Quantum communication networks with optical vortices

Şerban Suciu,[1,2] George Andrei Bulzan,[3,2] Tudor-Alexandru Isdrailă [iD],[1,4] Alexandra Maria Pălici,[1,5]
Stefan Ataman [iD],[6] Cristian Kusko [iD],[3] and Radu Ionicioiu [iD][1]

[1]*Horia Hulubei National Institute of Physics and Nuclear Engineering, 077125 Bucharest-Măgurele, Romania*
[2]*Faculty of Physics, University of Bucharest, P.O. Box MG-11, Bucharest-Măgurele, Romania*
[3]*National Institute for Research and Development in Microtechnologies IMT, Bucharest 077190, Romania*
[4]*Department of Physics, Tamkang University, 151 Yingzhuan Road, Tamsui District, New Taipei City 251301, Taiwan*
[5]*Department of Photonics Engineering, Technical University of Denmark, 2800 Kongens Lyngby, Denmark*
[6]*Extreme Light Infrastructure–Nuclear Physics, Horia Hulubei National Institute for Physics and Nuclear Engineering,
30 Reactorului Street, 077125 Bucharest-Măgurele, Romania*

Quantum communications introduce a paradigm change in internet security by using quantum resources to establish secure keys between parties. Present-day quantum communication networks are mainly point to point and use trusted nodes and key management systems to relay the keys. Future quantum networks, including the quantum internet, will have complex topologies in which groups of users are connected and communicate with each other. Here we investigate several architectures for quantum communication networks. We show that photonic orbital angular momentum (OAM) can be used to route quantum information between different nodes. Starting from a simple point-to-point network, we will gradually develop more complex architectures: point-to-multipoint, fully connected, and entanglement-distribution networks. As a particularly important result, we show that an n-node fully connected network can be constructed with a single OAM sorter and $n-1$ OAM values. Our results pave the way to construct complex quantum communication networks with minimal resources.

I. INTRODUCTION

Quantum computers pose a threat to present-day internet security, due to their ability to efficiently break public-key cryptography. One way to mitigate this quantum apocalypse is to deploy large-scale quantum communication networks. Current quantum communications are usually point to point, using trusted nodes and key management systems to establish secret keys between remote nodes.

Future quantum networks, including the quantum internet, will require one to both handle complex network topologies [1] and secure such networks [2]. These networks will need to connect users situated in different locations and/or domains. Consequently, in such networks it will be important to route a quantum state $|\psi\rangle_q$ between different locations.

Most of the information we exchange every day is encoded in photons and carried by optical fibers. The data capacity of a single optical fiber depends on the spectral bandwidth over which low-loss signal transmission can be achieved, on the one hand, and on our ability to use this bandwidth through suitable coding and decoding schemes, on the other.

Due to the constant increase of worldwide data traffic, nonlinear effects [3] impose limits on the capacity of optical fibers. To address this capacity crunch, space division multiplexing using multicore [4,5] and multimode [6] fibers has been developed. In the quest for larger data capacity, another solution is to use an extra degree of freedom, different from wavelength [7,8].

A good candidate for the extra degree of freedom is the orbital angular momentum (OAM) of the photon [9–11].

The phase front of an OAM beam is helical, with quantized angular momentum $l\hbar$, $l \in \mathbb{Z}$. Photons carrying OAM have been used for different applications, such as object identification [12], enhanced phase sensitivity [13], imaging [14,15], and metrology [16,17]. Classical and quantum communication with OAM states have both been demonstrated in fiber [8,18,19], including experimental mode-division multiplexing [20].

Long-distance, high-dimensional quantum key distribution (QKD) using OAM in both optical fibers [8] and free-space [21] have recently enjoyed a renewed interest. This is due to several benefits introduced by high-dimensional systems: reduced overall complexity of a quantum circuit via d-level gates [22,23], increased raw-key rates [24,25], robustness to noise [26–28], and hacking attacks [29]. Hybrid states of OAM and polarization have also been used in QKD protocols, in both fiber and free space [30–32]. Furthermore, recent advances have lowered the resource requirements for point-to-multipoint architectures [1] and have also enhanced quantum digital signatures protocols [2]. Orbital angular momentum multiplexing can offer an alternative to the development of wireless communications [33], because unlike wavelength-division multiplexing, it can generate orthogonal channels [33] in a line-on-site channel environment.

Due to this increased interest in both classical and quantum applications of OAM, dedicated optical fibers [34] and multiplexing and demultiplexing techniques [35–38] have been maturing recently. Thus new methods to route information encoded in OAM are needed. In contrast to wavelength, it is relatively easy to change OAM using passive optical elements

like spiral phase plates (SPPs) [39]. This makes OAM an attractive degree of freedom for network routing.

In this paper we discuss several architectures for quantum communication networks which use OAM for routing quantum states $|\psi\rangle_q$ around the network. The paper is structured as follows. In Sec. II we describe the quantum sorter [37], which is the main element in OAM multiplexing (mux) and demultiplexing (demux). In Sec. III we show OAM implementations of several topologies for quantum communications networks: point-to-point, point-to-multipoint, fully connected, and fully connected entanglement-distribution networks with a central network provider. Finally, we summarize the article in Sec. IV.

II. QUANTUM SORTER

A central element of all the networks discussed here is the d-dimensional quantum sorter U_d and its inverse $U_d^\dagger$ [37]. A short description is provided in Appendix A; U_d ($U_d^\dagger$) is a unitary operator which acts as a demultiplexer (multiplexer). In quantum information parlance, the sorter U_d is a controlled-X_d gate between the observable to be sorted and the path degree of freedom.

The sorter is universal, i.e., it can (de)multiplex any internal degree of freedom, i.e., wavelength, spin, radial angular momentum, OAM, etc., and has a theoretical efficiency of 100% [37]. A definite advantage of the sorter is that it can be implemented with linear optics. In Appendix A we provide a physical intuition behind the sorter. Experimentally, sorting photons according to their radial number has been realized in Refs. [40,41]. The same sorting mechanism has been recently applied to a novel method of mass spectrometry [42]. Standard telecom networks use wavelength as the extra degree of freedom (DOF) for multiplexing and demultiplexing. In this article we focus on the OAM degree of freedom as a tool for mux and demux. The actions of the sorter U_d and its inverse $U_d^\dagger$ are

$$|l\rangle_{\text{OAM}}|k\rangle_{\text{path}} \xrightarrow{U_d} |l\rangle_{\text{OAM}}|k \oplus l\rangle_{\text{path}} \quad \text{(demux)},$$

$$|l\rangle_{\text{OAM}}|k\rangle_{\text{path}} \xrightarrow{U_d^\dagger} |l\rangle_{\text{OAM}}|k \ominus l\rangle_{\text{path}} \quad \text{(mux)}, \quad (1)$$

respectively, with $\oplus$ ($\ominus$) addition (subtraction) mod d. Here both OAM and path DOFs are qudits, i.e., d-dimensional quantum systems. Thus, if photons with different OAM l are incident on port 0 of the U_d gate (demux), they will exit on output l, i.e., they will be sorted on different outputs according to their OAM value. The $U_d^\dagger$ gate (mux) works in reverse.

The addition and subtraction mod d result in a cyclic property which can be better understood for $l = \pm d$. In this case $|l\rangle_{\text{OAM}}$ will be sorted on path $|0\rangle_{\text{path}}$, like $l = 0$. This cyclic property will play a crucial role in the design of various network architectures for routing quantum states using OAM.

The cyclic property is also used in the construction of the X_d gate [43]. The X_d gate is a basic building block for qudit tomography [44,45] and for general qudit protocols. Another application of the quantum sorter is in the generation of high-dimensional entangled states between an observable and the path DOF. Hybrid quantum gates are a hot topic under active development [46–48]. Accessing a larger alphabet allows us to
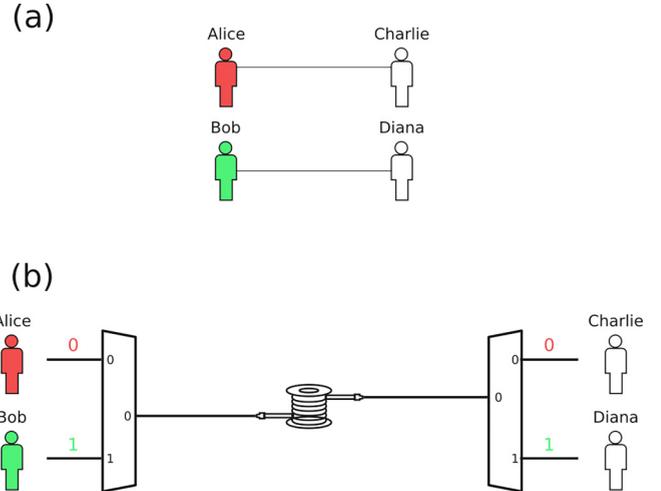

FIG. 1. (a) Logical network for two pairs connected in a point-to-point topology. (b) Two point-to-point pairs using a common channel. Signals from each pair are multiplexed into the common (long-range) channel and demultiplexed at the destination. The information can be recovered and separated because each sender-receiver pair has allocated a unique OAM value.

encode more information, resulting in higher channel capacity and better robustness to noise.

III. OAM-ASSISTED QUANTUM COMMUNICATION NETWORKS

In this section we start with a simple architecture and then gradually build more complex networks. All networks discussed here can be used for QKD, either in prepare-and-measure (BB84) or in entanglement-based protocols (E91 and BBM92). The only difference is in the equipment available to users. The networks can also be used to route quantum information as part of a larger protocol. What we denote by "senders" and "receivers" can represent anything from sources and detectors to other networks or protocols. The scale can also vary from waveguides in computer chips to optical fibers between cities or ground-to-satellite links.

For simplicity, in the following we use only positive OAM values. One can substitute the OAM $|l_{\text{max}} - n\rangle_{\text{OAM}} \mapsto |-n - 1\rangle_{\text{OAM}}$, where l_{max} is the largest OAM used in the protocol, and $n \in \{0, 1, \dots, \lfloor \frac{l_{\text{max}}}{2} \rfloor\}$, thus halving the maximum OAM values required.

A. Point-to-point architecture

Point-to-point networks are a simple case in which pairs of users are connected by their own quantum channel. In practice this results in a messy and convoluted network of cables. To reduce the number of cables needed, especially for long-distance communication, individual signals are in practice multiplexed into the same channel. For example, different laboratories from two cities can share the same channel for intercity transmission.

In Fig. 1 two pairs, i.e., Alice and Charlie, and Bob and Diana, share a single long-range quantum channel (instead of dedicated channels for each pair). Each pair has assigned

a unique OAM value. The pairs are indexed by consecutive numbers which represents their assigned OAM, input port at the multiplexer, and output port at the demultiplexer. For example, if Bob wants to send a quantum state $|\psi\rangle_q$ to Diana, he uses input port $|1\rangle_{\text{path}}$ with OAM $|1\rangle_{\text{OAM}}$. This state is input into the multiplexer, which redirects it to port $|0\rangle_{\text{path}}$ of the long-range channel:

$$|\psi\rangle_q|1\rangle_{\text{OAM}}|1\rangle_{\text{path}} \xrightarrow{\text{mux}} |\psi\rangle_q|1\rangle_{\text{OAM}}|0\rangle_{\text{path}}.$$

Diana recovers $|\psi\rangle_q$ on output port $|1\rangle_{\text{path}}$ of the demultiplexer at her end:

$$|\psi\rangle_q|1\rangle_{\text{OAM}}|0\rangle_{\text{path}} \xrightarrow{\text{demux}} |\psi\rangle_q|1\rangle_{\text{OAM}}|1\rangle_{\text{path}}.$$

The quantum state $|\psi\rangle_q$ can be any internal degree of freedom (different from OAM). Usually we use polarization to encode the quantum state $|\psi\rangle_q = |\psi\rangle_{\text{pol}} = \alpha|H\rangle + \beta|V\rangle$. In Appendix B we discuss an example of an OAM-assisted BB84 protocol in polarization.

Since the multiplexer and demultiplexer are modeled by a unitary operation, the protocol also works in reverse. We can reverse the direction in Fig. 1 such that Charlie and Diana are now the senders and everything works similarly. This is true for all communication protocols discussed here.

B. Point-to-multipoint architecture

A point-to-multipoint architecture is a natural extension from the point-to-point one. Instead of linking pairs of users, a point-to-multipoint network links a group of users with one or more other groups. However, members of the same group cannot communicate with each other. The logical network is a bipartite graph.

The simple setup with one multiplexer and one demultiplexer works in this case, but only if the numbers of senders and receivers are coprime (see Appendix C for a proof). Expanding on the previous example, different laboratories from two cities can now not only share a transmission line, but also choose to which laboratory from the other city to send data.

Figure 2 shows an example for two senders and three receivers. Alice (Bob) can communicate with any receiver (Charlie, Diana, or Eve) using an even (odd) OAM value.

For the general case, suppose we have a set of d_s senders and d_r receivers, with d_s and d_r relatively coprime. In this case any sender-receiver pair has an associated unique OAM; thus the receiver can distinguish between different senders. This value is determined by solving a system of congruence relations

$$l_{sr} \equiv s \pmod{d_s},$$
$$l_{sr} \equiv r \pmod{d_r},$$

where d_s and d_r are the dimensions of the multiplexer (sender) and demultiplexer (receiver), respectively. In order for a sender $s \in \{0, \ldots, d_s - 1\}$ to communicate with a receiver $r \in \{0, \ldots, d_r - 1\}$, they use the OAM value l_{sr} given by

$$l_{sr} = pd_s + s = qd_r + r \tag{2}$$

(see Appendix C). The total number of OAM values is $d_s d_r$.

Although in practice we can always choose the dimensions of the multiplexer and demultiplexer to be coprime (e.g., by
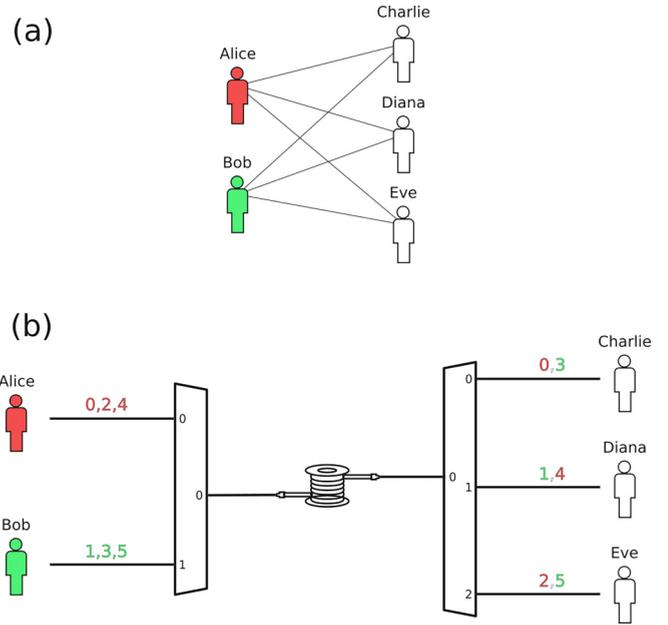

FIG. 2. (a) Logical network for two groups connected in a point-to-multipoint topology. (b) Two groups share a single long-range channel to communicate with members of the other group. To ensure that each pair has assigned a unique OAM value, the dimensions of multiplexer and demultiplexer must be coprime; here $d_s = 2$ and $d_r = 3$.

embedding them in a larger set), this can be an issue for more complex networks. The coprimality constraint can be eliminated by modifying the demultiplexer as in Fig. 3(b). We call this a group demultiplexer since it splits an input channel into $d_s d_r$ outputs and then groups them back together into d_r channels.

In Fig. 3(c) we use the group demultiplexer to create a more general network. Now any sender s can transmit to any receiver r by an appropriate OAM value l_{sr}:

$$l_{sr} = s + rd_s. \tag{3}$$

A step-by-step analysis of this protocol is given in Appendix D; here we only give the main result:

$$|\psi\rangle_q|l_{sr}\rangle_{\text{OAM}}|s\rangle_{\text{path}} \xrightarrow{\text{network}} |\psi\rangle_q|l_{sr}\rangle_{\text{OAM}}|r\rangle_{\text{path}}.$$

This ensures that quantum information, encoded in the state $|\psi\rangle_q$, is routed along the network from sender s to receiver r.

In the following schemes a group demultiplexer can be replaced by a simple demultiplexer provided that (i) the number of senders and receivers are coprime and (ii) the OAM values satisfy the congruence relations discussed above. Also, any network can work in reverse, i.e., receivers become senders, multiplexers become demultiplexers (and vice versa), and group demultiplexers become group multiplexers.

In point-to-multipoint networks, a group communicates with multiple other groups. A useful use-case scenario is a network connecting multiple cities: Laboratories in one city communicate with laboratories in multiple cities. However, one network connects just one city with others. This creates a physical star-network topology; the logical network topology remains the same. Each sender forms a logical star-network
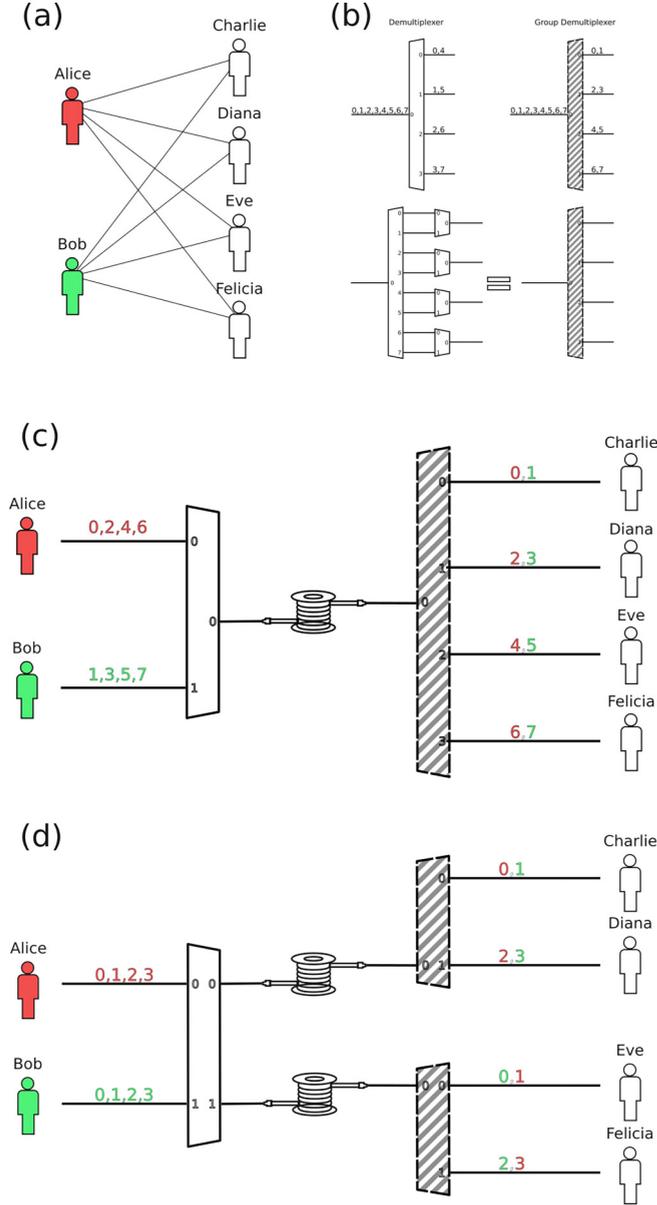
FIG. 3. (a) Logical network for two groups connected in a point-to-multipoint topology. (b) Schematic for a group demultiplexer. (c) General point-to-multipoint protocol for an arbitrary number of senders and receivers. On the receiver side, the demultiplexer has been replaced by a group demultiplexer (dashed outline). With this change we eliminate the coprimality condition and the OAM assignment is simplified. (d) General point-to-multipoint for multiple groups. Since the multiplexer is a unitary transformation, it has the same number of input and output ports. By using the other available outputs, one group can communicate with several other groups (situated at different locations).

topology with all receivers, yet as a group the point-to-multipoint logic is unchanged.

In Fig. 3(d) we split the group demultiplexer at the receivers' end into two. In large networks it will be useful to put a group multiplexer at the senders and have simple demultiplexers at the receivers. This helps to reduce the costs, since using group multiplexers scales as $d_s d_r$.

TABLE I. OAM assignments for the fully connected network in Fig. 4. Each row is obtained from the one above by a circular right shift.

Sender \ Receiver	A	B	C	D
A	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 2\rangle$	$\lvert 3\rangle$
B	$\lvert 3\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert 2\rangle$
C	$\lvert 2\rangle$	$\lvert 3\rangle$	$\lvert 0\rangle$	$\lvert 1\rangle$
D	$\lvert 1\rangle$	$\lvert 2\rangle$	$\lvert 3\rangle$	$\lvert 0\rangle$

Compared to the previous protocol, we now use other outputs of the multiplexer to communicate with different groups. Everything remains the same, except for an offset of the OAM value, which depends on the receiver group,

$$l_{sgr} = s + rd_s \ominus g, \tag{4}$$

where g is the group number (i.e., the output port of the multiplexer).

Consider the example in Fig. 3(d), where Bob intends to communicate to Eve; we have sender $s = 1$ transmitting to receiver $r = 0$ from group $g = 1$, with a multiplexer of size $d_s = 2$. Thus their OAM value is 0. Notice that this OAM value is no longer unique, since Alice uses the same OAM to communicate to Charlie.

This architecture helps to reduce the OAM bandwidth, i.e., the number of OAM values required. Both schemes in Fig. 3 have $d_s = 2$ senders and $d_r = 4$ receivers. However, in the case in Fig. 3(c) we need $d_s d_r = 6$ OAM values, whereas in Fig. 3(d) we need only $d_r = 4$ values. In both cases any sender can communicate with any receiver.

A variation of this architecture is to use a group multiplexer at the senders' side and only demultiplexers at the receivers' side. In this case the OAM value is

$$l_{sgr} = r + sd_r \ominus gd_s. \tag{5}$$

C. Fully connected networks

Finally, we generalize the previous schemes to a fully connected network, in which any two users can communicate with each other. In this case all nodes are both senders and receivers. In the previous point-to-multipoint protocol, this will work for a reasonable numbers of users, as the size of the group demultiplexer scales as $O(n^2)$.

Surprisingly however, a single mux-demux device is enough to create a fully connected network with n nodes (see Fig. 4 as well as Table I). Here the senders can view the OAM value as an indexing list: 0 for themselves, 1 for the next user (mod d), 2 for the second over (mod d), and so on. Now each node is both a sender and a receiver.

Thus a fully connected network with n users requires only a single n-dimensional quantum sorter (acting as a mux-demux device) and n OAM values. In fact, since the OAM value $\ell = 0$ is used to connect a node to itself, we need only $n - 1$ OAM values.

At first sight it looks like each node needs two different channels to connect to the network, one for sending and one for receiving. However, using two circulators, one at the user
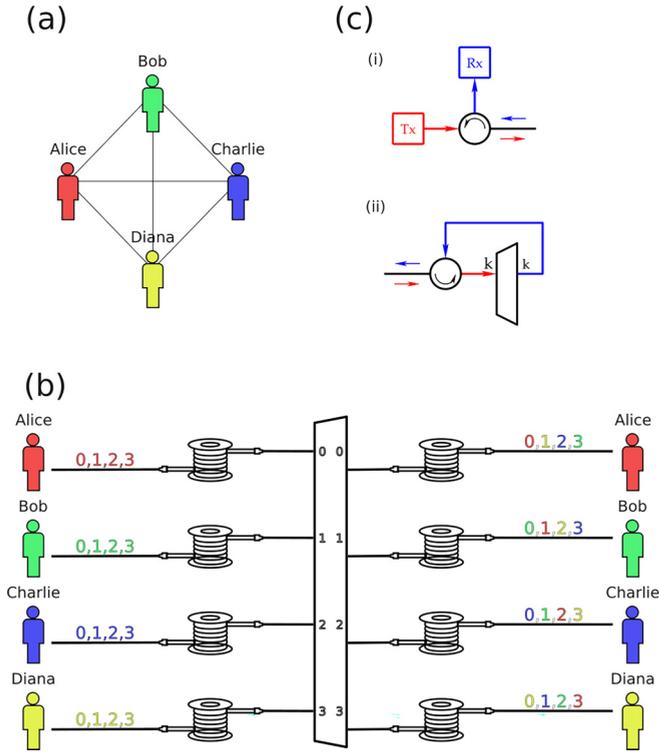
FIG. 4. (a) Logical network for a fully connected network topology. (b) Fully connected, n-node quantum network; each node is both a sender and a receiver. A single n-dimensional (mux-demux) sorter routes information between all the nodes. (c) Circulators on the (i) node side and (ii) demux side allow each node to be both a transmitter Tx and a receiver Rx. Each node is connected to the (central) demux by a single fiber and thus to the rest of the network.

side and the other at the mux-demux side, a node can use a single channel for both sending and receiving [see Fig. 4(c)].

This design is the most general possible, connecting all network nodes. It can be used as a fully connected network in prepare-and-measure QKD. The strength of this approach can be seen in Table II, since the fully connected network has the lowest resource requirements.

D. Entanglement-distribution networks

So far we have discussed networks for prepare-and-measure QKD protocols, such as BB84. Another important class of QKD protocols is entanglement-based ones, e.g., E91

TABLE II. Resource scaling for different network architectures. The fully connected network requires one quantum sorter, whereas all the other architectures require at least two.

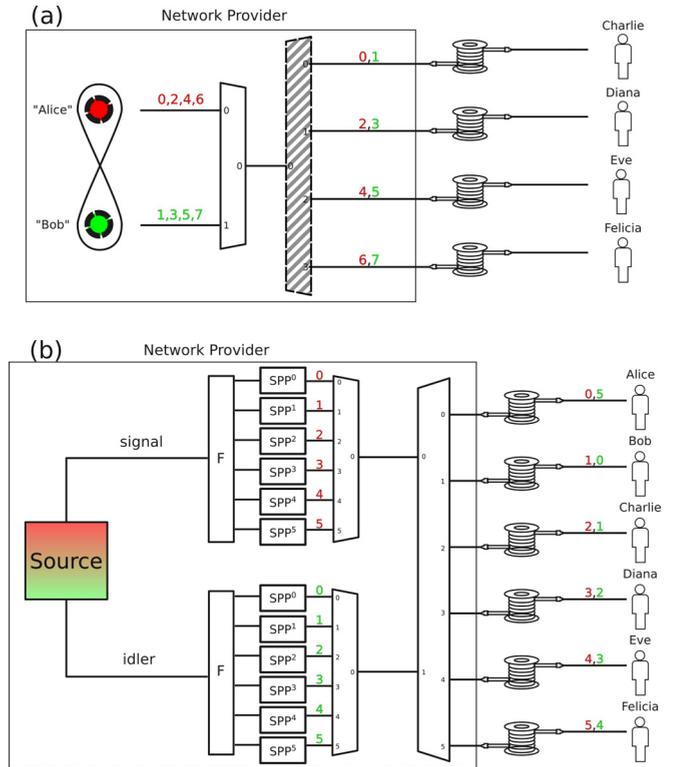| Network architecture	Resource scaling
point to point	$1 \times U_{d_s}$; $1 \times U_{d_r}$
point to multipoint (general)	$1 \times U_d$; $(\frac{d}{2} + 1) \times U_2$
point to multipoint (groups)	$1 \times U_{d_s}$; $d_s \times U_{d_r}$
fully connected	$1 \times U_d$
entanglement distribution (active)	$1 \times U_d$; $(\frac{d}{2} + 1) \times U_2$
entanglement distribution (passive)	$3 \times U_d$; $2d \times \text{SPP}(i)$

FIG. 5. (a) Fully connected network for entanglement distribution using an active central provider. If in the general point-to-multipoint network one group sends entangled pairs (or multipartite entangled states) to the other, the receiving group becomes a fully connected network for entanglement-based QKD. (b) Fully connected network for entanglement distribution from a passive central provider. In this scheme the senders are replaced by a source of entangled photons which are then randomly assigned OAM numbers, thus generating random pairs of users which share an entangled state.

or BBM92. Although entanglement-based protocols are more secure than prepare-and-measure ones, they are also more difficult to implement, as they require one to distribute entanglement between nodes.

Multiuser entanglement-distribution networks have been experimentally demonstrated for wavelength multiplexing [49,50]. Similar passive-switching networks with a central node can be designed for OAM.

Entanglement-distribution networks can be actively or passively switched. In an active network, the central node (the source) generates pairs of polarization-entangled photons. An active switch then assigns the correct OAM values r and s to the two photons and then distributes the photons to the corresponding nodes r and s. For example, the actively switched entanglement distribution scheme in Ref. [49] can be translated directly in the OAM domain with a general point-to-multipoint network, as in Fig. 5(a). Here "Alice" and "Bob" are two entangled photons that are distributed based on their assigned OAM value.

Notice that even though the network is not fully connected in the prepare-and-measure regime, it becomes so for entanglement distribution. It is fully connected, i.e., any two users can share an entangled pair. A passive-switching network for

entanglement distribution has been experimentally demonstrated in Ref. [50].

A passively switched network works in a similar way to the choice of measurement basis in BB84, where a beam splitter randomly chooses the basis. In the case of a passive OAM network, two Fourier gates F_d (which generalize the beam splitter for $d > 2$) put the signal and idler photon into two distinct multipath interferometers, one for the signal and one for the idler [see Fig. 5(b)]. For the signal photon we have

$$F_d |0\rangle_{\text{path}} = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_{\text{path}}.$$

Each path i of the interferometer has an ith-order spiral phase plate and changes the OAM $|0\rangle_{\text{OAM}} \rightarrow |i\rangle_{\text{OAM}}$:

$$\text{SPP}^i |0\rangle_{\text{OAM}} |i\rangle_{\text{path}} = |i\rangle_{\text{OAM}} |i\rangle_{\text{path}}.$$

The paths (channels) are then multiplexed into a common exit path. Subsequently, the two photons are input into path 0 (the signal) and path 1 (the idler) of a final OAM demultiplexer, respectively, which distributes the two photons to the final users [Fig. 5(b)]. The final quantum state of the two photons is (for simplicity we omit the polarization part)

$$\frac{1}{d} \sum_{i=0}^{d-1} \sum_{j=0}^{d-1} |i, j \ominus 1\rangle_{\text{OAM}} |i, j\rangle_{\text{path}}. \tag{6}$$

In this case entanglement distribution between nodes is done randomly, according to the OAM values of the signal and idler (via postselection). Similar to other passively switched networks [50], the pairs of nodes (randomly) receiving the entangled pair are identified by coincidences in their detectors.

E. Nonideal case

So far we have discussed the ideal noiseless case. We now briefly analyze the effect of noise. There are two types of losses: (i) in the quantum channel (optical fibers, free space, underwater, etc.) and (ii) in the quantum sorters. Losses in the quantum channel depend on the specific losses in the fibers (e.g., Raman absorption), atmospheric turbulence, water turbidity, etc. Since these are common to all quantum communication protocols using the same type of channel, we will not discuss them here.

Losses due to a nonideal mass sorter have been discussed in Ref. [42], including a discussion about decoherence. The OAM sorter and mass sorter have the same quantum network: They are both equivalent to a controlled-X_d gate $C(X_d)$. Thus the conclusion of the previous analysis also holds for the OAM sorter. Specifically, for $d = 3$ the probability of sorting correctly is greater than 96% even for phase errors as high as $2\pi/15$, representing 20% of the relevant phase for the system (see Fig. 6 of Ref. [42]).

IV. CONCLUSION

The development of quantum communication networks and the advent of the future quantum internet are contingent on the ability to route quantum information in networks with complex topologies. In the scenario investigated here, a set of users sends quantum states $|\psi\rangle_q$, entangled or not, to another

set of receivers. Similar to the classical case, the scarcity of certain resources, like long-distance optical cables, means that signals between different nodes use a common communication channel. This implies that we need to multiplex and demultiplex quantum signals from and to different users (nodes), respectively. In order to achieve this, here we use OAM to route the quantum state $|\psi\rangle_q$ between different users.

In this article we have discussed several network architectures for pairwise communication between multiple parties. Starting from a simple one-to-one network, we then developed one-to-many and fully connected networks for distributing quantum states. We have shown that a fully connected network with n nodes can be achieved with minimal resources: a single quantum sorter acting as a mux-demux device, connected to all n nodes. Moreover, this fully connected network requires only $n - 1$ OAM values. Finally, we have developed an entanglement-distribution protocol which has several advantages compared to the current wavelength-based networks.

The central element of all the networks discussed here is the quantum sorter which acts as a mux-demux device. The quantum sorter has a cyclic property which was used extensively in building a multitude of network architectures. These networks can be used to distribute quantum states between nodes, both in prepare-and-measure protocols (BB84) and in entanglement-based ones (E91 and BBM92).

The protocols described here can be implemented either in optical fibers or in free space. As future applications, we envisage our protocols being used in a wide range of communication tasks, such as terrestrial (intra- and intercity), satellite-to-satellite, or satellite-to-ground networks.

APPENDIX A: QUANTUM OAM SORTER

The OAM sorter U_d used here is an example of the more general universal quantum sorter introduced in [37]. The sorter is a Mach-Zehnder interferometer with d paths and with different phase shifts in each arm. For path k, the phase shifts are given by Dove prisms rotated with angles $\alpha_k = k\pi/d$,
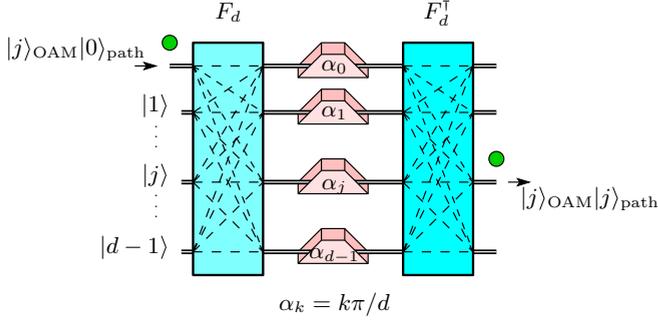
FIG. 6. The OAM sorter U_d is a Mach-Zehnder interferometer with d paths and with different phase shifts α_k on each path. A photon with OAM $|j\rangle$ enters on path 0 and exits through path $|j\rangle$ with unit probability, i.e., is sorted according to its OAM value.

$k = 0, \ldots, d-1$ (see Fig. 6). The F_d and $F_d^\dagger$ are discrete Fourier gates acting only on the path degree of freedom; they are equivalent to multimode couplers with appropriate phases

$$F_d|k\rangle_{\text{path}} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{kj} |j\rangle_{\text{path}},$$

with $\omega = e^{2\pi i/d}$ a root of unity of order d. We also have $F_d^4 = I$, $F_d^\dagger = F_d^3$, and $F_d^2|k\rangle = |-k\rangle = |d-k\rangle$.

Due to constructive interference, a particle with OAM $|j\rangle$ entering the interferometer on input 0 will exit with unit probability on path j: $|j\rangle_{\text{OAM}}|0\rangle_{\text{path}} \rightarrow |j\rangle_{\text{OAM}}|j\rangle_{\text{path}}$. This might seem quite abstract. We now give a physical intuition of how the sorter works. Consider first the simplest case of sorting two states, $d = 2$. In this case the sorter is a Mach-Zehnder interferometer with a Dove prism in each arm; the prisms are rotated relative to each other by $\pi/2$ [35]. Thus, an incoming photon with $\ell = 0$ will get a relative phase shift (between the two arms) $\delta\varphi = 0$ and will exit, with unit probability, through output port 0 (constructive interference). On the other hand, an incoming photon with $\ell = 1$ will get a relative phase shift $\delta\varphi = \pi/2$ and will exit through output port 1, again with unit probability (destructive interference).

The general case is similar. The sorter is now a Mach-Zehnder interferometer with d paths and its role is to induce state-dependent relative phases between the arms. For example, a photon in the state $\ell = 0$ will have relative phases $(0, 0, \ldots, 0)$ and will exit with unit probability through exit 0, a photon with $\ell = 1$ will have relative phases $(0, \pi/d, \ldots, (d-1)\pi/d)$ and will exit with unit probability through exit 1, and so on. Thus the relative phases experienced by a photon depend on the OAM value $\ell = k$. In turn, the relative phases determine, through constructive or destructive interference, the output k through which the photon will exit.

APPENDIX B: THE BB84 PROTOCOL

The OAM-assisted BB84 protocol in polarization encoding can be implemented with the network shown in Fig. 1. In this case there are d senders and receivers. Sender i sends to receiver i the qubit $|\psi_i\rangle_q := \alpha_i|H\rangle + \beta_i|V\rangle$, encoded in polarization. Each pair (sender i and receiver i) has allocated an OAM value $i \in \{0, \ldots, d-1\}$; thus the initial state at sender i

TABLE III. OAM correspondence chart for d_s senders and d_r receivers.

Sender \ Receiver	0	1	$\cdots$	$d_r - 1$
0	$|0\rangle$	$|d_s\rangle$	$\cdots$	$|(d_r-1)d_s\rangle$
1	$|1\rangle$	$|d_s+1\rangle$	$\cdots$	$|(d_r-1)d_s+1\rangle$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$d_s - 1$	$|d_s-1\rangle$	$|2d_s-1\rangle$	$\cdots$	$|d_r d_s-1\rangle$

is $|\psi_i\rangle_q|i\rangle_{\text{OAM}}|i\rangle_{\text{path}}$. Since the polarization qubit is unchanged by the mux-demux device, we will thus omit it for simplicity. The action of the device is

$$|i\rangle_{\text{OAM}}|i\rangle_{\text{path}} \xrightarrow{U_d^\dagger} |i\rangle_{\text{OAM}}|0\rangle_{\text{path}} \xrightarrow{U_d} |i\rangle_{\text{OAM}}|i\rangle_{\text{path}}.$$

In order to measure the polarization state, each receiver has the standard BB84 setup: a beam splitter, a half waveplate, two polarizing beam splitters, and four single-photon detectors.

The protocol also works for the networks discussed in Sec. III, if the sender chooses an appropriate OAM value. In Fig. 3 the sender s chooses an OAM value equal to r in order to send to receiver r (see Appendix D): $|\psi_{sr}\rangle_q|r\rangle_{\text{OAM}}|s\rangle_{\text{path}}$.

In Fig. 2 the sender s communicates with receiver r: $|\psi_{sr}\rangle_q|sqd_r + rpd_s\rangle_{\text{OAM}}|s\rangle_{\text{path}}$. Here p and q are the Bezout coefficients of the identity $pd_s + qd_r = 1$ and d_s and d_r are the numbers of senders and receivers, respectively (see Appendix C).

APPENDIX C: COPRIME CASE

For d_s senders and d_r receivers we can prove that any sender s can transmit to any receiver r if they share an OAM state $|l_{sr}\rangle_{\text{OAM}}$ satisfying the conditions

$$l_{sr} = pd_s + s,$$
$$l_{sr} = qd_r + r,$$

with $s \in \{0, \ldots, d_s - 1\}$, $r \in \{0, \ldots, d_r - 1\}$, and p and q integers. This is equivalent to the congruence relations

$$l_{sr} \equiv s \pmod{d_s},$$
$$l_{sr} \equiv r \pmod{d_r}. \tag{C1}$$

From the Chinese remainder theorem we know that d_s and d_r need to be coprime and only one $l_{sr} \in \{0, \ldots, d_s d_r - 1\}$ satisfies these conditions for fixed s and r. This means that we can design a network with only a d_s-dimensional mux $U_{d_s}^\dagger$ and a d_r-dimensional demux U_{d_r} (see Fig. 2).

Given a sender s and a receiver r, we can find their assigned OAM state $|l_{sr}\rangle_{\text{OAM}}$ by solving the congruence relations (C1). This gives $l_{sr} = sqd_r + rpd_s$, where p and q are the Bezout coefficients of the identity $pd_s + qd_r = 1$, which are calculated using the extended Euclidean algorithm.

The protocol requires the number of senders and the number of receivers to be coprime. In practice we can always satisfy the coprimality condition by embedding the number of senders and/or receivers into larger sets with coprime cardinality.

TABLE IV. Reference chart for $d_s = 2$, $d_r = 3$, and the OAM DOF spanning from $|0\rangle$ to $|5\rangle$.

Sender \ Receiver	0	1	2
0	$|0\rangle$	$|2\rangle$	$|4\rangle$
1	$|1\rangle$	$|3\rangle$	$|5\rangle$

APPENDIX D: GENERAL POINT-TO-MULTIPOINT OAM NETWORK

Our goal is to establish a general pairwise communication protocol between d_s senders and d_r receivers such that any sender s can communicate with any receiver r. The protocol must be free from the coprimality condition discussed in Appendix C. In this case there are $d_s d_r$ pairs (sender s and receiver r), with $s \in \{0, \ldots, d_s - 1\}$ and $r \in \{0, \ldots, d_r - 1\}$.

We group the OAM values as in Table III, where each row shows the OAMs available to sender s and each column the OAMs received by receiver r. Note that the element in row s, column r is $|s + rd_s\rangle$; thus we can assign each pair (sender s and receiver r) a unique OAM state $|l_{sr}\rangle_{\text{OAM}}$, with $l_{sr} = s + rd_s$, requiring $d_s d_r$ OAM states in total.

Example. For two senders ($d_s = 2$) and three receivers ($d_r = 3$), if sender 0 ($s = 0$) wants to communicate with receiver 1 ($r = 1$), the appropriate OAM state is $|l_{sr}\rangle_{\text{OAM}} = |s + rd_s\rangle_{\text{OAM}} = |0 + 1 \times 2\rangle_{\text{OAM}} = |2\rangle_{\text{OAM}}$ (see Table IV).

Figure 3(c) shows the physical implementation of the general point-to-multipoint network for two senders and four receivers. In general, sender s starts with the OAM state $|s + rd_s\rangle_{\text{OAM}}$ on path $|s\rangle_{\text{path}}$. The state is then multiplexed into a single transmission channel

$$|s + rd_s\rangle_{\text{OAM}} |s\rangle_{\text{path}} \xrightarrow{U_{d_s}^\dagger} |s + rd_s\rangle_{\text{OAM}} |0\rangle_{\text{path}}.$$

The demultiplexer at the receiver's end is much larger, splitting the channel into $d_s d_r$ paths, one for each OAM. These are then grouped into d_r groups of d_s channels and multiplexed back together by d_r multiplexers $U_{d_s}^\dagger$. For simplicity, we can take the demultiplexer and the d_r multiplexers to be a single device called a group demultiplexer G, represented by a dashed outline in the figures (see Appendix E). We mark the paths inside the device as local paths; therefore,

$$|s + rd_s\rangle_{\text{OAM}} |0\rangle_{\text{path}} \xrightarrow{U_{d_s d_r}} |s + rd_s\rangle_{\text{OAM}} |s + rd_s\rangle_{\text{local}},$$

$$|s + rd_s\rangle_{\text{OAM}} |s + rd_s\rangle_{\text{local}} \xrightarrow{U_{d_s}^\dagger} |s + rd_s\rangle_{\text{OAM}} |rd_s\rangle_{\text{local}}.$$

TABLE V. Outputs of a group demultiplexer.

Output \ OAM	0	1	$\cdots$	$d_s - 1$
0	$|0\rangle$	$|1\rangle$	$\cdots$	$|d_s - 1\rangle$
1	$|d_s\rangle$	$|d_s + 1\rangle$	$\cdots$	$|2d_s - 1\rangle$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$d_r - 1$	$|(d_r - 1)d_s\rangle$	$|(d_r - 1)d_s + 1\rangle$	$\cdots$	$|d_r d_s - 1\rangle$

There are gaps of d_s between output ports on the local path. We can map back to the global path by dividing the output port by d_s ($|rd_s\rangle_{\text{local}} \mapsto |r\rangle_{\text{path}}$). The full action of the group demultiplexer $G_{d_s}^{d_r}$ (makes d_r groups of dimension d_s) is then

$$|s + rd_s\rangle_{\text{OAM}} |0\rangle_{\text{path}} \xrightarrow{G_{d_s}^{d_r}} |s + rd_s\rangle_{\text{OAM}} |r\rangle_{\text{path}}.$$

Finally, the action of the protocol is

$$|s + rd_s\rangle_{\text{OAM}} |s\rangle_{\text{path}} \xrightarrow{U_{d_s}^\dagger,\, G_{d_s}^{d_r}} |s + rd_s\rangle_{\text{OAM}} |r\rangle_{\text{path}}.$$

If sender s wants, for example, to transmit a qubit to receiver r, they encode the information in the polarization DOF $\alpha_{sr} |H\rangle + \beta_{sr} |V\rangle$ with OAM $|s + rd_s\rangle_{\text{OAM}}$ on path $|s\rangle_{\text{path}}$. The receiver recovers the information encoded in the qubit via polarization state detection on path $|r\rangle_{\text{path}}$. This way we can ensure the general pairwise quantum communication between several parties through a single channel. Moreover, if the two groups of senders and receivers are the same, the network becomes effectively a fully connected network.

APPENDIX E: GROUP DEMULTIPLEXER

In Fig. 3(b) we introduced the group demultiplexer G. Imputing consecutive OAM numbers on port $|0\rangle_{\text{path}}$ into a demultiplexer U_d, we see that it distributes them on consecutive channels $l \mod d$ until it resets to output 0 when l reaches the next multiple of d. A group demultiplexer $G_{d_s}^{d_r}$ in the same situation outputs on the same channel $\lfloor \frac{l}{d_s} \rfloor$ until it moves to the next one when l reaches the next multiple of d_s as in Table V. Table V is just the transpose of Table III. Formally, we have

$$|l\rangle_{\text{OAM}} |k\rangle_{\text{path}} \xrightarrow{G_{d_s}^{d_r}} |l\rangle_{\text{OAM}} \left| \left\lfloor \frac{k \oplus l}{d_s} \right\rfloor \right\rangle_{\text{path}}.$$

[1] B. Fröhlich, J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, A quantum access network, Nature (London) **501**, 69 (2013).

[2] H.-L. Yin, Y. Fu, C.-L. Li, C.-X. Weng, B.-H. Li, J. Gu, Y.-S. Lu, S. Huang, and Z.-B. Chen, Experimental quantum secure network with digital signatures and encryption, Natl. Sci. Rev. **10**, nwac228 (2023).

[3] D. J. Richardson, Filling the light pipe, Science **330**, 327 (2010).

[4] J. Sakaguchi, B. J. Puttnam, W. Klaus, Y. Awaji, N. Wada, A. Kanno, T. Kawanishi, K. Imamura, H. Inaba, K. Mukasa *et al.*, 305 Tb/s space division multiplexed transmission using homogeneous 19-core fiber, J. Lightw. Technol. **31**, 554 (2012).

[5] J. Sakaguchi, W. Klaus, Y. Awaji, N. Wada, T. Hayashi, T. Nagashima, T. Nakanishi, T. Taru, T. Takahata, and T. Kobayashi, 228-spatial-channel bi-directional data communication system enabled by 39-core 3-mode fiber, J. Lightw. Technol. **37**, 1756 (2019).

[6] R. Ryf, S. Randel, A. H. Gnauck, C. Bolle, A. Sierra, S. Mumtaz, M. Esmaeelpour, E. C. Burrows, R.-J. Essiambre, P. J. Winzer *et al.*, Mode-division multiplexing over 96 km of few-mode fiber using coherent 6×6 MIMO processing, J. Lightw. Technol. **30**, 521 (2012).

[7] H. Huang, G. Xie, Y. Yan, N. Ahmed, Y. Ren, Y. Yue, D. Rogawski, M. Tur, B. Erkmen, K. Birnbaum *et al.*, *Proceedings of the 2013 Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference (OFC/NFOEC)* (IEEE, Piscataway, 2013), pp. 1–3.

[8] 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 **340**, 1545 (2013).

[9] G. Molina-Terriza, J. P. Torres, and L. Torner, Management of the angular momentum of light: Preparation of photons in multidimensional vector states of angular momentum, Phys. Rev. Lett. **88**, 013601 (2001).

[10] D. L. Andrews, *Structured Light and its Applications: An Introduction to Phase-Structured Beams and Nanoscale Optical Forces* (Academic, New York, 2011).

[11] Y. Zhou, M. Mirhosseini, S. Oliver, J. Zhao, S. M. H. Rafsanjani, M. P. J. Lavery, A. E. Willner, and R. W. Boyd, Using all transverse degrees of freedom in quantum communications based on a generic mode sorter, Opt. Express **27**, 10383 (2019).

[12] N. Uribe-Patarroyo, A. Fraine, D. S. Simon, O. Minaeva, and A. V. Sergienko, Object identification using correlated orbital angular momentum states, Phys. Rev. Lett. **110**, 043601 (2013).

[13] V. D'Ambrosio, N. Spagnolo, L. Del Re, S. Slussarenko, Y. Li, L. C. Kwek, L. Marrucci, S. P. Walborn, L. Aolita, and F. Sciarrino, Photonic polarization gears for ultra-sensitive angular measurements, Nat. Commun. **4**, 2432 (2013).

[14] F. Tamburini, G. Anzolin, G. Umbriaco, A. Bianchini, and C. Barbieri, Overcoming the Rayleigh criterion limit with optical vortices, Phys. Rev. Lett. **97**, 163903 (2006).

[15] A. M. Pălici, T.-A. Isdrailă, S. Ataman, and R. Ionicioiu, Interaction-free imaging of multipixel objects, Phys. Rev. A **105**, 013529 (2022).

[16] M. P. J. Lavery, F. C. Speirits, S. M. Barnett, and M. J. Padgett, Detection of a spinning object using light's orbital angular momentum, Science **341**, 537 (2013).

[17] N. Cvijetic, G. Milione, E. Ip, and T. Wang, Detecting lateral motion using light's orbital angular momentum, Sci. Rep. **5**, 15422 (2015).

[18] K. Ingerslev, P. Gregg, M. Galili, F. Da Ros, H. Hu, F. Bao, M. A. U. Castaneda, P. Kristensen, A. Rubano, L. Marrucci *et al.*, 12 mode, WDM, MIMO-free orbital angular momentum transmission, Opt. Express **26**, 20225 (2018).

[19] A. Sit, R. Fickler, F. Alsaiari, F. Bouchard, H. Larocque, P. Gregg, L. Yan, R. W. Boyd, S. Ramachandran, and E. Karimi, Quantum cryptography with structured photons through a vortex fiber, Opt. Lett. **43**, 4108 (2018).

[20] J. Zhang, J. Liu, L. Shen, L. Zhang, J. Luo, J. Liu, and S. Yu, Mode-division multiplexed transmission of wavelength-division multiplexing signals over a 100-km single-span orbital angular momentum fiber, Photon. Res. **8**, 1236 (2020).

[21] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi,

High-dimensional intracity quantum cryptography with structured photons, Optica **4**, 1006 (2017).

[22] A. S. Nikolaeva, E. O. Kiktenko, and A. K. Fedorov, Efficient realization of quantum algorithms with qudits, arXiv:2111.04384.

[23] T. C. Ralph, K. J. Resch, and A. Gilchrist, Efficient Toffoli gates using qudits, Phys. Rev. A **75**, 022313 (2007).

[24] L. Sheridan and V. Scarani, Security proof for quantum key distribution using qudit systems, Phys. Rev. A **82**, 030301(R) (2010).

[25] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of quantum key distribution using *d*-level systems, Phys. Rev. Lett. **88**, 127902 (2002).

[26] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber, Overcoming noise in entanglement distribution, Phys. Rev. X **9**, 041042 (2019).

[27] Z. Liu and H. Fan, Decay of multiqudit entanglement, Phys. Rev. A **79**, 064305 (2009).

[28] H. Bechmann-Pasquinucci and W. Tittel, Quantum cryptography using larger alphabets, Phys. Rev. A **61**, 062308 (2000).

[29] F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, High-dimensional quantum cloning and applications to quantum hacking, Sci. Adv. **3**, e1601915 (2017).

[30] D. Cozzolino, E. Polino, M. Valeri, G. Carvacho, D. Bacco, N. Spagnolo, L. K. Oxenløwe, and F. Sciarrino, Air-core fiber distribution of hybrid vector vortex-polarization entangled states, Adv. Photon. **1**, 046005 (2019).

[31] V. D'Ambrosio, E. Nagali, S. P. Walborn, S. S. Leandro Aolita, L. Marrucci, and F. Sciarrino, Complete experimental toolbox for alignment-free quantum communication, Nat. Commun. **3**, 961 (2012).

[32] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, Free-space quantum key distribution by rotation-invariant twisted photons, Phys. Rev. Lett. **113**, 060503 (2014).

[33] D. Lee, H. Sasaki, H. Fukumoto, K. Hiraga, and T. Nakagawa, Orbital angular momentum (OAM) multiplexing: An enabler of a new era of wireless communications, IEICE Trans. Commun. **E100.B**, 1044 (2017).

[34] P. Gregg, P. Kristensen, and S. Ramachandran, Conservation of orbital angular momentum in air-core optical fibers, Optica **2**, 267 (2015).

[35] J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial, Measuring the orbital angular momentum of a single photon, Phys. Rev. Lett. **88**, 257901 (2002).

[36] M. N. O'Sullivan, M. Mirhosseini, M. Malik, and R. W. Boyd, Near-perfect sorting of orbital angular momentum and angular position states of light, Opt. Express **20**, 24444 (2012).

[37] R. Ionicioiu, Sorting quantum systems efficiently, Sci. Rep. **6**, 25356 (2016).

[38] D. Fu, Y. Zhou, R. Qi, S. Oliver, Y. Wang, S. M. H. Rafsanjani, J. Zhao, M. Mirhosseini, Z. Shi, P. Zhang, and R. W. Boyd, Realization of a scalable Laguerre-Gaussian mode sorter based on a robust radial mode sorter, Opt. Express **26**, 33057 (2018).

[39] Z. Zhou, P. Li, J. Ma, S. Zhang, and Y. Gu, Generation and detection of optical vortices with multiple cascaded spiral phase plates, Photonics **9**, 354 (2022).

[40] Y. Zhou, M. Mirhosseini, D. Fu, J. Zhao, S. M. Hashemi Rafsanjani, A. E. Willner, and R. W. Boyd, Sorting photons by radial quantum number, Phys. Rev. Lett. **119**, 263602 (2017).

[41] X. Gu, M. Krenn, M. Erhard, and A. Zeilinger, Gouy phase radial mode sorter for light: Concepts and experiments, Phys. Rev. Lett. **120**, 103601 (2018).

[42] R. Ionicioiu, Interferometric mass spectrometry, J. Am. Soc. Mass Spectrom. **34**, 1160 (2023).

[43] T.-A. Isdrailă, C. Kusko, and R. Ionicioiu, Cyclic permutations for qudits in *d* dimensions, Sci. Rep. **9**, 6337 (2019).

[44] A. Asadian, P. Erker, M. Huber, and C. Klöckl, Heisenberg-Weyl observables: Bloch vectors in phase space, Phys. Rev. A **94**, 010301(R) (2016).

[45] A. M. Pălici, T.-A. Isdrailă, S. Ataman, and R. Ionicioiu, OAM tomography with Heisenberg-Weyl observables, Quantum Sci. Technol. **5**, 045004 (2020).

[46] J. Daboul, X. Wang, and B. C. Sanders, Quantum gates on hybrid qudits, J. Phys. A: Math. Gen. **36**, 2525 (2003).

[47] F. S. Khan and M. Perkowski, Synthesis of multi-qudit hybrid and *d*-valued quantum logic circuits by decomposition, Theor. Comput. Sci. **367**, 336 (2006).

[48] R. Fickler, R. Lapkiewicz, M. Huber, M. P. J. Lavery, M. J. Padgett, and A. Zeilinger, Interface between path and orbital angular momentum entanglement for high-dimensional photonic quantum information, Nat. Commun. **5**, 4502 (2014).

[49] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hubel, and R. Ursin, An entanglement-based wavelength-multiplexed quantum communication network, Nature (London) **564**, 225 (2018).

[50] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Loncaric, S. P. Neumann, T. S. Bo Liu, G. C. Lorenzo, Z. Samec, L. Kling, A. Qiu, M. Razavi, M. Stipcevic, J. G. Rarity, and R. Ursin, A trusted-node-free eight-user metropolitan quantum communication network, Sci. Adv. **6**, eaba0959 (2020).