Invited Paper

Quantum Key Distribution in a High-Dimensional State Space: Exploiting the Transverse Degree of Freedom of the Photon

Robert W. Boyd
The Institute of Optics and Department of Physics and Astronomy, University of Rochester, Rochester, NY 14627, USA and Department of Physics, University of Ottawa, Ottawa, ON K1N 6N5 Canada

Anand Jha, Mehul Malik, Colin O'Sullivan and Brandon Rodenburg
The Institute of Optics, University of Rochester, Rochester, NY 14627, USA

Daniel J. Gauthier
Department of Physics, Duke University, Box 90305, Durham, NC 27708, USA.

ABSTRACT

We describe a procedure to construct a free-space quantum key distribution system that can carry many bits of information per photon. We also describe the current status of our laboratory implementation of these plans.

Keywords: quantum key distribution, orbital angular momentum, quantum imaging

1. INTRODUCTION

In recent years, there has been great interest in the development of means for secure communication that are based on the fundamental laws of quantum mechanics.[1–5] Our group has been particularly interested in developing a free-space system for quantum key distribution (QKD) based on the use of Laguerre-Gauss (LG) modes and other field modes that carry orbital angular momentum (OAM).[6–9] The motivation for this approach is that the original proposal for QKD, the BB84 protocol of Bennet and Brassard,[1] encoded information into the polarization degree of freedom of an individual photon. As a result, only one bit of information can be impressed onto each photon. In the approach under development here, there is no limit to how many bits of information can be impressed onto a single photon, as the LG modes span an infinite-dimensional state space. Our current goal is to impress between 5 to 8 bits of information onto each photon. One motivation for doing this is that rate of data transmission is thereby increased. Another more subtle motivation for using a large state space is that the security of the protocol can be increased in this manner.[10–14] Work that adopts a similar approach has been reported in several recent publications.[15–19]

The system that we envision is illustrated in Fig. 1. It consists of a sender, A or Alice, and a receiver, B or Bob. Alice impresses information onto individual photons through use of a spatial light modulator. Bob then guesses which basis Alice is using and makes a measurement of the quantum state of this photon in this basis. The procedure for ensuring the security of the transmission is a generalization of that of the BB84 protocol.

Further author information: (Send correspondence to Robert Boyd: E-mail: boyd@optics.rochester.edu)

Advances in Photonics of Quantum Computing, Memory, and Communication IV,
edited by Zameer Ul Hasan, Philip R. Hemmer, Hwang Lee, Charles M. Santori, Proc. of SPIE
Vol. 7948, 79480L · © 2011 SPIE · CCC code: 0277-786X/11/$18 · doi: 10.1117/12.873491

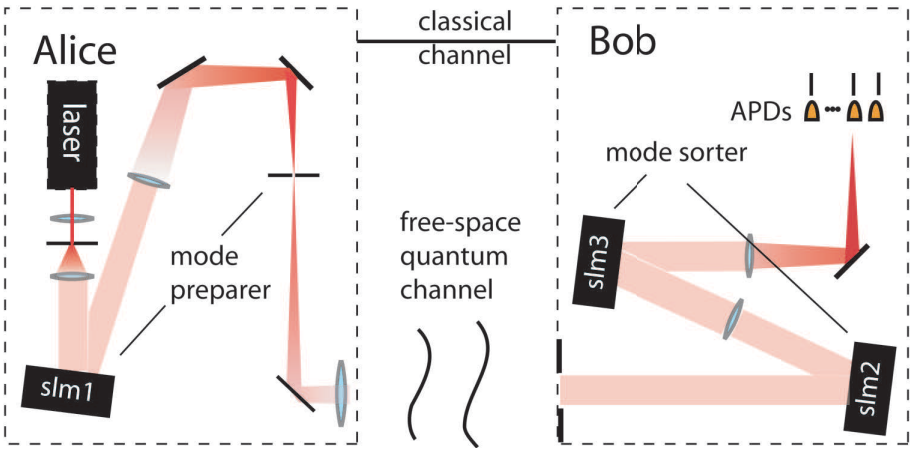

Figure 1. System schematic of the QKD protocol under development. A sender (A or Alice) impresses information onto an individual photon through use of a spatial light modulator (SLM). This photon is then sent to the receiver (B or Bob) through a free-space link, where it may experience degradation by means of atmospheric turbulence. The receiver then determines the quantum state of this photon.

2. ORBITAL ANGULAR MOMENTUM AND LAGUERRE-GAUSS MODES

We noted above that our enhanced protocol for QKD is based upon the properties of the Laguerre-Gauss modes. Let us recall the properties of these modes. The paraxial approximation to the Helmholtz equation $(\nabla^2 + k^2)E(k) = 0$ gives the paraxial wave equation which is written in a cartesian coordinate system as

$$\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + 2ik\frac{\partial}{\partial z}\right) E(x, y, z) = 0. \tag{1}$$

The paraxial wave equation is satisfied by the Laguerre-Gaussian modes, a family of orthogonal modes that have a well defined orbital angular momentum. The field amplitude $LG_p^l(\rho, \phi, z)$ of a normalized Laguerre-Gauss mode is given by

$$LG_p^l(\rho,\phi,z) = \sqrt{\frac{2p!}{\pi(|l|+p)!}}\frac{1}{w(z)}\left[\frac{\sqrt{2}\rho}{w(z)}\right]^{|l|} L_p^l\left[\frac{2\rho^2}{w^2(z)}\right] \times \exp\left[-\frac{\rho^2}{w^2(z)}\right]\exp\left[-\frac{ik^2\rho^2 z}{2(z^2+z_R^2)}\right]\exp\left[i(2p+|l|+1)\tan^{-1}\left(\frac{z}{z_R}\right)\right]e^{-il\phi}, \tag{2}$$

where k is the wave-vector magnitude of the field, z_R the Rayleigh range, $w(z)$ the radius of the beam at position z, l is the azimuthal quantum number, and p is the radial quantum number. L_p^l is the associated Laguerre polynomial. It can be shown that each photon in such a beam carries an orbital angular momentum of $l\hbar$.

3. OUR PROPOSED PROTOCOL

The BB84 QKD protocol entails Eve sending each photon in a randomly chosen basis. At least two mutually orthogonal bases (MUBs) must be used. Certain advantages accrue from using more than two MUBs. It known that the maximum number $B_{\max}$ of MUBs B is related to the dimension D of the state space by $B_{\max} = D + 1$, and for certain special cases it is know that there are exactly $D + 1$ such MUBs.[20] In our present laboratory investigations, we are using the minimum number of MUBs, $B = 2$. We choose this value for convenience and to maximize our data transmission rate, which is proportional to $1/B$. At some later time we hope to study the consequences of using larger values of B. The two basis sets currently under investigation are illustrated in Fig. 2. One basis is comprised of the LG states themselves. The other basis is composed of a linear combination of the LG states,which we take to be of the form

$$\Psi_{\mathrm{AB}}^N = \frac{1}{\sqrt{27}}\sum_{l=-13}^{13} \mathrm{LG}_{l,0}\exp\left(i2\pi Nl/27\right). \tag{3}$$

It is clear from the figure why we refer to this as an angular basis (AB). In plotting the intensity distributions of Fig. 2 for the LG basis, we have assumed that each state has the same value of the beam radius parameter $w(z)$. In this case, the transverse size of each mode scales with mode number as $\sqrt{l}$. However, it is possible to choose different values of $w(z)$ for each mode to keep each mode size approximately the same. Proceeding in the way makes the best use of the limited aperture of the transmitting and receiving lens apertures. In fact, in our laboratory implementation we routinely use different values of $w(z)$ for the various modes.

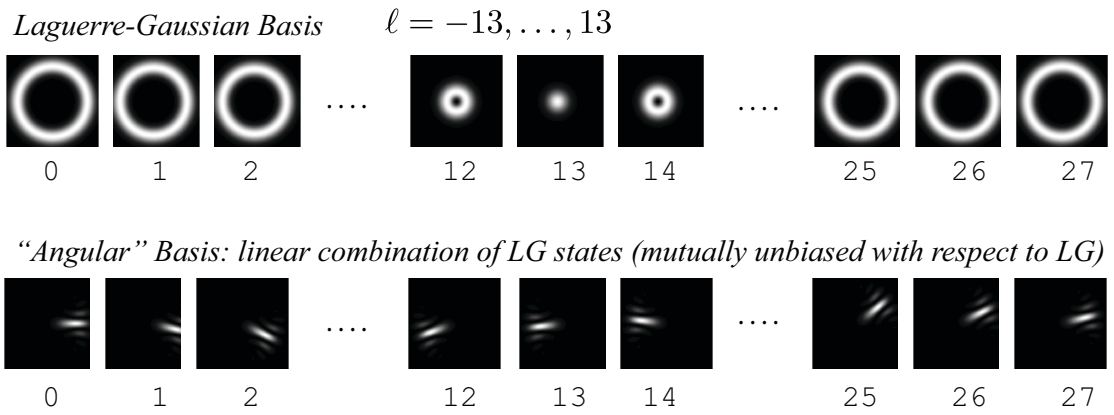

Figure 2. The LG basis (top) and a linear combination of the LG states that constitutes the angular basis (AB (bottom)).

An example of the implementation of our protocol is shown in Fig. 3. In this example, Alice is attempting to send the string of numbers 13, 3, 2, 3, 15, 14, 16, 8, 24, and 26 to Bob. For each transmitted photon, Alice chooses randomly between the LG basis and the AB. Also, for each transmitted photon, Bob chooses randomly between the LG basis and the AB. After the transmission of the entire data train is complete, Alice and Bob publicly disclose the basis they used for each measurement. If they used different bases (which occurs on average half of the time), they discard the results of that measurement. The remaining data string is known as the sifted data, and this data should contain no errors. Any error in this data string could be the result of measurement errors or to the presence of an eavesdropper. For reasons of extreme caution, they ascribe all errors to the presence of an eavesdropper. To test for errors, Alice and Bob sacrifice some fraction of their data for public comparison. If errors are detected, they conclude that an eavesdropper is present and take appropriate corrective measures.

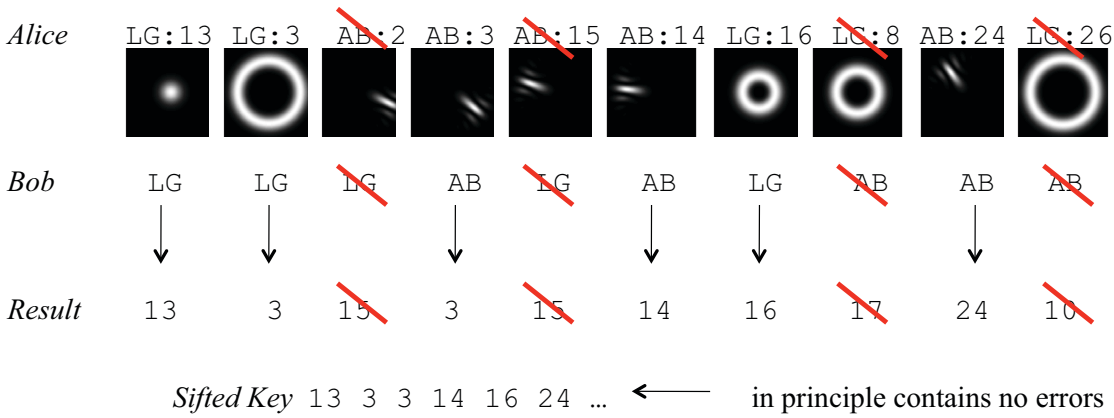

Figure 3. Example of the implementation of a generalized BB84 protocol in a high-dimensional (27-dimensions as illustrated) space.

4. LABORATORY IMPLEMENTATION

We have implemented this protocol in our laboratory. Figure 4 shows how Alice forms each of the basis states. Basically, she programs a spatial light modulator (SLM) to diffract an individual photon from a plane-wave input state into one of the desired LG or AB modes.[21] The upper row shows the LG basis and the lower row shows the angular basis (AB). The panel on the left shows representative examples of the pattern displayed on the SLM. The panels on the right show examples of the field distribution written onto the light field. These frames show actual laboratory results, although read out with intense classical light, not with single photons.

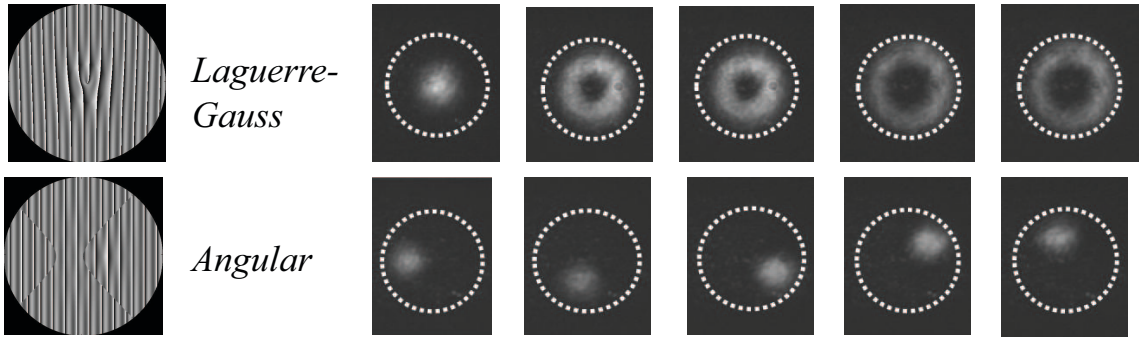

Figure 4. Illustration of our procedure for producing light fields in one of our basis states, shown for the case of five-state bases ($D = 5$).

A more demanding task is that required of Bob. He is presented with a single photon and needs to determine its quantum state. Thus, he is allowed to perform only one measurement to determine in which of a large number of quantum states his photon resides.[22–24] This task has eluded the scientific community until very recently. This past summer, the group of Miles Padgett[23,24] demonstrated a means for performing this task. We have succeeded in reproducing these results in our own laboratory. The key element of this approach is the ability to map the azimuthal phase distribution of an OAM mode onto a linear phase distribution. Of course, a linear phase ramp in one cartesian dimension is simply a wavefront tilt, and leads to a shift in the position of the beam in the far field. It turns out that one can determine analytically the form of the phase function that needs to be applied to a light field to perform this mapping. In both the original work of Berkhout et al. and in our own work, we apply this phase mapping through use of an SLM. Work is underway to construct lenses that will produce this mapping while introducing far fewer losses. To implement the QKD protocol, we also need to sort photons in the second basis, the angular basis. At present, we are performing this sorting by making use of the property that the lobes of the intensity distribution in the angular basis are nearly nonoverlapping. We then simply program the SLM to diffract different angular modes into the input ports of our array of avalanche photodiodes.

We are well along in our laboratory work on implementing this high-capacity QKD protocol. Some of our laboratory results are shown in Fig. 5. These results demonstrate our ability to discriminate among various quantum states in either the LG or angular basis. In each basis we include only four states. This limitation is due to the limited number of photodetectors (APDs) available to us. We see no fundamental limit to our ability to distinguish among all of the states in our protocol, 27 in this particular situation. We see that there is a small amount of cross talk among the various channels. Work is presently under way to improve the discrimination among the various modes.

5. CHOICE OF SINGLE-PHOTON SOURCE

A very subtle issue entails the best single-photon light source to be used with this protocol. For many years, it had been believed that it was necessary to use a true single-photon source, that is, a source that produces one and only one photon each time that the source is triggered. The reason for this belief is that if the source were to emit more than one photon, it would be possible for an eavesdropper to extract one of these photons for her own use without disturbing the other photon and thus revealing her presence. However, it has much more recently been shown[25,26] that the protocol can be modified by occasionally sending a decoy state which is

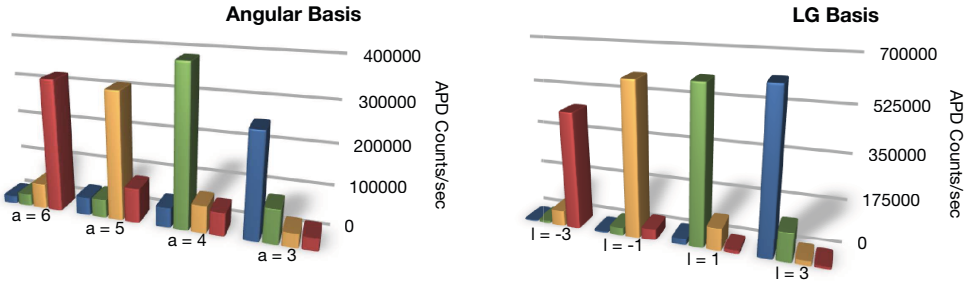

Figure 5. Some preliminary laboratory data demonstrating Bob's ability to discriminate among various quantum states in either the LG or angular basis.

carefully constructed in a manner designed to trick Eve into revealing her presence. By employing this procedure, it is permitted to use weak classical states (coherent states containing approximately one photon on the average) for encoding the secure information. This procedure is much more readily implemented in the laboratory, and is the method we are using in our laboratory investigations.

6. DISCUSSION AND SUMMARY

A potential limitation to the viability of free-space QKD is the corruption of the quantum state of the received photons as the result of atmospheric turbulence. Several groups[27–30] have studies this issue and have concluded that it is potentially a significant problem. One means of mitigating the problem of atmospheric turbulence is to make use of adaptive optics methods.[31] These methods are well developed and are known to be able to remove classical aberrations from light fields. It seems likely that the coherence of quantum states can also be restored by these methods, although detailed investigation still needs to be conducted.

In summary, by exploiting the transverse degree of freedom of the light field, it is possible to encode many bits of information onto an individual photon. In this work, we have described a procedure for implementing free-space QKD by making use of this ability. We have also presented a report on the status of our program on implementing these ideas in a laboratory setting.

Acknowledgments

We gratefully acknowledge discussions of these topics with Mark Gruneisen, Glenn Tyler, Warner Miller and Miles Padgett. The authors gratefully acknowledge support of the DARPA DSO InPho program.

REFERENCES

1. C. Bennett and G. Brassard, Proceedings of IEEE Inter- national Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175179.
2. A. K. Ekert, Quantum cryptography based on Bells theorem, Phys. Rev. Lett. 67, 661 (1991).
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. 74, 145 (2002).
4. N. Gisin and R. Thew, Quantum communication, Nature Photonics, 1, 165 (2007).
5. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. 81, 1301 (2009).
6. L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes, Phys. Rev. A, 45 8185 (1992).
7. A. Mair, A. Vaziri, G. Weihs and A. Zeilinger, Entanglement of the orbital angular momentum states of photons, Nature, 412, 313 (2001).
8. G. Molina-Terriza, J. P. Torres, and L. Torner, Management of the angular momentum of light: preparation of photons in multidimensional vector states of angular momentum, Phys. Rev. Lett. 88, 013601 (2002).

9. G. Gibson, J. Courtial, M. J. Padgett, M. Vasnetsov, V. Pas'ko, S. M. Barnett, and S. Franke-Arnold, Free-space information transfer using light beams carrying orbital angular momentum, Optics Express, 12, 5448 (2004).
10. H. Bechmann-Pasquinucci and A. Peres, Quantum Cryptography with 3-State Systems, Phys. Rev. Lett. 85, 3313 (2000).
11. M. Bourennane, A. Karlsson, G. Bjork, N. Gisin and N. J Cerf, Quantum key distribution using multilevel encoding: security analysis, J. Phys. A: Math. Gen. 35 10065 (2002).
12. N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using d-Level Systems, Phys. Rev. Lett. 88, 127902 (2002).
13. N. K. Langford, R. B. Dalton, M. D. Harvey, J. L. OBrien, G. J. Pryde, A. Gilchrist, S. D. Bartlett, and A. G. White, Measuring Entangled Qutrits and Their Use for Quantum Bit Commitment, Phys. Rev. Lett. 93, 053601 (2004).
14. S. Groblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger,Experimental quantum cryptography with qutrits, New Journal of Physics 8, 75 (2006).
15. F. M. Spedalieri, Quantum key distribution without reference frame alignment: Exploiting photon orbital angular momentum. Optics Commun. 260, 340 (2006).
16. L. Aolita and S. P. Walborn, Quantum Communication without Alignment using Multiple-Qubit Single-Photon States. Phys. Rev. Lett. 98 100501 (2007).
17. M. Stutz, S. Groblacher, T. Jennewein and A. Zeilinger, How to create and detect N-dimensional entangled photons with an active phase hologram. Appl. Phys. Lett. 90, 261114 (2007).
18. C. E. R. Souza, C. V. S. Borges, A. Z. Khoury, J. A. O. Huguenin, L. Aolita and S. P. Walborn, Quantum key distribution without a shared reference frame, Phys. Rev. A 77, 032345 (2008).
19. J. T. Barreiro, T.-C. Wei and P. G. Kwiat, Beating the channel capacity limit for linear photonic superdense coding, Nat. Phys. 4 282 (2008).
20. W. K. Wootters amd B. D. Fields, Optimal State-Determination by Mutually Unbiased Measurements, Annals of Physics, 191, 363 (1985).
21. M. T. Gruneisen, W. A. Miller, R. C. Dymale and A. M. Sweiti, Holographic generation of complex fields with spatial light modulators: application to quantum key distribution, Appl. Opt. 47, A33 (2008).
22. J Leach, J. Courtial, K. Skeldon, S. M. Barnett, S. Franke-Arnold and M. J. Padgett, Interferometric methods to measure orbital and spin, or the total angular momentum of a single photon, Phys. Rev. Lett. 92, 013601 (2004).
23. G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, Efficient Sorting of Orbital Angular Momentum States of Light, Phys. Rev. Lett. 105, 153601 (2010).
24. M. P. J. Lavery, G. C. G. Berkhout, J. Courtial and M. J. Padgett, Measurement of the light orbital angular momentum spectrum using an optical geometric transformation, J. Opt. 13 (2011).
25. W. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. 91, 057901 (2003).
26. H. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. 94, 230504 (2005).
27. C. Paterson, Atmospheric turbulence and orbital angular momentum of single photons for optical communication, Phys. Rev. Lett. 94, 153901 (2005).
28. C. Gopaul and R. Andrews, The effect of atmospheric turbulence on entangled orbital angular momentum states, New J. of Physics, 9, 94 (2007).
29. G. Gbur and R. K. Tyson, J. Opt. Soc. Am. A, Vortex beam propagation through atmospheric turbulence and topological charge conservation, 25, 255 (2008).
30. G. A. Tyler and R. W. Boyd, Influence of atmospheric turbulence on the propagation of quantum states of light carrying orbital angular momentum, Opt. Lett. 34 142 (2009).
31. See, for instance, the resource letter on adaptive optics for astronomy written by P. W. Milonni, Am. J. Phys. 67 (1999).