High-capacity quantum Fibonacci coding for key distribution

David S. Simon,[1,2] Nate Lawrence,[2] Jacob Trevino,[3] Luca Dal Negro,[2,3,*] and Alexander V. Sergienko[2,4,†]

[1]*Department of Physics and Astronomy, Stonehill College, 320 Washington Street, Easton, Massachusetts 02357, USA*

[2]*Department of Electrical and Computer Engineering & Photonics Center, Boston University, 8 Saint Mary's St., Boston, Massachusetts 02215, USA*

[3]*Division of Materials Science & Engineering, Boston University, 15 Saint Mary's St., Brookline, Massachusetts 02446, USA*

[4]*Department of Physics, Boston University, 590 Commonwealth Ave., Boston, Massachusetts 02215, USA*

(Received 25 June 2012; published 11 March 2013)

Quantum cryptography and quantum key distribution (QKD) have been the most successful applications of quantum information processing, highlighting the unique capability of quantum mechanics, through the no-cloning theorem, to securely share encryption keys between two parties. Here, we present an approach to high-capacity, high-efficiency QKD by exploiting cross-disciplinary ideas from quantum information theory and the theory of light scattering of aperiodic photonic media. We propose a unique type of entangled-photon source, as well as a physical mechanism for efficiently sharing keys. The key-sharing protocol combines entanglement with the mathematical properties of a recursive sequence to allow a realization of the physical conditions necessary for implementation of the no-cloning principle for QKD, while the source produces entangled photons whose orbital angular momenta (OAM) are in a superposition of Fibonacci numbers. The source is used to implement a particular physical realization of the protocol by randomly encoding the Fibonacci sequence onto entangled OAM states, allowing secure generation of long keys from few photons. Unlike in polarization-based protocols, reference frame alignment is unnecessary, while the required experimental setup is simpler than other OAM-based protocols capable of achieving the same capacity and its complexity grows less rapidly with increasing range of OAM used.

DOI: 10.1103/PhysRevA.87.032312 PACS number(s): 03.67.Dd, 42.25.Fx, 42.50.Tx, 62.23.St

I. INTRODUCTION

Much recent work in quantum key distribution (QKD) has shifted from the use of two-dimensional polarization spaces to larger Hilbert spaces. Increasing the dimension of the effective Hilbert space increases coding capacity, as well as allowing use of higher-dimensional nonorthogonal bases in security checks, thereby increasing detectable eavesdropper-induced error rates [1–5]. The most promising way to achieve larger Hilbert spaces is via optical orbital angular momentum (OAM) [6–8]. However, the only practical way to produce entangled OAM states is with spontaneous parametric down-conversion (SPDC), in which generating efficiencies drop rapidly with increasing OAM. The complexity of the apparatus for using such high-dimensional states in applications also increases rapidly with the size of Hilbert space.

Recently, optical beams carrying single OAM states have been produced using planar plasmonic interfaces [9]. Distinctive scattering resonances in nanoplasmonic Vogel spiral arrays have also been demonstrated to carry OAM modes [10]. Vogel spirals have been shown to support photonic band gaps with band-edge modes carrying multiple OAM values distributed among the Fibonacci numbers [11,12]. It has been analytically demonstrated that Vogel spiral arrays can generate multiple OAM states encoding well-defined numerical sequences in their far-field radiation patterns [13]. In the case of golden angle (GA) spirals, the generated states carry OAM that follow the Fibonacci sequence. (Recall that the Fibonacci sequence [14] obeys the recurrence relation $F_n = F_{n-1} + F_{n-2}$, with initial values $F_1 = 1$ and $F_2 = 2$.)

Here, we propose a different type of entangled QKD protocol which makes use of the automatic appearance of nonorthogonal states in the intermediate stages, formed from superpositions of elements arising randomly from among a fixed discrete set. Although the general principle behind the protocol can be applied using other physical degrees of freedom, such as phase, we will primarily focus on illustrating the idea here using optical OAM states. A source of entangled Fibonacci-valued OAM states based on a Vogel spiral is arranged so that these nonorthogonal states naturally appear and randomly change with each entangled pair. The protocol works due to combined action of the random nonorthogonal intermediate states together with the fact that if one participant receives a particular Fibonacci number, there is still a twofold uncertainty in the Fibonacci number the other receives. We combine a GA spiral array with SPDC in a nonlinear crystal to engineer a source of entangled light, producing photon pairs whose OAM values always sum to a Fibonacci number, allowing efficient production of states with large OAM values that can be exploited in new ways. We show that the properties of these states *allow encryption keys with large numbers of digits to be generated by much smaller numbers of photons*, exceeding the two bits per photon provided by quantum dense coding [15], while maintaining high security.

The proposed Fibonacci protocol has a number of advantages. Please note the following, for example: (i) The protocol is high capacity in the sense that it allows secure generation of long keys from few photons. The number of digits of the key that can be carried per photon is limited only by practical considerations, not by any matter of principle. (ii) If carried out in free space, irrelevant photons coming from ambient light

*dalnegro@bu.edu
†alexserg@bu.edu

tend to be automatically screened out since only photons with Fibonacci-valued OAM (or other physical degree of freedom) contribute. (iii) Fewer of the detected entangled pairs have to be discarded by the legitimate users after basis comparison than is the case in BB84 or E91 protocols (see Sec. IV). Combined with the increased key capacity per photon and the ability to vary the detection bases in a passive and automatic manner (see the next paragraph), this has potential to greatly speed up key generation rates. (iv) Beyond the first few, the Fibonacci numbers have gaps between them, greatly reducing misattribution errors. (v) From a purely mathematical point of view, Fibonacci coding is more efficient than binary coding for some purposes [16]. (vii) Unlike the case in polarization-based QKD, no reference frame alignment is needed.

A further significant advantage of the procedure to be described is as follows. Any OAM-based analog of standard QKD protocols, with randomly modulated preparation and detection bases, for high values (say up to $l = 100$) of OAM would require active modulation of bases in a 100-dimensional space, and this modulation needs to be done after each trial. This would be extremely complicated; even for a three-state basis, the procedure used in [5], for example, involves actively displacing multiple holograms by precise amounts. Increasing the size of the basis would correspondingly increase the complexity, making the use of very large bases prohibitively difficult. For such high-dimensional spaces, the protocol described here involves a technically much simpler procedure: modulation only occurs *between two fixed bases*, and can be done passively by means of beam splitters with appropriate reflection and transmission coefficients. Going to larger basis sets involves only the addition of more detectors and beam splitters and (if the detection procedure of Sec. VI is used) additional images superimposed on a hologram.

The outline of the paper is as follows. We describe the most general setting in Sec. II, before narrowing our focus to the specific implementation involving Fibonacci-valued OAM for the remainder of the paper. In Sec. III, we describe the source of Fibonacci-valued OAM-entangled photon pairs, before explaining in detail the QKD protocol in Sec. IV. For most trials, the classical information exchange between the two users of the system simply requires them to tell each other which measurement basis was used on the trial; however, on some of the trials some additional information is needed. One way of exchanging this information while minimizing the useful information gained by unauthorized parties listening in on the classical channel is discussed in Sec. V. Section VI describes briefly describes one possible means of detecting and sorting the OAM superposition states required for the protocol, with more detailed explanation in the Appendix. It is then shown in Sec. VII that the capacity of the system can be doubled by one additional change to the setup. Brief discussion of turbulence effects and OAM sorting errors is given in Sec. VIII, before discussion and conclusions in Sec. IX.

II. GENERAL APPROACH

Consider some physical variable x; for example OAM, phase, frequency, time, etc. Appropriate filters can be placed at the input of a down-conversion crystal, selecting out some discrete subset of x values $X_{\text{in}} = \{x_1, x_2, \ldots, x_N\}$. Filters at output (identical filters in both outgoing beams) similarly select out a set of values $X_{\text{out}} = \{x'_1, x'_2, \ldots, x'_N\}$ in such a way that each element of X_{in} can uniquely be written as a sum of two elements in X_{out}. If x is a conserved quantity, then we know that the ingoing value x_n and the outgoing values x'_{m_1} and x'_{m_2} must obey

$$x_n = x'_{m_1} + x'_{m_2}. \tag{1}$$

If x is not conserved, then some additional means must be implemented to enforce such a relation. More generally, we could replace the summation requirement of Eq. (1) by any relation of the form $x_n = f(x'_{m_1}, x'_{m_2})$ with some function $f(x,y)$ which is only required to be single-valued and symmetric, $f(x,y) = f(y,x)$. However, we will restrict ourselves to the linear relation of Eq. (1). The incoming value then determines the two outgoing values; but, *which* of the outgoing photons has which value is not determined, so that bipartite outgoing states carrying these values will be entangled. This ordering ambiguity is the key to much that follows in Sec. IV. Under these conditions, regardless of the physical nature of the variable x, the protocol then proceeds as described in the next section. Only the means of enforcing the summation condition and the means of carrying out the sorting and detection will differ for different physical variables.

If X_{in} and X_{out} are taken to be subsets of the same larger set X ($X_{\text{in}}, X_{\text{out}} \subset X$), then a very natural way to satisfy the relation (1) is to let X be a collection of consecutive Fibonacci numbers, in which the Fibonacci recurrence relation $F_n = F_{n-1} + F_{n-2}$ automatically enforces the required relationship. This is the case we will focus on here, although it should be noted that any other two-term recurrence relation will work just as well.

We now focus specifically on the details of the protocol using the Fibonacci relation. This relation can be imprinted on a number of physical variables, but we will illustrate the idea by concentrating on the specific case of photon orbital angular momentum. This not only provides an example in which the physics is simple and where a conservation law is available to automatically enforce the summation relation of Eq. (1), but it also allows an opportunity to illustrate the use of a different type of entangled OAM source based on scattering from Fibonacci spirals combined with spontaneous parametric down-conversion.

III. ENTANGLED FIBONACCI SPIRAL SOURCE

Before describing the proposed QKD protocol, we discuss a different entangled light source which may be used to physically implement the OAM-based realization of it. A Vogel spiral is an array of N particles with polar positions (r_n, θ_n) given in terms of scaling factor a_0 and divergence angle α by $r_n = \sqrt{n} a_0$ and $\theta_n = n\alpha$. An array of point scatterers, as in Fig. 1(a), is then represented by a density function:

$$\rho(r,\theta) = \sum_{n=1}^{N} \delta(r - \sqrt{n} a_0)\delta(\theta - n\alpha). \tag{2}$$

The Fraunhofer far field of Vogel spirals can be calculated analytically, within scalar diffraction theory, for arbitrary α and a_0 [13]. In cylindrical coordinates, the far field of a diffracted

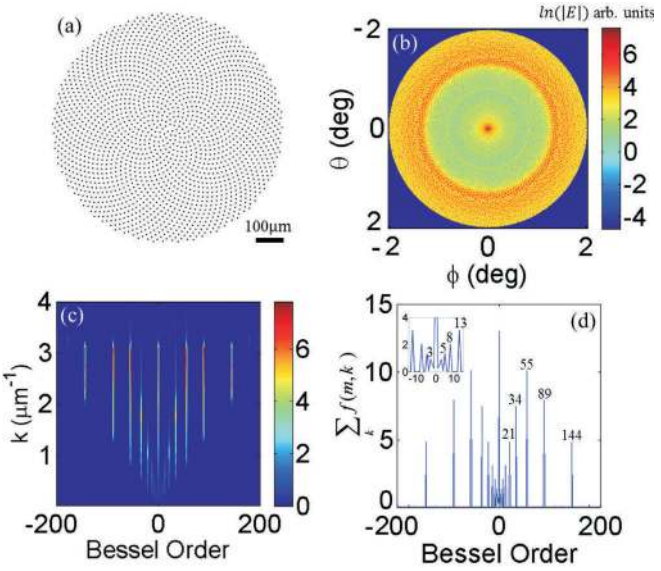

FIG. 1. (Color online.) (a) Schematic of GA spiral Fibonacci OAM generator. (b) Far-field pattern of GA spiral within a 2° half-angle cone for a structure with 2000 particles and $a_0 = 9.28\ \mu$m at 405 nm. (c) Hankel transform of image in (b). (d) Sum of (c) over k, with peaks at Fibonacci values.

input beam is [13]

$$E_\infty(\nu_r,\nu_\theta) = E_0 \sum_{n=1}^{N} e^{j2\pi\sqrt{n}a_0\nu_r\cos(\nu_\theta - n\alpha)}, \tag{3}$$

where (ν_r,ν_θ) are the Fourier conjugate variables of (r,θ). As seen in Fig. 1(c), Fourier-Hankel analysis of the calculated far-field radiation [Fig. 1(b)] is performed to decompose it into radial and azimuthal components, providing the OAM values [11,13,17]. We see in Fig. 1(d) that for GA spirals, the OAM azimuthal numbers follow the Fibonacci sequence. This follows directly from the geometrical properties of GA spirals encoded in the far-field patterns [11,13]. Figure 2 then shows a schematic of our full QKD setup, in which the properties of the spiral source lead to a different approach to high-capacity QKD. Filters after the crystal can be used to equalize the probability of detecting different Fibonacci numbers, compensating for the different production amplitudes seen in Fig. 1(d).

Although down-conversion offers low-pair-production rates, and the post-selection involved in the protocol described below will lower the output rate further, it should be noted that the spiral source can be strongly pumped. When combined with the fact that multiple digits of the key can be produced with a single photon pair, the number of pairs needed to generate a key of given length can be made competitive to the number needed in other entanglement-based protocols, which also involve post-selection and low-production rates.

IV. FIBONACCI PROTOCOL WITH OAM STATES

In E91 [18] and BB84 [19] protocols, photon polarization provides digits of a key (assigning, for example, 1 to horizontal polarization and 0 to vertical) and also provides security against eavesdropping: Alice and Bob each randomly pick

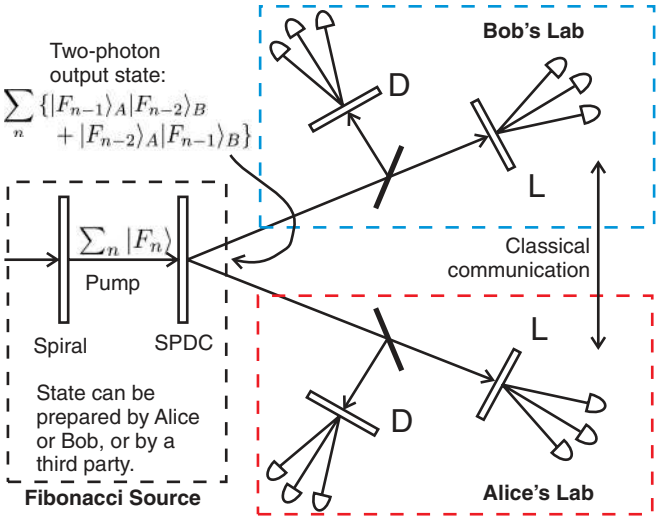

FIG. 2. (Color online.) Setup for QKD with Fibonacci-valued OAM. A laser interacts with a Vogel spiral array, producing intense superpositions of states with Fibonacci OAM, $l = F_n$, that then pump the nonlinear crystal, producing signal-idler pairs through SPDC. The OAM sorters (labeled L) are arranged to only allow photons to reach the arrays of single-photon detectors if they also are Fibonacci valued. Similarly, the devices labeled D only allow passage of allowed "diagonal" superpositions of the form $\frac{1}{\sqrt{2}}(|F_n\rangle + |F_{n+2}\rangle)$.

one of two complementary bases in which to measure the photon polarization, keeping only photons for which the bases match. Eavesdropping is detectable by a drop in polarization correlations. OAM analogs of these protocols work in a similar manner, but with increased key generation capacity [2–5], allowing multiple-digit segments of key to be transmitted by a single photon. The increasing capacity in the latter case is, however, accompanied by a much greater degree of technical complication.

In the present case, light coming from the entangle spiral source of the previous section will be in a superposition of states with OAM equal to Fibonacci numbers. For the protocol, we choose N consecutive Fibonacci values $\mathcal{F} = \{F_{n_0}, F_{n_0+1}, \ldots, F_{n_0+N-1}\}$, and assign a block of binary digits to each in such a way that equal numbers of 0′s and 1′s occur. If OAM values in this set are used, each photon generates enough digits to encode $\log_2 N$ bits of information. Here, we assume $N = 8$ to illustrate the potential for high capacity. For example, the Fibonacci numbers from 3 to 89 may be assigned three-digit blocks as follows:

$$\begin{array}{llll} 3 = 000 & 8 = 010 & 21 = 100 & 55 = 110 \\ 5 = 001 & 13 = 011 & 34 = 101 & 89 = 111. \end{array} \tag{4}$$

Three digits of the key are then carried by the OAM of each photon. The SPDC spiral bandwidth (the range of OAM values) must be sufficient to span the largest gap in $\mathcal{F}$. The entangled OAM bandwidths that can be reached experimentally are increasing rapidly; for example, a down-conversion bandwidth of over 40 has been achieved in [20], and recently entanglement between photons with OAM on the order of 600 has been demonstrated [21]. So, the values used here are well within current practicality. Greater bandwidths

allow larger sets $\mathcal{F}$, increasing the information capacity. For simplicity, assume here that OAM sorters [22–24] only allow positive OAM values to reach the detectors. (We remove this restriction below.)

The setup is shown in Fig. 2. The Fibonacci source may belong to either Alice or Bob, or to a third party, with each of the two legitimate participants, Alice and Bob, receiving half of each entangled pair on which to make their measurements. In each of the two laboratories, there is a beam splitter directing some fixed proportion of the beam to an OAM sorter (L) and the remainder to a different type of detection stage (D). This second arrangement D is designed to detect various pairwise OAM superpositions of the form $|F_n\rangle + |F_{n+2}\rangle$. (See Sec. VI below for more detail on how the D-type superposition states sorting can be accomplished.) The sorters are arranged to direct any non-Fibonacci values away from the detectors.

The states leaving the spiral and entering the down-conversion crystal are superposition states of the form $\sum_{n=n_0}^{n_0+N-1} |F_n\rangle$. Down-conversion breaks each F_n into two lower OAM values. The outgoing values are not *a priori* Fibonacci valued, but OAM sorters can be arranged to block any outgoing states that are not Fibonacci, and more specifically, to block any values that are not in $\mathcal{F}$. (Thus, any values not in $\mathcal{F}$ at *either* the transmission or detection end are blocked; this protects against various possible problems, such as turbulence-induced OAM changes, that could arise otherwise.) For collinear SPDC (either type I or type II), OAM conservation implies $F_{n_i} + F_{n_s} = F_n$. Together with Fibonacci recurrence relation and the restriction to outgoing values in $\mathcal{F}$, this forces F_{n_i} and F_{n_s} to be the two Fibonacci numbers immediately preceding F_n: the signal and idler values are F_{n-1} and F_{n-2}. However, either value can be in either beam, so the result is an *OAM-entangled* outgoing state:

$$\sum_n \{|F_{n-1}\rangle_A |F_{n-2}\rangle_B + |F_{n-1}\rangle_A |F_{n-2}\rangle_B\}. \tag{5}$$

Note that if pump values F_n between 3 and 89 are used, then only values of F_{n_i} and F_{n_s} between 1 and 54 should appear.

In the absence of eavesdropping, there are three possible cases for the outcomes at Alice's and Bob's detectors:

(1) *The beam splitters in both laboratories send the two photons to the L sorters*. So, both Alice and Bob detect a definite OAM value. If Alice measures value F_m, then Bob must measure either F_{m-1} or F_{m+1}. Exchange of a single bit of information each way (using the scheme described in Sec. V, for example) allows them to determine each other's values, and therefore the pump value. The exchange carries some information about Alice's and Bob's values, but not enough for anyone listening on the classical line to uniquely determine the key values (see Sec. V for details). Alice and Bob can then reconstruct each other's values, and add them to get the pump value. The pump value can then be used as the key. Or they could instead, by prior arrangement, agree to use either Alice's or Bob's value for the key on trials where both measurements are L type.

(2) *The beam splitter in one laboratory sends the photon to the L sorter, while in the other laboratory the photon goes to the D sorter*. If, for example, Alice (in the L basis) measures value F_m, then Bob (in the D basis) must receive the superposition state $|F_{m-1}\rangle + |F_{m+1}\rangle$. One bit of classical information is exchanged again, but in this case it need not contain *any* information about the outcome, just information about whether each participant detected a given event in the D detectors or the L detectors. Once each knows that the other has detected an event in the opposite detector type, that is sufficient for each to know the other's state. For that segment of the key, they can then agree to use the value obtained by whoever got the L-type signal.

(3) *The beam splitters in both laboratories send the two photons to theD sorters*. In this case, both Alice and Bob receive superposition states, and the pump itself remains a superposition. Alice and Bob can not uniquely determine each other's value or the pump value, so the trial is discarded.

Therefore, only one in four trials has to be discarded, in contrast to BB84 or Ekert protocols, which require discarding half. The classical information exchange carries information about the actual measured values (as opposed to the measurement bases) in only $\frac{1}{3}$ of the trials that are kept.

The states obtained in the L-type measurement are nonorthogonal to the states in the D-type measurement, just as states of the horizontal-vertical basis are nonorthogonal to the diagonal-basis states in the BB84 and Ekert protocols. But, it is an unusual feature of the current case that, while the states that can be detected in the L-type measurement (the OAM eigenstates) form a mutually orthogonal set among themselves, those found in the D-type measurements are not all orthogonal to each other: the latter states form a chain, where each state is nonorthogonal to the two adjacent states in the chain.

If an eavesdropper is acting, say on the photon heading to Bob, she does not know which type of detection (D or L) will occur in Alice's and Bob's laboratories. If Alice measures an eigenstate, then the state arriving at Bob's end should be a superposition, whereas if Alice measures a superposition, then the state heading toward Bob should be an eigenstate. If Eve makes a D-type measurement when Bob's photon is in an L state or if she makes an L-type measurement when Bob's photon is in a D state, a 50% chance of error is introduced into Bob's measurements, which will become apparent when he compares a random subset of his trials with Alice's.

In more detail: (i) Suppose Eve makes a D-type measurement on a photon which is actually in the eigenstate $|F_m\rangle$. She will detect one of the two superpositions $|F_m\rangle + |F_{m-2}\rangle$ or $|F_m\rangle + |F_{m+2}\rangle$, each with 50% probability, and send on a copy of it. If Bob receives one of these superpositions and makes an L measurement, he will see one of the values F_m, F_{m-2}, or F_{m+2}, with respective probabilities of $\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{4}$. In Eve's absence, he should only see F_m with 100% probability.

(ii) On the other hand, suppose Eve makes an L-type measurement on a photon which is actually in the superposition state $|F_m\rangle + |F_{m-2}\rangle$. She will detect one of the two eigenstates $|F_m\rangle$ or $|F_{m-2}\rangle$, each with 50% probability, and send on a copy of it. If Bob receives one of these eigenstates and makes a D measurement, he will see one of the superpositions $|F_m\rangle + |F_{m-2}\rangle$, $|F_m\rangle + |F_{m+2}\rangle$, or $|F_{m-2}\rangle + |F_{m-4}\rangle$, with respective probabilities of $\frac{1}{2}$, $\frac{1}{4}$, $\frac{1}{4}$. In Eve's absence, he should only see $|F_m\rangle + |F_{m-2}\rangle$ with 100% probability.

In either of these two cases, if Eve is acting on a fraction η of the trials, then when Bob compares his results with Alice's, the two will find that their outcomes are inconsistent a fraction

f of the time, where

$$f = (\text{fraction of times Eve interferes}) \times (\text{fraction of times Eve guesses wrong basis}) \times (\text{fraction of time wrong basis leads to error}) \quad (6)$$

$$= \eta \times \left(\tfrac{1}{2}\right) \times \left(\tfrac{1}{2}\right) \quad (7)$$

$$= \frac{\eta}{4}, \quad (8)$$

which is exactly the same as for the BB84 or Eckert protocols.

One potential misconception should be noted at this point, regarding the notion of "orthogonal bases." In standard QKD protocols such as the BB84 and Ekert protocols, two or more sets of bases are used for polarization measurements. These bases are nonorthogonal both in the physical three-dimensional state *and* in the Hilbert space. Each polarization vector defines both a direction in physical space and a state in the Hilbert space; in other words, there is a direct correspondence between directions in the physical plane perpendicular to the propagation direction and directions in the Hilbert space. In the case of orbital angular momentum, this correspondence breaks down: states that are orthogonal in Hilbert space are not necessarily associated to orthogonal vectors in physical space. It is the nonorthogonality of states in *Hilbert space*, not in *physical three-dimensional space*, that is essential to QKD. Exposure of eavesdropping in the protocol presented here uses states that are nonorthogonal to each other in Hilbert space, but these states do not have associated nonorthogonal physical *spatial* vectors.

V. CLASSICAL COMMUNICATION EXCHANGE

As discussed in Sec. IV, on $\frac{2}{3}$ of the trials that survive the basis comparison and sifting the classical and potentially public exchange need only contain information about which measurement basis was used by each party. On the remaining $\frac{1}{3}$ of the surviving trials, the classical exchange must carry some information about the actual values that were measured by Alice and Bob, so that they may reconstruct each other's values. Obviously, this needs to be done in such a way that anyone else listening over the public channel can not also determine the values. We now discuss one way in which this can be done. (Of course, anyone listening on *both* the classical and quantum channels *can* determine the values, but only at the expense of introducing errors and being detected, as described in the last section.)

Imagine a photon with OAM in $\mathcal{F}$ (take $l = F_n = 21$ as an example) entering the crystal. Suppose both Alice and Bob make L-type measurements, so that each obtains an OAM eigenvalue a result. As in Sec. IV, the setup is arranged so that the two OAM values they obtain must be the two Fibonacci values preceding that of the pump ($F_{n-2} = 8$ and $F_{n-1} = 13$ in our example). However, which reaches Bob and which reaches Alice is undetermined, so there are two possibilities [Fig. 3(a)]. Suppose Bob receives $l_i = 8$ and Alice receives $l_s = 13$. Then, Alice does not know if Bob has 8 or 21 (the value before hers, or the one after). Similarly, Bob does not know if Alice has 5 or 13. To determine each other's values, each must send one classical (potentially public) bit to the other. By prior agreement, they can then use either Alice's or Bob's value as one segment of the key, or add their values in order to use the pump value $F_n = 21$.

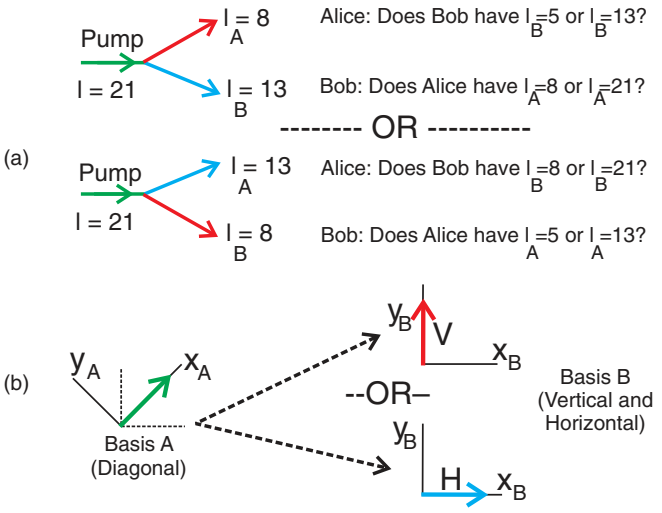

FIG. 3. (Color online.) Possible outcomes (a) for the example of $l = 21$. Neither Alice nor Bob knows the value received by the other; each knows that the two transmitted values must be adjacent Fibonacci numbers, but neither knows if the other's value is larger or smaller than their own. Ambiguity from the superposition of these replaces the ambiguity introduced in standard protocols by the nonorthogonality of the possible polarization bases (b), where a vector along one axis in the A basis could be measured along *either* axis in the B basis.

One possible scheme for the classical information exchange is the following. Alice first sends either a 0 or 1 to Bob in the following manner:

Alice has	1	2	3	5	8	13	21	34	55
Alice sends	0	0	1	1	0	0	1	1	0

(9)

Once Bob receives this information, he can determine Alice's value since he already knows it has to be one of the two values adjacent to his. Then, if he determines that Alice's value is even, he sends one bit to Alice according to the same scheme she used; if Alice's value is odd, he uses the conjugate scheme with zeros and ones interchanged. Alice then has sufficient information to figure out his value as well. But, for an eavesdropper listening in on the classical channel, the information exchanged is insufficient to determine the value since each classical exchange leads to ambiguous results for her:

Eve sees	00	01	10	11
l could be	3,21,34,89	3,5,13,21	8,55,89	5,13,34,55

(10)

(In the top row, the first digit in each pair is the bit sent by Alice, the second is that sent by Bob.) Note that each l value except 8 can be represented by two different classical exchanges, and that each exchange can represent three or four different l values: if Eve intercepts the classical exchange (but not the quantum exchange), she has a probability of only $\frac{1}{4}$ to $\frac{1}{3}$ of correctly guessing the value of F_n, with the *average* probability of a correct guess being 27.08%. This probability drops as the number N of Fibonacci values used increases. Alice and Bob can determine each other's values, while Eve can not.

This is possible only because of the combined action of the entanglement and the use of a recurrence relation.

The classical exchange clearly carries some information about the key, but the setup is designed to keep the mutual information between the outcomes of the classical exchange and those of the photon exchange sufficiently low so that those listening to the public exchange can not uniquely reconstruct the key. This level of mutual information *is*, however, sufficient for the legitimate users since each had already started with half of the needed information.

The protocol utilizes two complementary sources of ambiguity for secure communication: uncertainty in how the OAM Fibonacci state is decomposed between Alice and Bob [Fig. 3(a)] minimizes the information an eavesdropper could obtain from the classical exchange (as discussed above), whereas Eve reveals her interception of the quantum channel through her inability to know which of the two detection bases will be used in Alice's and Bob's labs (as discussed in Sec. IV).

VI. DISTINGUISHING SUPERPOSITIONS

We now look at one way that the D-type sorter required for the OAM-based protocol may be implemented. Any such detection system will need to preserve phases between different OAM basis states contained in the superposition, so that Alice and Bob can avoid being fooled by mistaking an incoherent mixture of eigenstates for the required coherent superposition. Various methods of detecting superpositions can be imagined, with varying degrees of practicality. They all require use of the fact that photons can interfere with themselves. Here, we focus on one particular method, making use of holographic matched filtering; this is essentially a generalization of a method used in [25] to distinguish different images by means of single-photon probes.

The general idea (described in more detail in the Appendix) is to use a multiple-exposure hologram designed to distinguish between several different states of light: each incoming state produces a different output after the hologram. It is important to realize that this can be done at the single-photon level [25]. We will use interference between modes propagating in a single direction, but the hologram can also be used to cause different input states to produce output with different spatial momentum modes, as well. (This was the approach actually used in [25].) Moreover, holograms have been produced which have superpositions of up to 10 000 different patterns [26], allowing the ability to distinguish between very large numbers of different single-photon states. In this way we can easily distinguish between different OAM superpositions. This amounts to designing a device that directly sorts the particular superpositions of interest, rather than the more usual case of devices that sort the eigenstates. This holographic approach is simply an optical implementation of the well-known information processing technique of matched filtering [27]. Also, note that this method works both for the spatially structured photons examined in [25] and for the OAM-structured photons in which we are interested since OAM states are really just states with extended spatial structure in the azimuthal direction. See the Appendix for a more detailed technical description of how the method works.

VII. DOUBLING THE INFORMATION CAPACITY

We assumed above that only positive OAM values were used. The OAM sorters before the detectors in Fig. 1 allow diversion of negative OAM away from the detectors, keeping only positive signal and idler values. This in turn implies that only positive OAM pump photons contribute. However, negative OAM values are also created by the source, at the same rate as the positive values. It is to our advantage to expand the setup to make use of these, rather than letting half of the created photons go to waste. When we do this, we find that the number of bits of key generation per photon can be doubled.

Alice and Bob can record both positive and negative OAM values, and let each other know the signs they received. They then only keep trials on which they received the same signs. Each positive or negative Fibonacci number can then represent a four-digit binary string:

l	Binary string	l	Binary string
3	0000	−3	1000
5	0001	−5	1001
8	0010	−8	1010
13	0011	−13	1011
21	0100	−21	1100
34	0101	−34	1101
55	0110	−55	1110
89	0111	−89	1111

So we now have 16 possible outcomes for the key segment, with each segment capable of encoding 4 bits of information via a single photon.

VIII. TURBULENCE AND MEASUREMENT ERRORS

One important consideration in evaluating the usefulness of any communication channel is the effect of noise on the system, and the error rate produced as a result. In the present case, the main source of noise in the communication channel itself (as opposed to noise in the detection system) is turbulence, which has the effect of adding random spatially varying fluctuations to the phase of the optical wavefront. Like all forms of communication with OAM, the realization of the Fibonacci protocol described in this paper is sensitive to the effects of turbulence, which can turn a single well-defined input OAM value into a broad distribution of outgoing values. In the scheme being discussed, turbulence will introduce losses and thereby decrease the transmission rate; however, the structure of the protocol provides a large measure of protection against errors in the measurement of the photon pairs that survive.

The effects of turbulence on OAM states can be analyzed using the methods described in [28]. We define a conditional probability $P(l|l_0)$ for the detection of OAM value l given that the value l_0 was sent. This probability is given by

$$P(l|l_0) = \frac{1}{2\pi}\int_0^\infty \int_0^{2\pi} R(r,z)C_\phi(r,\Delta\theta)e^{-il\Delta l\ \Delta\theta}dr\ d(\Delta\theta), \tag{11}$$

where

$$C_\phi(r,\Delta\theta) = e^{-\frac{1}{2}D_\phi[|2r\sin(\Delta\theta/2)|]} \tag{12}$$

is the angular coherence function. The phase structure function

$$D_\phi(|\Delta x|) = \langle|\phi(x) - \phi(x+\Delta x)|^2\rangle \tag{13}$$

is given in the Kolmogorov model [29,30] by

$$D_\phi(|\Delta x|) = 6.88\left(\frac{\Delta x}{r_0}\right)^{5/3}. \tag{14}$$

For horizontal line-of-sight communication, the Fried parameter r_0 can be taken to be

$$r_0 = 3.02\left(k^2 z C_n^2\right)^{-3/5}, \tag{15}$$

where $k = \frac{2\pi}{\lambda}$ is the wave number of the photon and C_n^2 is the index of refraction structure constant. Typically, C_n^2 ranges from about 10^{-16}–10^{-17} m$^{-2/3}$ for weak turbulence, to 10^{-12}–10^{-13} m$^{-2/3}$ for strong turbulence. The probability of transmission without an error is then given by $p \equiv P(l_0|l_0)$. The probability of the *particular* error $l_0 \to l_0 + \Delta l$ is $P(l_0 + \Delta l|l_0)$, while the probability of *any* error occurring (for given l_0) is $1 - p$. OAM eigenstates are particularly vulnerable to errors due to turbulence-induced mixing of OAM states; for example, in the case of initial value $l_0 = 0$ (Fig. 4), the probability of error-free propagation drops rapidly with distance in the presence of reasonable turbulence levels, limiting the error-free transmission range to well under a kilometer. The highest probability error is due to the nearest-neighbor transition $\Delta l = 1$, also plotted in Fig. 4, which grows correspondingly with distance. The transition probabilities drop with increasing Δl.

In the present situation, however, only Fibonacci-valued outcomes for l are measured; photons which make transitions to non-Fibonacci values are discarded and do not contribute to the error rate. Thus, only transitions from Fibonacci values to Fibonacci values are relevant, and the dominant transitions are to the nearest Fibonacci-valued neighbors, as in Fig. 5, where the probabilities of transitions from the Fibonacci number $l_0 = 5$ to its nearest Fibonacci neighbors 3 and 8 are plotted versus distance for strong turbulence. Because of the gaps between the Fibonacci numbers and the reduced transition

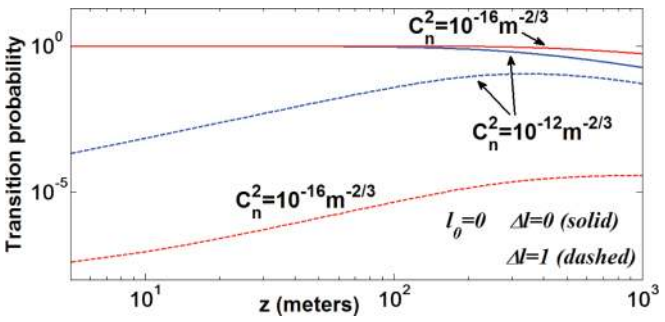

FIG. 4. (Color online) For initial value $l_0 = 0$, probability of measuring values $l = 0$ and 1 versus propagation distance in the presence of turbulence. The solid curves represent the probability of transmission with no error ($\Delta l = 0$), while the dashed curves represent the probability of the dominant $\Delta l = 1$ error. The error probabilities start becoming appreciable after distances on the order of a 100 m for strong turbulence ($C_n^2 = 10^{-12}$ m$^{-2/3}$, blue curves online). For weak turbulence ($C_n^2 = 10^{-12}$ m$^{-2/3}$, red curves online), the errors accumulate more slowly, but still become appreciable after a few kilometers.

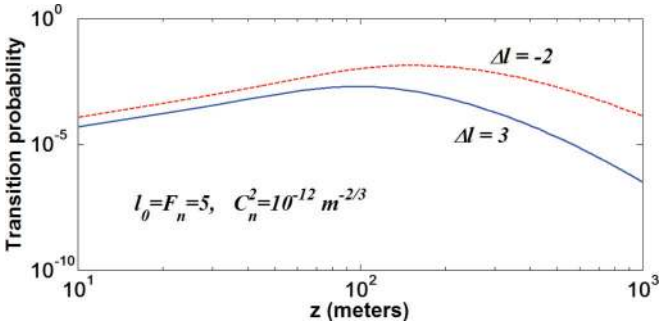

FIG. 5. (Color online) For initial value $l_0 = 5$, probability of measuring values of the nearest Fibonacci-valued neighbors $l = 3$ ($\Delta l = -2$) and $l = 8$ ($\Delta l = +3$). The probabilities are plotted versus distance for strong turbulence ($C_n^2 = 10^{-12}$ m$^{-2/3}$). The error rates are similar to the strong turbulence case of Fig. 4 for $\Delta l = 2$, but an order of magnitude lower for $\Delta l = 3$. They continue to drop rapidly as l_0 increases (see Fig. 6).

probabilities for larger Δl, the error rate is therefore smaller in the Fibonacci scheme than in other OAM-based protocols. The errors are correspondingly smaller as the range of Fibonacci numbers used is shifted to higher values. This is shown in Fig. 6, where nearest Fibonacci neighbor transitions are shown at three distances in the presence of strong turbulence. With each increase in initial $l_0 = F_n$, the probability of a transition to neighboring Fibonacci values decreases significantly. Thus, by avoiding the use of the lowest-lying Fibonacci values in the encoding alphabet, transmission errors can be made negligible.

The process of sorting the OAM values at the end will similarly have reduced errors due to the gaps between the values being used. Once the sorting has been done and the digital OAM values have been converted into binary numbers, the analysis of error rates, error correction, and privacy amplification are identical to those involved in any other QKD protocol.

The price to be paid for the low error rate, of course, will be a high rate of loss: any photons making transitions from Fibonacci to non-Fibonacci values will be lost from the system.

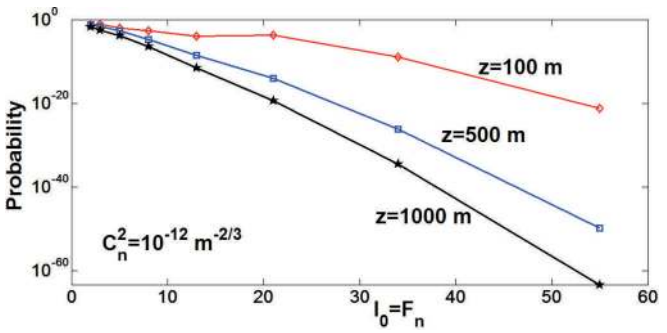

FIG. 6. (Color online) Given initial angular momentum F_n, the probability of measuring values of the next *lower* nearest Fibonacci-valued neighbor $l = F_{n-1}$ at several distances z. The probabilities are plotted versus initial F_n for strong turbulence ($C_n^2 = 10^{-12}$ m$^{-2/3}$). The induced error rates become rapidly smaller as F_n increases. (Note that transitions upward to the next *higher* nearest Fibonacci neighbor can also be obtained from this plot since the probability of $l_0 = F_n \to l = F_{n+1}$ and of $l_0 = F_{n+1} \to l = F_n$ are equal.)

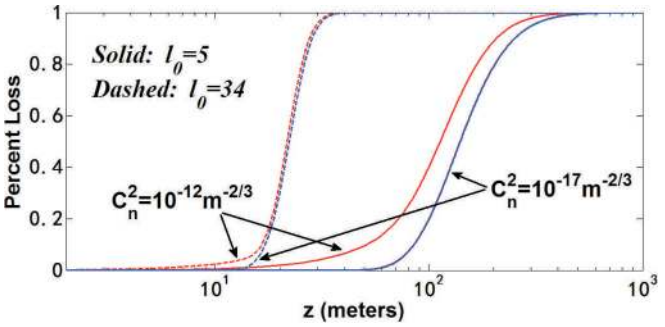

FIG. 7. (Color online) Loss rate versus distance for strong ($C_n^2 = 10^{-12}$ m$^{-2/3}$, red online) and weak ($C_n^2 = 10^{-17}$ m$^{-2/3}$, blue online) turbulence.

Figure 7 plots these transmission losses for $l_0 = 5$ and 34 for strong and weak turbulence. We see that the losses accumulate rapidly with distance. This can be compensated for to some extent by the fact that the source can be strongly pumped, putting out a high initial rate of pair production; only one photon pair per pulse needs to survive in order to generate a key segment. But, losses in the presence of turbulence are over 99% after only about 35 m for $l_0 = 34$ and 350–500 km (depending on degree of turbulence) for $l_0 = 5$, so it is clear that the OAM-based realization of the Fibonacci protocol can only be useful for applications involving short distances or situations in which turbulence is expected to be negligible. (This could be the case, for example, if multimode fibers can be engineered that can carry multiple Fibonacci OAM values.) We see from the plot that there is an essential tradeoff involved: use of high-l values can lead to extremely low error rates, but only over short distances, while lower values of l can travel longer distances but at the expense of higher error rates.

We stress again that the basic protocol can be implemented in terms of other degrees of freedom instead of angular momentum. The analysis of losses and transmission errors will be different for each physical implementation since each degree of freedom will have its own unique physical sources of disruption. However, it should be expected that in *all* implementations, there should be low error rates due to the gaps between the allowed values. Implementations based on encoding in phase shifts or time bins, in particular, will be largely immune to the turbulent effects that are the source of so much trouble for free-space angular-momentum-based communication, and so should be much more promising for simultaneously achieving long distances and low error rates.

IX. DISCUSSION AND CONCLUSIONS

We have proposed a different form of high-capacity, high-efficiency quantum cryptography, and described a specific physical realization of it using specially engineered OAM-entangled states of light and the recurrence properties of the Fibonacci sequence. We have also introduced a type of OAM-entangled two-photon source that is capable of producing the states needed for this particular realization of the protocol. The proposed approach is general enough to lead to different QKD implementations using other physical variables aside from OAM, such as by encoding Fibonacci numbers onto phase shifts. This latter variation, which is currently under investigation, is an especially promising avenue due to the fact that phase encoding is more stable against turbulence and other disruptive effects than OAM encoding.

We iterate once again that the basic principles described here are much more general than the specific realization detailed in this paper. For example, the protocol depends only on the structure of the Fibonacci recurrence relation, not on the initial values used: changing the starting values ($F_1 = 1$, $F_2 = 2$) of the sequence does not change anything fundamental. Thus, an identical procedure will also work for the Lucas sequence [14], which obeys the Fibonacci recursion relations but starts from different initial values. More generally, similar protocols can be constructed using other two-term recurrence relations in place of the Fibonacci relation.

Note added in proof. Recently, an experimental verification of the far-field spectrum simulation displayed in Fig. 1 has been published [31].

ACKNOWLEDGMENTS

This research was supported by the DARPA InPho program through US Army Research Office award W911NF-10-1-0404, by the DARPA QUINESS program through US Army Research Office award W31P4Q-12-1-0015, by the AFOSR programs under Award numbers FA9550-10-1-0019 and FA9550-13-1-001, and by NSF Career Award No. ECCS-0846651. The authors are extremely grateful to Professor G. Jaeger for very helpful discussions.

APPENDIX: HOLOGRAPHIC SORTING OF SUPERPOSITIONS

Here, we describe in more detail one method of carrying out the sorting of superposition states that was described in more schematically in Sec. VI. We will eventually want to distinguish between multiple possible objects by matched filtering. But, start first by supposing that we want to compare an unknown object $U_0(x)$ to a *single* known object $C_0(x)$. The setup for forming the hologram is shown in Fig. 8. The object $C_0(\boldsymbol{x}_0)$ is placed in the (x_0, y_0) plane and the blank hologram in the (x, y) plane. The image of the object is superposed with a reference beam $R(\boldsymbol{x})$ in the hologram plane. Assume that the reference beam is a plane wave propagating with wave vector k, which may be at a nonzero angle to the z axis. Then, in the

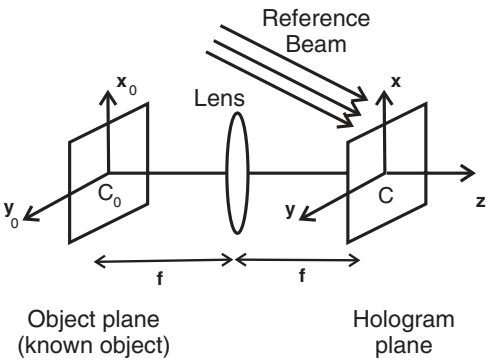

FIG. 8. Creating the hologram. $C_0(\boldsymbol{x})$ is a known object whose Fourier transform is to be stored on the hologram using plane-wave reference beam R.

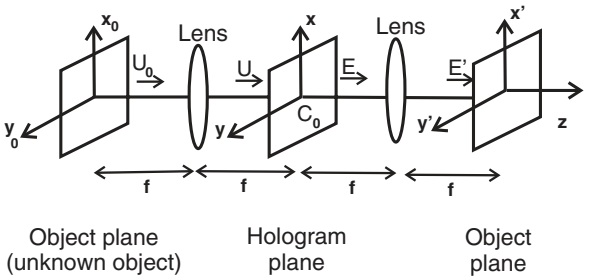

FIG. 9. Using the hologram as matched filter to detect whether an unknown object $U_0(\boldsymbol{x})$ matches the stored object $C(\boldsymbol{x})$.

hologram plane the incident field is

$$E(\boldsymbol{x}) = R(\boldsymbol{x}) + C(\boldsymbol{x}), \tag{A1}$$

where

$$R(\boldsymbol{x}) = R_0 e^{i\boldsymbol{k}\cdot\boldsymbol{x}}, \tag{A2}$$

$$C(\boldsymbol{x}) = -\frac{i}{\lambda f}\int C_0(\boldsymbol{x}) e^{\frac{ik}{f}\boldsymbol{x}\cdot\boldsymbol{x}_0} d^2x_0. \tag{A3}$$

(For simplicity, the fields are treated as scalars here.) The transmittance of the hologram will then be proportional to the incident intensity:

$$t(\boldsymbol{x}) \propto |E(\boldsymbol{x})|^2 \tag{A4}$$

$$= R_0^2 + |C(\boldsymbol{x})|^2 + R_0 C(\boldsymbol{x}) e^{-i\boldsymbol{k}\cdot\boldsymbol{x}} + R_0 C^*(\boldsymbol{x}) e^{i\boldsymbol{k}\cdot\boldsymbol{x}}. \tag{A5}$$

The relevant term is the last one, which we will denote by $t'(\boldsymbol{x})$:

$$t'(\boldsymbol{x}) = R_0 C^*(\boldsymbol{x}) e^{i\boldsymbol{k}\cdot\boldsymbol{x}}. \tag{A6}$$

Once the hologram has been constructed, it is used in the $4f$ setup shown in Fig. 9. Place the unknown object $U_0(\boldsymbol{x}_0)$ in the (x_0, y_0) plane and the previously prepared hologram in the (x, y) plane. The field incident on the hologram from the object is now

$$U(\boldsymbol{x}) = -\frac{i}{\lambda f}\int U_0(\boldsymbol{x}_0')\, e^{\frac{ik}{f}\boldsymbol{x}\cdot\boldsymbol{x}_0'}\, d^2x_0'. \tag{A7}$$

The relevant part of the transmitted field just after the hologram is

$$E(\boldsymbol{x}) = U(\boldsymbol{x})t'(\boldsymbol{x}) \tag{A8}$$

$$= \frac{R_0}{(\lambda f)^2} e^{i\boldsymbol{k}\cdot\boldsymbol{x}} \int U_0(\boldsymbol{x}_0')\, C_0^*(\boldsymbol{x}_0) \times e^{\frac{ik}{f}\boldsymbol{x}\cdot(\boldsymbol{x}_0'-\boldsymbol{x}_0)}\, d^2x_0 d^2x_0'. \tag{A9}$$

The field in the final (x', y') plane is

$$E'(\boldsymbol{x}') = \left(-\frac{i}{\lambda f}\right)\int E(\boldsymbol{x}) e^{\frac{ik}{f}\boldsymbol{x}\cdot\boldsymbol{x}'} d^2x. \tag{A10}$$

Using Eq. (A9) and carrying out the $\boldsymbol{x}$ integration, we have

$$E'(\boldsymbol{x}') = -\left(\frac{4\pi^2 i R_0}{(\lambda f)^3}\right)\int U_0(\boldsymbol{x}_0')\, C_0^*(\boldsymbol{x}_0) \times \delta^{(2)}\left[\frac{k}{f}(\boldsymbol{x}_0' - \boldsymbol{x}_0 + \boldsymbol{x}' + f\hat{\boldsymbol{k}})\right] d^2x_0 d^2x_0' \tag{A11}$$

$$= K\int U_0(\boldsymbol{x}_0' - \boldsymbol{x}_0 + \boldsymbol{x}' + f\hat{\boldsymbol{k}}) \times C_0^*(\boldsymbol{x}_0)\, d^2x_0, \tag{A12}$$

where $K = -\frac{f}{k}\left(\frac{4\pi^2 i R_0}{(\lambda f)^3}\right) = -\frac{2\pi i R_0}{c^2}$ and c is the speed of light.

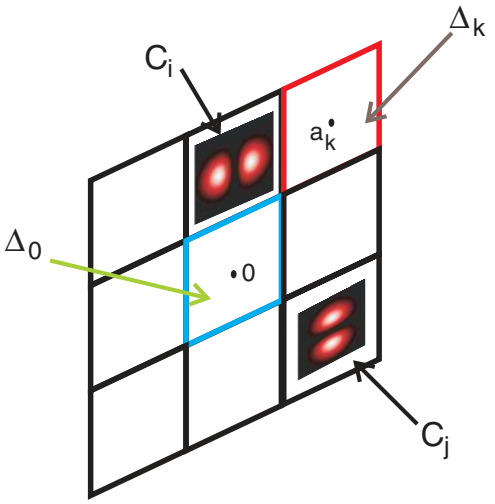

FIG. 10. (Color online) Array of images stored on lattice of nonoverlapping cells, forming a tiling of the hologram. Images $\{C_k\}$ are stored on cells $\{\Delta_k\}$ centered at points $\{\mathbf{a_k}\}$. Each cell is a copy of a unit cell Δ_0 centered at the origin.

Now, suppose that instead of a single object, the image stored on the hologram is of a collection of objects C_i. These images are contained in nonoverlapping cells Δ_i, centered at an array of points $\boldsymbol{a}_i$ (Fig. 10). We will assume that the Δ_i are displaced copies of some Δ_0 centered at the origin. We will assume here that each of the images uses the same reference beam of wave vector $\boldsymbol{k}$, although different reference beams can be used for each if desired. The total stored object is therefore of the form

$$C_0(\boldsymbol{x}) = \sum_k C_k(\boldsymbol{x} + \boldsymbol{a}_k), \tag{A13}$$

where $C_k(\boldsymbol{x} + \boldsymbol{a}_k)$ is nonzero only on Δ_k [or equivalently, $C_k(\boldsymbol{x})$ is nonzero only on Δ_0]. We assume that the C_i are orthogonal to each other in the usual sense,

$$\int C_j(\boldsymbol{x}) C_k(\boldsymbol{x}) d^2x = \delta_{jk} \tag{A14}$$

(so the C_j could be Laguerre-Gauss functions for example) and that Δ_0 is sufficiently large that the orthogonality relation is still approximately true when carried out only over Δ_0; in other words, the images of the C_k drop to approximately zero intensity near the edges of the Δ_k.

Assume now that the unknown object happens to be one of the objects whose images are stored on the hologram; for example, suppose that $U_0(\boldsymbol{x}) = C_j(\boldsymbol{x})$. Inserting the array of stored images, Eq. (A13) into Eq. (A12), we find then that the field at detector j is given by a correlation function which

compares the jth image with all the others,

$$E'_j(\boldsymbol{x}') = K\sum_k \int C_j(\boldsymbol{x}_0 - \boldsymbol{x}' + f\hat{k})C_k^*(\boldsymbol{x}_0 + \boldsymbol{a}_k)d^2x_0$$
$$= K\sum_k \int C_j(\boldsymbol{x}_0)C_k^*(\boldsymbol{x}_0 + \boldsymbol{a}_k + \boldsymbol{x}' - f\hat{k})d^2x_0.$$

Suppose we place a set of detectors in the output plane at an array of points given by $x'_n = f\hat{\boldsymbol{k}} - \boldsymbol{a}_n$, for $n = 1,2,\ldots$. Then,

$$E'_j(\boldsymbol{x}'_n) = K\sum_k \int C_j(\boldsymbol{x}_0)C_k^*(\boldsymbol{x}_0 + \boldsymbol{a}_k - \boldsymbol{a}_n)d^2x_0. \quad \text{(A15)}$$

The C_j and C_k functions will only be nonzero at the same time if they are evaluated in the same Δ_k; this forces $\boldsymbol{a}_k = \boldsymbol{a}_n$, and so $k = n$:

$$E'_j(\boldsymbol{x}'_n) = K\int C_j(\boldsymbol{x}_0)C_n^*(\boldsymbol{x}_0)d^2x_0. \quad \text{(A16)}$$

But, by the orthogonality relation, we finally have

$$E'_j(\boldsymbol{x}'_n) = K\delta_{jn}. \quad \text{(A17)}$$

Thus, only one of the detectors will fire, and which one fires will identify which of the $\{C_k\}$ the object was.

To detect the desired superposition, we then carry out the following procedure. First note from Eq. (A17) that regardless of the input OAM, the output field from the hologram is (approximately) constant over the area of the given cell; thus, these output fields carry no OAM. Since these outputs all have $l = 0$ and the same propagation direction, they are indistinguishable except for their exit location. So, if we erase the information about which cell the output leaves, then the two possibilities in each superposition state will be able to interfere with each other. We may replace the detectors at the different possible output locations by pinholes, then allow the light from these pinholes to fall on an opaque screen or on a detector. If there are two possible paths the photon could have taken (two OAM eigenstates in the superposition) and therefore the photon could have exited through either of two pinholes, then these two possibilities will constructively interfere only at certain possible locations on the screen. We can easily arrange for the interference maxima from different pinhole pairs to be located at distinct positions from the maxima for other pairs. If necessary, phase shifts can be added selectively before some of the pinholes to steer the maxima to locations where they can be more easily distinguished. Thus, from the locations of the detections at the final outputs, we can determine which two OAM components were present in the incoming superposition. This effectively acts as a sorter for superposition states. Note that an incoherent mixture of photons will not produce the required interference pattern.

[1] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[2] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[3] M. Bourennane, A. Karlsson, and G. Björk, Phys. Rev. A **64**, 012306 (2001).
[4] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[5] S. Groblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, New J. Phys. **8**, 1 (2006).
[6] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, Phys. Rev. A **45**, 8185 (1992).
[7] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature (London) **412**, 313 (2001).
[8] A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **89**, 240401 (2002).
[9] N. Yu, P. Genevet, M. A. Kats, F. Aieta, J-P. Tetienne, F. Capasso, and Z. Gaburro, Science **334**, 333 (2011).
[10] J. Trevino, H. Cao, and L. Dal Negro, Nano Lett. **11**, 2008 (2011).
[11] S. F. Liew, H. Noh, J. Trevino, L. Dal Negro, and H. Cao, Opt. Express **19**, 23631 (2011).
[12] J. Trevino, S. F. Liew, H. Noh, H. Cao, and L. Dal Negro, Opt. Express **20**, 3015 (2012).
[13] L. Dal Negro, J. Trevino, and N. Lawrence, Opt. Express **20**, 18209 (2012).
[14] T. Koshy, *Fibonacci and Lucas Numbers with Applications* (Wiley, New York, 2001).
[15] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[16] S. T. Klein and M. K. Ben-Nissan, Comput. J. **53**, 701 (2010).
[17] N. Lawrence, J. Trevino, and L. Dal Negro, J. Appl. Phys. **111**, 113101 (2012).
[18] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[19] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 1984* (IEEE Computer Society Press, Los Alamitos, CA, 1984), p. 175.
[20] J. Romero, D. Giovannini, S. Franke-Arnold, S. M. Barnett, and M. J. Padgett, arXiv:1205.1968v1.
[21] R. Fickler, R. Lapkiewicz, W. N. Plick, M. Krenn, C. Schaeff, S. Ramelow, and A. Zeilinger, Science **338**, 640 (2012).
[22] J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial, Phys. Rev. Lett. **88**, 257901 (2002).
[23] G. C. G. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, Phys. Rev. Lett. **105**, 153601 (2010).
[24] M. P. J. Lavery, D. J. Robertson, G. C. G. Berkhout, G. D. Love, M. J. Padgett, and J. Courtial, Opt. Express **20**, 2110 (2012).
[25] C. J. Broadbent, P. Zerom, H. Shin, J. C. Howell, and R. W. Boyd, Phys. Rev. A **79**, 033802 (2009).
[26] X. An, D. Psaltis, and G. W. Burr, Appl. Opt. **38**, 386 (1999).
[27] G. L. Turin, IEEE Trans. Info. Th. **6**, 311 (1960).
[28] C. Paterson, Phys. Rev. Lett. **94**, 153901 (2005).
[29] L. C. Andrews and R. L. Philips, *Laser Beam Propaga- tion through Random Media*, 2nd ed. (SPIE, Bellingham, WA, 2005).
[30] M. C. Roggemann and B. M. Welsh, *Imaging Through Turbulence* (CRC Press, Boca Raton, FL, 1996).
[31] N. Lawrence, J. Trevino, and L. Dal Negro, Opt. Lett. **37**, 5076 (2012).