_L\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|1\rangle_2 - |1\rangle_1|0\rangle_2) \tag{1a}$$

and

$$|1_L\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2) \tag{1b}$$

are angular momentum eigenstates with zero eigenvalue, and are thus invariant under bilateral $\mathbf{R}^y(\theta)\otimes\mathbf{R}^y(\theta)$ rotations (rotations around the y axis in the Bloch sphere), where

$$\mathbf{R}^y(\theta)|0\rangle \rightarrow \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle, \tag{2a}$$

$$\mathbf{R}^y(\theta)|1\rangle \rightarrow \cos\frac{\theta}{2}|1\rangle - \sin\frac{\theta}{2}|0\rangle. \tag{2b}$$

For any rotation there exist states that are invariant, provided that the rotation acts collectively on the qubits. This is only approximately true for closely spaced ions in the same trap or closely spaced photons traveling in the same optical fiber, for example.

In Ref. [10], it was shown that two-qubit states defined in the polarization and transverse spatial degrees of freedom of the same photon satisfy the "collective condition" perfectly. For quantum communication using polarization of photons, the required reference frame is a well-established axis in the plane transverse to the propagation direction. The lack of this reference frame can be expressed as a random $\mathbf{R}^y(\theta)$ rotation of the polarization degree of freedom. The same is true for the first-order Hermite-Gaussian (HG) transverse spatial modes [10,11]. Thus, qubits 1 and 2 in Eq. (1a) and (1b) can be represented by the polarization and HG mode of a single photon by making the identification $|0\rangle_1 \equiv |H\rangle$, $|1\rangle_1 \equiv |V\rangle$, $|0\rangle_2 \equiv |h\rangle$, $|1\rangle_2 \equiv |v\rangle$, where H and V stand for horizontal and vertical polarization, and h and v stand for horizontal (HG_{01}) and vertical (HG_{10}) HG modes [11,12]. For the sake of simplicity, we consider different Hilbert spaces for the different degrees of freedom of the same photon, which, although a slight abuse of notation, allows us to make a simple analogy with multiqubit entangled states.

Here we report an experimental investigation of a SRF-free Bennett-Brassard 1984 (BB84) key distribution protocol using these two degrees of freedom of the same photon. First, let us briefly summarize the BB84 quantum-key-distribution protocol in the context of photon polarization [13,14]. Traditionally, Alice sends photons to Bob, each polarized in one of four directions $|H\rangle$, $|V\rangle$, $|+\rangle \equiv (|H\rangle + |V\rangle)/\sqrt{2}$, or $|-\rangle \equiv (|H\rangle - |V\rangle)/\sqrt{2}$, and records which polarization state she sent. Bob then measures randomly in either the H/V or $+/-$ basis, recording each basis chosen and the corresponding result. Using classical communication, Alice and Bob sift through their results, keeping only those cases in which Bob measured in the "correct basis." Bob's sifted results should coincide with each polarization that Alice sent and will serve as a key in a classical cryptography protocol. They can check the error rate in their key strings to determine the security achieved and can apply classical error correction and privacy amplification techniques [14]. The lack of a SRF in the BB84 protocol results in a larger quantum bit error rate, which may compromise the success of the key distribution. We note that a procedure for a rotation-invariant

*swalborn@if.ufrj.br

 ©2008 The American Physical Society

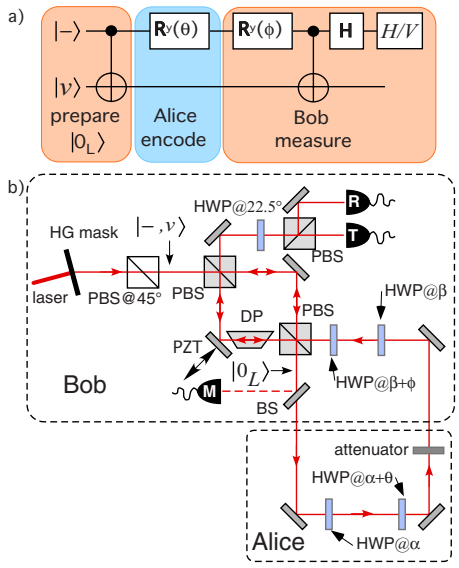

FIG. 1. (Color online) (a) Quantum circuit illustration of the BB84 protocol with logical states. The upper wire represents the polarization and the lower wire the transverse mode of the same photon. (b) Schematic of the experiment. PBS are polarizing beam splitters, DP is a Dove prism oriented at −45°, and HWP are half-wave plates. α and β are the angles of Alice's and Bob's reference frames. M is a detector used for monitoring the phase of Bob's interferometer.

quantum key distribution using higher-order angular momentum states of single photons was proposed in Ref. [15].

II. EXPERIMENT

The quantum-key-distribution scheme presented here uses logical states defined in the polarization and HG modes of the same photon. We chose to implement the scheme in a "plug-and-play" configuration [14], in which Bob sends Alice a photon or pulse, and Alice implements a rotation to one of the four states used and then sends the photon back to Bob. This type of system has been shown to offer technical advantages due to fluctuations in optical fibers [14]. Here we implement this setup due to its experimental simplicity and the fact that it illustrates the "no reference frame" feature more clearly.

Figure 1(a) shows a quantum logic circuit which outlines the experiment. In the first step, Bob creates a single-photon logical state using polarization and HG mode, represented by the upper and lower wires, respectively. This can be achieved through a controlled-not (CNOT) gate acting on the initial product state $|-\rangle|v\rangle$, which creates the logical state $|0_L\rangle$. The logical rotation operator $\mathbf{R}_L^y(\theta)$ can be implemented on the logical states by applying the $\mathbf{R}^y(\theta)$ operator on the first qubit or $\mathbf{R}^y(-\theta)$ on the second qubit [10]. Thus, Alice transforms $|0_L\rangle$ into one of the four states $|0_L\rangle$, $|1_L\rangle$, or $|\pm_L\rangle = (|0_L\rangle \pm |1_L\rangle)/\sqrt{2}$, depending on the angle θ of rotation $\mathbf{R}^y(\theta)$ on the polarization qubit. Finally, Bob chooses either the $0_L/1_L$ or $+_L/-_L$ basis by adjusting the angle ϕ of rotation $\mathbf{R}^y(\phi)$. He then performs a CNOT gate and a Hadamard rotation ($\mathbf{H}$) on the polarization qubit, and finally measures the polarization qubit in the H/V basis. We note that since the four logical states used are all eigenstates of the $\mathbf{R}_L^y(\theta)$ operator, the entire key distribution protocol is fault-tolerant, in the sense that it occurs entirely within the logical subspace.

Figure 1(b) shows the experimental setup. Bob sends a red HeNe laser through a holographic mask designed to produce the first-order HG-mode v [16,17]. The diffracted beam in the v mode then passes through a polarizing beam splitter (PBS) aligned at −45° to produce the state $|-\rangle|v\rangle$. Next, Bob uses a Mach-Zehnder interferometer to implement a polarization-controlled CNOT gate to create the logical state $|0_L\rangle$. The interferometer is constructed with polarizing beam splitters and has a Dove prism (DP) in the V-polarized arm [18,19]. The DP is aligned at −45°, so that the HG mode of a V-polarized photon transforms as $|V\rangle|v\rangle \rightarrow |V\rangle|h\rangle$ and $|V\rangle|h\rangle \rightarrow |V\rangle|v\rangle$. Since nothing happens to the H-polarized photons, the action of the interferometer corresponds to a CNOT gate. The relative phase between the two arms of the interferometer was maintained at zero with a piezoelectric translator (PZT) attached to one of the mirrors. A nonzero relative phase δ switches the action of the CNOT gate, so that Bob generates a state which does not belong to the logical basis defined in Eq. (1a) and (1b). The phase can be monitored at Bob's auxiliary detector M before attenuation, which does not require communication with Alice and does not decrease the transmission rate.

Bob then sends the state $|0_L\rangle$ to Alice, who implements the logical $\mathbf{R}_L^y(\theta)$ rotation by applying only polarization rotations using two half-wave plates (HWPs). The matrix describing the action of a single HWP aligned at angle α is

$$\mathrm{HWP}(\alpha) = \begin{pmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{pmatrix}. \tag{3}$$

Two consecutive HWPs at angles α and $\alpha+\theta$ give

$$\mathrm{HWP}(\alpha+\theta)\mathrm{HWP}(\alpha) = \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}, \tag{4}$$

which is equivalent to the $\mathbf{R}^y(4\theta)$ rotation operator on the polarization qubit. Thus, two adjustable HWPs transform $|0_L\rangle$ into $|0_L\rangle$, $|1_L\rangle$, or superposition states $|\pm_L\rangle \equiv (|0_L\rangle \pm |1_L\rangle)\sqrt{2}$ when their relative angle is θ=0°, 45°, or ±22.5°, respectively.

Bob measures in either the $0_L/1_L$ logical basis or the $+_L/-_L$ logical basis by first performing a logical $\mathbf{R}_L^y(\phi)$ rotation to choose the basis (two HWPs with relative angles ϕ =0 or ϕ=22.5°) and then a polarization-HG mode CNOT gate, followed by a polarization measurement. Taking advantage of the unused entrance and exit ports, we use the same Mach-Zehnder interferometer as in the preparation stage, as shown in Fig. 1(b). However, now the DP is in the H-polarized arm. The interferometer then corresponds to a X_1 CNOTX_1 gate, which flips the transverse mode when the control is in the "0" state. Here X is the first Pauli operator. Applying the X_1 CNOTX_1 transforms the logical states as

$$|0_L\rangle \rightarrow \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)|h\rangle = |-\rangle|h\rangle, \tag{5a}$$

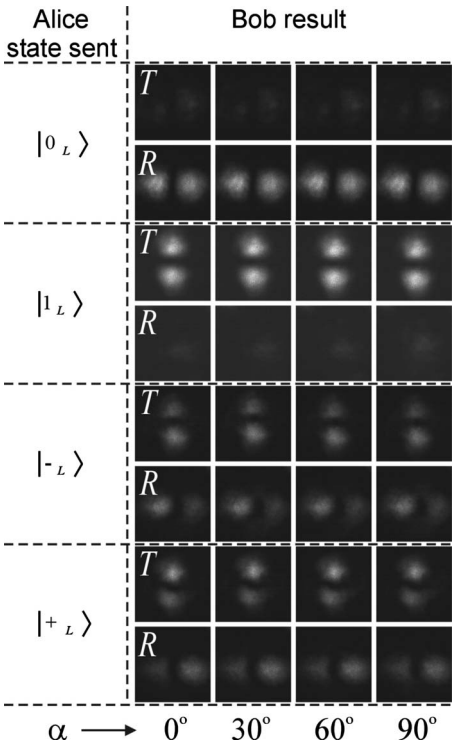

FIG. 2. Images from a CCD camera at detection positions R and T when Bob measures in the $0_L/1_L$ logical basis and Alice's laboratory frame is rotated by $\alpha=0°$, 30°, 60°, and 90°.

$$|1_L\rangle \rightarrow \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)|v\rangle = |+\rangle|v\rangle. \tag{5b}$$

These two states are then distinguished through polarization measurements, which are performed using a HWP at 22.5° and a PBS to measure in the $+/-$ polarization basis, so that detector T registers $|+\rangle$ and detector R registers $|-\rangle$.

We first discuss the results for the case in which Alice and Bob's laboratory angles are equal ($\alpha=\beta=0°$), and then show that these results are independent of the laboratory orientation defined by α. In all cases an intense laser beam was used. However, attenuation to the single-photon level is straightforward [14] and should give similar results. Figure 2 shows images registered with a charge-coupled-device (CCD) camera at detector positions R and T when Bob's wave-plate angles are $\beta=0°$ and $\phi=0°$, which corresponds to the $0_L/1_L$ detection basis. One can see that when Alice sends either state $|0_L\rangle$ or $|1_L\rangle$, Bob detects light at only the correct detector. When Alice sends the $|\pm_L\rangle$ states, the light intensity is split between both detectors, which is necessary for the security of the BB84 protocol. Similarly, when Bob detects in the $+_L/-_L$ basis he distinguishes states $|\pm_L\rangle$, while states $|0_L\rangle$ and $|1_L\rangle$ are split randomly between detector R and T, as shown in Fig. 3. Equivalently, the CCD images shown in Figs. 2 and 3 show that the same results could have been obtained through transverse-mode measurements, as Eq. (5a) and (5b) suggests.

Alice's laboratory reference frame is easily changed by varying the angle α. Figures 2 and 3 show the images at

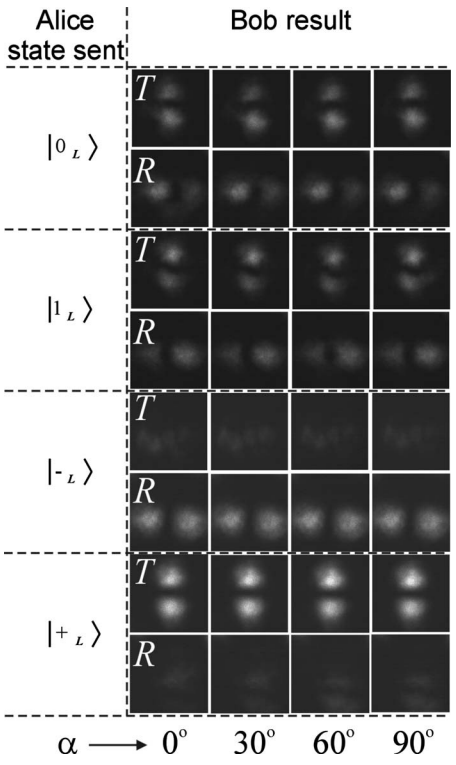

FIG. 3. Images from a CCD camera at detection positions R and T when Bob measures in the $+_L/-_L$ logical basis and Alice's laboratory frame is rotated by $\alpha=0°$, 30°, 60°, and 90°.

Bob's detectors when Alice's reference frame is rotated by $\alpha=\{0°,30°,60°,90°\}$ and Bob detects in the $0_L/1_L$ and $+_L/-_L$ bases, respectively. It can be seen in both figures that Bob's measurement results are independent of the global rotation angle α of Alice's station. To achieve more quantitative results, we also measured the intensity at detectors R and T with an optical power meter. Figure 4 shows the intensity as a function of α when Alice sends the state $|0_L\rangle$ and Bob measures in the correct $(0_L/1_L)$ and wrong $(+_L/-_L)$ bases. In all cases, the intensity remains nearly constant as α is varied. Figure 4 shows that there is a slight probability ($\sim 5/73 = 0.068$) that Bob measures the wrong state even when he chooses the correct basis. This error is mostly due to misalignment of the interferometer.

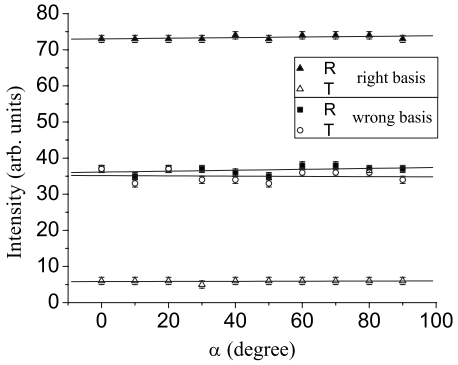

FIG. 4. Intensity measured with a power meter as a function of Alice's laboratory angle α. Solid lines are linear curve fits.

Alice's station contains only the $\mathbf{R}^y(\theta)$ operator, which depends only on the relative angle θ between the two half-wave plates and is thus independent of the orientation angle α of Alice's station. However, the equivalence between the physical $\mathbf{R}^y(\theta)$ $[\mathbf{R}^y(-\theta)]$ operator on the first (second) qubit and the logical operator $\mathbf{R}_L^y(\theta)$ is valid only for the logical basis defined in Eq. (1a) and (1b). Thus, the "alignment-free" aspect of the experiment reported here is built into the logical encoding. It is interesting to note that a similar plug-and-play experiment based on $\mathbf{R}^y(\theta)$ operators and using only photon polarization would allow the implementation of a reference-free BB84 scheme, provided that Bob prepares and measures the photons relative to the same reference frame. The logical states defined in Eq. (1a) and (1b), on the other hand, are invariant even for different preparation and measurement reference frames.

As in the usual BB84 protocol, an eavesdropper Eve can attempt many different types of attacks. Let us briefly mention possible eavesdropping strategies that are particular to our protocol. First, we emphasize that, since each photon is in a polarization-mode entangled state, no information is available if Eve measures only the polarization or transverse mode of the photons. Second, any operation which removes the state from the logical subspace defined by $|0_L\rangle$ and $|1_L\rangle$ will produce errors in the key string and will be detected by Alice and Bob in the error-check procedure. The only advantageous strategies available to Eve are those that are analogous to the usual BB84 attacks, such as intercept-resend or cloning, for which the allowable quantum bit error rates for secure communication are well-known [14]. Moreover, since our experiment applies either to single photons or attenuated laser pulses, techniques such as decoy states [20,21] are also applicable.

III. CONCLUSION

We have demonstrated a proof-of-principle quantum-key-distribution experiment which does not require a shared reference frame between Alice and Bob, using the polarization and first-order transverse spatial modes of the same photon. Our experiment was performed using an intense laser beam. Of course, actual security is only guaranteed for single photons or attenuated pulses and can be straightforwardly achieved by attenuating the laser to the single-photon level.

ACKNOWLEDGMENTS

Financial support was provided by Brazilian agencies CNPq, PRONEX, CAPES, FAPERJ, FUJB, and the Millennium Institute for Quantum Information. We would like to thank Julio Barreiro, L. H. D. Cescato, and L. F. Ávila for helpful discussions.

[1] A. Peres and P. F. Scudo, Phys. Rev. Lett. **86**, 4160 (2001).
[2] A. Peres and P. F. Scudo, Phys. Rev. Lett. **87**, 167901 (2001).
[3] A. Cabello, Phys. Rev. Lett. **91**, 230403 (2003).
[4] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, Phys. Rev. Lett. **91**, 027901 (2003).
[5] Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich, Phys. Rev. Lett. **91**, 087901 (2003).
[6] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Phys. Rev. Lett. **92**, 017901 (2004).
[7] J.-C. Boileau, R. Laflamme, M. Laforest, and C. R. Myers, Phys. Rev. Lett. **93**, 220501 (2004).
[8] T.-Y. Chen, J. Zhang, J.-C. Boileau, X.-M. Jin, B. Yang, Q. Zhang, T. Yang, R. Laflamme, and J.-W. Pan, Phys. Rev. Lett. **96**, 150504 (2006).
[9] G. M. Palma, K. A. Suominen, and A. K. Ekert, Proc. R. Soc. London, Ser. A **452**, 567 (1996).
[10] L. Aolita and S. P. Walborn, Phys. Rev. Lett. **98**, 100501 (2007).
[11] A. T. O'Neil and J. Courtial, Opt. Commun. **181**, 35 (2000).
[12] B. E. A. Saleh and M. C. Teich, *Fundamentals of Photonics* (Wiley, New York, 1991).
[13] C. H. Bennet and G. Brassard, in *Proceedings of the International Conference on Computer Systems and Signal Processing, Bangalore, 1984* (IEEE, New York, 1984), p. 175.
[14] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[15] F. Spedalieri, e-print arXiv:quant-ph/0409057.
[16] N. K. Langford, R. B. Dalton, M. D. Harvey, J. L. O'Brien, G. J. Pryde, A. Gilchrist, S. D. Bartlett, and A. G. White, Phys. Rev. Lett. **93**, 053601 (2004).
[17] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Phys. Rev. Lett. **95**, 260501 (2005).
[18] M. Fiorentino and F. N. C. Wong, Phys. Rev. Lett. **93**, 070502 (2004).
[19] A. N. de Oliveira, S. P. Walborn, and C. H. Monken, J. Opt. B: Quantum Semiclassical Opt. **7**, 288 (2005).
[20] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[21] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).