Open access • Journal Article • DOI:10.1103/PHYSREVLETT.96.090501

Quantum key distribution with higher-order alphabets using spatially encoded qudits.

— Source link

Stephen P. Walborn, D. S. Lemelle, Marcelo P. Almeida, P. H. Souto Ribeiro

Institutions: Federal University of Rio de Janeiro

Published on: 08 Mar 2006 - Physical Review Letters (American Physical Society)

Topics: Quantum cryptography, Quantum network, Quantum key distribution and Byte

Quantum Key Distribution with Higher-Order Alphabets Using Spatially Encoded Qudits

S. P. Walborn,* D. S. Lemelle, M. P. Almeida, 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 12 October 2005; published 8 March 2006)

We present a proof of principle demonstration of a quantum key distribution scheme in higher-order d-dimensional alphabets using spatial degrees of freedom of photons. Our implementation allows for the transmission of 4.56 bits per sifted photon, while providing improved security: an intercept-resend attack on all photons would induce an average error rate of 0.47. Using our system, it should be possible to send more than a byte of information per sifted photon.

DOI: 10.1103/PhysRevLett.96.090501 PACS numbers: 03.67.Dd, 42.25.Kb, 42.50.Ar

Though quantum key distribution (QKD) has become a commercial reality [1], there is still much interest in fundamental research. One topic of fundamental importance is the design of protocols and implementations which increase the bit transmission rate and/or the security of the QKD scheme. It has been pointed out recently that one can achieve both of these objectives by increasing the dimensionality of the system, that is, encoding a random key string in d-dimensional qudits instead of the usual binary qubits [2,3].

It is straightforward to generalize the well-known BB84 protocol [4] to qudits [2,3,5], for which it is possible to send on average $\log_2 d$ bits per sifted qudit. Higher-dimensional qudits are advantageous not only for an increased bit transmission rate, but also increased security. An eavesdropper employing an intercept-resend strategy would induce a qudit 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 $(d-1)/d$ [2,3].

Experimentally, there are several methods of encoding d-dimensional qudits in photons, including time-bin [2], orbital angular momentum [6], the polarization state of more than one photon [7], and, more recently, position and linear momentum of entangled photons [8,9].

Here we provide an experimental demonstration of quantum key distribution using higher-order d-dimensional alphabets encoded in the transverse spatial profile of single photons. Our scheme is based on the standard BB84 protocol [4], in which Alice chooses which state to send based on the value of a random bit a_1, while her choice of basis is selected using random bit a_2. A two-basis BB84 protocol using qudits works the same way [2,3], however, Alice sends states according to the value of a random d-level "dit". A simple illustration of our scheme is shown in Fig. 1. Let us first discuss the choice of basis. In our scheme, Alice (A) and Bob (B) encode (Alice) and decode (Bob) information in the transverse profile of single photons by choosing randomly between optical imaging systems and optical Fourier transform systems. In order to avoid the quadratic phase factors that generally appear in an imaging system [10], it is necessary to use a telescopic lens system, consisting of two confocal lenses. This is equivalent to applying the Fourier transform operation twice, so that, as part of the protocol, Alice and Bob will each choose randomly between a single or double Fourier transform lens system. For simplicity, let us assume that Alice and Bob use identical imaging systems, consisting of two lenses with focal length f, as well as identical Fourier systems consisting of a single lens with focal length $2f$. The "quantum channel" consists of a telescopic lens system consisting of two lenses with focal length f_c which transmits Alice's output to Bob's input.

In the following we will assume that the input field is a single-photon state, which in the paraxial approximation can be described by

$$|\psi\rangle = \int v(\mathbf{q})|\mathbf{q}\rangle d\mathbf{q}, \tag{1}$$

where $v(\mathbf{q})$ is the angular spectrum defined by

$$v(\mathbf{q}) = \int \mathcal{W}(\boldsymbol{\rho}, 0)e^{-i\mathbf{q}\cdot\boldsymbol{\rho}}d\boldsymbol{\rho}, \tag{2}$$

and $\mathcal{W}(\boldsymbol{\rho}, 0)$ is the input field at $z = 0$ (plane $P_{A\text{in}}$). Here $\boldsymbol{q}$ is the transverse component of the wave vector and $\boldsymbol{\rho}$ is the transverse position coordinate. The detection probability in plane P_B for a given combination of lens configurations is given by $\mathcal{P}_{\alpha\beta}(\boldsymbol{\rho}) = |\mathcal{A}_{\alpha\beta}(\boldsymbol{\rho})|^2$, where $\mathcal{A}(\boldsymbol{\rho}) = \langle\text{vac}|\mathsf{E}^{+}_{\alpha\beta}(\boldsymbol{\rho})|\psi\rangle$ is the detection amplitude, $\mathsf{E}^{+}_{\alpha\beta}(\boldsymbol{\rho})$ is the field operator for the entire lens system [11,12], and

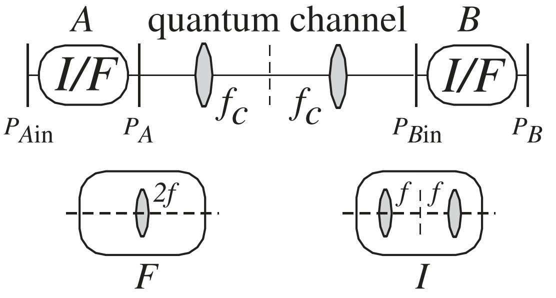

FIG. 1. Illustration of QKD using imaging (I) and Fourier (F) optical systems.

$\alpha, \beta = I, F$ denotes either imaging or Fourier configurations. For a series of n confocal lenses, $\mathsf{E}^{+}_{\alpha\beta}(\boldsymbol{\rho})$ simplifies to

$$\mathsf{E}^{+}_{\alpha\beta}(\boldsymbol{\rho}) = \mathcal{E}\int d\boldsymbol{q}\int d\boldsymbol{q}_1 \cdots \int d\boldsymbol{q}_n\, \mathsf{a}(\boldsymbol{q}_n) e^{i\boldsymbol{q}\cdot\boldsymbol{\rho}} \times e^{-if_1/k\boldsymbol{q}_1\cdot\boldsymbol{q}} \ldots e^{-if_n/k\boldsymbol{q}_n\cdot\boldsymbol{q}_{n-1}}, \tag{3}$$

where $\mathcal{E}$ is a constant, k is the magnitude of the wave vector, f_j is the focal length of the jth lens, and $\mathsf{a}(\mathbf{q})$ is the usual destruction operator. For the four possible lens systems illustrated in Fig. 1, the detection amplitudes are

$$\mathcal{A}_{FF}(\boldsymbol{\rho}) = \frac{\mathcal{E}k^2}{2f_c f}\mathcal{W}(\boldsymbol{\rho}, 0), \tag{4}$$

$$\mathcal{A}_{II}(\boldsymbol{\rho}) = \frac{\mathcal{E}k^3}{f_c f^2}\mathcal{W}(-\boldsymbol{\rho}, 0), \tag{5}$$

$$\mathcal{A}_{IF}(\boldsymbol{\rho}) = \frac{\mathcal{E}k^3}{2f_c f^2}v\left(\frac{k}{2f}\boldsymbol{\rho}\right), \tag{6}$$

and

$$\mathcal{A}_{FI}(\boldsymbol{\rho}) = \frac{\mathcal{E}k^3}{2f_c f^2}v\left(\frac{k}{2f}\boldsymbol{\rho}\right). \tag{7}$$

In our scheme, Alice encodes information into the input field by positioning an aperture $A(\boldsymbol{\rho} - \boldsymbol{\rho}_d)$ in plane P_{Ain}, such that each aperture position $\boldsymbol{\rho}_d$ corresponds to a character in the d-dimensional alphabet. Assuming that the incident field is a plane wave, the input field is equivalent to the aperture function: $\mathcal{W}(\boldsymbol{\rho}, 0) = A(\boldsymbol{\rho} - \boldsymbol{\rho}_d)$. Equations (4) and (5) show that when Alice and Bob choose the same lens configuration, Bob's detection amplitudes will reproduce the aperture function, and Bob should decode the correct character. For complementary lens configurations the detection amplitudes are given by Eqs. (6) and (7), and are proportional to the Fourier transform of the aperture. A well-known property of the Fourier transform is that a shift in position space manifests as a phase in the Fourier transform ($\mathcal{F}$) space: $\mathcal{F}[A(\boldsymbol{\rho} - \boldsymbol{\rho}_d)] = \exp(ik\boldsymbol{\rho}\boldsymbol{\rho}_d/2f)\mathcal{F}[A(\boldsymbol{\rho})]$. Thus the detection probabilities $\mathcal{P}_{IF}$ and $\mathcal{P}_{FI}$ contain no information concerning the aperture position $\boldsymbol{\rho}_d$. Even though Alice and Bob discard these results as part of the BB84 protocol, it is important that no information is available, as this guarantees that an eavesdropper cannot obtain information without causing an increase in the error rate.

Figure 2 shows the setup for an experimental demonstration of QKD using spatially encoded qudits. As is common in most QKD implementations, our experiment was performed with an attenuated laser beam, which, though there are zero- and multiphoton terms present, can be used to approximate a single-photon state [13]. The attenuated beam from a Coherent Verdi V5 laser (514 nm) was expanded by a factor of 4 using a beam expander consisting of 25 and 100 mm focal length lenses. Information was encoded into the spatial profile by positioning a 200 μm pinhole in Alice's transverse plane P_{Ain}. The pinhole was mounted on a manual x-y translation stage, though in principle a randomly driven mechanical device could be used. In order to implement both imaging and Fourier configurations, we constructed a Mach-Zehnder interferometer using 50-50 beam splitters (BS), in which one arm contained a telescopic imaging system (f = 100 mm), while the other contained a 200 mm focal length lens in a Fourier configuration. To switch between imaging and Fourier configurations, we toggled manually between the two arms of the interferometer. As interference is not actually used in the QKD scheme, the interferometer functions merely as a router. However, the interference is useful for initial alignment. Pinholes were placed in the focal planes of the imaging and Fourier lenses in order to filter higher spatial frequencies. As a result, the aperture function $A(\boldsymbol{\rho} - \boldsymbol{\rho}_d)$ can be approximated by a Gaussian. The quantum channel consisted of a telescopic lens system (f_c = 150 mm).

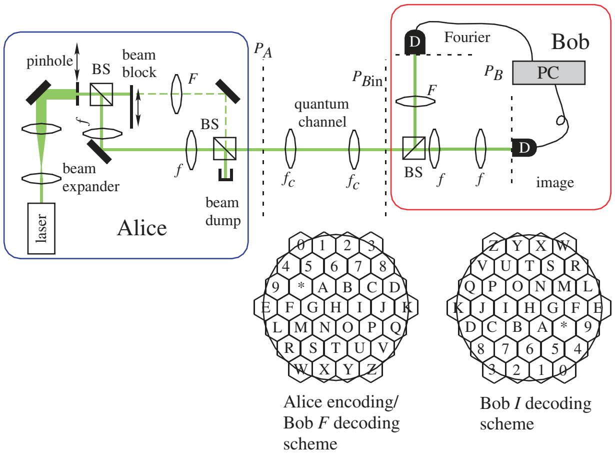

FIG. 2 (color online). Experimental setup.

Using a BS, Bob chose randomly between imaging and Fourier systems. His optical systems were identical to Alice's. One single-photon detector (equipped with 200 μm diameter circular detection aperture and ~250 nm bandwidth filter) was scanned throughout the Fourier detection plane, and one throughout the image detection plane. Ideally, the detection system would consist of either two-dimensional multidetector arrays, or CCD cameras with single-photon sensitivity [14].

The dimension d of Alice and Bob' s alphabet is determined by the size of the aperture $A(\boldsymbol{\rho})$ and its Fourier transform. Alice and Bob must decide on the best way to define positions in transverse planes P_{Ain} (Alice's aperture) and P_B (Bob's detector) that will correspond to the characters in their alphabet. To use the area available in the most efficient manner, we chose to approximate Alice's circular aperture and Bob's circular detection aperture with a hexagon (center to vertex distance 200 μm). Using this method, we were able to work with a 37-dimensional ("septrigesimal") alphabet. Alice and Bob's encoding/decoding scheme is shown at the bottom of Fig. 2. The circle corresponds to the area containing 99% of the large Gaussian profile obtained using complementary *IF* or *FI* configurations.

Figure 3 shows the intensity pattern at Bob's detection plane for the four possible lens configurations when Alice sends the character "7". The distributions were obtained by placing the detector at each of the predefined detection positions, so that each of the 37 squares in the figures correspond to a character in the alphabet. For *II* and *FF* configurations, Bob detects the character 7 with high probability, while for *IF* and *FI* configurations, he obtains a widened (Gaussian) distribution, which provides little information about the character Alice sent.

As a better visualization of our results, Figs. 4 and 5 show probability distributions as a function of each character for Bob's Fourier and image detection systems, respectively. In both figures, Alice has sent the characters "4", "7", "G", "H", "P", and "Z". When Bob uses the same lens configuration as Alice (left side in both figures), he detects the correct character with a high probability. We obtained error rates $\mathcal{D}_k^{FF} \sim 0.06$–$0.11$ for the *FF* configuration and $\mathcal{D}^{II} \sim 0.10$–$0.19$ for the *II* configuration. Roughly 25% of the error was due to photocounts caused by unwanted ambient light and dark counts ($\sim$200 counts/sec), while the rest is due to misalignment and erroneous counts due to the hexagon pattern. Using narrow band interference filters and detectors with a reduced dark count rate ($\sim$25–50 counts/sec), we estimate that the error rates could easily be reduced to about 5%–15%. Further methods to reduce the *II* and *FF* error rate involve "decoy" alphabet states and will be discussed elsewhere [12].

Figures 4 and 5 also show the results when Alice and Bob use conjugate *IF* or *FI* configurations, from which it can be seen that the detection probabilities $\mathcal{P}_{IF}$ and $\mathcal{P}_{FI}$ are the approximately the same for all characters sent by Alice. We note that Bob's detection positions were defined according to the two-dimensional detection scheme shown in Fig. 2, so the several peaks shown in the *IF* and *FI* patterns are actually slices of a 3D Gaussian distribution. There is a difference between our QKD implementation and others: the detection probabilities for complementary measurements are not constant for all states: $\mathcal{P}_{IF} = \mathcal{P}_{FI} \neq 1/d$ and thus the sifted key is not completely random. However, after sifting, Alice and Bob can discard some of their results in order to obtain a completely random key string.

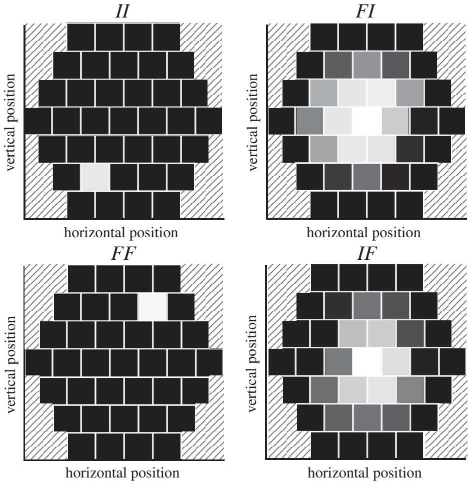

FIG. 3. Intensity distributions at Bob's detection plane for the four lens configurations *II*, *IF*, *FI*, and *FF* for the case when Alice sends the character 7. Here lighter squares correspond to a larger number of photocounts.

In order to minimize Eve's information, Alice should choose characters based on the distributions $\mathcal{P}_{IF}$ and $\mathcal{P}_{FI}$. Suppose that Alice sends each character k with probability P_k, obtained by averaging the *IF* and *FI* detection results. The amount of information that can be sent from Alice to Bob is given by the Shannon information [3,13], which in our case is

$$I^{AB} = I^A + \sum_{k=0}^{d-1} P_k(1-\mathcal{E}_k)\log_2(1-\mathcal{E}_k) + \sum_{k=0}^{d-1}\sum_{j=0,j\neq k}^{d-1}\frac{P_k\mathcal{E}_kP_j}{1-P_k}\log_2\frac{\mathcal{E}_kP_j}{1-P_k}, \qquad (8)$$

where $\mathcal{E}_k$ is the error probability and $I^A = -\sum_{k=0}^{d-1} P_k\log_2 P_k = 4.56$ bits/photon is the information transmission in the absence of errors. Our experimental error rates $\mathcal{D}^{II}$ and D^{FF} varied between 0.06 and 0.19, giving $3.00 \le I^{AB} \le 3.96$ bits/photon. For an intercept-

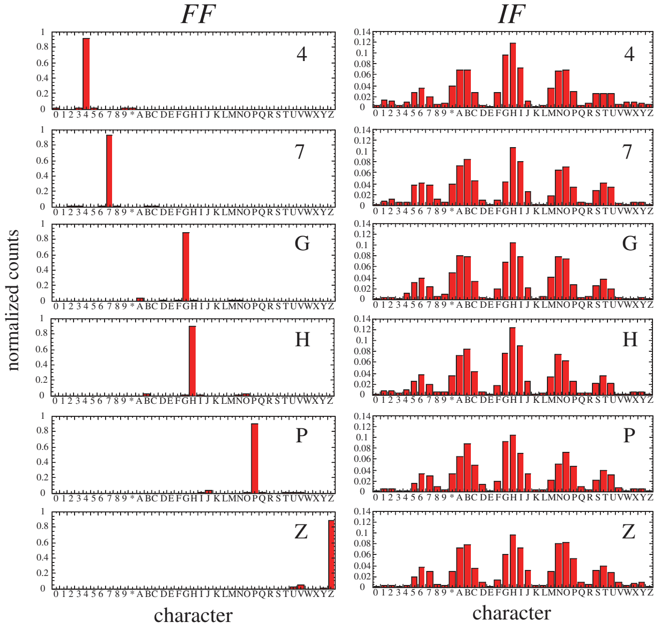

FIG. 4 (color online). Normalized counts for Bob's Fourier (F) detection system when Alice uses Fourier (left) and image (right) encoding.

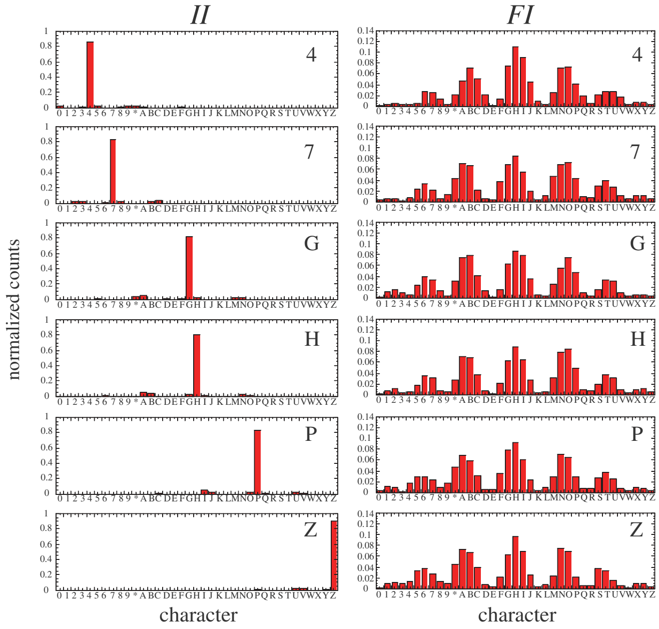

FIG. 5 (color online). Normalized counts for Bob's image (I) detection system when Alice uses image (left) and Fourier (right) encoding.

resend attack on a fraction η of the photons, the error rate is $\mathcal{E}_k = \frac{\eta}{2}(1 - P_k)$, which varies between 0.450η and 0.499η. In this case, Eve's information is given by $I^E = -\frac{\eta}{2}\sum_{k=0}^{d-1} P_k \log_2 P_k = 2.28\eta$ bits/photon. In order to employ classical error correction and privacy amplification, it is necessary that $I^{AB} > I^E$ [13]. $I^{AB} = I^E = 1.858$ bits/photon occurs when the average error rate $\mathcal{E} = \sum_k P_k \mathcal{E}_k$ is about 0.38, much larger than our values of 0.06–0.19. We note that the allowable error rate for cloning-based individual attacks on a two-basis $d = 37$ protocol is 0.42 [5,15]

Let us briefly discuss an important security issue particular to this implementation. A more detailed security analysis will be provided elsewhere [12]. In order for the transmission to be secure, an eavesdropper Eve should not be able to determine when Alice is using the imaging or Fourier system to encode information. If there exist detection positions at which Eve can detect photons that *probably* correspond to an IF or FI (Alice-Eve) configuration, then she can deduce that she measured in the wrong basis, and choose not to resend the photon. Eve's presence would then be marked only as the loss of a photon, and not a registered error. In order to avoid this situation, Alice and Bob must define their alphabet so that every detection position with a nonzero IF or FI detection probability also has a nonzero II or FF detection probability. In this fashion, Eve cannot deduce whether she is measuring in the same basis as Alice or not. On the other hand, if Eve can deduce that she probably measured in the correct basis, she gains nothing by not sending the photon. Of course she has gained information and left no disturbance, but Alice and Bob can minimize these cases by removing these characters from the final sifted key string, at the cost of a reduction in the size d of the alphabet.

We have presented a proof of principle demonstration of QKD using spatially encoded qudits. Generalization of our scheme to even larger dimensions is straightforward. Using an even smaller aperture, it should be possible to encode an extremely large amount of information, increasing both the transmission rate as well as the security of the QKD protocol. For example, using a 60 μm pinhole, should give an alphabet of roughly 400 characters in each photon, resulting in a transmission capacity of more than 1 byte per sifted photon. In terms of a real-world application, QKD based on spatial qudits seems best suited for free-space transmission as opposed to optical fibers. In a free-space setup, disturbances in the wave front due to propagation through the atmosphere might be monitored using a reference beam, and then corrected.

The authors acknowledge financial support from the Brazilian Millennium Institute for Quantum Information, CNPq, CAPES, FAPERJ, FUJB, and PRONEX.

*Electronic address: swalborn@if.ufrj.br

[1] Gary Stix, Sci. Am. **292**, No.1, 78 (2005).

[2] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).

[3] M. Bourennane, A. Karlsson, and G. Bjork, Phys. Rev. A **64**, 012306 (2001).

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

[5] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[6] J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial, Phys. Rev. Lett. **88**, 257901 (2002).

[7] 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).

[8] L. Neves, G. Lima, J. G. Aguirre Gómez, C. H. Monken, C. Saavedra, and S. Pádua, Phys. Rev. Lett. **94**, 100501 (2005).

[9] M. N. O'Sullivan-Hale, I. A. Khan, R. W. Boyd, and J. C. Howell, Phys. Rev. Lett. **94**, 220501 (2005).

[10] J. W. Goodman, *Introduction to Fourier Optics* (McGraw-Hill, Boston, 1996).

[11] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge University Press, New York, 1995).

[12] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro (to be published).

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

[14] A. F. Abouraddy, M. B. Nasr, B. E. A. Saleh, A. V. Sergienko, and M. C. Teich, Phys. Rev. A **63**, 063803 (2001).

[15] We expect this limit to be slightly lower for our scheme, since the IF and FI results are not completely random.