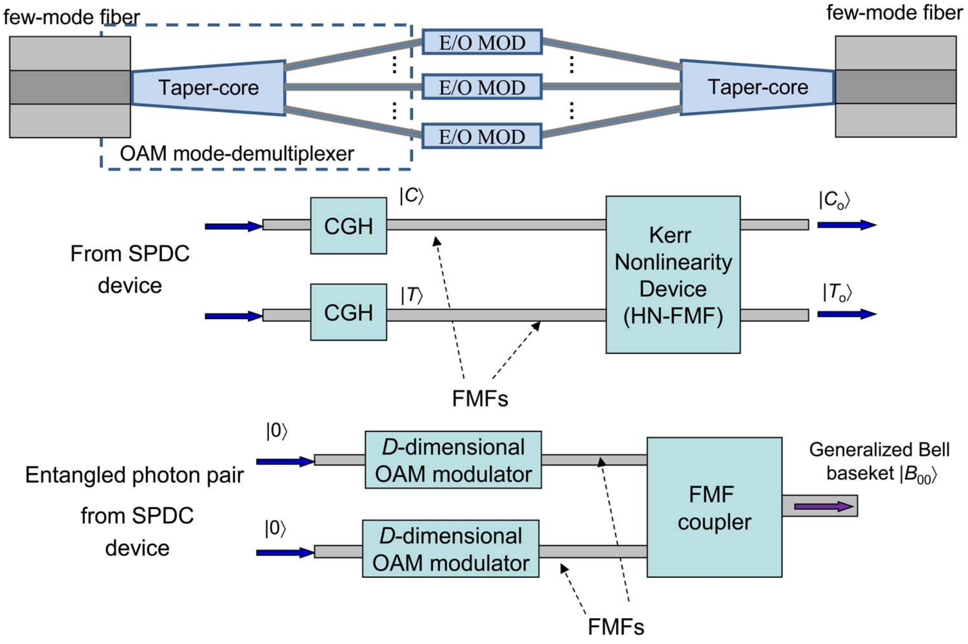
IEEE Photonics Journal
An IEEE Photonics Society Publication

Open Access

Multidimensional QKD Based on Combined Orbital and Spin Angular Momenta of Photon

Volume 5, Number 6, December 2013

Ivan B. Djordjevic



DOI: 10.1109/JPHOT.2013.2292301
1943-0655 © 2013 IEEE

Multidimensional QKD Based on Combined Orbital and Spin Angular Momenta of Photon

Ivan B. Djordjevic

Department of Electrical and Computer Engineering, University of Arizona, Tucson AZ 85721 USA
College of Optical Sciences, University of Arizona, Tucson AZ 85721 USA
Department Electrical Engineering and Information Technology, Technische Universität Darmstadt, 64283 Darmstadt, Germany

DOI: 10.1109/JPHOT.2013.2292301
1943-0655 ©2013 IEEE

Manuscript received October 7, 2013; revised November 8, 2013; accepted November 10, 2013. Date of publication November 21, 2013; date of current version December 3, 2013. This work was supported in part by the National Science Foundation (NSF) CAREER Grant CCF-0952711. Corresponding author: I. B. Djordjevic (e-mail: ivan@email.arizona.edu).

Abstract: It has been widely recognized that the underlying principles of quantum mechanics could be used to enable secure communications, without any additional conventional cryptographic systems, while utilizing the properties of the photons. Considerable research efforts have been invested to develop an efficient quantum key distribution (QKD) scheme over either free-space optical or fiber-optics channels. Most of these research efforts have been focused on a two-dimensional QKD, commonly realized by the use of the polarization state of photons. However, the data rates for the quantum key exchange in two-dimensional QKD are still low, while transmission distance is limited. On the other hand, it is well known that photons can carry both the spin angular momentum (SAM) and the orbital angular momentum (OAM), associated with the polarization and azimuthal phase of the complex electric field, respectively. Accordingly, we can define the combined-OAM–SAM state of a photon as $|l, \sigma\rangle$, where l and σ correspond to OAM and SAM indexes, respectively. Since the OAM eigenstates are orthogonal, an arbitrary number of bits per single photon can be transmitted, which could considerably increase the total secure bit rate. To improve secure data rates, we propose two types of protocols, namely, nonentangled-based (such as weak coherent state) and entanglement-assisted protocols, both employing the photon combined-OAM–SAM state, which can be used for secure key distribution over free-space optical and few-mode fiber channels. Two types of entanglement-assisted protocols are described, namely, two-basis and $(D+1)$-basis protocols (D is dimensionality of corresponding Hilbert space). We further describe how to implement the qudit gates required for implementation of these protocols. Finally, we discuss the security issues of the proposed protocols and determine both infinite and finite secret key fraction rates.

Index Terms: Quantum information processing (QIP), quantum qudit gates, quantum key distribution (QKD), orbital angular momentum (OAM), spin angular momentum (SAM), low-density parity-check (LDPC) codes.

1. Introduction and Motivation

Quantum information processing (QIP) is an exciting research area with a very wide range of applications including quantum computing, quantum memories, quantum key distribution (QKD), quantum metrology, quantum lithography, and quantum communications [1]–[15]. Unfortunately, the QIP relies on very fragile superposition states, which are highly sensitive to the interactions with the environment, resulting in decoherence and introducing the quantum errors. Therefore, to overcome this problem the use of quantum error-correction is essential. The QKD is probably the most promising concept of quantum information theory. The impossibility for an eavesdropper to tap the quantum channel and distinguish between nonorthogonal states without introducing disturbance to the channel ensures that the QKD system is secure. Even though significant advances have been made recently in QKD research and commercialization, the transmission speed of quantum key exchange is still low, and transmission distance even over optical fiber is still limited. Most research efforts so far have been focused on two-dimensional qubits, implemented based on photon polarization.

Several methods have recently been proposed to increase the information content of photons for quantum communications. These methods rely on encoding information either using time and frequency [16], [17], linear momentum [18], [19], orbital angular momentum (OAM) [20]–[27], or using multiple degrees of freedom made available through hyper-entangled states [28], [29]. Single-photon multidimensional QKD has been implemented using OAM [5], [8], as well as exploiting photon position and linear momentum [30].

Because photons can carry both spin angular momentum (SAM), associated with polarization ($\sigma\hbar = \pm\hbar$, for circular polarization) and OAM $l\hbar$ ($l = 0, \pm 1, \pm 2, \ldots, \pm L, \ldots$), associated with azimuthal phase of the complex electric field $\exp(-\mathrm{j}l\phi)$ [1], [10], the corresponding combined-OAM–SAM state of photon can be denoted as $|l, \sigma\rangle$, where l and σ correspond to OAM and SAM indexes, respectively. The corresponding baskets $|l, \sigma\rangle$ are orthogonal to each other as $\langle m, \sigma | n, \sigma' \rangle = \delta_{mn}\delta_{\sigma\sigma'}$. This notation has certain similarities with hybrid logical qubit notation introduced in [26]. It is possible to exploit nonorthogonal mutually unbiased bases (MUBs), defined on combined-OAM–SAM states, for multidimensional QKD (MQKD). By limiting OAM index l to maximum L, the corresponding space is $D = 2(2L + 1)$-dimensional. The key idea is to use both SAM and OAM MUBs to improve the security against both individual and coherent attacks. Notice that this concept of combined-OAM–SAM photon states is different from the total angular momentum (TAM) of photon defined as $j\hbar = (l + \sigma)\hbar$ and introduced in [10]. The corresponding number of basekets in TAM representation is $2L + 3$, while in combined-OAM–SAM representation introduced above it is $2(2L + 1)$. Since in TAM-notation for instance for $j = 2$ we cannot distinguish between $|l = 3, \sigma = -1\rangle$ and $|l = 1,\ \sigma = 1\rangle$ OAM–SAM states, we prefer the use of combined-OAM–SAM notation. We propose to use either computer generated holograms (CGHs) or few-mode fibers (FMFs) to perform simultaneous amplitude and phase modulation according to the randomly selected MUB and employ the OAM of photons. The second phase is similar to BB84 protocol, where we randomly choose the polarization basis out of computational, diagonal, and circular ones. Notice that it would be possible to define the MUBs by using TAM-basis as described in [10]. However, this approach requires the use of numerous Dove prisms and half-wave plates, while the proposed protocols based on MUBs defined on combined-OAM–SAM states are quite straightforward to implement, as shown in incoming sections. By employing these multidimensional QKD protocols we can significantly increase the threshold for the maximum tolerable rate due to the quantum nature of channel while preventing the possibility of eavesdropping. Various types of photon OAM–SAM based protocols can be categorized into two broad categories: nonentangled-based (such as the weak coherent state) protocols and entanglement-assisted protocols. We will study different strategies for entanglement-assisted protocols, by varying the dimensionality of MUBs and the number of MUBs, which can be categorized into two broad classes of protocols: (i) two-basis protocols, representing a generalization of BB84 protocol; and (ii) $(D + 1)$-basis protocols, representing the generalization of three-basis (six-state) protocol. The classes of type-ii are particularly suitable for various implementations, ranging from purely OAM-based protocols to fully combined-OAM–SAM-based protocols. Once the MQKD protocol is completed, Alice and Bob perform a series of classical steps. The security bounds of these two types of protocols will be provided for both infinitely long and finite secure keys, based on security theory introduced in [4], [12], [13]. As the transmission distance and key distribution speed grow, error correction becomes increasingly important. By performing information reconciliation based on low-density parity check (LDPC) codes constructed using large (high)-girth *irregular* quasi-cyclic code construction techniques, in which irregularity can be precisely controlled, the threshold for maximum tolerable error rate can be improved. Privacy amplification is then performed to eliminate any information obtained by an eavesdropper.

The paper is organized as follows. In Section 2, we describe the nonentanglement-based multidimensional combined-OAM–SAM-based protocols. In Section 3, we discus multidimensional QKD over few-mode fibers, together with corresponding gates required to implement such protocols. The security study of various entanglement-assisted combined-OAM–SAM-based QKD protocols is studied in Section 4. Some important concluding remarks are provided in Section 5.

2. Multidimensional QKD Based on Combined OAM–SAM States of Photons

As we indicated in the introduction, photons can carry both SAM, associated with polarization given by $\sigma\hbar = \pm\hbar$ (for circular polarization); and OAM, associated with azimuthal phase of the complex electric field [5], [7], [10]. Each photon with azimuthal phase dependence of the form $\exp(-jl\phi)$ $(l = 0, \pm 1, \pm 2, \ldots)$ can carry an OAM of $l\hbar$. We can associate with each photon a combined OAM–SAM state $|l, \sigma\rangle$, where l and σ correspond to OAM and SAM indexes. Because OAM eigenstates are orthogonal, in principle, arbitrary number of bits per single photon can be transmitted. The ability to generate/analyze states with different combined-OAM–SAM states, by using holographic methods [5] and polarization-beam splitters, allows the realization of quantum states in multidimensional Hilbert space. Because OAM states provide an infinite basis state, while SAM states are two-dimensional only, OAM can be used to increase security of QKD. The secure transmission in QKD is ensured by employing the MUBs.

We first outline a protocol for multidimensional QKD based on OAM states, which does not require the use of entangled states. The initialization is performed by employing the conventional BB84 protocol to exchange the random seed to be used in MQKD protocol. The sender A (Alice) sends a state by arbitrary selecting one among a number of available OAM MUBs. The receiver B (Bob) performs the measurement in one of OAM MUBs selected at random. Notice that both A and B can first select the dimensionality at random using the same seed (obtained by conventional BB84 protocol, used for initialization), and then select the one of many available OAM MUBs of a given dimension from a look-up table (LUT). The rest of the protocol is similar to BB84 scheme. The security of this protocol has been enhanced by first selecting the OAM MUB at random and then selecting the SAM MUB (out of computational, diagonal, or circular MUBs) again at random, resulting in new MQKD scheme. The basis vectors for OAM based MUB_0 corresponding to the angular momentum $l\ \hbar; l = -L, \ldots, -1, 0, 1, \ldots, L$ can be written as follows:

$$MUB_0 = \{|-L\rangle, \ldots, |-1\rangle, |0\rangle, |1\rangle, \ldots, |L\rangle\}. \tag{1}$$

The base kets are orthogonal to each other

$$\langle m|n\rangle = \delta_{mn}; \quad m, n \in \{-L, \ldots, -1, 0, 1, \ldots, L\} \tag{2}$$

and span the $(2L + 1)$-dimensional Hilbert space H_{2L+1}. Arbitrary sate $|\psi\rangle$ can be represented as linear superposition of base kets

$$|\psi\rangle = \sum_{l=-L}^{L} c_l |l\rangle; \quad \sum_{l=-L}^{L} |c_l|^2 = 1. \tag{3}$$

Any other MUB_i must have for basis kets an orthonormal set and any baseket within it must be equally distributed over the base kets in MUB_0 as follows:

$$|\langle l|l_i\rangle|^2 = 1/(2L + 1); \quad l \in \{-L, \ldots, -1, 0, 1, \ldots, L\}, l_i \in \{-L_i, \ldots, -1, 0, 1, \ldots, L_i\}. \tag{4}$$

One example for $2L + 1 = 3$ is provided in [5]. The second level of our protocol is direct employment of BB84 protocol. The photon SAM basis $\{|0\rangle, |1\rangle\}$, $\{|+\rangle = (|0\rangle + |1\rangle)/\sqrt{(2)}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{(2)}\}$, or $\{(|0\rangle + j|1\rangle)/\sqrt{2}, (|0\rangle - j|1\rangle)/\sqrt{2}\}$ is selected randomly. The arbitrary state is then transmitted over a public quantum optical communication channel (free-space optical or few-mode fiber-optic channels). Therefore, in our combined-OAM–SAM-based QKD we perform two separate random

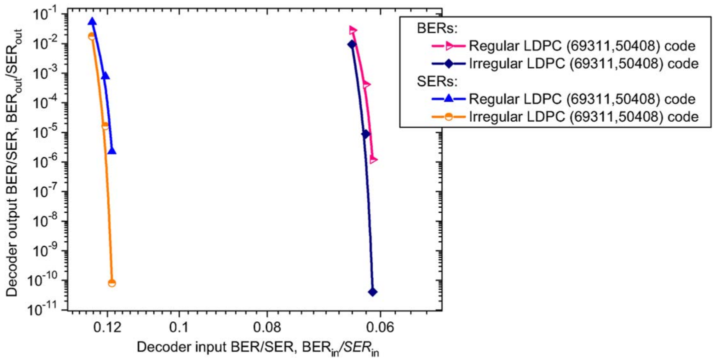


Fig. 1. BER and SER performance of 4-ary LDPC (69311, 50408) code suitable for use in information reconciliation.

bases selections (OAM and SAM). The reason for such approach is to simplify the implementation. To impose OAM states, the CGHs can be used as explained in [5].

For the nonentanglement-based protocol, the sequence to be transmitted over public quantum channel is first LDPC encoded by using a systematic LDPC code of large girth, in which information symbols stay intact while generalized parity-symbols are algebraically related to the information symbols. The information symbols are transmitted over the quantum channel, while the generalized parity symbols are transmitted over the classical channel. Notice that when q-ary $[n, k]$ LDPC code is used the number of possible syndromes is q^{n-k}, and for every syndrome they are q^k possible error patterns. Given that the codeword lengths are at least in the order of tens of thousands, the security of the protocol is not reduced by transmitting the generalized parity-check symbols over the classical channel. In particular, the use of nonbinary irregular quasi-cyclic (QC) LDPC codes, derived from pairwise balanced designs (PBDs) provide the best reported net coding gains as shown in [31] and as such are excellent candidates to be used for information reconciliation. This class of nonbinary LDPC codes is very well suitable for rate adaptation, to adjust the error correction strength depending on the channel conditions. Namely, the quantum channel conditions are time-variant, in particular for free-space optical applications. By using this code construction, we designed a 4-ary irregular QC LDPC (69311, 50408) code of rate 0.727273 and average column weight of 2.8181. In Fig. 1 we provide bit-error rate (BER) and symbol-error rate (SER) performance of this code and evaluate its performance against corresponding 4-ary regular LDPC code of column eight 3. Clearly, this code provides more than five orders in magnitude improvement in SER compared to regular LDPC code (at SER of 0.118), and can tolerate more than 11% of symbol errors.

The free-space optical based MQKD scheme suffers from the atmospheric turbulence [15], [24], [32]. To deal with atmospheric turbulence someone may use the adaptive optics or wavefront correction method described in [6]. Another possible solution for MKQD and teleportation based on combined-OAM–SAM states, which does not suffer from atmospheric turbulence but suffers from mode coupling, based on few-mode fibers, is described in next section.

3. Multidimensional QKD Over Few-Mode Fiber and Free-Space Optical Channels

This section is devoted to combined-OAM–SAM-based multidimensional QKD over few-mode fiber and free-space optical channels. An arbitrary photon sate $|\psi\rangle$ can be represented as a linear superposition of basekets

$$|\psi\rangle = \sum_{l=-L}^{L} \sum_{\sigma=\pm 1} c_{l,\sigma} |l, \sigma\rangle, \quad \sum_{l=-L}^{L} \sum_{\sigma=\pm 1} |c_{l,\sigma}|^2 = 1 \tag{5}$$

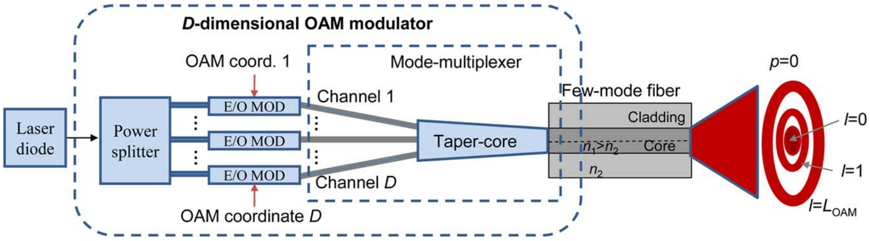


Fig. 2. Illustration of D-dimensional signaling by employing orthogonal OAM modes. E/O MOD: electro-optical modulator and it can be amplitude modulator, phase modulator, I/Q modulator or polar modulator.

where the basekets given by $|l,\sigma\rangle$ are orthogonal to each other

$$\langle m,\sigma|n,\sigma'\rangle=\delta_{mn}\delta_{\sigma\sigma'};\quad m,n\in\{-L,\ldots,-1,0,1,\ldots,L\};\sigma,\sigma'\in\{-1,1\}. \tag{6}$$

Therefore, the combined-OAM–SAM kets live in $D=2(2L+1)$-dimensional Hilbert space $H_{2(2L+1)}$. Instead of double-indexing of basekets, we can use single index $d\in\{0,1,\ldots,D-1\}$ so that the computation basis (CB) is given by

$$\{|0\rangle,|1\rangle,\ldots,|D-1\rangle\},D=2(2L+1). \tag{7}$$

As already indicated in Introduction, this concept of combined-OAM–SAM photon states is different from the TAM of photon defined as $j\hbar=(l+\sigma)\hbar$ (see ref. [10]). The corresponding number of basekets in TAM representation is $2L+3$, while in combined-OAM–SAM representation the number of basekets is $2(2L+1)$. Since the process of creation of TAM states, based on Dove prisms and half-wave plates has already been discussed in [10], here we restrict our attention to MQKD protocols based on combined-OAM–SAM states.

Before describing the photon combined-OAM–SAM-based entanglement-assisted protocols, we discuss the implementation of qudit quantum gates, required for both multidimensional QKD and quantum teleportation applications, based on integrated optics and FMF technology. For the implementation of proposed qudit gates only short sections of FMFs are used to avoid the mode coupling effects. To facilitate the explanations, we employ only OAM modes in this discussion and set, without loss of generality, D to $2L+1$. The employment of SAM modes requires just addition of polarization beam splitters/combiners. Let us first explain the classical version of D-dimensional modulator, which is shown in Fig. 2. A continuous wave laser diode signal is split into D branches by using a power splitter (such as 1: D star coupler) to feed D-dimensional electro-optical modulators, each corresponding to one out of D OAM modes. The OAM mode multiplexer is composed of D waveguides, taper-core fiber and few-mode fiber, properly designed to excite orthogonal OAM modes in few-mode fiber. Namely, the azimuthal modes $u_{l,p}$, where $l=0,\pm1,\ldots,\pm L$ for fixed radial number p, which are illustrated in Fig. 2, are mutually orthogonal as

$$(u_{m,p},u_{n,p})=\int u^*_{m,p}(r,\phi,z)u_{n,p}(r,\phi,z)rdrd\phi=\begin{cases}\int|u_{m,p}|^2rdrd\phi, n=m\\ 0, n\neq m\end{cases} \tag{8}$$

and can be used as basis functions for multi-dimensional signaling. (In (8), r denotes the radial distance, ϕ denotes the azimuthal angle and z denotes the propagation distance.) In addition, for $p=0$ the intensity of a Laguerre-Gaussian (LG) mode is a ring of radius proportional to $|l|$ and as such it can easily be detected by donut-shaped photodetector designed to capture the lth mode. One such photodetector structure has been proposed in [33]. However, given the mode crosstalk effect, the donut-shaped photodetection approach is applicable only in short links. For longer links, the OAM demultiplexing should be performed first followed by the wavefront correction, similar to that reported in [6], and photodetection. This circuit can be used to create the superposition of all basis kets each occurring with the same probability amplitude $D^{-1/2}$, namely $D^{-1/2}\sum_d|d\rangle=QFT|0\rangle$, where QFT is the quantum Fourier transform gate introduced below.

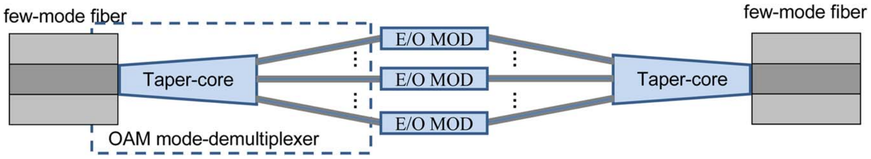


Fig. 3. Single-qudit gate implementation based on integrated optics and FMF technology.

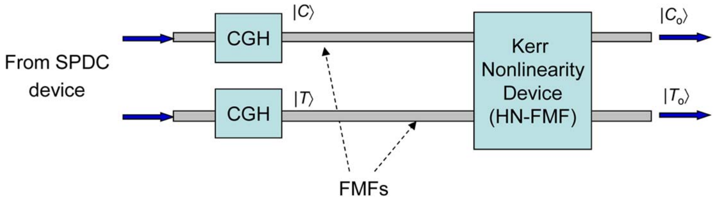


Fig. 4. Implementation of generalized CNOT-gate based on HN-FMF, combined with integrated optics.

The E/O modulators are amplitude modulators used to ensure that a desired probability amplitude is obtained in each dth brunch, corresponding to the dth OAM mode. If E/O modulators are instead polar modulators (corresponding to polar coordinates $re^{j\theta}$), by ensuring that $\sqrt{\kappa}\cdot r = D^{-1/2}$ (κ is the power splitting ratio of power splitter) and that the phase shift in dth brunch is proportional to d then the following superposition state is obtained:

$$D^{-1/2}\sum_d e^{j\frac{2\pi}{D}d}|d\rangle = QFT|1\rangle.$$

The OAM demodulator is obtained by reversing the outputs and inputs in OAM modulator. From Shannon's theory we know that channel capacity is a logarithmic function of signal-to-noise ratio, but a *linear* function in number of dimensions. Therefore, by using D-dimensional signaling based on OAM modes, we can dramatically improve overall spectral efficiency. Notice that when OAM multiplexer is implemented as shown in Fig. 2 it would be quite challenging to distinguish between OAM modes with azimuthal mode numbers of the same absolute value but of opposite sign $(\exp(\pm j|l|\phi))$, which is not a problem when holographic based OAM (de$-$) multiplexers are used. Nevertheless, distinguishable azimuthal modes $l = 0, 1, \ldots, L_{\text{OAM}}$ (for fixed p) are still orthogonal. Alternatively, specially developed fibers, vortex fibers [34], supporting OAM modes with both positive and negative l's can be used. Unfortunately, the attenuation of vortex fiber is still high, and this is the reason why in the rest of the paper we consider conventional FMFs instead.

The single-qudit gate is now quite straightforward to implement based on OAM multiplexer/demultiplexer as shown in Fig. 3. Namely, the photon, whose quantum state is represented by

$$|\psi\rangle = \sum_{l=0}^{D-1} c_l|l\rangle, \quad \sum_{l=0}^{D-1} |c_l|^2 = 1,$$

arrives at the input of single-qudit gate. In OAM demultiplexer we separate the basekets and by the set of D E/O MODs we introduce the required phase shifts and/or amplitude changes to perform the desired single-qudit operation. After that the basekets are recombined into single-qudit in OAM modulator as illustrated in Fig. 3. The basic idea of this qudit gate is to implement the CGH between the fan-in and fan-out type waveguide couplers. For initial design of OAM multiplexer please refer to ref. [35]. The controlled gate operation, is much more challenging to implement as we need a nonlinear element to interact two qudits. Possible implementation would be to combine integrated optics with CQED in similar fashion as we described in [11] for SAM based quantum computation/communication applications. Another option for the implementation of generalized OAM-based qudit gate, with a help of highly nonlinear few-mode fiber (HN-FMF), is illustrated in Fig. 4. Two photons generated by a spontaneous parametric down-conversion (SPDC) device arrive simultaneously at the input ports of generalized CNOT-gate. They have the same polarization and corresponding OAM mode is $|0\rangle$. We use two CGHs to impose corresponding OAM states for control $|C\rangle$ and target $|T\rangle$ basekates. The FMF couplers have been used to couple the single photons to corresponding nonlinear device based on HN-FMF. The nonlinear coupling introduces the generation of $|C+T\rangle$ baseket at the target qudit output $|T_o\rangle$. In order to support nonlinear interaction required for quantum gating, the few-mode optical fibers need to be optimized with respect to its refractive index profile in order to support the required nonlinear interaction. Namely, the assessment of the nonlinear interaction should be performed by assessing coupling coefficients among modes m and n as

$$c_{mn} = \frac{k_0^2}{2\beta_m} \frac{\int\int n_d^2 E_n E_m r dr d\phi}{\left(\int\int E_m^2 r dr d\phi \int\int E_n^2 r dr d\phi\right)^{1/2}},$$

where E_m and E_n are corresponding electrical fields, β_m is the propagation constant of the mth mode, and $k_0 = 2\pi/\lambda$ is the wavenumber. The inverse scattering theory should then be applied in order to determine needed refractive index profile n_d, in a similar fashion to that performed in case where just two modes were considered [36], but now with inclusion of the impact of nonlinear Kerr effect. Since the generalized CNOT gates are not required for MQKD applications, but for quantum teleportation and quantum computation applications, such optimization is not considered here. The quantum mechanical description of this qudit gate is very similar to SAM-based qubit gate described in [1] (see Chapter 13).

The single-qudit and generalized CNOT-gates are in particular straightforward to implement when the number of OAM modes is chosen to be a prime P. The basic gates are generalized Pauli-X and Pauli-Z gates, whose action is given by

$$X(a)|x\rangle = |x+a\rangle, \quad Z(b)|x\rangle = e^{j\frac{2\pi}{P}bx}|x\rangle \tag{9}$$

where the addition operation is mod P addition. The quantum Fourier transform (QFT) gate, for this case, is defined by

$$QFT|x\rangle = P^{-1/2}\sum_y e^{j\frac{2\pi}{P}xy}|y\rangle. \tag{10}$$

These three basic qudit gates can be implemented based on gates from Figs. 2 and 3 and text just below Eqn. (8).

Another important quantum gate is Weyl gate W, whose action is given by

$$W_{mn} = \sum_{d=0}^{D-1} \omega^{dn}|d+m\rangle\langle d|; \quad \omega = e^{\frac{j2\pi}{D}}; \quad m,n \in \{0,1,\ldots,D-1\} \tag{11}$$

which represents a generalization of both QFT gudit gate and generalized Pauli-X gate, and can be, therefore, implemented based on circuits from Figs. 1–3. The set of gates defined by Eqn. (11) can be use to obtain generalized Bell basekets starting from the generalized Bell baseket $|B_{00}\rangle$, defined as

$$|B_{00}\rangle = D^{-1/2}\sum_d |d\ d\rangle \tag{12}$$

which is clearly invariant under the action of $W_{mn}W_{mn}^*$. By applying the Weyl gate on $|B_{00}\rangle$, we obtain

$$I \otimes W_{mn}|B_{00}\rangle = D^{-1/2}\sum_d \omega^{dn}|d\ d+m\rangle = |B_{mn}\rangle \tag{13}$$

the desired generalized Bell baseket $|B_{mn}\rangle$. What remains to explain is how to generate the Bell state $|B_{00}\rangle$. Two entangled photons enter respective D-dimensional modulators as shown in Fig. 5, with configuration of D-dimensional OAM modulator provided in Fig. 1. The E/O modulators inside OAM

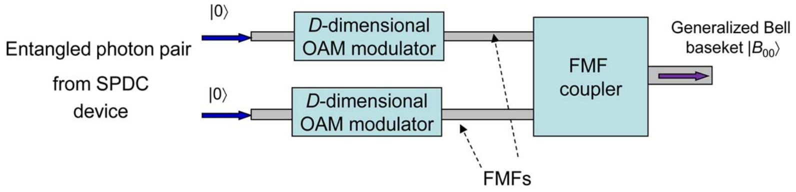

Entangled photon pair
from SPDC
device
|0⟩
|0⟩
D-dimensional OAM modulator
D-dimensional OAM modulator
FMF coupler
Generalized Bell baseket |B00⟩
FMFs

Fig. 5. Generation of generalized Bell baseket $|B_{00}\rangle$ in integrated optics combined with FMF technology. The D-dimensional OAM modulator has already been shown in Fig. 1.

modulators serve as amplitude modulators used to ensure that a desired probability amplitude is obtained in each dth brunch corresponding to the dth OAM mode. The resulting state at the output of OAM modulators is given by $D^{-1/2}\sum_d |d\rangle \otimes |d\rangle$, and after FMF coupling this resulting state represents the generalized Bell $|B_{00}\rangle$ baseket. In order to avoid the reflection and mode coupling problems the use of integrated optics, combined with FMF technology, is necessary. Any imperfection introduced in fabrication will affect the overall MQKD protocol, and we need to assume that different steps in protocol will fail with certain probability, which is the subject of investigation in Section 4.

These FMF-based qudit gates can be used in both free-space optical (FSO) and FMF links. Namely, this SAM–OAM qudit imposed as described in Fig. 1 can be transmitted either over FMF link or by using an expanding telescope be sent over an FSO link to the remote receiver. When the OAM baseket $|l\rangle$ is transmitted over the atmospheric turbulence channel, it can be detected on the receiver side as baseket $|l'\rangle$ $(l' \neq l)$ with certain probability as we have shown in [37] (see also [32]), which will affect the MQKD protocols over FSO links. On the other hand, due to mode coupling the portion of observed OAM baseket $|l\rangle$ will flow to neighboring OAM modes, resulting in crosstalk [38]. To improve the performance of proposed MQKD protocols, LDPC coding should be combined with the Gerchberg-Saxton algorithm based phase retrieval technique [39] to compensate for the phase distortion of an OAM mode introduced by either atmospheric turbulence or mode coupling.

Now we have all elements required to formulate *entanglement-assisted* protocols. Alice prepares $|B_{00}\rangle$ baseket, as described above, and sends one of the qudits to Bob. Alice further performs the measurement in eigenbasis of one of the W_{mn} selected at random. Bob performs the measurement in eigenbasis of one of the W^*_{mn} also selected at random. Only the items for which both (Alice and Bob) used the same bases are kept in sifting phase. For information reconciliation, Alice then performs (n, k) LDPC coding on positions in which both have used the same basis. Alice further sends $n - k \ll n$ parity symbols to Bob, who performs LDPC decoding. The privacy amplification is then performed to distil for a shorter key so that the correlation with Eve's string is minimized, as explained in [14]. The security analysis of two related classes of entanglement-assisted protocols, two-basis protocols and $(D + 1)$-basis protocols, is discussed in incoming section.

4. Security Analysis of Entanglement-Assisted Combined-OAM–SAM-Based Multidimensional QKD Systems

We are concerned here with the security against collective attacks, the attacks in which the Eve's interaction during QKD is i.i.d. The eigenkets of W_{mn} can be used to create the MUBs. For $D = 2(L_{\text{OAM}} + 1)$-dimensional systems there are $D^2 - 1$ nontrivial W_{mn}'s, however, some of them are redundant. It is well known that they are at least two MUBs and maximum $D + 1$ MUBs for arbitrary D-dimensional system. For two-basis protocol we can select the following set $\{W_{01}, W_{10}\}$, while for $(D+1)$-basis protocols the following set $\{W_{01}; W_{10}, \ldots, W_{1,D-1}\}$. Since $[W_{mn}W^*_{mn}, W_{m'n'}W^*_{m'n'}] = 0$, it can be easily shown that the Alice-Bob density operator ρ_{AB} is diagonal in the generalized Bell basis

$$\rho_{AB} = \sum_{m,n=0}^{D-1} \lambda_{mn}|B_{mn}\rangle\langle B_{mn}|; \qquad \sum_{m,n=0}^{D-1} \lambda_{mn} = 1. \tag{14}$$

The parameters to be estimated in entanglement-assisted protocols are related to probabilities that Alice and Bob's outcomes, denoted as a and b, differ by $d \in \{0, 1, \ldots, D-1\}$; when both chose randomly the basis of W_{mn}, observed per mod D, denoted as $q_{mn}(d)$, and can be determined as

$$q_{01}(d) = \sum_{n=0}^{D-1} \lambda_{d,n}, \quad q_{1n}(d) = \sum_{n=0}^{D-1} \lambda_{m,(mn-d)\mathrm{mod}D}. \tag{15}$$

(Notice that in this paper we use p to denote *a priori* probabilities and q to denote *a posteriori* probabilities.) Clearly, the probability that there is no error can be found as $q_{mn}(0) = 1 - \sum_{d=1}^{D-1} q_{mn}(d)$. The Eve's accessible information (maximum of mutual information, where maximization is performed over all generalized positive operator valued measurement (POVM) schemes) is upper bounded by Holevo information (see [1], Chapter 12)

$$\chi(A : E|\rho_{AB}) = S(\rho_E) - \sum_{a=0}^{D-1} p(a) S(\rho_{E|a}), \quad S(\rho) = -Tr(\rho \log \rho) = -\sum_{\lambda_i} \lambda_i \log \lambda_i \tag{16}$$

where $S(\rho)$ is the von Neumann entropy and with λ_i we denoted the eigenvalues of ρ. In generalized Bell diagonal state, we have that $p(a) = 1/D$ and in order to estimate $S(\rho_{E|a})$ we need to perform the purification of ρ_{AB} as follows: $|\phi_{AB,E}\rangle = \sum_{m,n} \sqrt{\lambda_{mn}} |B_{mn}\rangle_{AB} |\phi_{mn}\rangle_E$, where the Eve's basis $|\phi_{mn}\rangle_E$ is properly chosen so that the state $|\phi_{AB,E}\rangle$ is pure. Since the $\rho_{E|a}$ is a diagonal in the generalized Bell basis, and given the that von Neumann entropy is equal to the Shannon entropy when quantum states are mutually orthogonal, we have that $S(\rho_{E|a}) = H(q_{01}(0), \ldots, q_{01}(D-1))$. Finally, based on the above discussion, the Eve's mutual information is given by

$$I_E = \begin{cases} \chi(A : E|\rho_{AB}), & \text{for } (D+1)\text{– basis protocols} \\ \max \chi(A : E|\rho_{AB}), & \text{for two - basis protocols} \end{cases};$$
$$\chi(A : E|\rho_{AB}) = H(\lambda_{mn}) - H(\underbrace{q_{01}(0), \ldots, q_{01}(D-1)}_{q_{01}}). \tag{17}$$

As an illustration, let us consider the generalized depolarization channel to model error probabilities $q_{mn}(d)$

$$q_{mn}(d) = \begin{cases} 1-q, d=0 \\ q/(D-1), d \neq 0 \end{cases} \tag{18}$$

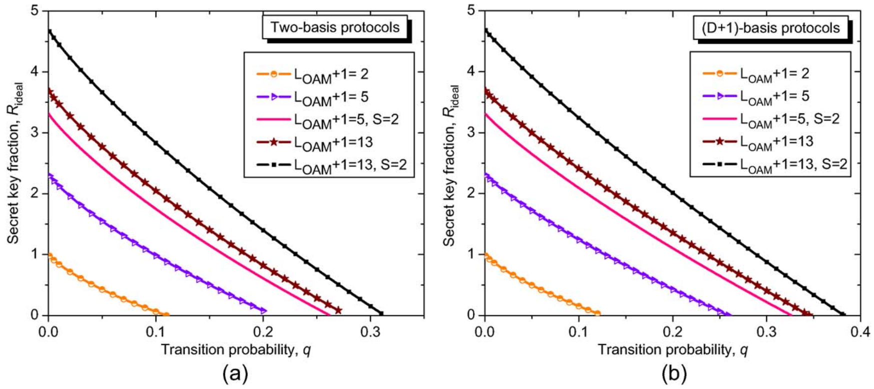
which represents the generalization of classical D-ary symmetric channel. Notice that error probability $q_{mn}(d)$ typically decreases as d increases, indicating that this model represents the worst-case scenario. In this model the Eve's mutual information can be determined in closed form

$$I_E = \begin{cases} -(1-q)\log(1-q) - (D-1)\frac{q}{D-1}\log\left(\frac{q}{D-1}\right) \doteq H(\boldsymbol{q}), & \text{for two - basis protocols} \\ -\left(1-q-\frac{q}{D}\right)\log\left(1-q-\frac{q}{D}\right) - \left(q+\frac{q}{D}\right)\log\left[\frac{q}{D(D-1)}\right] - H(\boldsymbol{q}), & \text{for } (D+1)\text{– basis protocols.} \end{cases} \tag{19}$$

The corresponding secret key fraction rate, for infinitely long keys, is given by

$$R_{\text{ideal}} = \log_2(D) - I_E(q) - H(\boldsymbol{q}). \tag{20}$$

The results for infinitely long secure keys, assuming perfect information reconciliation and privacy amplification, are shown in Fig. 6 for number of combined-OAM–SAM states given by $D = S \times (L_{\text{OAM}} + 1)$, where S is the number of SAM states ($S = 2$) and the number of OAM states for FMF-based implementation is given by $L_{\text{OAM}} + 1$ (see Fig. 2). Clearly, combined-OAM–SAM-based protocols can improve the secure key rates of two-dimensional-based protocols. It is also evident that the values of transition probability q for which the secure finite rates become zero ($R_{\text{ideal}} = 0$) are higher for $(D+1)$-basis based protocols. For instance, for $(D+1)$-basis protocol for $D =$



(a)

(b)

Fig. 6. Secret key fraction rate for infinitely long keys: (a) two-basis protocols and (b) $(D+1)$-basis protocols. The number of combined-OAM-SAM states is given by $D = S \times (L_{\text{OAM}}+1)$, where S is number of SAM states $(S=2)$ and the number of OAM states for FMF-based implementation is given by $L_{\text{OAM}}+1$ (see Fig. 2).

$2(L_{\text{OAM}}+1) = 10$ combined-OAM–SAM states, the secure key rate becomes zero at 32.64%, while for two-basis protocols the zero rate is obtained at 26.21%.

Practical key lengths are finite, and we need to assume that various steps in entanglement-assisted protocols will fail with certain probability [12], [13]. To deal with such scenarios, the concept of ε-security is introduced in [12]. We say that the key *Key* is *ε-secure* with respect to an eavesdropper E if the trace distance between the joint state $\rho_{Key,E}$ and $\rho_U \otimes \rho_E$, where ρ_U is the completely mixed state, is smaller than or equal to ε. Since each step can fail with certain probability, we can write: $\varepsilon = \varepsilon_{EC} + \varepsilon_{PA} + \varepsilon_{PE} + \bar{\varepsilon}$, where ε is the security of the final key; while with ε_{EC}, ε_{PA}, and ε_{PE} we denoted the securities of error correction, privacy amplification and parameter estimation steps, respectively. Finally, with $\bar{\varepsilon}$ we denoted the failure probability of Renyi entropies estimates (please refer to [12], [13] for additional details). Based on security theory described in [12], [13], the bound for secret finite key rate is given by

$$R_K = \frac{k}{K}\left\{H(A|E) - H(A|B) - \frac{1}{k}\log\left(\frac{2}{\varepsilon_{EC}}\right) - \frac{2}{k}\log\left(\frac{2}{\varepsilon_{PA}}\right) - (2D+3)[\log(2/\bar{\varepsilon})/k]^{\frac{1}{2}}\right\} \tag{21}$$

where the ratio k/K indicates that only portion of the sequence of length $k < K$ is used for the key, the rest is used for parameters' estimation. (Log-functions in (21) are the base-2 logarithms.) In (21), $H(A|E)$ is determined by $\log(D) - I_E$, but now with error probabilities $q_{mn}(d)$ subject to fluctuations

$$\tilde{q}_{mn}(d) \in [q_{mn}(d) - \Delta q_{mn}, q_{mn}(d) + \Delta q_{mn}], \quad \Delta q_{mn} = \xi(b,D)/[2(D-1)] \tag{22}$$

where $\xi(b,D) = [2\ln(1/\varepsilon_{PE})/b + D\ln(b+1)/b]^{1/2}, b = Kp_{mn}^2$, with p_{mn} being the probability of selecting base m and n. The expression for $\xi(b,D)$ follows from the law of large numbers as explained in [12]. In calculations that follow, we assume the uniform distribution of $\tilde{q}_{mn}$ in (22), with the normalization constraint $\sum_d \Delta q_{mn}(b,d) = 0$. The results of calculations are summarized in Fig. 7, for fixed total error rate ε of 10^{-5}, tolerable error correction rate ε_{EC} of 10^{-10}, and fixed transition probability $q = 0.05$. The results are obtained by numerical maximization of (21), with respect to unknown parameters $(\varepsilon_{\text{PA}}, \varepsilon_{\text{PE}}, p_{mn})$. For sufficiently long keys, the $(D+1)$-basis protocols outperform two-basis protocols in terms of finite secure key rate. On the other hand, the two-basis protocols show earlier saturation of secure key rates (against key length) compared to $(D+1)$-basis protocols. Both types of proposed protocols significantly outperform conventional two-dimensional QKD protocols.

5. Concluding Remarks

Considerable research effort has been invested in the field of quantum information with the goal of utilizing properties of quantum mechanics for computation and communication applications. In the communications area, it has been widely recognized that the underlying principles of quantum

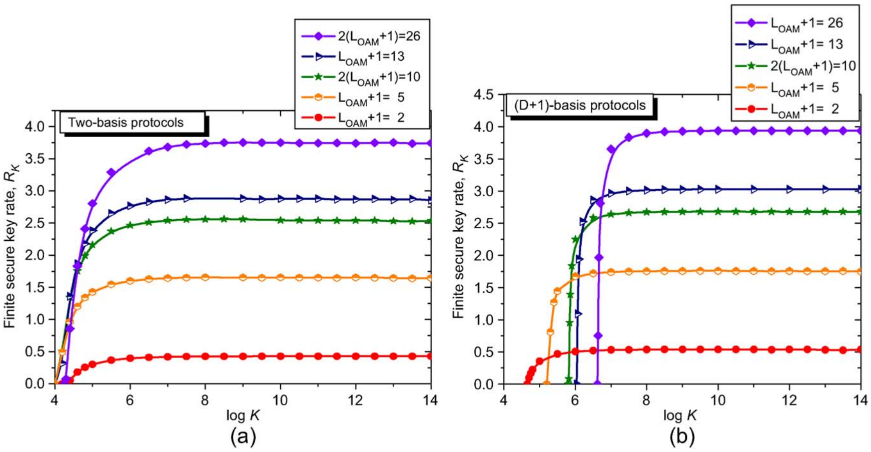


Fig. 7. Secret key fraction rate for finite keys: (a) two-basis protocols and (b) $(D+1)$-basis protocols. The parameters are set as follows: $\varepsilon = 10^{-5}$, $\varepsilon_{EC} = 10^{-10}$, $q = 0.05$.

mechanics can be used to enable secure communications. Specifically, the impossibility for an eavesdropper to tap the quantum channel and distinguish among nonorthogonal states without introducing disturbance to the channel ensures that the QKD system is secure. However, most of these previous research efforts have focused on two-dimensional QKD, commonly performed by use of the polarization state of photons. Unfortunately, data rates for quantum key exchange in two-dimensional QKD are still low, while the transmission distance also is limited by the available power budget.

To address these key challenges through a photon angular momentum approach, we invoke the well-known fact that photons can carry both SAM and OAM, which are associated with the polarization and the azimuthal phase of the complex electric field, respectively. Accordingly, we can associate the combined-OAM–SAM state of each photon, defined as $|l, \sigma\rangle$, where l and σ correspond to OAM and SAM indexes, respectively. Since the OAM eigenstates are orthogonal, additional degrees of freedom can be utilized in the QKD process, thus increasing the total secure bit rate that can be transmitted.

To improve the secure data rates, we have proposed two types of protocols, nonentanglement-based and entanglement-assisted protocols, both employing photon combined-OAM–SAM. Both types of protocols can be used for secure key distribution over free-space and few-mode fiber channels. Two types of entanglement-assisted protocols have been described: two-basis and $(D+1)$-basis protocols. We have further described how to implement the qudit gates required for implementation of these protocols by using integrated optics and FMF technology. Finally, we have studied the security issues of proposed protocols, and determined both infinite and finite secret key fraction rates.

References

[1] I. B. Djordjevic, *Quantum Information Processing and Quantum Error Correction: An Engineering Approach*. Amsterdam, The Netherlands: Elsevier, Apr. 2012.

[2] I. B. Djordjevic, "Quantum LDPC codes from balanced incomplete block designs," *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 389–391, May 2008.

[3] I. B. Djordjevic, "Photonic quantum dual-containing LDPC encoders and decoders," *IEEE Photon. Technol. Lett.*, vol. 21, no. 13, pp. 842–844, Jul. 1, 2009.

[4] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using*d*-level systems," *Phys. Rev. Lett.*, vol. 88, no. 12, pp. 127902-1–127902-4, Mar. 25, 2002.

[5] M. T. Gruneosen, W. A. Miller, R. C. Dymale, and A. M. Seiti, "Holographic generation of complex fields with spatial light modulators: Application to quantum key distribution," *Appl. Opt.*, vol. 47, no. 4, pp. A32–A42, Feb. 1, 2008.

[6] A. Jesacher, A. Schwaighofer, S. Fürhapter, C. Maurer, S. Bernet, and M. Ritsch-Marte, "Wavefront correction of spatial light modulators using an optical vortex image," *Opt. Exp.*, vol. 15, no. 9, pp. 5801–5808, Apr. 27, 2007.

[7] Z.-K. Su, F.-Q. Wang, R.-B. Jin, R.-S. Liang, and S.-H. Liu, "A simple scheme for quantum networks based on orbital angular momentum," *Opt. Commun.*, vol. 281, no. 19, pp. 5063–5066, Oct. 2008.

[8] R. W. Boyd, A. Jha, M. Malik, C. O'Sullivan, B. Rodenburg, and D. J. Gauthier, "Quantum key distribution in a high-dimensional state space: exploiting the transverse degree of freedom of the photon," presented at the Proc. SPIE 7948, San Francisco, CA, USA, 2011, Paper 79480L.

[9] T. Yamamoto, J. Shimamura, S. K. Özdemir, M. Koashi, and N. Imoto, "Faithfull qubit distribution assisted by one additional qubit against collective noise," *Phys. Rev. Lett.*, vol. 95, no. 4, pp. 040503-1–040503-4, Jul. 22, 2005.

[10] 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.*, vol. 92, no. 1, pp. 013601-1–013601-4, Jan. 9, 2004.

[11] I. B. Djordjevic, "Cavity Quantum Electrodynamics (CQED) based quantum LDPC encoders and decoders," *IEEE Photon. J.*, vol. 3, no. 4, pp. 727–738, Aug. 2011.

[12] R. Renner, "Security of quantum key distribution," Ph.D. dissertation, Swiss Fed. Inst. Technol., Zurich, Switzerland, Sep. 2005.

[13] V. Scarani and R. Renner, "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing," *Phys. Rev. Lett.*, vol. 100, no. 20, pp. 200501-1–200501-4, May 22, 2008.

[14] C. R. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.

[15] C. Paterson, "Atmospheric turbulence and orbital angular momentum of single photons for optical communication," *Phys. Rev. Lett.*, vol. 94, no. 15, pp. 153901-1–153901-4, Apr. 22, 2005.

[16] H. de Riedmatten, I. Marcikic, V. Scarani, W. Tittel, H. Zbinden, and N. Gisin, "Tailoring photonic entanglement in high-dimensional Hilbert spaces," *Phys. Rev. A, At. Mol. Opt. Phys.*, vol. 69, no. 5, pp. 050304-1–050304-4, May 2004.

[17] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin, "Bell-type test of energy-time entangled qutrits," *Phys. Rev. Lett.*, vol. 93, no. 1, pp. 010503-1–010503-4, Jul. 2004.

[18] M. N. O'Sullivan-Hale, I. A. Khan, R. W. Boyd, and J. C. Howell, "Pixel entanglement: Experimental realization of optically entangled d = 3 and d = 6 qudits," *Phys. Rev. Lett.*, vol. 94, no. 22, pp. 220501-1–220501-4, Jun. 2005.

[19] L. Neves, G. Lima, J. G. A. Gómez, C. H. Monken, C. Saavedra, and S. Pádua, "Generation of entangled states of qudits using twin photons," *Phys. Rev. Lett.*, vol. 94, no. 10, pp. 100501-1–100501-4, Mar. 2005.

[20] A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental two-photon, three-dimensional entanglement for quantum communication," *Phys. Rev. Lett.*, vol. 89, no. 24, pp. 240401-1–240401-4, Nov. 2002.

[21] N. K. Langford, R. B. Dalton, M. D. Harvey, J. L. O'Brien, 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.*, vol. 93, no. 5, pp. 053601-1–053601-4, Jul. 2004.

[22] G. Molina-Terriza, A. Vaziri, J. Reháček, Z. Hradil, and A. Zeilinger, "Triggered qutrits for quantum communication protocols," *Phys. Rev. Lett.*, vol. 92, no. 16, pp. 167903-1–167903-4, Apr. 2004.

[23] S. Groblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," *New J. Phys.*, vol. 8, no. 5, p. 75, May 2006.

[24] G. Gibson, J. Courtial, M. Padgett, M. Vasnetsov, V. Pas'ko, S. Barnett, and S. Franke-Arnold, "Free-space information transfer using light beams carrying orbital angular momentum," *Opt. Exp.*, vol. 12, no. 22, pp. 5448–5456, Nov. 2004.

[25] S.-M. Zhao, L.-Y. Gong, Y.-Q. Li, H. Yang, Y.-B. Sheng, and W.-W. Cheng, "A large-alphabet quantum key distribution protocol using orbital angular momentum entanglement," *Chin. Phys. Lett.*, vol. 30, no. 6, p. 060305, Jun. 2013.

[26] V. D'Ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino, "Complete experimental toolbox for alignment-free quantum communication," *Nat. Commun.*, vol. 3, no. 7, p. 961, Jul. 17, 2012.

[27] N. Bozinovic, Y. Yue, Y. Ren, M. Tur, P. Kristensen, H. Huang, A. E. Willner, and S. Ramachandran, "Terabit-scale orbital angular momentum mode division multiplexing in fibers," *Science*, vol. 340, no. 6140, pp. 1545–1548, Jun. 2013.

[28] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, "Generation of hyperentangled photon pairs," *Phys. Rev. Lett.*, vol. 95, no. 26, pp. 260501-1–260501-4, Dec. 2005.

[29] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, "Beating the channel capacity limit for linear photonic superdense coding," *Nat. Phys.*, vol. 4, no. 4, pp. 282–286, Apr. 2008.

[30] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro, "Quantum key distribution with higher-order alphabets using spatially encoded qudits," *Phys. Rev. Lett.*, vol. 96, no. 9, pp. 090501-1–090501-4, Mar. 2006.

[31] I. B. Djordjevic, "On the irregular nonbinary QC-LDPC-coded hybrid multidimensional OSCD-modulation enabling beyond 100 Tb/s optical transport," *J. Lightw. Technol.*, vol. 31, no. 16, pp. 2969–2975, Aug. 15, 2013.

[32] M. Malik, M. O'Sullivan, B. Rodenburg, M. Mirhosseini, J. Leach, M. P. J. Lavery, M. J. Padgett, and R. W. Boyd, "Influence of atmospheric turbulence on optical communications using orbital angular momentum for encoding," *Opt. Exp.*, vol. 20, no. 12, pp. 13 195–13 200, Jun. 2012.

[33] S. H. Murshid and J. Iqbal, "Array of concentric CMOS photodiodes for detection and de-multiplexing of spatially modulated optical channels," *J. Opt. Laser Technol.*, vol. 41, no. 6, pp. 764–769, Sep. 2009.

[34] Y. Ren, Y. Zhang, Y. Yue, N. Bozinovic, G. Xie, H. Huang, M. Tur, P. Kristensen, I. B. Djordjevic, S. Ramachandran, and A. E. Willner, "Efficient crosstalk mitigation of OAM based 400-Gbit/s QPSK data transmission in 1.1-km vortex fiber by using soft-decision LDPC codes," presented at the Proc. CLEO, San Jose, CA, USA, Jun. 9–14, 2013, Paper CM2G.5.

[35] S. H. Murshid and A. M. Khayrattee, "Orbital angular momentum in spatially multiplexed optical fiber communications," U.S. Patent 8 396 371, Mar. 12, 2013.

[36] M. Cvijetic and G. Lukatela, "Design considerations of dispersion-free dual-mode optical fibers: 1.55μm wavelength operation," *IEEE J. Quantum Electron.*, vol. QE-23, no. 5, pp. 469–472, May 1987.

[37] Y. Zhang, I. B. Djordjevic, and X. Gao, "On the quantum channel capacity for Orbital Angular Momentum (OAM) based free-space optical communications," *Opt. Lett.*, vol. 37, no. 15, pp. 3267–3269, Aug. 1, 2012.

[38] C. Lin, I. B. Djordjevic, and M. Cvijetic, "Quantum few-mode fiber communications based on the orbital angular momentum," *IEEE Photon. Technol. Lett.*, vol. 25, no. 1, pp. 3–6, Jan. 1, 2013.

[39] R. W. Gerchberg and W. O. Saxton, "A practical algorithm for the determination of the phase from image and diffraction plane pictures," *Optik*, vol. 35, no. 2, pp. 237–246, 1972.