PHYSICAL REVIEW A **85**, 060304(R) (2012)

Secure information capacity of photons entangled in many dimensions

Jonathan Leach,[1] Eliot Bolduc,[1] Daniel J. Gauthier,[2] and Robert W. Boyd[1,3]
[1]*Department of Physics, University of Ottawa, Ottawa, Ontario, Canada*
[2]*Department of Physics, Duke University, Durham, North Carolina, USA*
[3]*Institute of Optics, University of Rochester, Rochester, New York, USA*
(Received 9 March 2012; published 28 June 2012)

We quantify precisely the maximum secure information capacity of photons entangled in high dimensions for entanglement in the orbital angular momentum and angular degrees of freedom. Our analysis takes careful account of the influence of experimental imperfections, such as nonunity detection efficiency, on the degree of Einstein-Podolsky-Rosen (EPR) entanglement and hence on the secure information capacity of the photon pairs. We find that there is is an optimal dimension that maximizes the secure information capacity whose value can be predicted analytically from the knowledge of only a few experimental parameters.

DOI: 10.1103/PhysRevA.85.060304 PACS number(s): 03.67.Hk, 03.67.Bg, 03.67.Mn, 42.50.−p

Introduction. Entanglement is one of the defining properties of quantum mechanics and is a key resource for many quantum information protocols. Systems entangled in high dimensions have recently been proposed as a resource for loophole-free tests of nonlocality [1] in addition to providing dense coding for quantum key distribution (QKD) [2–11]. It is therefore important to understand the mechanisms that affect the degree of entanglement in high-dimensional systems.

The characteristic signature of quantum entanglement is the observation of correlations of spatially separated particles in two or more mutually unbiased bases. One can deduce that the particles are entangled provided that the correlations violate appropriate bounds for separability [12]. The degree of violation of the bound is an important quantity in certain quantum information protocols such as QKD. Crucially, it is known that entanglement is a precondition for secure quantum key distribution [13] and that all entangled states contain secret correlations [14].

Quantum key distribution is a protocol that allows two parties, Alice and Bob, to generate a secure key with which to encode a private message [15–17]. In the Ekert protocol for QKD, Alice and Bob make use of pairs of entangled photons. The protocol is secure against attacks by an eavesdropper, who would necessarily have to disturb the system when attempting to intercept the key. QKD implemented in a high dimensionally entangled space provides the advantages of increased information capacity and higher tolerance to eavesdropping [2–11].

Recent work on high-dimensional spatial entanglement has included studies of full-field position and momentum correlations [18,19] and orbital angular momentum (OAM) and angular position correlations [20–24]. Here, the large Hilbert space of the spatial degree of freedom enables increased information-carrying capacity of the photons compared the two-dimensional polarization degree of freedom.

In this Rapid Communication, we demonstrate the relationship between the degree of Einstein-Podolsky-Rosen (EPR) entanglement of high dimensionally entangled photon pairs and their maximal secure information-carrying capacity. The discrete nature of the OAM states allows us to directly control the size of the state space over a wide range. We find that, because of unavoidable experimental imperfections, there exist both an optimal dimension that maximizes the degree of entanglement and a threshold dimension beyond which there is no entanglement and therefore no secure information. By extracting the key parameters that influence our experiment, we provide a model to predict the maximal secure information capacity of general high dimensionally entangled systems.

OAM states, angle states, and entanglement. We consider the OAM modes of light for which there are, in principle, an infinite number of discrete eigenstates. The OAM eigenstates, associated with helical phase fronts $\exp(i\ell\phi)$, are denoted by $|\ell\rangle$. Restricting the size of the state space to a D-dimensional space enables the photons to act as qu$D$its. The specific OAM states we consider in our experiment range from $\ell_{\min} = -[(D-1)/2]$ to $\ell_{\max} = [D/2]$, where $[x]$ is the integer part of x. Consequently, a basis mutually unbiased with respect to the OAM basis is the angle basis in which the eigenstates are defined by [25–27]

$$|\phi\rangle = \frac{1}{\sqrt{D}} \sum_{\ell=\ell_{\min}}^{\ell_{\max}} e^{i\ell\phi}|\ell\rangle. \tag{1}$$

Here, $\phi = 2\pi n/D$ and n is an integer that ranges from 1 to D.

The two photons produced through parametric down-conversion (PDC) are entangled in the OAM and angle degrees of freedom [20–23,28]. The entangled state in the OAM basis is given by

$$|\Psi\rangle = \sum_{\ell=-\infty}^{\infty} c_\ell |\ell_A\rangle|-\ell_B\rangle, \tag{2}$$

where c_ℓ is the complex coefficient of the modes, the range of $|c_\ell|^2$ is considered as the spiral bandwidth, and subscripts A and B refer to the signal and idler modes. We probe the state defined in Eq. (2), and we restrict the dimension of the state space by projecting over a finite range of modes.

Entropic uncertainty relations. To establish the information content present in a high dimensionally entangled system, consider first the implications of an entropic form of the uncertainty principle for a single particle and then for two entangled particles. For a single particle, one form of the uncertainty principle, which relates the entropies of conjugate variables X and Y, is [29,30]

$$H(X) + H(Y) \geqslant \log_2 D. \tag{3}$$

 ©2012 American Physical Society

The Shannon entropy $H(X)$, which is a measure of information content, is defined by

$$H(X) = -\sum_{n=1}^{D} P(x_n) \log_2 P(x_n), \tag{4}$$

where $P(x_n)$ is the probability of the outcome x_n and D is the dimension of the space. As it is not possible for a single particle to violate inequality (3), it follows that one has complete uncertainty regarding one variable [$H(Y)$ or $H(X) = \log_2 D$] if one has complete knowledge about the other [$H(X)$ or $H(Y) = 0$].

Now consider a pair of high dimensionally entangled particles in systems A and B that exhibit correlations in conjugate degrees of freedom. EPR entanglement can be demonstrated by the violation of the entropic uncertainty relation [12,22,31,32],

$$H_{\text{Inf}}(X_B) + H_{\text{Inf}}(Y_B) \geqslant \log_2 D. \tag{5}$$

Here, $H_{\text{Inf}}(X_B) = H(X_B|X_A)$ and $H_{\text{Inf}}(Y_B) = H(Y_B|Y_A)$ are the inferred entropies of B, given precise knowledge of the state of A, for the variables X and Y. For a maximally entangled system with no noise, perfect correlations will be observed [$H_{\text{Inf}}(X_B) = H_{\text{Inf}}(Y_B) = 0$], and the inequality will be maximally violated.

Finally, consider the implications of Eq. (5) for the secure information capacity of photons entangled in the OAM and angle degrees of freedom. The inferred entropies, $H_{\text{Inf}}(X_B)$ and $H_{\text{Inf}}(Y_B)$, become $H_{\text{Inf}}(\ell_B)$ and $H_{\text{Inf}}(\phi_B)$ respectively, when we associate X with the OAM basis and Y with the angle basis. For the most general eavesdropping attack (i.e., a coherent attack) the EPR entanglement condition requires the violation of Eq. (5) to have a secure information capacity greater than zero [4,13,14]. Thus, we reformulate Eq. (5) to provide the upper limit of the secure information capacity measured in bits per photon pair, defined through the relation

$$\Delta I \leqslant \log_2 D - [H_{\text{Inf}}(\ell_B) + H_{\text{Inf}}(\phi_B)]. \tag{6}$$

We note that due to the symmetry of the system and the fact that the OAM and angle measurements are mutually unbiased, Eq. (6) is consistent with the general result of Berta *et al.*, who recently considered the uncertainty principle in the presence of quantum memory [33–35].

Experiment. A brief summary of the experimental procedure is as follows. First, we choose a pump power to set the photon-pair generation rate. Second, we select a dimension size to restrict the number of states in the Hilbert space. Third, we record the coincidence rates for the projective measurements over ranges ℓ_A and $\ell_B \in \{\ell_{\min}, \ldots, \ell_{\max}\}$, and ϕ_A and $\phi_B \in \{2\pi/D, \ldots, 2\pi\}$. From the resulting data set, we calculate the secure information capacity via Eq. (6). The second and third stages are repeated for a range of dimensions. Finally, we repeat the above procedures for a range of different pump powers.

To produce entangled photons, we use a 3-mm-long type I BBO (β barium borate) crystal pumped with mode-locked ultraviolet laser of 150 mW average power and $\lambda = 355$ nm (Xcyte, JDSU); see Fig. 1. We use the first diffracted orders of spatial light modulators (Pluto, Holoeye) in combination with optical fibers, 10-nm bandpass filters (Chroma), and

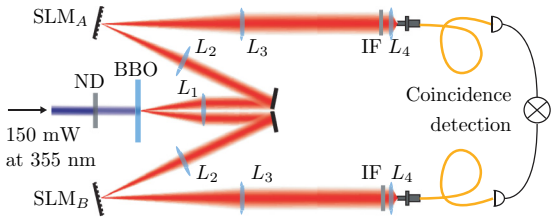

FIG. 1. (Color online) ND, neutral density filter; BBO, β barium borate crystal; SLM, spatial light modulator; IF, interference filter; L_1, 150 mm; L_2, 500 mm; L_3, 1000 mm; and L_4, 1.45 mm. The combination of the lenses L_1 and L_2 (L_3 and L_4), act as a $4f$ imaging system; thus the distance from the crystal to each SLM is 1300 mm (the distance from the SLMs to the fibers is ∼2003 mm).

single-photon avalanche photodiodes (Perkin-Elmer) to make projective mode measurements on the entangled photons. The coincidence counting is performed with a timing resolution of 25 ns (National Instruments, PCI-6601). While faster timing electronics are available, our coincidence electronics enables us to investigate the interplay between coincidence rates arising from correlated and uncorrelated events.

For state-space sizes ranging from $D = 2$ to $D = 31$, we perform projective measurements for all possible combinations of the eigenstates in both the OAM and angle bases. These measurements are repeated for four separate pump powers of 0.47, 1.5, 47, and 150 mW. The coincidence counts in the OAM basis are measured using phase-only holograms and single-mode fibers. The angle-state coincidence counts are measured using multimode fibers with the holograms on the SLMs encoded with both the phase and intensity profile of the mode.

Results. Samples of the measured correlations are shown in Fig. 2. The two identifiable sources of errors in the data are cross-talk events and uncorrelated coincidences that arise from a nonunity heralding efficiency and finite-timing coincidence electronics. To quantify the degree of EPR entanglement, we calculate $H_{\text{Inf}}(\ell_B)$ and $H_{\text{Inf}}(\phi_B)$ for all of the state space sizes and pump powers; see Fig. 3. As a result of the reduced uncorrelated coincidence count rate, the maximal violation occurs with lowest pair generation rate (ND = 1.5). We can see clearly that increasing the state-space size beyond a certain threshold leads to an inability to confirm the entanglement.

Estimation of the secure information. In our model we assume that we generate a maximally entangled state and that the signal and idler arms have identical properties. Thus, the

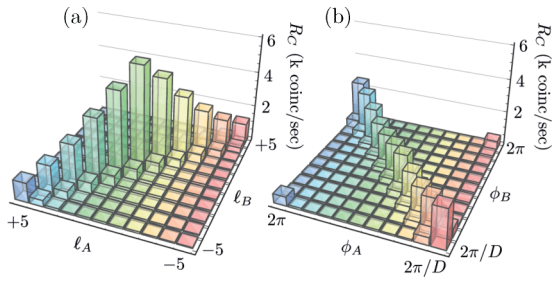

FIG. 2. (Color online) Coincidence count rates for the OAM basis (a) and the angle basis (b) for the case of $D = 11$. For this data set, there is no neutral density filter placed between the pump and the BBO crystal. The integration time for each measurement point is 1 s.

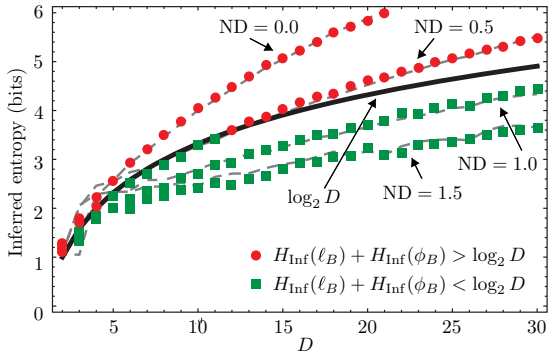

FIG. 3. (Color online) Inferred entropy $H_{\rm Inf}(\ell_B) + H_{\rm Inf}(\phi_B)$ as a function of dimension D and pair generation rate. The green squares represent the conditions where inequality (5) is violated and hence the secure information is greater than zero; the red circles represent the conditions where it is not violated and hence there can be no secure information. The gray dashed lines are the theoretical predictions based on our model.

only sources of error are accidental coincidences and cross talk among measurement channels. The parameters that we include are the heralding efficiency η, the single-photon rates at each detector S, the finite resolution of the timing electronics Δt, and the cross-talk probability P_X. We define cross-talk counts as coincidences measured in the two channels adjacent to the signal channel minus the anticipated uncorrelated coincidences.

The joint detection of a photon at detector A and a photon at detector B results in a coincidence. This can be either a coincidence arising from an entangled photon pair or an accidental coincidence arising from uncorrelated events with a probability $P_U = S(1-\eta)^2\Delta t$. The coincidence rates arising from the entangled pairs R_C, cross talk R_X, and uncorrelated events R_U are given by

$$R_C = S\eta, \quad R_X = R_C P_X, \quad \text{and} \quad R_U = S P_U. \tag{7}$$

Given the assumptions that we have made, the inferred entropies in each basis will be equal. Thus, the calculation of the secure information only requires the inferred entropy in one basis. Assuming $P(x_A) = P(x_B) = 1/D$, the inferred entropy of X_B can be expressed as

$$H_{\rm Inf}(X_B) = -\frac{R_C + R_U}{R_T}\log_2\frac{R_C + R_U}{R_T} - 2\frac{R_X + R_U}{R_T} \times \log_2\frac{R_X + R_U}{R_T} - (D-3)\frac{R_U}{R_T}\log_2\frac{R_U}{R_T}. \tag{8}$$

Here, the total coincidence rate is given by $R_T = R_C + 2R_X + (D \times R_U)$.[1] The first term of Eq. (8) can be associated with coincidences arising from both entangled pairs and uncorrelated events, the second with both cross-talk and uncorrelated events, and the third solely with uncorrelated events. To gain insight as to why we may not violate Eq. (5), we see that to the first approximation, the third term in Eq. (8) causes $H_{\rm Inf}(X_B)$ to increase linearly as a function of the size

[1]For the case of $D = 2$, we include only the first two terms of Eq. (8) and the second term is divided by two.

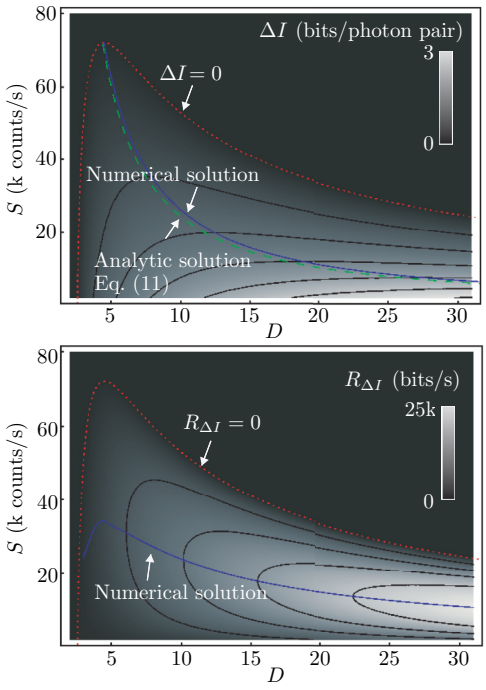

FIG. 4. (Color online) Contour plots of the maximum secure information capacity ΔI and information rate $R_{\Delta I}$ ($\eta = 5\%$, $P_X = 10\%$, and $\Delta t = 25$ ns). The red dotted lines indicate the threshold to achieve a positive ΔI and $R_{\Delta I}$, the green dashed line indicates the analytical solution for the optimal dimension $D_{\rm opt}$ given singles rate S, and the blue solid lines indicate the numerically found maxima.

of the space. As a result, the left-hand side of Eq. (5) will be greater than $\log_2 D$ beyond a certain dimension.

An estimate of the maximum secure information capacity is given by inserting Eq. (8) into Eq. (6) [33]:

$$\Delta I(S,\eta,P_U,P_X,D) \leqslant \log_2 D - 2[H_{\rm Inf}(X_B)]. \tag{9}$$

Equation (9) can be used to determine the experimental conditions that are required to obtain a given level of performance for various situations. For example, the information rate $R_{\Delta I} = S\eta D\Delta I$ measured in bits per sec is most important for QKD, whereas the degree of entanglement ΔI in bits per photon pair is most important for tests of local hidden variable theories. If one is concerned with maximizing $R_{\Delta I}$, one operates in the maximal possible dimension D and then finds the optimal singles rate $S_{\rm opt}$. On the other hand, one operates in the maximal possible dimension D with the lowest possible singles rate S if one is concerned with maximizing ΔI.

For parameters appropriate to our experimental conditions, Fig. 4 illustrates the influence of the singles rate and dimension on the secure information capacity and maximum achievable secure bit rate. Note that for a given singles channel rate, there is a maximum in the secure information capacity that occurs at a specific dimension. By solving $\partial_D \Delta I = 0$ for D, we we find that

$$D_{\rm opt}(P_U,\eta) = \frac{\eta}{P_U}\left(\sqrt{\left(\ln\frac{\eta}{P_U}\right)^2 + 1} - \ln\frac{\eta}{P_U}\right), \tag{10}$$

where we have made use of the approximation $(\eta + P_U)/P_U \approx \eta/P_U$ (see the green dashed line in Fig. 4). Equation (10)

provides the optimal dimension for both ΔI and, to first approximation, the equation scales as $1/S$.

The secure information capacity and maximum secure information rate can fall to zero; the threshold for this behavior is indicated in the figure by the red dotted lines. A secure information capacity of zero occurs at high single-photon rates, where uncorrelated coincidences dominate, and when the dimension of the space is low, where cross talk dominates. In addition, the maximum secure information rate is optimized by maximizing D and then finding the appropriate singles rate S. As $\partial_S R_{\Delta I} = 0$ is not easily solved for S, we numerically solve to find the optimal singles rate for a given dimension.

Conclusions. We experimentally demonstrate the relationship between state-space size and the degree of EPR entanglement for the case of high dimensionally entangled photons. By relating the degree of entanglement of the photon pairs to the maximal secure information-carrying capacity, we find that, because of experimental limitations, there is an optimal dimensionality that maximizes the secure information capacity. Under the conditions of our experiment, the maximum secure information per photon ΔI is 1.3 bits. The model presented here provides a clear pathway for obtaining even larger values of ΔI, for example by using coincidence circuitry with a smaller time window Δt.

Acknowledgments. We thank N. Lütkenhaus for discussions regarding this work. This work was supported by the Canada Excellence Research Chairs (CERC) Program and the DARPA InPho program.

[1] T. Vértesi, S. Pironio, and N. Brunner, Phys. Rev. Lett. **104**, 060401 (2010).
[2] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[3] N. Gisin *et al*., Rev. Mod. Phys. **74**, 145 (2002).
[4] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[5] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[6] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).
[7] J. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Phys. Rev. Lett. **95**, 260501 (2005).
[8] S. Gröblacher *et al*., New J. Phys. **8**, 75 (2006).
[9] I. Ali-Khan and J. C. Howell, Phys. Rev. A **73**, 031801 (2006).
[10] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. **98**, 060503 (2007).
[11] L. Zhang, C. Silberhorn, and I. A. Walmsley, Phys. Rev. Lett. **100**, 110504 (2008).
[12] M. Reid *et al*., Rev. Mod. Phys. **81**, 1727 (2009).
[13] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[14] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
[15] C. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, Ottawa, Canada, 1984), p. 175.
[16] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[17] A. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).
[18] J. Leach *et al*., Phys. Rev. A **85**, 013827 (2012).
[19] P. B. Dixon, G. A. Howland, J. Schneeloch, and J. C. Howell, Phys. Rev. Lett. **108**, 143603 (2012).
[20] A. Mair *et al*., Nature (London) **412**, 313 (2002).
[21] J. Goette, S. Franke-Arnold, and S. M. Barnett, J. Mod. Opt. **53**, 627 (2006).
[22] J. Leach *et al*., Science **329**, 662 (2010).
[23] A. Dada *et al*., Nat. Phys. **7**, 677 (2011).
[24] M. Agnew, J. Leach, M. McLaren, F. S. Roux, and R. W. Boyd, Phys. Rev. A **84**, 062101 (2011).
[25] E. Yao *et al*., Opt. Express **14**, 9071 (2006).
[26] B. Jack, M. Padgett, and S. Franke-Arnold, New J. Phys. **10**, 103013 (2008).
[27] S. Franke-Arnold *et al*., New J. Phys. **6**, 103 (2004).
[28] J. Torres, A. Alexandrescu, and L. Torner, Phys. Rev. A **68** (2003).
[29] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[30] A. Rojas González, J. Vaccaro, and S. M. Barnett, Phys. Rev. A **205**, 247 (1995).
[31] S. Walborn, B. G. Taketani, A. Salles, F. Toscano, and R. L. de Matos Filho, Phys. Rev. Lett. **103**, 160505 (2009).
[32] S. P. Walborn, A. Salles, R. M. Gomes, F. Toscano, and P. H. Souto Ribeiro, Phys. Rev. Lett. **106**, 130402 (2011).
[33] M. Berta *et al*., Nat. Phys. **6**, 659 (2010).
[34] Prevedel *et al*., Nat. Phys. **7**, 757 (2011).
[35] C. F. Li *et al*., Nat. Phys. **7**, 752 (2011).