Schemes for quantum key distribution with higher-order alphabets using single-photon fractional Fourier optics

S. P. Walborn,* D. S. Lemelle, D. S. Tasca, and P. H. Souto Ribeiro
Instituto de Física, Universidade Federal do Rio de Janeiro, Caixa Postal 68528, Rio de Janeiro, RJ 21941-972, Brazil
(Received 7 February 2008; revised manuscript received 29 April 2008; published 13 June 2008)

We propose generalized quantum key distribution schemes using spatially encoded d-dimensional qudits based on fractional Fourier transform operations. We determine the necessary conditions on the orders of the transforms which ensure a shared secret random key string and briefly discuss the transmission rate and a possible encoding procedure. We also show that the fractional Fourier transform can be used to analyze more general eavesdropping strategies, including an intermediate-basis attack. The error rate and information gain for the intercept-resend and intermediate-basis attacks are briefly analyzed for a particular example. Effects of atmospheric turbulence in a free-space transmission are considered.

DOI: 10.1103/PhysRevA.77.062323 PACS number(s): 03.67.Dd, 42.25.Kb, 42.50.Ar

I. INTRODUCTION

For centuries, cryptographers have exploited all types of available technology in order to establish secure communication. In this respect, quantum cryptography or, more appropriately, quantum key distribution (QKD), is perhaps one of the most beautiful applications of quantum mechanics. Not only is QKD based on very fundamental concepts of quantum mechanics such as the complementarity principle and the no-cloning theorem, and highly linked to classical and quantum information theory, but also commercial quantum cryptography systems are readily available [1].

The object of key distribution in general is to establish a random key string between two separate parties Alice and Bob. Once a secret key string is established, Alice and Bob can communicate secretly using the classical one-time pad protocol [2], which allows for secure communication between two parties provided they can establish a sufficiently large string of random characters (i.e., bits). In seminal work by Wiesner [3] and Bennett and Brassard [4], it was shown that the nature of quantum states would allow for the secure transmission or storage of a random key. The first experimental demonstration of QKD was performed in 1989 [5], and since then experimental QKD has been implemented up to about 120 km in optical fibers [6] and over 144 km in free-space systems [7,8].

Although the main roadblocks to real-world QKD are technical issues, there is still interest in fundamental research: one would like to develop QKD protocols which increase the bit transmission rate and increase the sensitivity to eavesdropping. It has been pointed out that one can increase both the transmission rate and sensitivity to eavesdropping by increasing the dimensionality of the system [9,10]. It is straightforward to generalize the Bennett-Brassard (BB84) protocol [4] to entangled qudits, for which it is possible to send on average $\log_2 d/2$ sifted bits per photon, while an eavesdropper employing an intercept-resend strategy would induce an error rate of $E_d=\frac{1}{2}\frac{d-1}{d}$, since half the time she measures in the wrong basis and consequently sends the wrong state with a probability of $(d-1)/d$. One can easily see that while there is no bound for the bit transmission rate, the upper bound for the bit error rate induced by an intercept-resend attack for this two-basis protocol is 1/2.

Photons are the obvious choice for quantum key distribution, since they are easily transported through free space or optical fibers. Experimentally, there are several methods of encoding d-dimensional qudits in photons, including time bin [11–13], orbital angular momentum [14–16], Hermite-Gaussian modes [17,18], the polarization state of more than one photon [19,20], position and linear momentum of entangled photons [21,22], and multiple degrees of freedom simultaneously [23–26]. Higher-dimensional QKD has been implemented for time-bin qudits [13] and orbital angular momentum qutrits [16].

Recently, we performed a demonstration of quantum key distribution using higher-order d-dimensional alphabets encoded in the transverse spatial degrees of freedom of single photons [27]. We used conjugate optical lens systems to encode and decode information: an imaging system, which is similar to measuring the position of the photon in a given transverse plane, and a Fourier transform system, which is equivalent to measuring the momentum of the photon. One might think of these optical systems as complementary bases. Here we show theoretically that a spatial QKD system can be implemented with general fractional Fourier transform (FRFT) operations. The FRFT is reviewed in Sec. II and the QKD system is presented in Sec. II C. We discuss simple eavesdropping attacks based on the FRFT in Sec. III. In Sec. IV, free-space transmission of spatial qudits is briefly considered.

II. SPATIAL QUANTUM KEY DISTRIBUTION

A. Fractional Fourier transform

The FRFT has found widespread use in signal processing and optics [28] as well as quantum mechanics [29–31]. The FRFT of order ϕ of a function $E(\boldsymbol{\rho})$ can be defined as [32]

*swalborn@if.ufrj.br

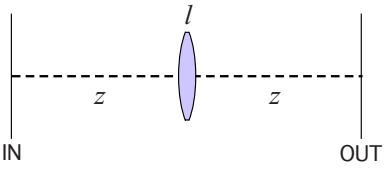

FIG. 1. (Color online) Optical system used to implement a FRFT.

$$\mathcal{F}_\phi[E](\boldsymbol{\xi}) \propto \int \exp\left(-\frac{i\xi^2 \cot\phi}{2}\right)\exp\left(-\frac{i\rho^2 \cot\phi}{2}\right) \times \exp\left(\frac{i\boldsymbol{\rho}\cdot\boldsymbol{\xi}}{\sin\phi}\right)E(\boldsymbol{\rho})d\boldsymbol{\rho}, \tag{1}$$

where $\boldsymbol{\rho}$ and $\boldsymbol{\xi}$ are two-dimensional variables. We note that $\phi=\pi/2$ corresponds to the usual Fourier transform. It has been shown that the FRFT appears naturally in the context of Fresnel diffraction [32], just as the Fourier transform appears in the Fraunhofer diffraction regime. One might also recognize the FRFT kernel as the propagator associated with the harmonic oscillator [28]. It has also been shown that one can implement a FRFT using lenses [33,34]. For example, consider the symmetrical optical system shown in Fig. 1. Here ℓ is the focal length of the lens and z is the propagation distance before and after the lens. Using $z=2\ell \sin^2(\phi/2)$ and $f=\ell \sin\phi$, this optical system implements a transformation given by

$$\mathcal{F}_\phi[E](\boldsymbol{\xi}) \propto \int \exp\left(-\frac{ik\xi^2 \cot\phi}{2f}\right)\exp\left(-\frac{ik\rho^2 \cot\phi}{2f}\right) \times \exp\left(\frac{ik\boldsymbol{\rho}\cdot\boldsymbol{\xi}}{f\sin\phi}\right)E(\boldsymbol{\rho})d\boldsymbol{\rho}. \tag{2}$$

Choosing scaled adimensional coordinates $\boldsymbol{\rho}'=\sqrt{k/f}\boldsymbol{\rho}$ and $\boldsymbol{\xi}'=\sqrt{k/f}\boldsymbol{\xi}$, the transformation (2) is equivalent to the FRFT given in Eq. (1). An important and useful property of the FRFT is additivity. That is, applying transformation (2) twice gives

$$\mathcal{F}_{\phi_1}\{\mathcal{F}_{\phi_2}[E(\boldsymbol{\rho})]\} = \mathcal{F}_{\phi_1+\phi_2}[E(\boldsymbol{\rho})]. \tag{3}$$

Thus, propagation through lenses and free space is well described by FRFT operations, provided one uses properly scaled coordinates [32].

1. Fractional Fourier transform in geometric optics

The FRFT can also be described using geometric optics. Generally, a ray $\mathbf{s}=(s,\vartheta)$ at some transverse plane is described by its position s and angle ϑ with respect to the optical axis. Free propagation of an optical ray can be represented by the *ABCD* matrix [35]

$$\mathbf{S}_z = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}, \tag{4}$$

where z is the propagation distance. Passage through a thin lens is given by the matrix

$$\mathbf{L}_l = \begin{pmatrix} 1 & 0 \\ -1/l & 1 \end{pmatrix}, \tag{5}$$

where l is the focal length of the lens. Again, we set $z=2l \sin^2(\phi/2)$ and define $f=l \sin\phi$ as a scaled focal length. Let us switch coordinates to $r=s/\sqrt{f}$ and $\theta=\sqrt{f}\vartheta$, so that the complete optical FRFT system is given by the matrix

$$\mathbf{F}_\phi = \mathbf{S}_z\mathbf{L}_l\mathbf{S}_z = \begin{pmatrix} \cos\phi & \sin\phi \\ -\sin\phi & \cos\phi \end{pmatrix}. \tag{6}$$

Matrix (6) represents a ϕ-order FRFT and transforms a ray $\mathbf{r}=(r,\theta)$ as

$$\mathbf{F}_\phi\begin{pmatrix} r \\ \theta \end{pmatrix} = \begin{pmatrix} \cos(\phi)r + \sin(\phi)\theta \\ -\sin(\phi)r + \cos(\phi)\theta \end{pmatrix}. \tag{7}$$

Then, recognizing that the ray matrix in Eq. (6) describes a rotation, it is straightforward to show that the FRFT is additive—that is, $\mathbf{F}_{\phi_1}\mathbf{F}_{\phi_2}=\mathbf{F}_{\phi_1+\phi_2}$—such that the order of the combined optical FRFT is $\phi_1+\phi_2$.

B. Single-photon Fourier optics

Our QKD system will be based on propagation of single photons through simple optical lens systems. Let us assume that the input field to the lens system is a single-photon state described by

$$|\psi\rangle = \int v(\mathbf{q})|\mathbf{q}\rangle d\mathbf{q}, \tag{8}$$

where $\mathbf{q}$ is the transverse component of the wave vector $\mathbf{k}$ and $v(\mathbf{q})$ is the angular spectrum defined by

$$v(\mathbf{q}) = \int \mathcal{W}(\boldsymbol{\rho},0)e^{i\mathbf{q}\cdot\boldsymbol{\rho}}d\boldsymbol{\rho}, \tag{9}$$

and $\mathcal{W}(\boldsymbol{\rho},0)$ is the transverse part of the input field at $z=0$. We assume that the field is polarized and is well described by the paraxial approximation around the z axis. We use $\boldsymbol{\rho} \equiv (x,y)$ as the transverse component of the position vector. The detection probability at position $\mathbf{r}$ is given by

$$\mathcal{P}(\mathbf{r}) = |\Psi(\mathbf{r})|^2, \tag{10}$$

where $\Psi(\mathbf{r})$ is the detection amplitude,

$$\Psi(\mathbf{r}) = \langle \mathrm{vac}|\mathbf{E}^+(\boldsymbol{\rho})|\psi\rangle, \tag{11}$$

and $\mathbf{E}^+(\boldsymbol{\rho})$ is the field operator in the paraxial approximation. In the special case of a monochromatic single-photon state $|\psi\rangle$ with well-defined polarization, the detection amplitude $\Psi(\mathbf{r})$ plays the role of the spatial wave function [36].

First, let us consider a single-lens system as shown in Fig. 1. In the paraxial approximation, the field operator that detects a photon at the output plane is

$$\mathbf{E}^+(\boldsymbol{\rho}) \propto \int d\mathbf{q} \int d\mathbf{q}'\ \mathbf{a}(\mathbf{q}')e^{i\ell/2k|\mathbf{q}-\mathbf{q}'|^2}e^{i(\mathbf{q}\cdot\boldsymbol{\rho}-q^2/2kz-q'^2/2kz)}, \tag{12}$$

where $\mathbf{a}(\mathbf{q})$ is the usual destruction operator and ℓ is the focal length of the lens. Again, to identify the FRFT opera-

tion we can define the angle ϕ and length f such that $z=2\ell \sin^2(\phi/2)$ and $f=\ell \sin\phi$. Substituting in Eq. (12), we obtain the field operator associated with the FRFT operation:

$$\mathbf{E}_{\phi}(\boldsymbol{\rho}) \propto \exp\left(-i\frac{\tan\phi}{2}\rho^2\right)\int d\mathbf{q}\, \exp\left(-i\frac{\tan\phi}{2}q^2\right) \times \exp\left(i\frac{\boldsymbol{\rho}\cdot\mathbf{q}}{\cos\phi}\right)\mathbf{b}(\mathbf{q}), \tag{13}$$

where from here on we adopt the adimensional scaled coordinates $\sqrt{k/f}\boldsymbol{\rho}\rightarrow\boldsymbol{\rho}$ and $\sqrt{f/k}\mathbf{q}\rightarrow\mathbf{q}$ and defined $\mathbf{b}(\mathbf{q})$ as the adimensional destruction operator. One can see that Eq. (13) is similar, but not identical to the FRFT defined in Eq. (2). In fact, the tangent and cosine functions appear in (13) instead of cotangent and sine functions due to the fact that the FRFT is now being performed in q space. For the special case of the usual Fourier transform ($\phi=\pi/2$), Eq. (12) gives

$$\mathbf{E}_{\pi/2}(\boldsymbol{\rho}) \propto \mathbf{b}(\boldsymbol{\rho}). \tag{14}$$

When applied to the input field given by Eq. (8), the detection amplitude is proportional to the angular spectrum of the input field:

$$\Psi_{\pi/2}(\boldsymbol{\rho}) = A_{\pi/2}\upsilon(\boldsymbol{\rho}), \tag{15}$$

where $A_{\pi/2}$ is a normalization constant. Similarly, it is possible to derive a field operator for an imaging system ($\phi=\pi$):

$$\mathbf{E}_{\pi}(\boldsymbol{\rho}) \propto \int d\mathbf{q}\, \mathbf{b}(\mathbf{q}) e^{-i\mathbf{q}\cdot\boldsymbol{\rho}}. \tag{16}$$

When applied to the input field (8), the detection amplitude is

$$\Psi_{\pi}(\boldsymbol{\rho}) = A_{\pi}\mathcal{W}(-\boldsymbol{\rho}). \tag{17}$$

Moreover, due to the additivity property (3), any combination of lenses that implements an overall FRFT of order $(2n+1)\pi/2$ results in a detection amplitude

$$\Psi_{(n+1/2)\pi}(\boldsymbol{\rho}) = A_{(n+1/2)\pi}\upsilon[(-1)^n\boldsymbol{\rho}], \tag{18}$$

while a lens system that implements an overall FRFT of $n\pi$ results in a detection amplitude

$$\Psi_{n\pi}(\boldsymbol{\rho}) = A_{n\pi}\mathcal{W}[(-1)^n\boldsymbol{\rho}]. \tag{19}$$

With these basic building blocks, we will now construct a spatial QKD system.

C. QKD system

The basic idea of our spatial QKD system is illustrated in Fig. 2. Alice and Bob randomly implement one of two FRFT systems, denoted by the angles α_1 and α_2 (Alice) and β_1 and β_2 (Bob). The FRFT angles are chosen so that

$$\alpha_1 + \beta_1 = n\pi, \tag{20a}$$

$$\alpha_2 + \beta_2 = m\pi, \tag{20b}$$

$$\alpha_1 + \beta_1 = \left(s+\frac{1}{2}\right)\pi, \tag{20c}$$

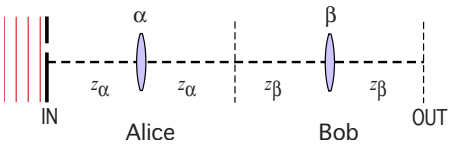

FIG. 2. (Color online) Lens system for quantum key distribution.

$$\alpha_2 + \beta_1 = \left(t+\frac{1}{2}\right)\pi, \tag{20d}$$

where n, m, s, and t are integers. We note that conditions (20a)–(20d) state that $\beta_2-\beta_1=(s-n+1/2)\pi$ and $\alpha_1-\alpha_2=(t-m+1/2)\pi$, requiring that α_1 and α_2 (β_1 and β_2) differ by odd multiples of a Fourier transform ($\pi/2$), which guarantees that "1" and "2" are conjugate lens configurations. In the experiments reported in Refs. [27,37,38], the angles $\alpha_1=\beta_1=\pi/2$ and $\alpha_2=\beta_2=\pi$ were used, which clearly satisfy conditions (20a)–(20d).

Choosing randomly between optical systems 1 and 2, Alice and Bob's overall optical system, which consists of a series of FRFT operations, always corresponds to an imaging system or a Fourier transform system. Using the additivity property (3), the conditions Eqs. (20a)–(20d), the FRFT operator (13), and the input state (8), the resulting detection amplitudes at Bob's plane P_B are

$$\Psi_{11}(\boldsymbol{\rho}) = A_{n\pi}\mathcal{W}[(-1)^n\boldsymbol{\rho},0], \tag{21}$$

$$\Psi_{22}(\boldsymbol{\rho}) = A_{m\pi}\mathcal{W}[(-1)^m\boldsymbol{\rho},0], \tag{22}$$

$$\Psi_{12}(\boldsymbol{\rho}) = A_{(s+1/2)\pi}\upsilon[(-1)^s\boldsymbol{\rho}], \tag{23}$$

and

$$\Psi_{21}(\boldsymbol{\rho}) = A_{(t+1/2)\pi}\upsilon[(-1)^t\boldsymbol{\rho}]. \tag{24}$$

The QKD system is based on the fact that when Alice and Bob implement the correct configuration (α_1,β_1 or α_2,β_2), the output field at plane P_B is proportional to the field profile of the input field at plane P_{Ain}, as shown in Eqs. (21) and (22). When Alice and Bob employ incorrect configurations, the output field at P_B is proportional to the angular spectrum of the input field, as shown in Eqs. (23) and (24). Suppose that Alice encodes information into the spatial properties of the input field by positioning a narrow aperture $\mathcal{A}(\boldsymbol{\rho}-\boldsymbol{\rho}_A)$ at position $\boldsymbol{\rho}_A$ in plane P_{in}. If the initial field is constant over the area of the aperture, the field profile at plane P_{in} will reproduce the aperture function: $\mathcal{W}(\boldsymbol{\rho},0)=\mathcal{A}(\boldsymbol{\rho}-\boldsymbol{\rho}_A)$. When Alice and Bob use correct configurations, Bob should detect photons only at the detector position corresponding to the position of the aperture. However, if they use conjugate lens configurations, the field at Bob's detection plane corresponds to the angular spectrum of the single-photon field. In this case Bob, or equivalently an eavesdropper Eve, obtains no information about the position of the aperture, since a shift in position space manifests as a phase in the Fourier transform ($\mathcal{F}$) space: $\mathcal{F}[\mathcal{A}(\boldsymbol{\rho}-\boldsymbol{\rho}_A)]=\exp(i\boldsymbol{\rho}\boldsymbol{\rho}_A/2)\times\mathcal{F}[\mathcal{A}(\boldsymbol{\rho})]$. Thus the detection probabilities $\mathcal{P}_{12}(\mathbf{r})$ and $\mathcal{P}_{21}(\mathbf{r})$ contain no information concerning the aperture position $\boldsymbol{\rho}_A$.

1. Geometric optics explanation of spatial QKD

It is rather interesting that spatial QKD can also be understood using geometric optics. In particular, suppose that Alice encodes an input ray $\mathbf{r}_A=(r_A,0)$. When $\phi=\alpha+\beta=n\pi$, the ray at Bob's output plane given by Eq. (7) is $\mathbf{r}_B=([-1]^n r_A,0)$. If Bob detects the position of the single-photon field at his output plane, he obtains r_A. When $\alpha+\beta=(t+1/2)\pi$, we have $\mathbf{r}_B=(0,[-1]^t\theta_A)$, and Bob obtains no information from a position measurement. Alice and Bob will thus discard these cases. For a single-photon field one can measure either the position or the angle component of the ray. In this way, since Alice and Bob each implement sets of conjugate lens systems, an eavesdropper will necessarily measure incorrectly in half the cases, which causes an increase in the error rate, which can be detected by Alice and Bob.

2. Encoding and decoding

Let us suppose that Alice positions her aperture $\mathcal{A}$ at position $\boldsymbol{\rho}_A$ as described above and that Bob employs a set of detectors $\mathcal{B}(\boldsymbol{\rho}-\boldsymbol{\rho}_B)$ placed at different positions $\boldsymbol{\rho}_B$. When Alice and Bob use the same lens configurations, their combined optical systems map Alice's input plane to Bob's detection plane. In order to create a QKD system based on this feature, they must define a set of aperture positions $\{\boldsymbol{\rho}_{A0},\ldots,\boldsymbol{\rho}_{Ad-1}\}$ (Alice) and a corresponding set of detection positions $\{\boldsymbol{\rho}_{B0},\ldots,\boldsymbol{\rho}_{Bd-1}\}$ (Bob), which are associated with the characters in some d-dimensional alphabet. Ideally, these sets of positions should be defined so that when both Alice and Bob use correct configurations, they see a perfect correlation: $P(k|j)=\delta_{jk}$, where $P(k|j)$ is the probability that Bob detects the photon at detector position $\boldsymbol{\rho}_{Bk}$ given that Alice's aperture position was $\boldsymbol{\rho}_{Aj}$. Furthermore, to guarantee security, when $\alpha\neq\beta$, they expect to see $P(k|j)>0$ for all j,k. In an actual implementation, Bob would employ an array of d detectors, one detector located at each position $\{\boldsymbol{\rho}_{B0},\ldots,\boldsymbol{\rho}_{Bd-1}\}$.

It is advantageous to work with a narrow aperture $\mathcal{A}(\boldsymbol{\rho})$ whose Fourier transform is much broader than $\mathcal{A}$, as this will allow Alice and Bob to increase the size of their alphabet by defining many aperture positions. Let us consider an aperture given by a Gaussian function, so that the input field is equivalent to the aperture function,

$$\mathcal{W}(\boldsymbol{\rho},0)=\mathcal{A}(\boldsymbol{\rho})=\frac{1}{w\sqrt{\pi}}e^{-\rho^2/(2w^2)}, \tag{25}$$

and the angular spectrum $v(\mathbf{q})$ is equal to the Fourier transform of the aperture function,

$$v(\mathbf{q})=\mathcal{F}[A(\boldsymbol{\rho})]=\frac{w^2}{\sqrt{\pi}}e^{-w^2q^2/2}, \tag{26}$$

where w is a dimensionless parameter. As a reminder, we note that dimensionless ρ and w are related to the dimensional variables ρ' and w' by $\rho=\sqrt{k/f}w'$ and $w=\sqrt{k/f}w'$, where k is the wave number and f' the fractional focal length. It is well known that 99% of the intensity falls within a circle with radius of three standard deviations, so let us define $3w$ and $3/w$ as cutoff parameters for the Gaussian distributions. Then, to each aperture position we can associate a circle of radius $3w$, while the Fourier pattern is characterized by $3/w$. If Bob uses a circular detector with radius $3w$, properly aligned at the proper position, he will detect 99% of the input light.

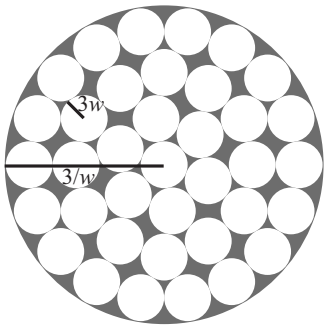

FIG. 3. Aperture layout following a hexagonal pattern. The large circle (radius $R=3/w$) is the two-dimensional slice of the angular spectrum v, while the smaller circles (radius $r=3w$) correspond to the different detector and aperture positions.

Alice and Bob must decide on the most advantageous encoding scheme: a d-dimensional "alphabet" of aperture and detection positions that maximizes the transmission rate while limiting the information available to an eavesdropper. This problem is somewhat related to the "packing problem" of how to best arrange a set of d circles of the same radius r so that they fit into a larger circle with smallest possible radius R. The most efficient method is the hexagonal packing scheme, in which the circles are centered on a lattice composed of equilateral triangles [39]. As an example, Fig. 3 shows a possible coding scheme for an alphabet of dimension $d=37$. The small circles (radius $r\equiv 3w$) correspond to the 37 aperture and detection positions, while the large circle corresponds to the $R\equiv 3/w$ area of the Fourier transform of the aperture function. For $d=37$, it is most efficient to maintain the ratio $R/r=6.758\,77$ [40], which gives an aperture width of $w=1/\sqrt{6.758\,77}\approx 0.3847$ (we note again that w is adimensional, as are $\boldsymbol{\rho}$ and $\mathbf{q}$). The packing density is $37\pi r^2/\pi R^2\approx 0.81$. In the limit of small r and $R=1$, the packing density is $d\pi r^2/\pi R^2=\pi/\sqrt{12}\approx 0.907$ [39]. Decreasing w, it is possible to increase the dimension d of the alphabet used, which increases the transmission rate as well as sensitivity to eavesdropping of the QKD protocol.

It can be seen that there is an unused area ($\sim$19%) between and around the black circles. In these regions, Bob or, equivalently, the eavesdropper Eve will only detect photons corresponding to complementary configurations $\alpha_1+\beta_2$ or $\alpha_2+\beta_1$. If Eve can deduce that she has chosen the wrong FRFT system, she can choose not to resend the photon. Her presence would then be marked only as a photon loss and not a registered error. Thus, it is advantageous for Alice and Bob to try to eliminate these unused regions from Bob's detection plane. One possible solution to this problem is for Alice to use additional aperture positions to fill in the gaps. Photons sent with these aperture positions could be used only as security checks, and not part of the actual key [22]. Another option is to arrange the aperture positions using a smaller hexagonal lattice, which will eliminate excess space, but in-

creases the quantum bit error rate. This type of encoding pattern was in fact used in [27].

Following the usual BB84 protocol [4], Alice would send a number of photons to Bob, each randomly choosing a lens system for each photon. They then perform basis reconciliation and evaluate the bit error rate using a sample of their key strings. If the error rate is below a certain threshold, they can use classical privacy amplification to minimize Eve's information [2].

3. Transmission rate

A principal difference between this QKD scheme and those based on polarization or phase is that the detection probabilities for complementary measurements are not constant for all characters of the alphabet ($\mathcal{P}_{12}=\mathcal{P}_{21}\neq 1/d$), but rather weighted according to a Gaussian distribution. Thus, some characters in the key string appear more frequently than others. To obtain a completely random key string, Alice and Bob can discard some of the more frequent results after sifting.

Since the security of QKD lies in the fact that an eavesdropper Eve cannot gain any information when she chooses the wrong basis, in order to minimize Eve's information, Alice should choose characters (aperture positions) according to the distributions $\mathcal{P}_{12}$ and $\mathcal{P}_{21}$. Suppose that Alice sends each character k with probability P_k, which we will define as

$$P_k = \int d\boldsymbol{\rho}\, \mathcal{A}(\boldsymbol{\rho}-\boldsymbol{\rho}_A)\mathcal{P}_{12}(\boldsymbol{\rho}). \tag{27}$$

The total amount of information I^A that Alice can encode in each photon is given by the entropy

$$I^A = -\sum_{k=0}^{d-1} P_k \log_2 P_k. \tag{28}$$

For the encoding scheme shown in Fig. 3 with $d=37$ and $w=0.3847$, we have $I^A \approx 4.45$ bits, as compared to $\log_2 37 \approx 5.21$ bits for $\mathcal{P}_{12}=\mathcal{P}_{21}\neq 1/37$. Therefore, for nonuniform $\mathcal{P}_{12},\mathcal{P}_{21}$, the amount of encoded information is reduced. The ratio $I^A/\log_2 d$ generally increases as w decreases [27], indicating that the efficiency of the protocol grows with the alphabet dimension d. In the limit in which k is a continuous parameter, the aperture $\mathcal{A}(\boldsymbol{\rho}-\boldsymbol{\rho}_A)\to\delta(\boldsymbol{\rho}-\boldsymbol{\rho}_A)$ and $P_k \to \mathcal{P}_{21}(\boldsymbol{\rho}_k)=\mathcal{P}_{21}(\boldsymbol{\rho}_k)$. For the Gaussian distribution given in Eq. (26), we have [41]

$$I^A = -\int_{-\infty}^{\infty} \mathcal{P}_{12}(\boldsymbol{\rho}_k)\log_2 \mathcal{P}_{12}(\boldsymbol{\rho}_k)d\boldsymbol{\rho}_k = \log_2\left(\frac{\pi e}{w^2}\right) \text{ bits}, \tag{29}$$

which is the upper limit on the amount of information which Alice can safely encode into a single photon. Figure 4 shows the information per photon as a function of w. For $w=0.3847$, we have $I^A=5.85$ bits, which is larger than the value of 5.21 bits calculated above due to the fact that we are considering a continuous distribution [41]. Recalling that the adimensional width w is equal to the actual aperture width σ scaled by $\sqrt{k/f}\approx 10$ mm^{-1}, one can encode $\log_2(\pi e f/k\sigma^2) \approx 1$ byte of information per photon with an aperture with size on the order of about $\sigma=15$ μm. The $\mathcal{P}_{12}$ distribution in this case would have a width of about a centimeter.

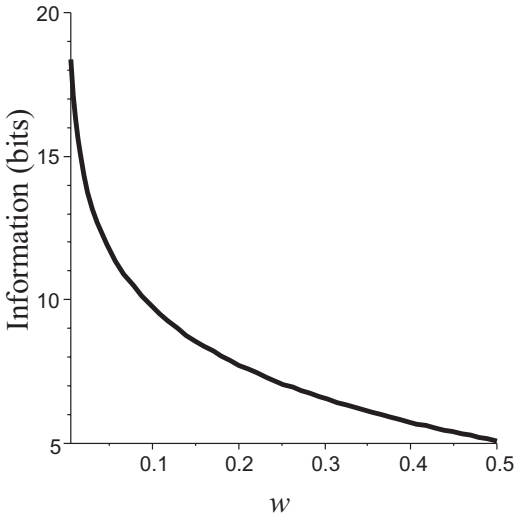

FIG. 4. Information capacity per photon as a function of the adimensional width w.

The amount of information that is sent from Alice to Bob in the presence of noise and errors corresponds to the mutual information [2,10] given by the decrease in entropy:

$$I^{AB} = H_i - H_f, \tag{30}$$

where the entropy is averaged over all possible results k: $H_f=\Sigma_k P_k H(j|k)$, with $H(j|k)=-\Sigma_j P(j|k)\log_2 P(j|k)$, and $P(j|k)$ is the *a posteriori* probability that Alice had sent j when the result was k. The conditional probability $P(k|k)$ depends only on the error rate, $P(k|k)=1-\mathcal{E}_k$, while the conditional probability $P(j|k)=P_k\mathcal{E}_j/(1-P_j)$, where $P_k/(1-P_j)$ is the probability to detect incorrect k given that an error occurred. Thus, the amount of information sent from Alice to Bob in the presence of noise or eavesdropping is then [2]

$$I^{AB} = I^A + \sum_{k=0}^{d-1} P_k(1-\mathcal{E}_k)\log_2(1-\mathcal{E}_k) + \sum_{j=0}^{d-1}\sum_{k=0,j\neq k}^{d-1} \frac{P_j\mathcal{E}_j P_k}{1-P_j}\log_2\frac{\mathcal{E}_j P_k}{1-P_j}. \tag{31}$$

III. EAVESDROPPING

Let us now consider some basic eavesdropping strategies. The mutual information between Alice and Bob is given in Eq. (31) and depends on the error rate $\mathcal{E}_k$. Eve's objective is to obtain a large amount of information I^E without inducing a large error rate $\mathcal{E}_k$, which can be detected by Alice and Bob. There are many possible eavesdropping strategies. Here we focus on attacks on individual photons, in which Eve steals the photon while in the transmission line from Alice to Bob, measures it, and then prepares and resends a second photon to Bob. Let us further assume that Eve performs a FRFT

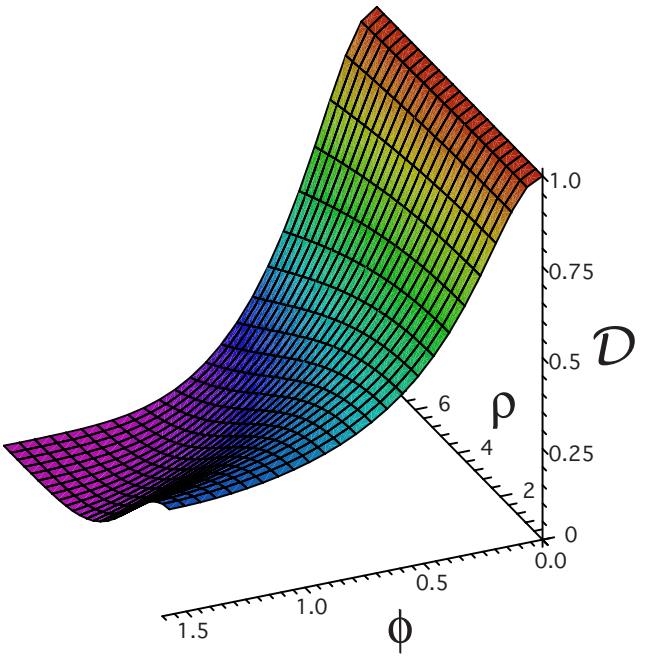

FIG. 5. (Color online) Probability $\mathcal{D}$ that Eve measures the correct state as a function of $\phi=\alpha+\varepsilon$ and $\rho_A=|\boldsymbol{\rho}_A|$.

operation of order ε on Alice's output field and then detects the position of the incident photon. The single-photon field incident on Eve's detector is given by a FRFT operation:

$$\Psi_\phi(\boldsymbol{\rho}) = \langle 0|\mathbf{E}_\phi(\rho)|\Psi\rangle, \tag{32}$$

where $\phi=\alpha+\varepsilon$. For the Gaussian field given in Eq. (25), we have

$$\Psi_\phi(\boldsymbol{\rho},\boldsymbol{\rho}_A) = \frac{w^2 \exp\left(-\frac{i\tan\phi}{2}\rho^2\right)\exp\left(-\frac{(\boldsymbol{\rho}-\cos\phi\boldsymbol{\rho}_A)^2}{2\cos^2\phi(w^2+i\tan\phi)}\right)}{\sqrt{\pi}(w^4\cos^2\phi+\sin^2\phi)}. \tag{33}$$

The probability $\mathcal{D}$ that Eve detects the correct state is given by the overlap of the field at her detection plane with Alice's initial field:

$$\mathcal{D}_\phi(\boldsymbol{\rho}_A) = \left|\int d\boldsymbol{\rho}\, \Psi_A(\boldsymbol{\rho})\Psi_\phi(\boldsymbol{\rho})\right|. \tag{34}$$

Using the Gaussian distribution (25), gives

$$\mathcal{D}_\phi(\boldsymbol{\rho}_A) = \left[\frac{2w^2\exp\left(-\frac{2\rho_A^2w^2(1-\cos\phi)}{w^4(1-\cos\phi)+(1+\cos\phi)}\right)}{\sqrt{4w^4\cos^2\phi+(1+w^4)^2\sin^2\phi}}\right]^{1/2}. \tag{35}$$

Figure 5 shows the probability $\mathcal{D}$ as a function of $|\boldsymbol{\rho}_A|$ and the FRFT angle ϕ. One can see that for all $|\boldsymbol{\rho}_A|$, the overlap between Eve's field with Alice's initial field is close to 1 only near $\phi=0$. Since Alice randomly chooses between two conjugate FRFT systems (which differ by FRFT order $\pi/2$), it is impossible for Eve to correctly choose $\phi=\alpha+\varepsilon=0$ (or multiples of π) for both α_1 and α_2 configurations. Consequently, Eve will obtain at best partial information about Alice's aperture position $\boldsymbol{\rho}_A$ in some cases and will be unable to perfectly reproduce the field when she resends a photon to Bob. This inevitably causes detectable errors in Bob's key string. In the following, we will calculate the error rate and information obtained by Eve in two important cases.

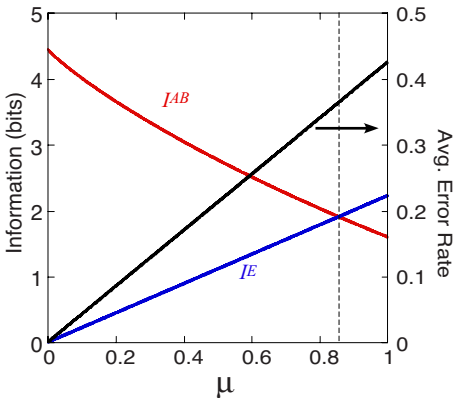

FIG. 6. (Color online) Information I^{AB} and I^E and average error rate for an intercept-resend attack as a function of the fraction μ of photons which Eve intercepts.

A. Intercept-resend attack

In the usual intercept-resend attack strategy, Eve measures the field using the same optical configurations as Alice and Bob. So for half of her measurements Eve will discover the correct aperture position ($\phi=0$), while for half she will have only little information ($\phi=\pi/2$). The error rate for each character k is $\mathcal{E}_k=\frac{\mu}{2}(1-p_k)$, where μ is the fraction of photons that Eve measures and p_k is the probability that Eve measures character k. In this case, Eve's information is given by $I^E=-\frac{\mu}{2}\Sigma_{k=0}^{d-1}p_k\log_2 p_k$ bits/photon.

For the Gaussian distribution in Eq. (11), the error rate is $\mathcal{E}_k=\frac{\mu}{2}(1-P_k)$, where P_k is defined in Eq. (27). The average error rate is obtained by averaging over all characters k: $\mathcal{E}=\mu\Sigma_k P_k\mathcal{E}_k\approx 0.425\mu$ for the 37-dimensional coding scheme illustrated in Fig. 3. That is, for each photon Eve intercepts and resends, Bob detects the wrong character with probability 0.425. Figure 6 shows Eve's information and the Alice-Bob mutual information (31) as a function of μ for an intercept-resend attack. Also shown is the average error rate (right y axis) corresponding to μ. In order to employ classical error correction and privacy amplification, it is necessary that $I^{AB}>I^E$ [2], which occurs at about $\mu=0.8565$, corresponding to a maximum allowable error rate of $\mathcal{E}=0.364$, for which $I^{AB}=I^E=1.906$ bits/photon. This is a considerable improvement over the usual BB84 protocol with $d=2$, in which the maximum allowed error rate is about 0.15 for which $I^{AB}=I^E\approx 0.4$ bits/photon.

B. Intermediate-basis attacks

Using the FRFT operators given in Eq. (13), it is also possible for Eve to implement attacks in an intermediate ba-

sis [2]. This is the basis for which Eve has equal (but probabilistic) information about the character Alice sends, regardless of Alice's choice of basis. In our scheme, these are FRFTs for which $\mathcal{D}_{\alpha_1+\varepsilon}(\boldsymbol{\rho}_A)=\mathcal{D}_{\alpha_2+\varepsilon}(\boldsymbol{\rho}_A)$. Examining Eq. (35), we see that this relation is true whenever $\cos(\alpha_1+\varepsilon)=\cos(\alpha_2+\varepsilon)$ and $\sin^2(\alpha_1+\varepsilon)=\sin^2(\alpha_2+\varepsilon)$. Using the conditions for the FRFT orders Eq. (20), we find $\tan(\alpha_2+\varepsilon)=-(-1)^{(t-m)}$, which limits $\alpha_2+\varepsilon$ to an odd multiple of $\pi/4$, $\alpha_2+\varepsilon=(2c+1)\pi/4$, and gives $\alpha_1+\varepsilon=(t-m-\frac{c}{2}+\frac{1}{4})\pi/4$. Using the detection positions corresponding to Fig. 3, we define $P(j|k)$ as

$$P(j|k)=\left|\int d\boldsymbol{\rho}\ \Psi_{7\pi/4}(\boldsymbol{\rho},\boldsymbol{\rho}_j)\mathcal{A}(\rho-\boldsymbol{\rho}_k)\right|. \tag{36}$$

Eve's information is $I^E=I^A-\Sigma_k P_k H(j|k)\approx 0.88$ bits/photon, which is considerably less than the intercept-resend strategy (≈ 2.23 bits/photon). Assuming that when Eve detects character k she sends $\Psi_{7\pi/4}(\boldsymbol{\rho},\boldsymbol{\rho}_k)$ to Bob, the error rate is

$$\mathcal{E}_{IB}=\sum_j P_k \sum_k P(j|k)\sum_m P(k|m). \tag{37}$$

In our example, Eve introduces an error rate of $\mathcal{E}_{IB}=0.89$ in Bob's key string, while obtaining only 0.88 bits of information per photon. Thus, the intercept-resend attack is much more advantageous than an intermediate-basis attack.

Using quantum cloning operations, it is possible to implement more advantageous eavesdropping attacks. The maximum bit error rate allowed for quantum cloning attacks for the two-basis BB84 protocol using d-dimensional systems was computed in Ref. [42]. For example, for $d=37$, the maximum allowed error rate for secure transmission is 0.42. However, we expect this limit to be lower for our system, since the characters are not sent with equal probability, but rather are chosen according to a Gaussian distribution, which has a lower Shannon entropy than a constant distribution.

Recently, eavesdropping strategies which take advantage of dark counts and channel losses have been considered for QKD based on spatial variables of entangled photon pairs [43]. It was shown that the Gaussian nature of Alice and Bob's fields provides higher allowable bit error rates. This is due to the fact that dark counts appear as a constant background count, and thus the total distribution of dark counts and actual photons is non-Gaussian, which limits Eve's eavesdropping strategies and allows for higher acceptable error rates. We expect QKD with spatial variables of single photons to present this same advantage.

IV. TRANSMISSION OF SPATIAL QUDITS

Real-world implementation of QKD over long distances is a considerable technical challenge, regardless of the type of qubit used or whether they be sent in optical fibers or free space [2]. Certain problems, such as photon losses, are problematic in nearly all systems. Let us focus here on technical problems of long-distance transmission which are particular to our spatial encoding. The spatial structure of the field rules out the use of ordinary optical fibers in our scheme, and thus it is more appropriate for free-space transmission. However, there do exist image-carrying conduits (coherent bundle of fibers) which could be employed. In terms of free-space transmission, we expect the scheme proposed here to be similar to the orbital angular momentum of light, as both rely on the spatial structure of the field. In Ref. [44], light beams carrying orbital angular momentum were sent over a short-distance free-space link (15 m length), and in Refs. [45,46], the effect of atmospheric turbulence on orbital angular momentum was considered.

Aside from losses due to absorption, the most prevalent effects of atmospheric turbulence are phase fluctuations, in which the field $\Psi(\boldsymbol{\rho})$ becomes $\exp[i\Delta(\boldsymbol{\rho})]\Psi(\boldsymbol{\rho})$. Here $\Delta(\boldsymbol{\rho})$ describes the effect due to changes in the index of refraction due to atmospheric turbulence. The probability P_c that the correct field arrives at Bob's input plane is given by the overlap integral of the actual field $\exp[i\Delta(\boldsymbol{\rho})]\Psi(\boldsymbol{\rho})$ with the ideal field $\Psi(\boldsymbol{\rho})$:

$$\begin{aligned}P_c&=\left|\int d\boldsymbol{\rho}\ \Psi(\boldsymbol{\rho})\exp[i\Delta(\boldsymbol{\rho})]\Psi_{(\boldsymbol{\rho})}\right|\\&=\left\{\int\int d\boldsymbol{\rho}\,d\boldsymbol{\rho}'|\Psi(\boldsymbol{\rho})|^2|\Psi(\boldsymbol{\rho}')|^2 e^{i[\Delta(\boldsymbol{\rho})-\Delta(\boldsymbol{\rho}')]}\right\}^{1/2}.\end{aligned} \tag{38}$$

It is customary to assume that the phase fluctuations are isotropic and a random Gaussian process. Then, taking the ensemble average, we have

$$\begin{aligned}\langle\exp\{i[\Delta(\boldsymbol{\rho})-\Delta(\boldsymbol{\rho}')]\}\rangle&=\exp[-\langle|\Delta(\boldsymbol{\rho})-\Delta(\boldsymbol{\rho}')|^2\rangle/2]\\&=\exp[-6.88(|\boldsymbol{\delta}|/r_0)^{5/3}/2]\end{aligned}$$

[45,47], where $\boldsymbol{\delta}=\boldsymbol{\rho}-\boldsymbol{\rho}'$. Here r_0 is the Fried parameter, which corresponds to the length scale of the phase fluctuations. We then have

$$P_c=\left\{\int\int d\boldsymbol{\rho}\,d\boldsymbol{\delta}|\Psi(\boldsymbol{\rho})|^2|\Psi(\boldsymbol{\rho}+\boldsymbol{\delta})|^2 e^{-6.88/2(|\boldsymbol{\delta}|/r_0)^{5/3}}\right\}^{1/2}. \tag{39}$$

In the QKD scheme discussed above, the intensity distribution of the field sent by Alice is always described by a shifted Gaussian distribution, independent of the FRFT angle she uses. As a concrete example, let us consider a Gaussian field profile $\mathcal{W}(\boldsymbol{\rho}-\boldsymbol{\rho}_0)$ as given by (11), but with dimensional width w. It is straightforward to calculate

$$P_c=\left\{\frac{2}{\pi w(z)^2}\int d\boldsymbol{\delta}\, e^{-\delta^2/2w(z)^2}e^{-6.88/2(|\boldsymbol{\delta}|/r_0)^{5/3}}\right\}^{1/2}. \tag{40}$$

We note that the probability P_c is independent of the mean position $\boldsymbol{\rho}_0$ and that we have explicitly included the dependence of the beamwidth on the propagation distance z: $w(z)=w_0\sqrt{1-z^2/z_0^2}$, where w_0 is the beam waist and z_0 the Rayleigh range. When the beamwidth is much smaller than the turbulence length parameter, the disturbance of the transmitted field is negligible. However, as the beam diverges, the atmospheric phase fluctuations become quite important. Typical values for r_0 are 10–60 cm [48]. Let us assume a beam with waist $w_0=1$ mm and $\lambda=500$ nm, so that $z_0=2\pi$ m. The beamwidth $w(z)$ is then comparable to r_0

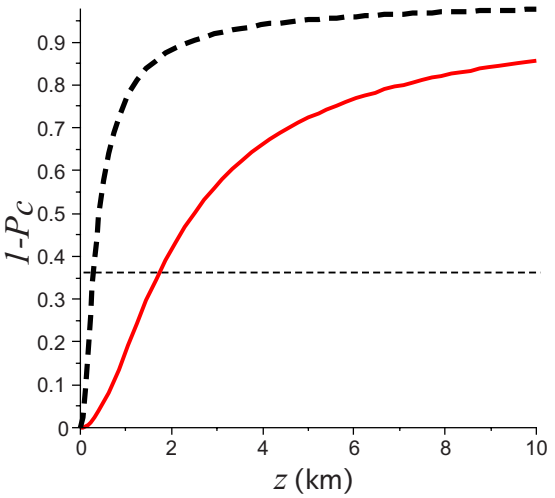

FIG. 7. (Color online) Error probability $1-P_c$ as a function of the transmission distance z for $r_0=0.1$ m (dashed black line) and $r_0=0.6$ m (solid red line). The dashed line corresponds to the error limit for the intercept-resend strategy for the $d=37$ example considered in Sec. III.

after 1–4 km. Figure 7 shows the error probability $1-P_c$ as a function of z using these parameters for $r_0=10$ cm and $r_0=60$ cm. The dashed line marks the allowable error rate (~ 0.36), calculated for the intercept resend strategy for the $d=37$ example considered above. One can see that the maximum transmission distance is about 0.3 km for $r_0=10$ cm (dashed black line) and 2 km for $r_0=60$ cm (solid red line). In these cases the transmission rate, given by the mutual information (31), is about 1.9 bits/photon.

Thus, atmospheric fluctuations will certainly limit the transmission length and transmission rate of a spatial QKD system. However, recent work in optical communications suggests that it is possible to partially correct these effects with adaptive optics, even in the case of high turbulence [48–50]. One might also consider an optical relay system consisting of a series of confocal lenses [51], which maintain a beamwidth smaller than the diameter of the lenses. In this way diffraction effects are circumvented and the beam waist can be kept smaller than the turbulence length.

V. CONCLUSION

We have presented a generalized quantum key distribution scheme using spatial degrees of freedom of single photons, which allows for d-dimensional encoding. Alice and Bob each use lens systems to implement a fractional Fourier transform on their fields. We determine the orders α and β which allow for secure key transmission. Alice encodes information into the transverse field profile by positioning a small aperture in the input plane, and Bob registers the detection position of the photon. The transmission rate and sensitivity to eavesdropping are briefly analyzed. We estimate a transmission of about 4.45 bits/photon for a 37-dimensional alphabet, taking into account the characteristics of a Gaussian beam and the geometry of the apertures. For the usual intercept-resend strategy, the allowable error rate is about 0.425. Using the fractional Fourier transform, we define intermediate-basis attacks for this system and show that Eve obtains considerably less information with this strategy than the intercept-resend attack, while inducing a higher error rate. A brief analysis of free-space transmission of spatial qudits was performed, showing that this kind of system can be reliably implemented in free space for distances of the order of about 1 km. This distance might be considerably increased using adaptive optics or other means to correct distortion of the transverse field.

ACKNOWLEDGMENTS

The authors thank P. Pellat-Finet and F. Toscano for helpful discussions and acknowledge financial support from the Brazilian funding agencies CNPq, FAPERJ, and CAPES. This work was performed as part of the Brazilian Millennium Institute for Quantum Information.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, e-print arXiv:0802.4155.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3] S. Wiesner, SIGACT News **15**, 78 (1983).
[4] C. H. Bennett and G. Brassard, in Proceedings of the International Conference on Computer Systems and Signal Processing, Bangalore, 1984 (IEEE, New York, 1984), p. 175.
[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[6] C. Gobby, Z. L. Duan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[7] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek *et al.*, Nat. Phys. **3**, 481 (2007).
[8] T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).
[9] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[10] M. Bourennane, A. Karlsson, and G. Bjork, Phys. Rev. A **64**, 012306 (2001).
[11] R. T. Thew, A. Acin, H. Zbinden, and N. Gisin, Quantum Inf. Comput. **4**, 93 (2003).
[12] H. de Riedmatten, I. Marcikic, V. Scarani, W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **69**, 050304(R) (2004).
[13] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. **98**, 060503 (2007).
[14] A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **89**, 240401 (2002).
[15] G. Molina-Terriza, A. Vaziri, J. Reháček, Z. Hradil, and A. Zeilinger, Phys. Rev. Lett. **92**, 167903 (2004).

[16] S. Groblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, New J. Phys. **8**, 75 (2006).
[17] S. P. Walborn, S. Pádua, and C. H. Monken, Phys. Rev. A **71**, 053812 (2005).
[18] X. F. Ren, G. P. Guo, and G. C. Guo, Phys. Lett. A **341**, 81 (2005).
[19] Y. I. Bogdanov, M. V. Chekhova, S. P. Kulik, G. A. Maslennikov, A. A. Zhukov, C. H. Oh, and M. K. Tey, Phys. Rev. Lett. **93**, 230503 (2004).
[20] E. V. Moreva, G. A. Maslennikov, S. S. Straupe, and S. P. Kulik, Phys. Rev. Lett. **97**, 023602 (2006).
[21] L. Neves, G. Lima, J. G. Aguirre Gómez, C. H. Monken, C. Saavedra, and S. Pádua, Phys. Rev. Lett. **94**, 100501 (2005).
[22] M. N. O'Sullivan-Hale, I. A. Khan, R. W. Boyd, and J. C. Howell, Phys. Rev. Lett. **94**, 220501 (2005).
[23] A. N. de Oliveira, S. P. Walborn, and C. H. Monken, J. Opt. B: Quantum Semiclassical Opt. **7**, 288 (2005).
[24] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Phys. Rev. Lett. **95**, 260501 (2005).
[25] S. P. Walborn, M. P. Almeida, P. H. S. Ribeiro, and C. H. Monken, Quantum Inf. Comput. **6**, 336 (2006).
[26] M. P. Almeida, S. P. Walborn, and P. H. Souto Ribeiro, Phys. Rev. A **73**, 040301(R) (2006).
[27] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. Souto Ribeiro, Phys. Rev. Lett. **96**, 090501 (2006).
[28] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The Fractional Fourier Transform: with Applications in Optics and Signal Processing* (Wiley, West Sussex, 2001).
[29] V. Namias, J. Inst. Math. Appl. **25**, 241265 (1980).
[30] A. C. McBride and F. H. Kerr, IMA J. Appl. Math. **39**, 159 (1987).
[31] S. Chountasis, A. Vourdas, and C. Bendjaballah, Phys. Rev. A **60**, 3467 (1999).
[32] P. Pellat-Finet, Opt. Lett. **19**, 1388 (1994).
[33] A. W. Lohmann, Opt. Commun. **115**, 437 (1995).
[34] A. W. Lohmann, J. Opt. Soc. Am. A **10**, 2181 (1993).
[35] G. R. Fowles, *Introduction to Modern Optics* (Dover, New York, 1989).
[36] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, New York, 1995).
[37] M. P. Almeida, S. P. Walborn, and P. H. Souto Ribeiro, Phys. Rev. A **72**, 022313 (2005).
[38] D. S. Lemelle, M. P. Almeida, P. H. S. Ribeiro, and S. P. Walborn, Am. J. Phys. **74**, 542 (2006).
[39] S. Kravitz, Math. Mag. **40**, 65 (1967).
[40] R. Graham, B. Lubachevsky, and P. O. K. J. Nurmela, Discrete Math. **181**, 139 (1998).
[41] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, Hoboken, NJ, 2006).
[42] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[43] L. Zhang, C. Silberhorn, and I. Walmsley, e-print arXiv:quant-ph/0711.4631.
[44] G. Gibson, J. Courtial, M. J. Padgett, M. Vasnetsova, V. Pas'ko, S. J. Barnett, and S. Franke-Arnold, Opt. Express **12**, 5448 (2004).
[45] C. Paterson, Phys. Rev. Lett. **94**, 153901 (2005).
[46] B. J. Smith and M. G. Raymer, Phys. Rev. A **74**, 062104 (2006).
[47] D. L. Fried, J. Opt. Soc. Am. **56**, 1372 (1966).
[48] M. W. Wright, M. Srinivasan, and K. Wilson, IPN Prog. Rep. **42**, 1 (2005).
[49] R. K. Tyson, J. Opt. Soc. Am. A **19**, 753 (2002).
[50] R. K. Tyson and D. E. Canning, Appl. Opt. **42**, 4239 (2003).
[51] B. E. A. Saleh and M. C. Teich, *Fundamental Photonics* (Wiley, New York, 1991).