Quantum Key Distribution with Full Laguerre-Gauss Encoding

Robert W. Boyd

Department of Physics and
Max-Planck Centre for Extreme and Quantum Photonics
University of Ottawa

The Institute of Optics and
Department of Physics and Astronomy
University of Rochester

Department of Physics and Astronomy
University of Glasgow

The visuals of this talk are available at boydnlo.ca/presentations/

Presented at the OSA Imaging and Applied Optics Congress, Orlando, FL, USA June 26, 2018.

Prospectus

1. QKD with Twisted Light
2. Why We Need to Encode in Azimuth and Radius
3. New Developments in Mode Sorters
4. Advances in Free-Space QKD

1. QKD with Twisted Light

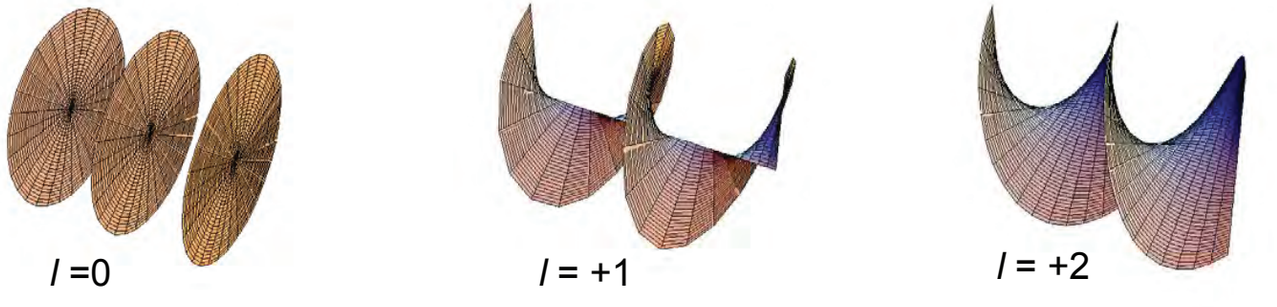
Our Research: BB84 in a High-Dimensional State Space

- Instead of using the two-dimensional state space of polarization, we use a (potentially) infinite dimensional state space of the orbital angular momentum (OAM) modes of the photon.
- One motivation is to send more than one bit of information per photon.
- Another motivation is to increase the security of the protocol.

What Are the Orbital Angular Momentum (OAM) States of Light?

- Light can carry spin angular momentum (SAM) by means of its circular polarization.
- Light can also carry orbital angular momentum (OAM) by means of the phase winding of the optical wavefront.
- A well-known example are the Laguerre-Gauss modes. These modes contain a phase factor of $\exp(i l\varphi)$ and carry angular momentum of $\hbar k$ per photon. (Here φ is the azimuthal coordinate.)

Phase-front structure of some OAM states



See, for instance, A.M. Yao and M.J. Padgett, Advances in Photonics 3, 161 (2011).

Laguerre-Gauss Modes

The paraxial approximation to the Helmholtz equation $(\nabla^2 + k^2)E(\boldsymbol{k}) = 0$ gives the paraxial wave equation which is written in the cartesian coordinate system as

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

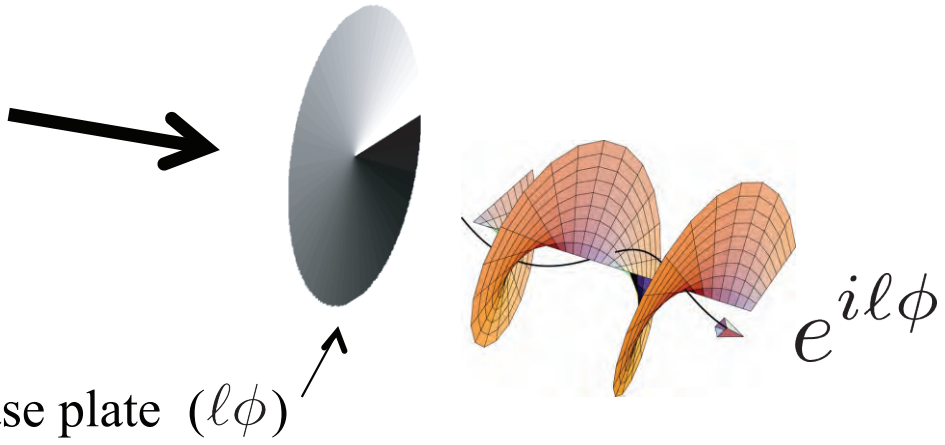
The paraxial wave equation is satisfied by the Laguerre-Gaussian modes, a family of orthogonal modes that have a well defined orbital angular momentum. The field amplitude $LG_p^l(\rho, \phi, z)$ of a normalized Laguerre-Gaussian modes is given by

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

where k is the wave-vector magnitude of the field, z_R the Rayleigh range, $w(z)$ the radius of the beam at z, l is the azimuthal quantum number, and p is the radial quantum number. L_p^l is the associated Laguerre polynomial.

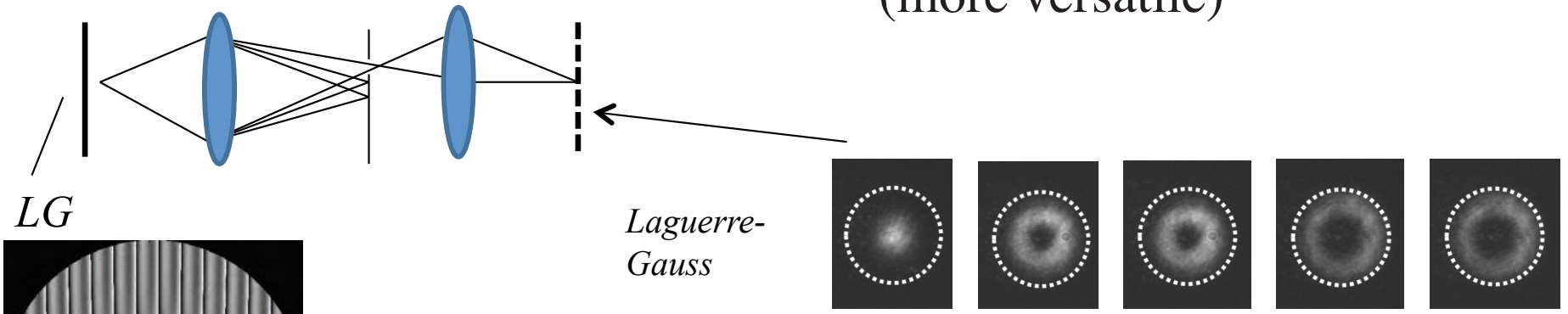
How to create a beam carrying orbital angular momentum?

Pass beam through a spiral phase plate



Use a spatial light modulator acting as a computer generated hologram

(more versatile)



Exact solution to simultaneous intensity and phase masking with a single phase-only hologram, E. Bolduc, N. Bent, E. Santamato, E. Karimi, and R. W. Boyd, Optics Letters 38, 3546 (2013).

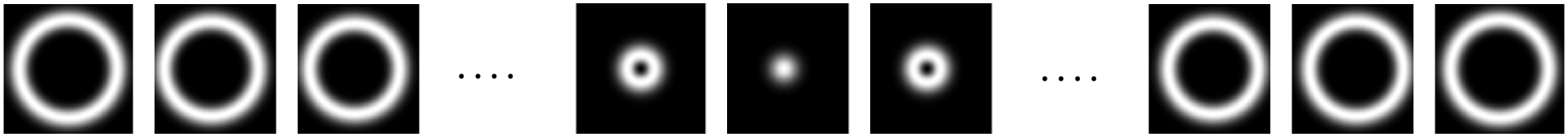
High Capacity QKD Protocol

We are developing a free-space quantum key distribution system that can carry many bits per photon (think about it!).

We encode either in the Laguerre-Gauss modes or in their linear superpositions (or in other transverse modes).

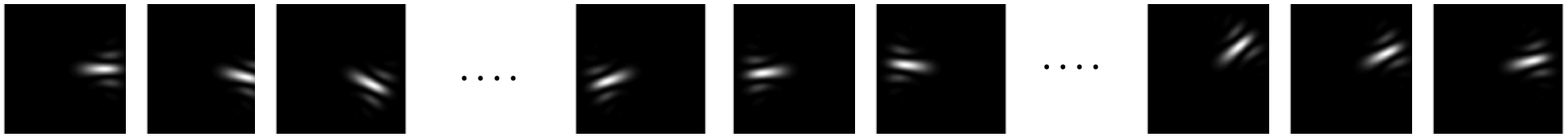
We are developing means to mitigate the influence of atmospheric turbulence

Laguerre-Gaussian Basis $\ell = -13, \ldots, 13$



0 1 2 12 13 14 25 26 27

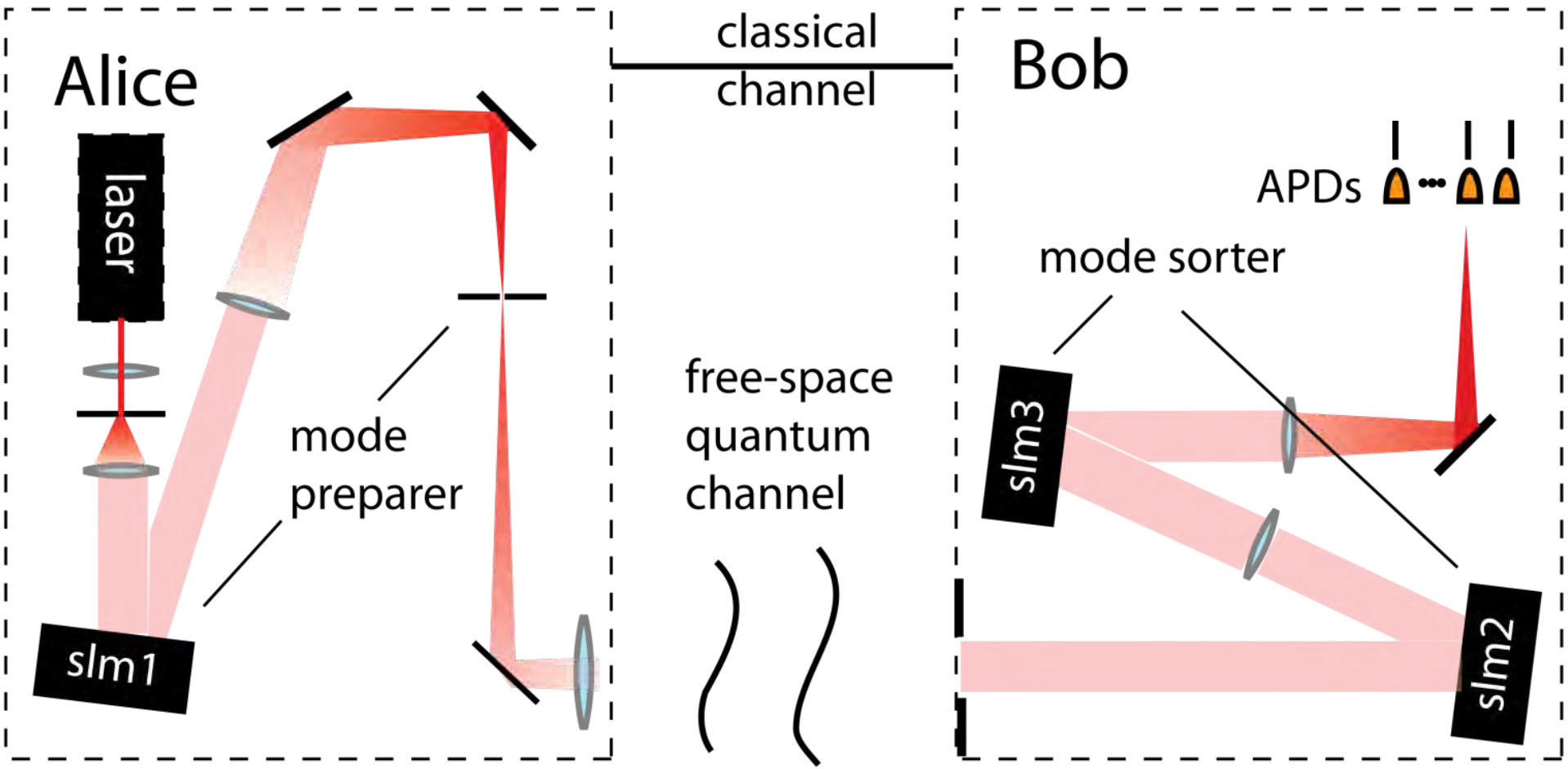
"Angular" Basis (mutually unbiased with respect to LG)



0 1 2 12 13 14 25 26 27

$$\Psi_{\mathrm{AB}}^{N} = \frac{1}{\sqrt{27}} \sum_{l=-13}^{13} \mathrm{LG}_{l,0} \exp\left(i 2\pi N l/27\right)$$

Spatially-Based QKD System



Source

Weak Coherent Light

Heralded Single Photon

Protocol

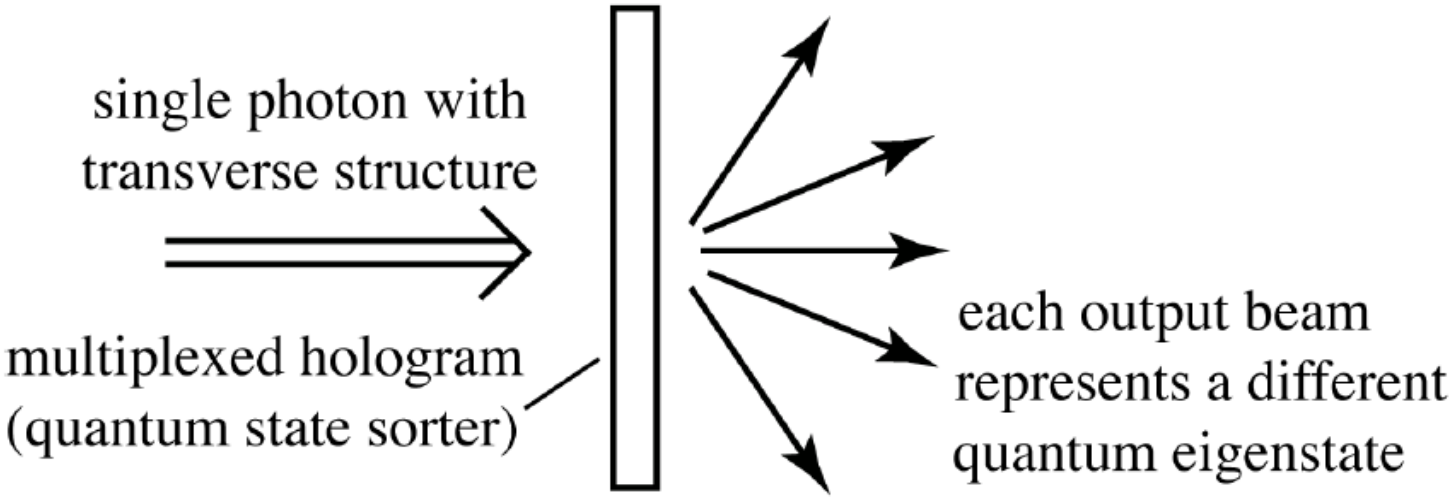
Modified BB84 as discussed

Challenges

1. State Preparation
2. State Detection
3. Turbulence

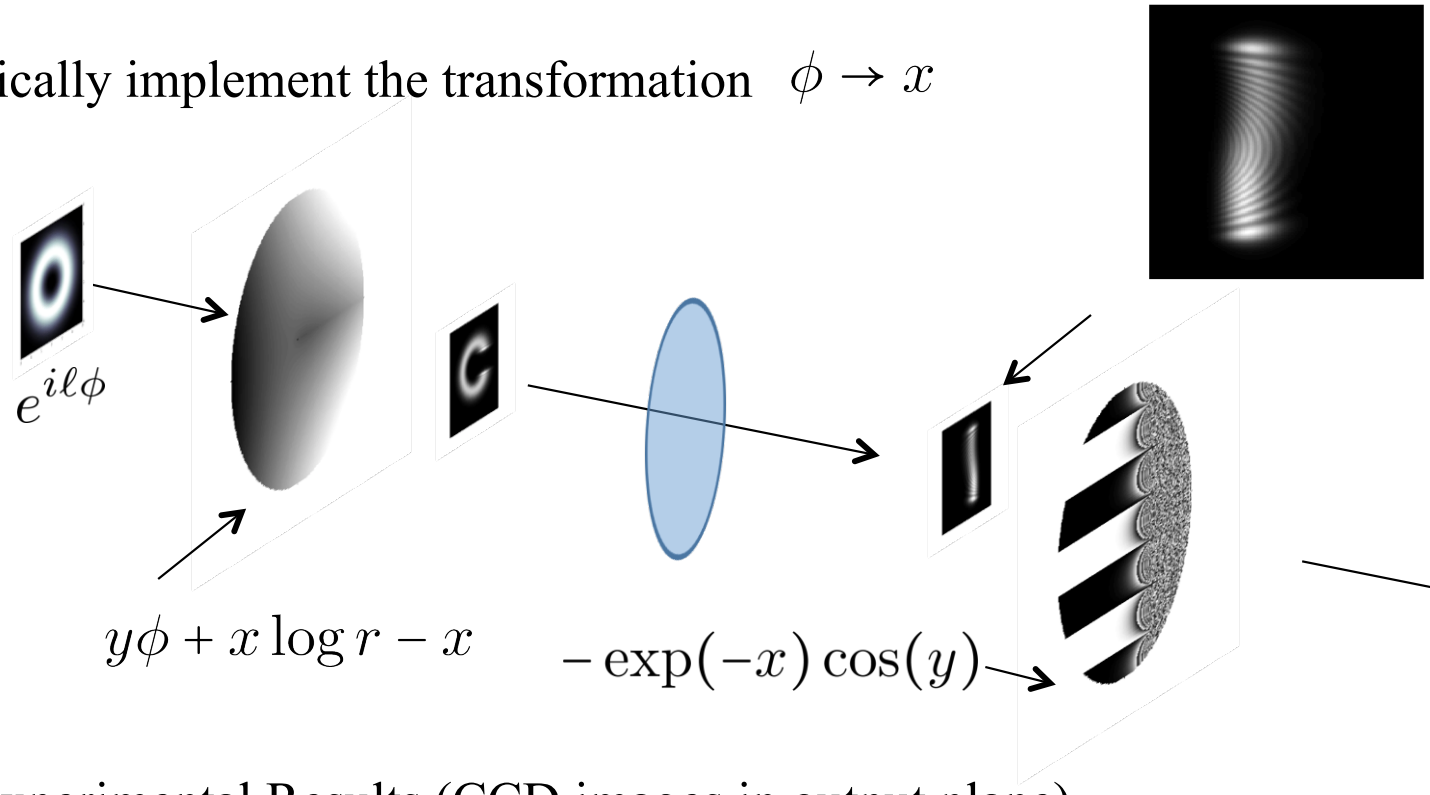
Mode Sorting

A mode sorter

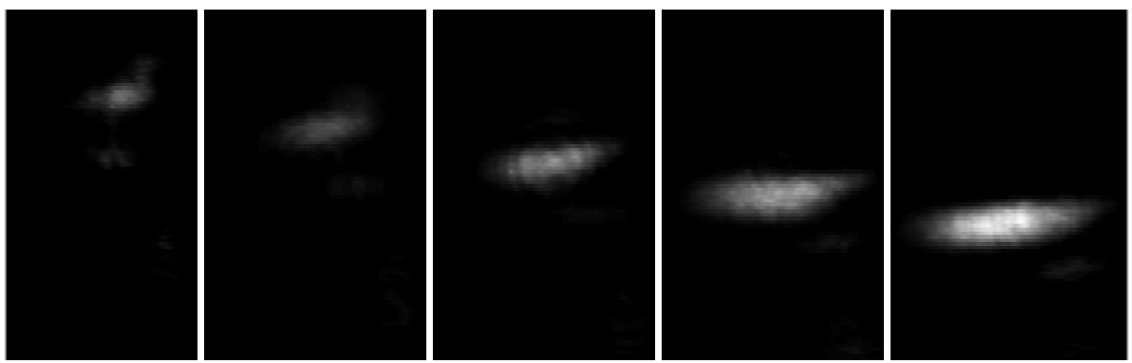


Sorting OAM using Phase Unwrapping

Optically implement the transformation $\phi \rightarrow x$



Experimental Results (CCD images in output plane)



-Can also sort angular position states.

-Limited by the overlap of neighboring states.

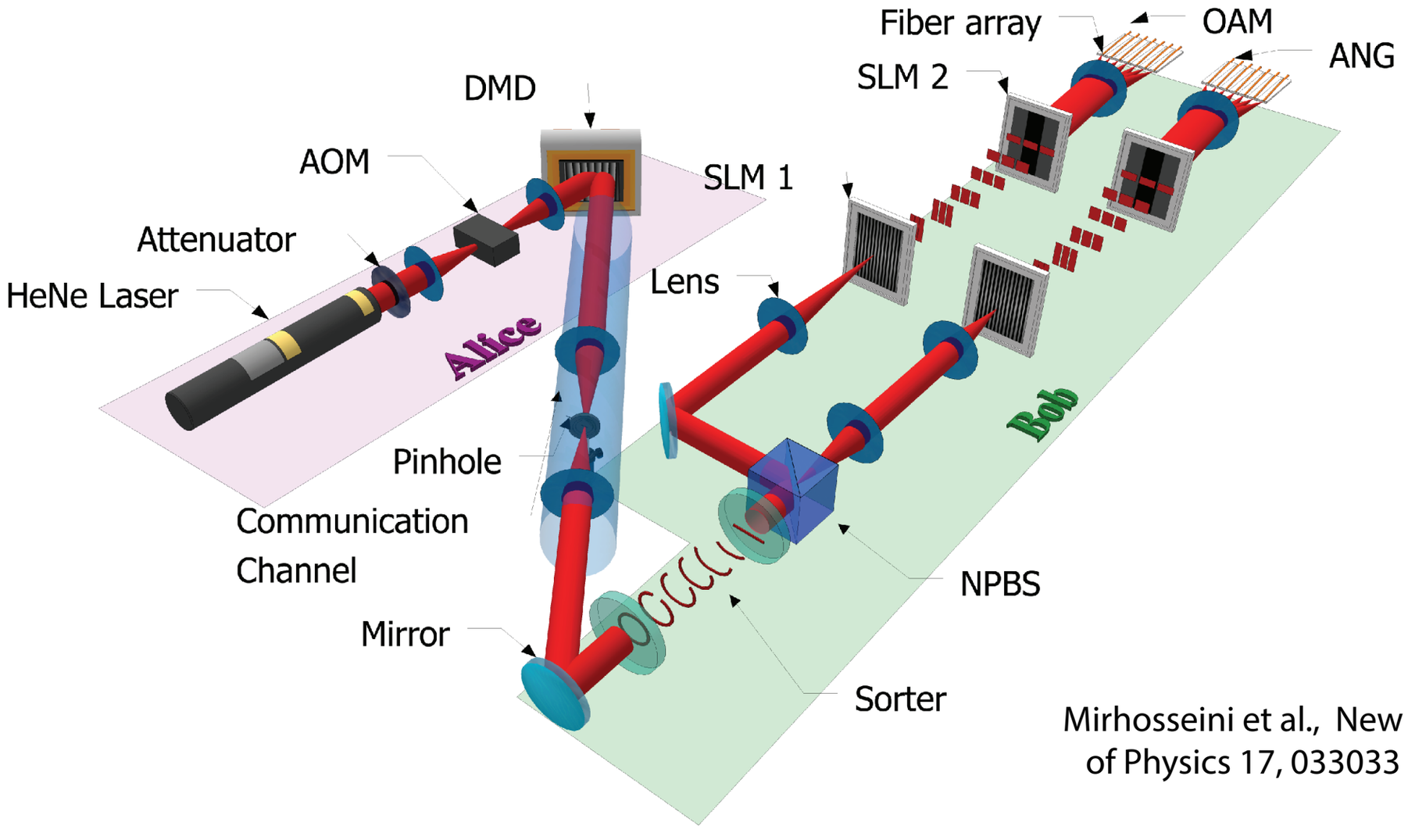
*Berkhout *et al. PRL* **105,** 153601 (2010).

O. Bryngdahl, *J. Opt. Soc. Am.* **64**, 1092 (1974).

UNIVERSITY of ROCHESTER

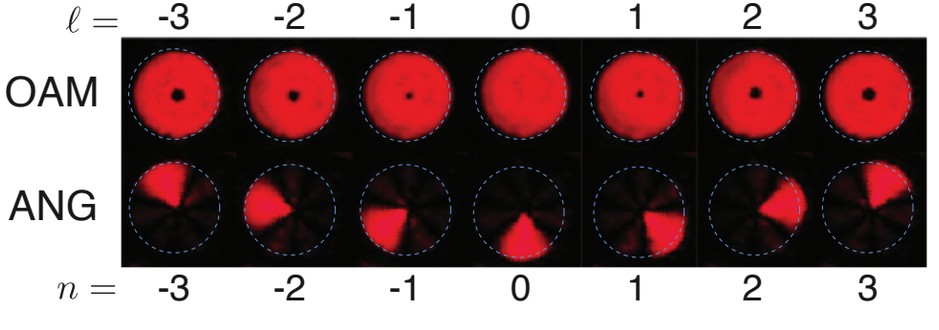
Nonlinear Optics Group

Our Laboratory Setup



Mirhosseini et al., New Journal of Physics 17, 033033 (2015).

We use a seven-dimensional state space.



Laboratory Results - OAM-Based QKD

Alice

```
0631336021320454444456141026645
5450503636030252616432155241 64
2301466025134016132224515510 26
```

Bob

```
0630336011320214444456141026645
5450223536030252616432155241 64
2301466025154036134224515510 26
```

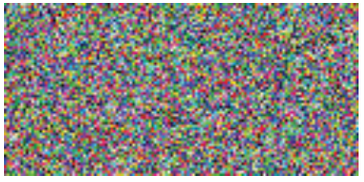
Error Correction

```
0000 0100 0111 0100 0101 0001 1100 0010 1100 1001 0010 0100 1101 0001 0000
0001 0011 0100 0000 0100 0010 0001 0001 0011 0000 0101 0010 0111 1000 0101
1101 0011 0001 1001 1011 0101 0000 0100 0111 0100 0011 0110 0101 0000 1101
0101 0010 1111 1010 1111 0010 1000
```

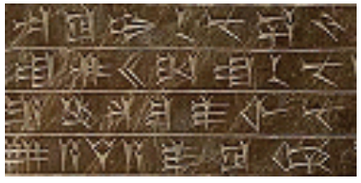
Privacy Amplification

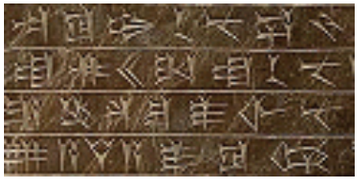
```
0001 0100 1011 1111 1111 1010 1010 0111 1010 1011 1111 0001 0000 1101 1111
1110 1110 1101 1110 0001 0011 1000 0101 1101 1100 0011 0111 1101 0001 1001
0100 0110 1011 0000 0110 1010 1
```

Alice Encrypts

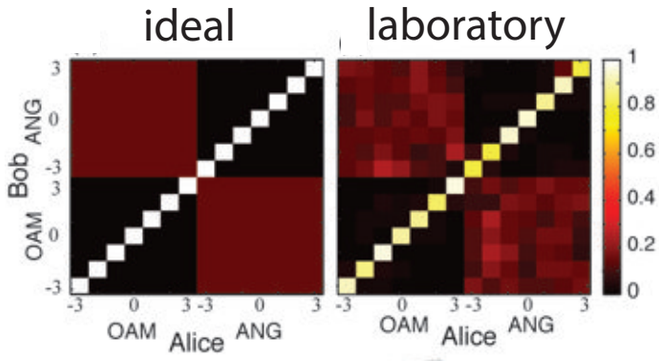


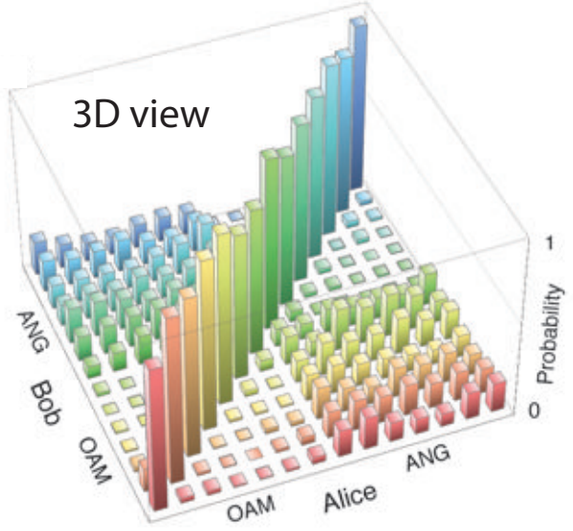
Bob Decrypts



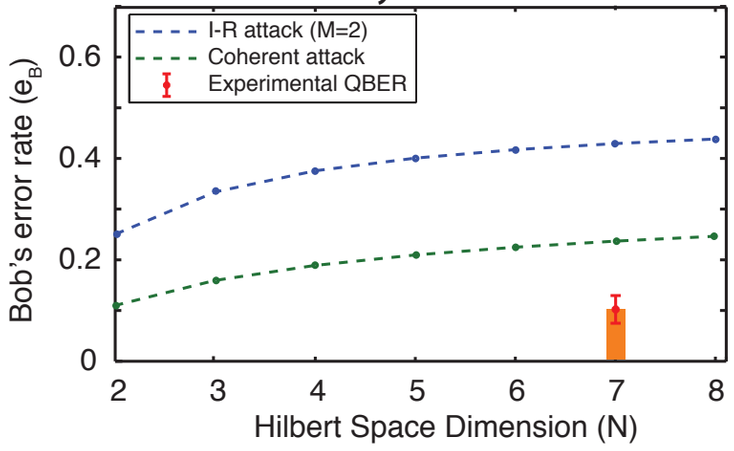


cross-talk matrices





- error bounds for security



We use a 7-letter alphabet, and achieve a channel capacity of 2.1 bits per sifted photon.

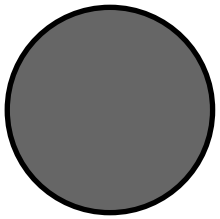
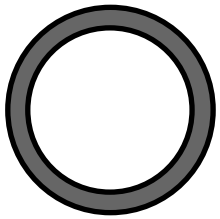
We do not reach the full 2.8 bits per photon for a variety of reasons, including dark counts in our detectors and cross-talk among channels resulting from imperfections in our sorter.

Nonetheless, our error rate is adequately low to provide full security,

2. Why We Need to Encode in Azimuth and Radius

Why We Need to Encode in Azimuth and Radius

- Large telescopes are expensive; we want to make full use of our resources

This?  Or this? 

- In concept we want to encode in communication modes, but for large Fresnel numbers they approximate Laguerre-Gauss modes.

- Laguerre-Gauss modes are described by two mode indices, one (*l*) for azimuthal variation and one (*p*) for radial variation.

- We can roughly square the size of Hilbert space by encoding in both *l* and *p*.

- Miles Padgett showed earlier how to sort in *l* . Only recently have people shown how to sort in *p*.

3. New Developments in Mode Sorters

RAPID COMMUNICATIONS

PHYSICAL REVIEW B **95**, 161108(R) (2017)

Custom-tailored spatial mode sorting by controlled random scattering

Robert Fickler,[1] Manit Ginoya,[1] and Robert W. Boyd[1,2]

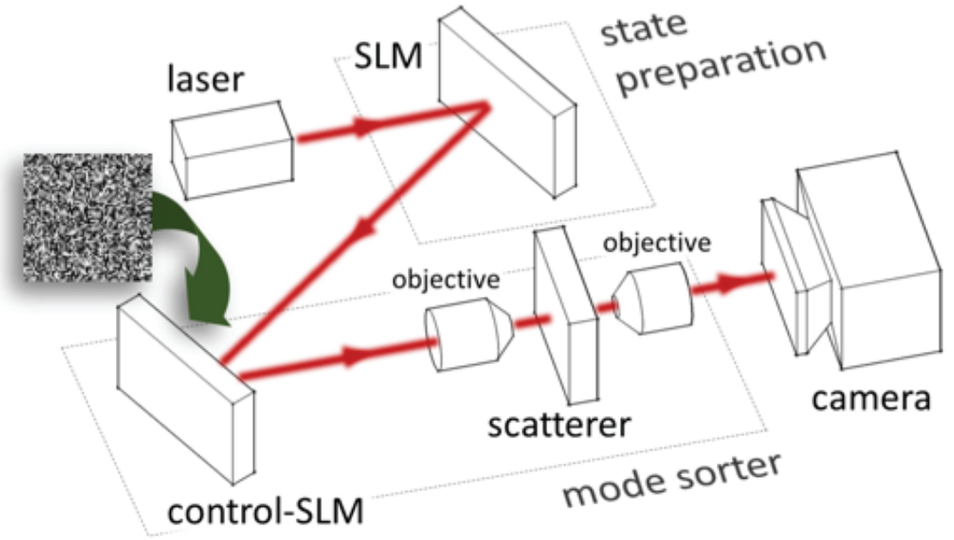
[1]*Department of Physics, University of Ottawa, Ottawa, Canada K1N 6N5*

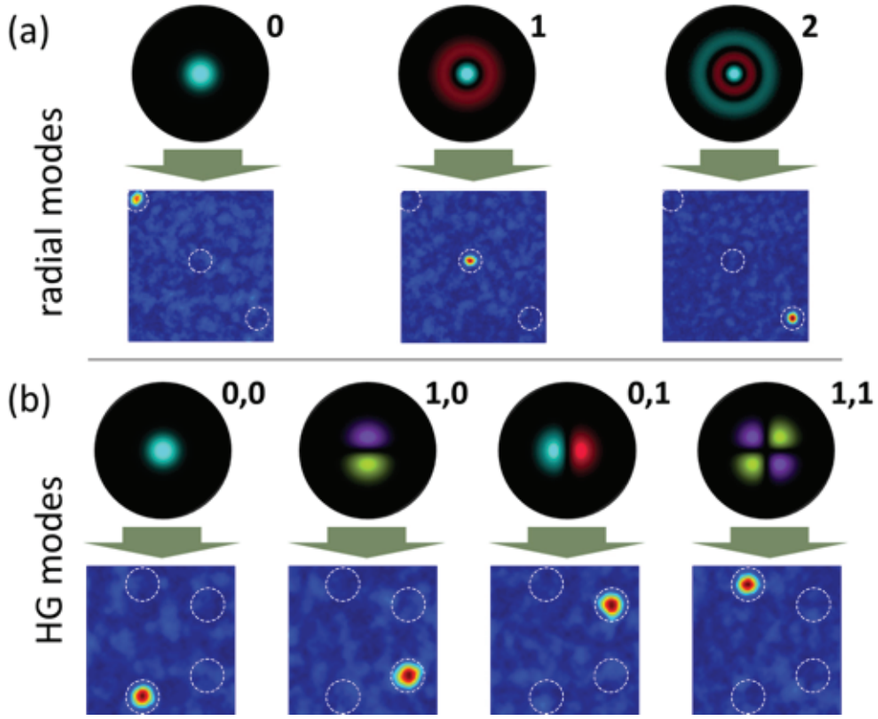
[2]*Institute of Optics, University of Rochester, Rochester, New York 14620, USA*

(Received 18 January 2017; revised manuscript received 17 March 2017; published 14 April 2017)

fidelity = 97%
efficiency = 0.2%

A genetic algorithm determines the pattern on the control SLM



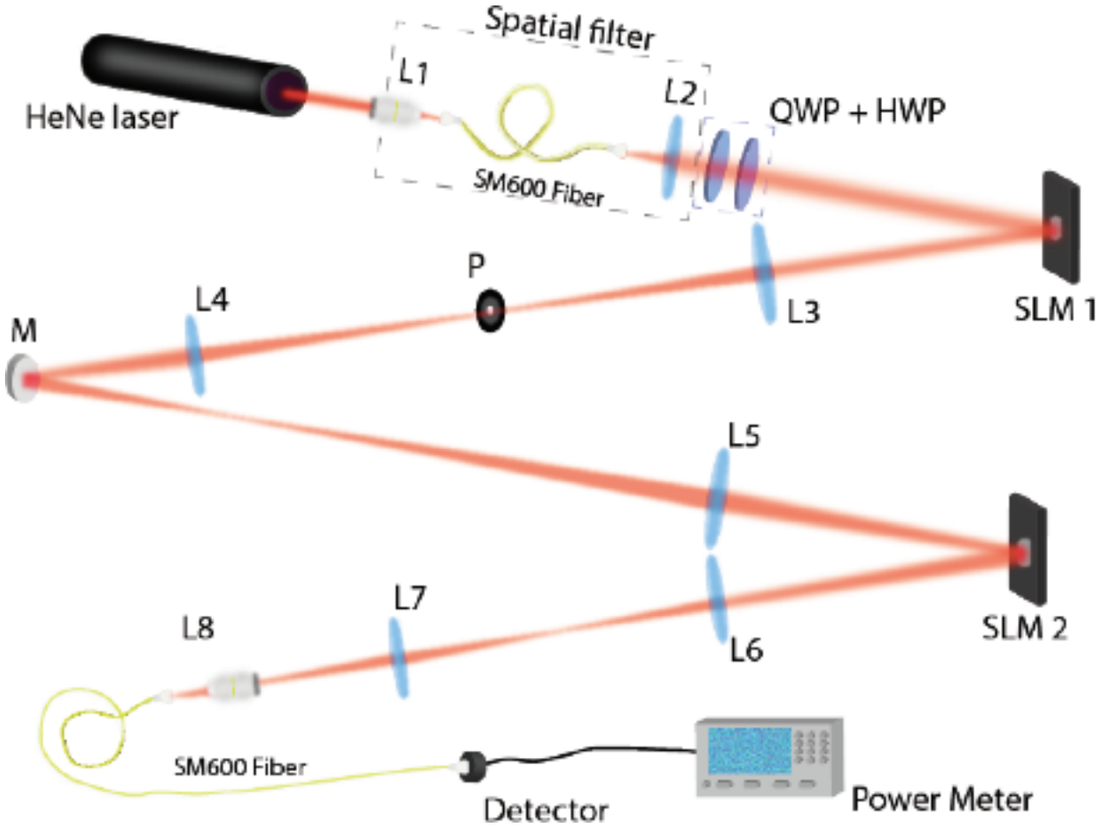


Measurement of the radial mode spectrum of photons through phase-retrieval

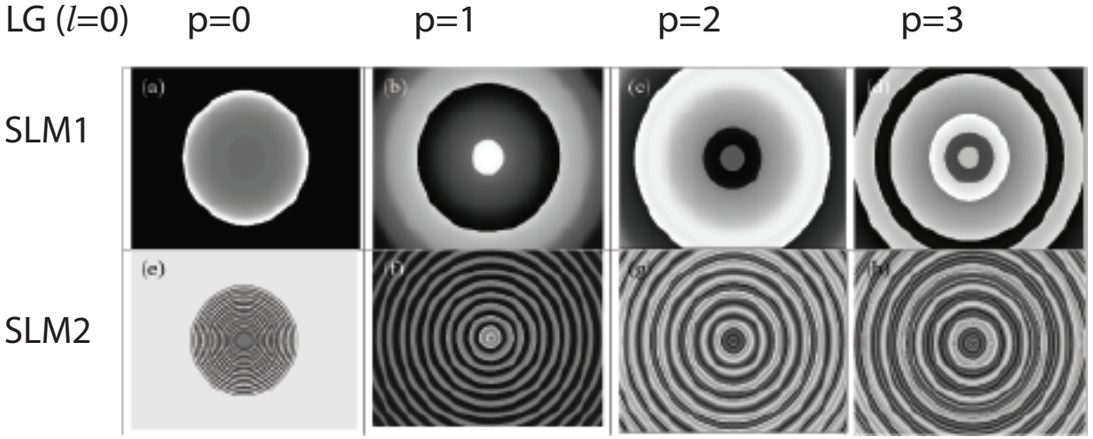
Saumya Choudhary[1], Syed Mohammad Hashemi Rafsanjani[2,*], Yoko Miyamoto[3], Rachel Sampson[4], Omar S. Magana-Loaiza[5], Mohammad Mirhosseini[6], and Robert W. Boyd[1,7]

Use Gerchberg-Saxton phase-retrieval algorithm

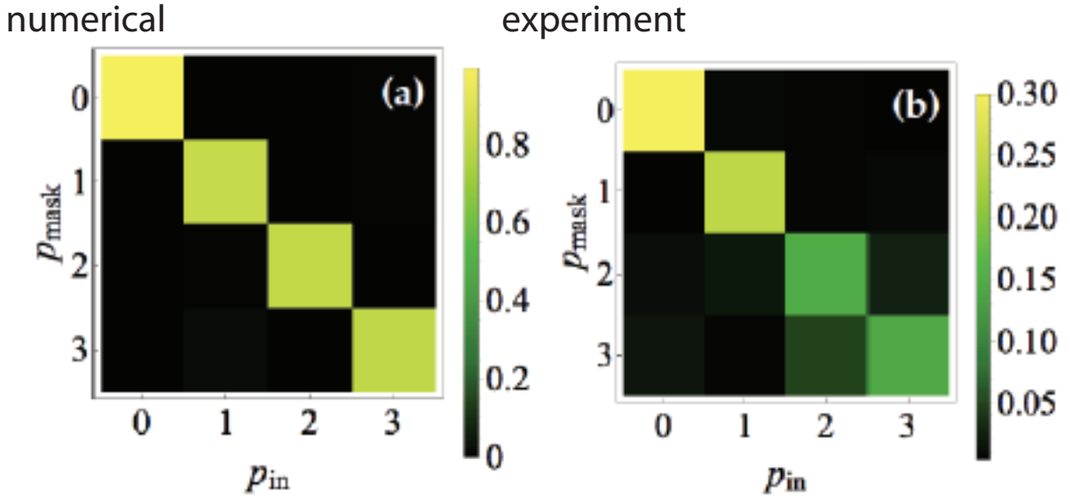
Laboratory Setup



Phase Screens



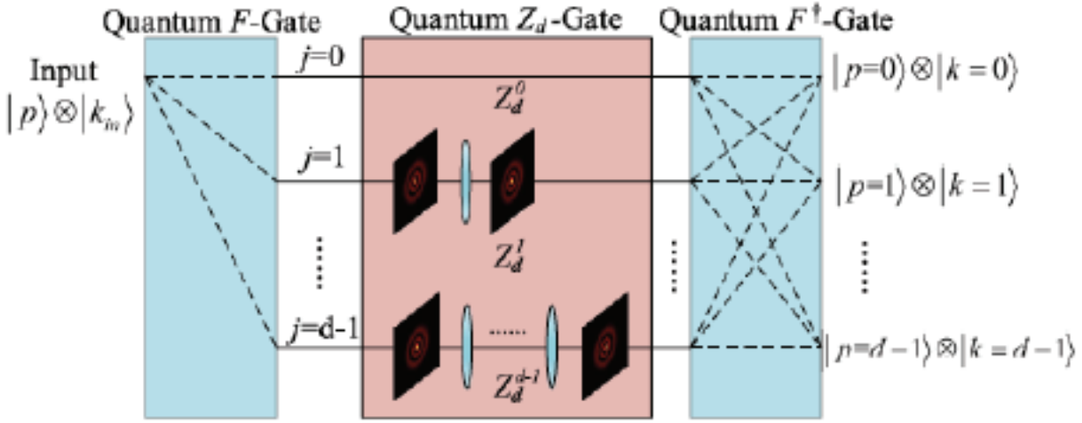
Crosstalk Matrices



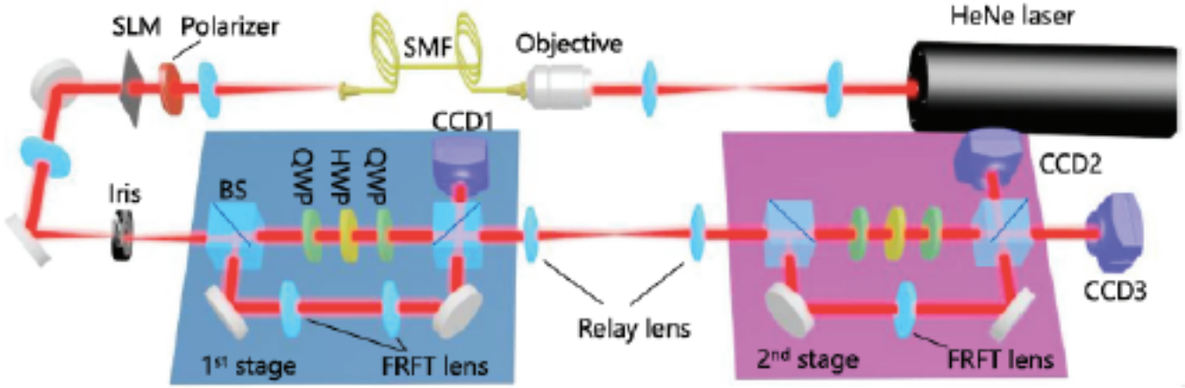
Sorting Photons by Radial Quantum Number

Yiyu Zhou,[1] Mohammad Mirhosseini,[1,*] Dongzhi Fu,[1,2] Jiapeng Zhao,[1] Seyed Mohammad Hashemi Rafsanjani,[1] Alan E. Willner,[3] and Robert W. Boyd[1,4]

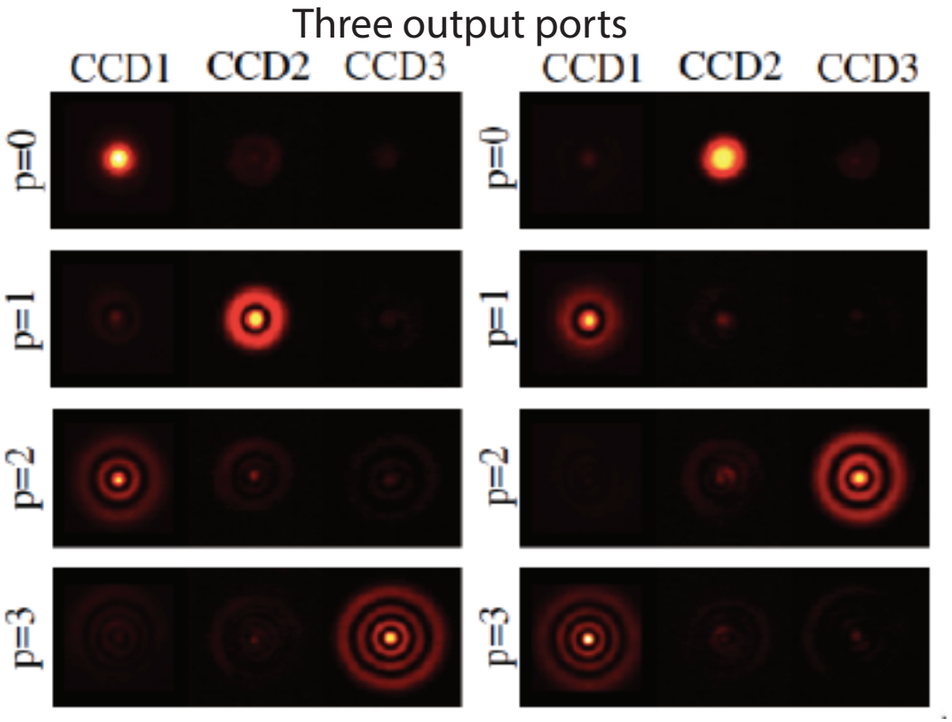
- We implement a theoretical proposal of R. Ionicioiu, Sci. Rep. 6, 25356 (2016).



F-gate is a Fourier transform; Z_d-gate is a mode-dependent phase shifter implement by a fractional fourier transform.



- Results

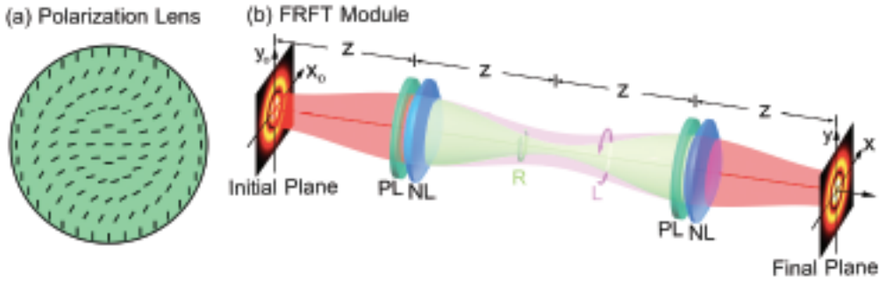


First Z_d-gate is retuned for second column to remove p=0 and p=2 ambiguity.

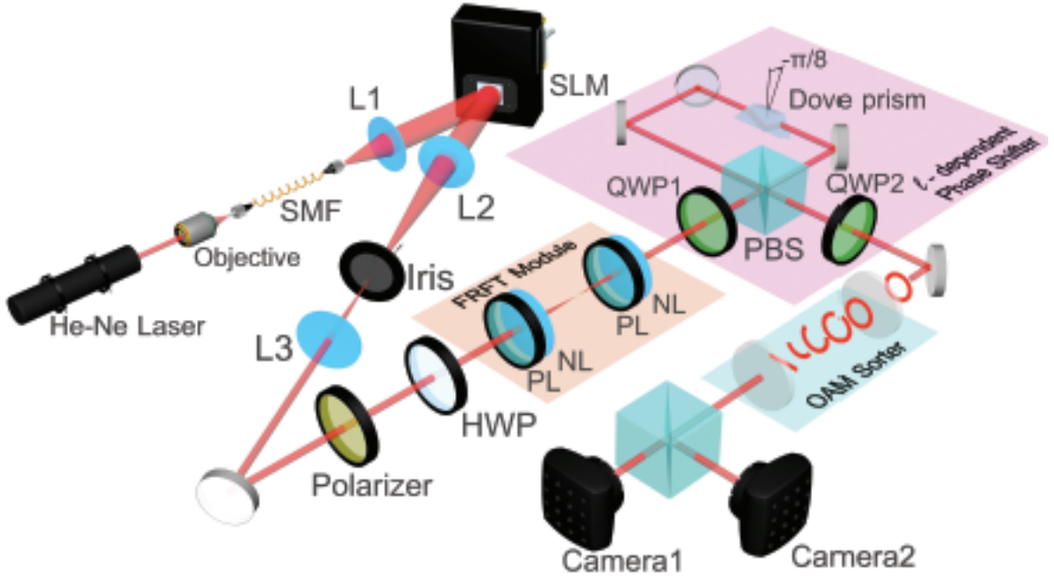
Realization of a robust Laguerre-Gaussian mode sorter

Dongzhi Fu,[1,2] Yiyu Zhou,[2,*] Rui Qi,[2] Stone Oliver,[3] Yunlong Wang,[1] Seyed Mohammad Hashemi Rafsanjani,[2] Jiapeng Zhao,[2] Mohammad Mirhosseini,[2] Zhimin Shi,[4] Pei Zhang,[1,†] and Robert W. Boyd[2,5]

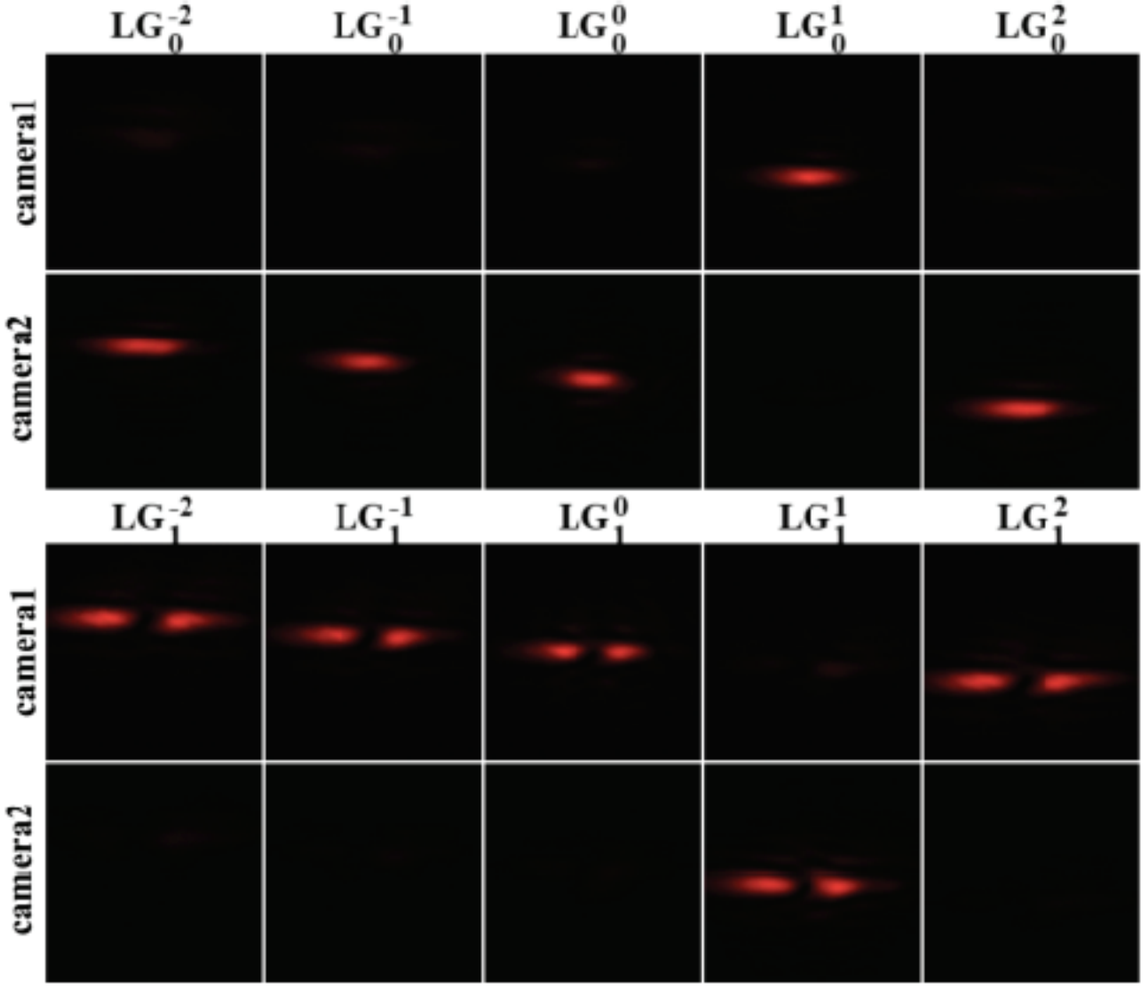
- We use a polarization lens to create a common-path FRFT (ractional Fourier transform) module



- Laboratory layout



Results for sorting both azimuthal and radial dependence



4. Advances in Free-Space QKD

Optics Letters

Spatially multiplexed orbital-angular-momentum-encoded single photon and classical channels in a free-space optical communication link

Yongxiong Ren,[1,4,*] Cong Liu,[1] Kai Pang,[1] Jiapeng Zhao,[2] Yinwen Cao,[1] Guodong Xie,[1] Long Li,[1] Peicheng Liao,[1] Zhe Zhao,[1] Moshe Tur,[3] Robert W. Boyd,[2] and Alan E. Willner[1]

[1]Department of Electrical Engineering, University of Southern California, Los Angeles, California 90089, USA
[2]Department of Physics and Astronomy, The Institute of Optics, University of Rochester, Rochester, New York 14627, USA
[3]School of Electrical Engineering, Tel Aviv University, Ramat Aviv 69978, Israel
[4]Currently at FutureWei Technologies Inc., Santa Clara, California 95050, USA
*Corresponding author: yongxior@usc.edu

Received 11 September 2017; revised 15 October 2017; accepted 16 October 2017; posted 23 October 2017 (Doc. ID 303043); published 22 November 2017

We experimentally demonstrate spatial multiplexing of an orbital angular momentum (OAM)-encoded quantum channel and a classical Gaussian beam with a different wavelength and orthogonal polarization. Data rates as large as 100 MHz are achieved by encoding on two different OAM states by employing a combination of independently modulated laser diodes and helical phase holograms. The influence of OAM mode spacing, encoding bandwidth, and interference from the co-propagating Gaussian beam on registered photon count rates and quantum bit error rates is investigated. Our results show that the deleterious effects of intermodal crosstalk effects on system performance become less important for OAM mode spacing $\Delta \geq 2$ (corresponding to a crosstalk value of less than –18.5 dB). The use of OAM domain can additionally offer at least 10.4 dB isolation besides that provided by wavelength and polarization, leading to a further suppression of interference from the classical channel.

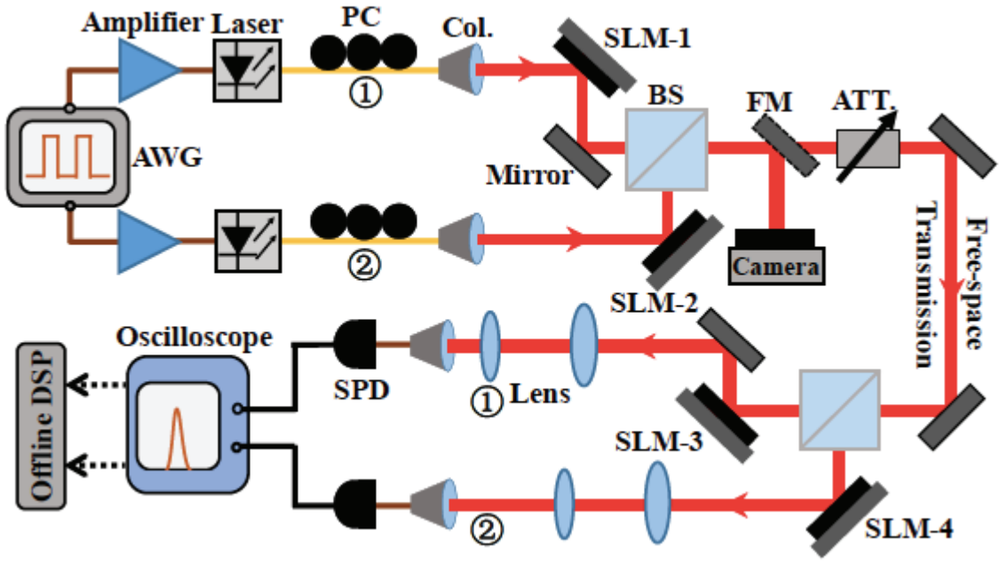
robustness against eavesdropping [6–8]. One example of enabling encoding by multilevel states is employing a set of orthogonal spatial modes for which the photon can occupy one of many states at a given time slot [8–10]. A possible spatial basis set that has recently received increasing interest is orbital angular momentum (OAM) modes [11]. A light beam with a helical wavefront carries an OAM corresponding to $\ell\hbar$ per photon, where $\hbar$ is the reduced Planck constant and ℓ is an unbounded integer [11]. OAM modes with different ℓ values are mutually orthogonal [12], which allows for the simultaneous transmission of multiple data channels [13,14]. Recent advances have shown the use of OAM modes for terabit/s classical optical links and for up to 143-km free-space transmission [13,15,16].

OAM states span a large Hilbert space and can be utilized for high-dimensional quantum encoding based on their orthogonality [10,17]. Moreover, quantum OAM encoding is in principle compatible with data encoding in other domains, such as polarization encoding [17,18]. A proof-of-concept OAM encoding-based quantum link has been recently demonstrated by using a digital micromirror device to switch between

Demonstration of a 10-Mbit/s quantum communication link by encoding data on two Laguerre-Gaussian modes with different radial indices

KAI PANG,[1,*] CONG LIU,[1] GUODONG XIE,[1] YONGXIONG REN,[1] ZHE ZHAO,[1] RUNZHOU ZHANG,[1] YINWEN CAO,[1] JIAPENG ZHAO,[2] HAOQIAN SONG,[1] HAO SONG,[1] LONG LI,[1] MOSHE TUR,[3] ROBERT BOYD,[2] AND ALAN E. WILLNER[1]

- Each LG channel is driven by a separate laser diode
- High transmission rate is achieved by modulating the laser diode



Research Article Vol. 4, No. 9 / September 2017 / Optica 1006

optica

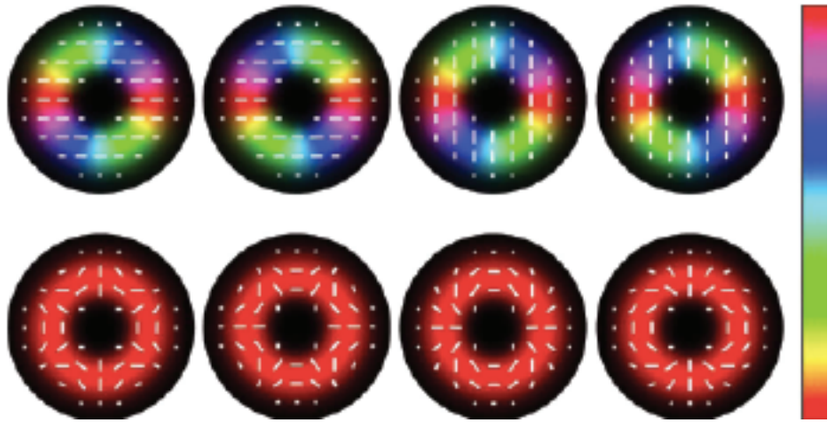
High-dimensional intracity quantum cryptography with structured photons

Alicia Sit,[1] Frédéric Bouchard,[1] Robert Fickler,[1] Jérémie Gagnon-Bischoff,[1] Hugo Larocque,[1] Khabat Heshami,[2] Dominique Elser,[3,4] Christian Peuntinger,[3,4] Kevin Günthner,[3,4] Bettina Heim,[3,4] Christoph Marquardt,[3,4] Gerd Leuchs,[1,3,4] Robert W. Boyd,[1,5] and Ebrahim Karimi[1,6,*]

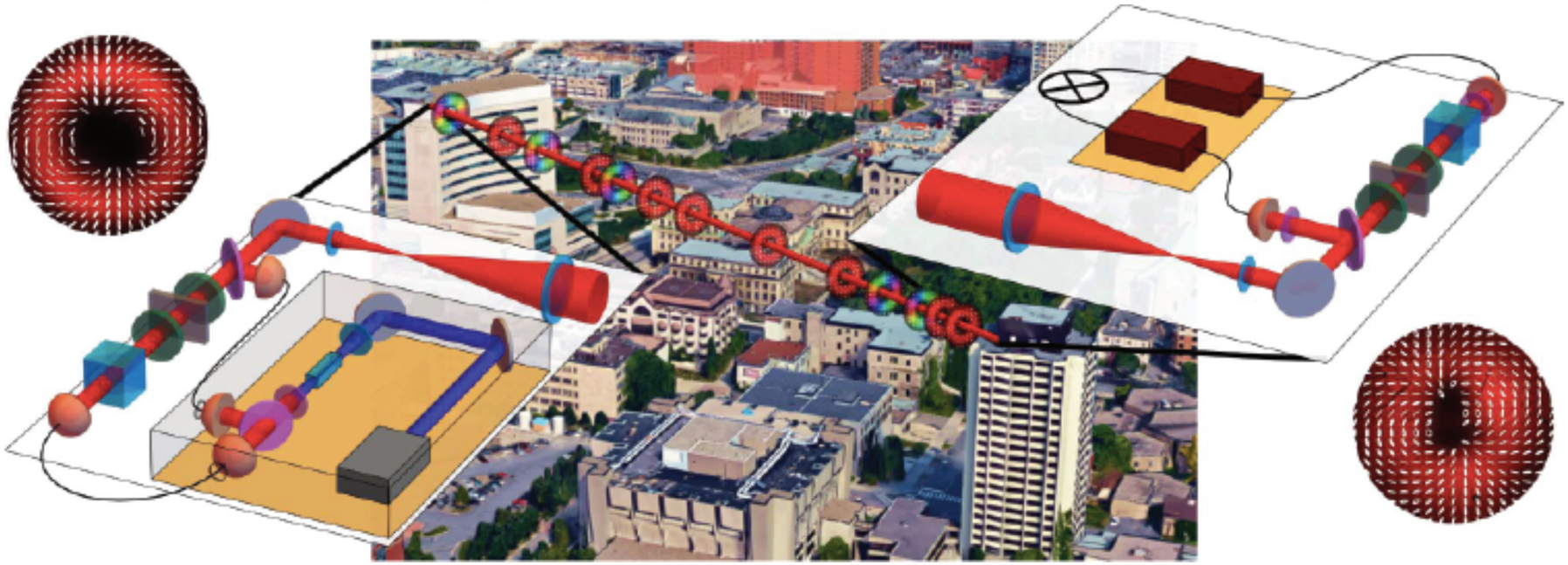
- Encode in a 4-D space of vector (polarization and OAM) modes

MUB-1

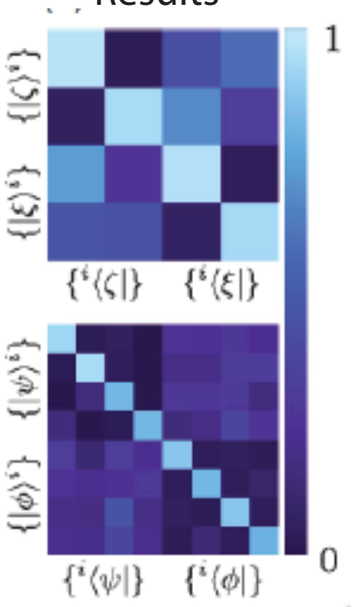
MUB-2



The link (300 m pathlength)



Results



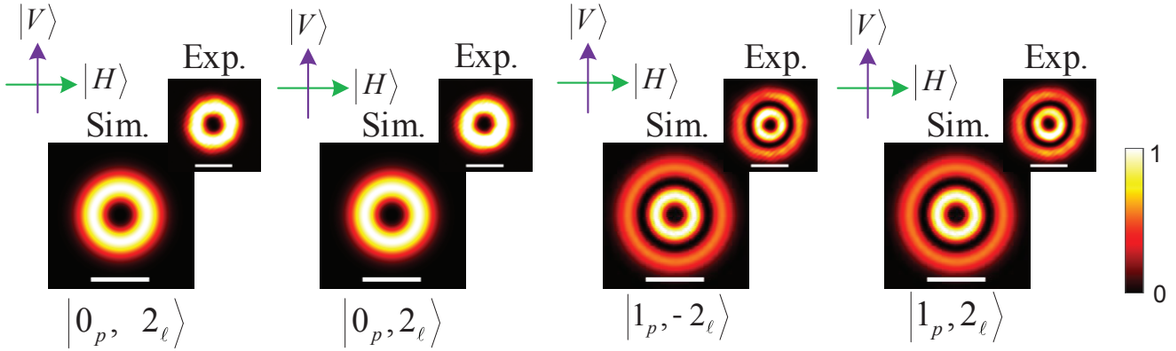
0.65 bits per sifted photon

Quantum key distribution using all transverse degrees of freedom

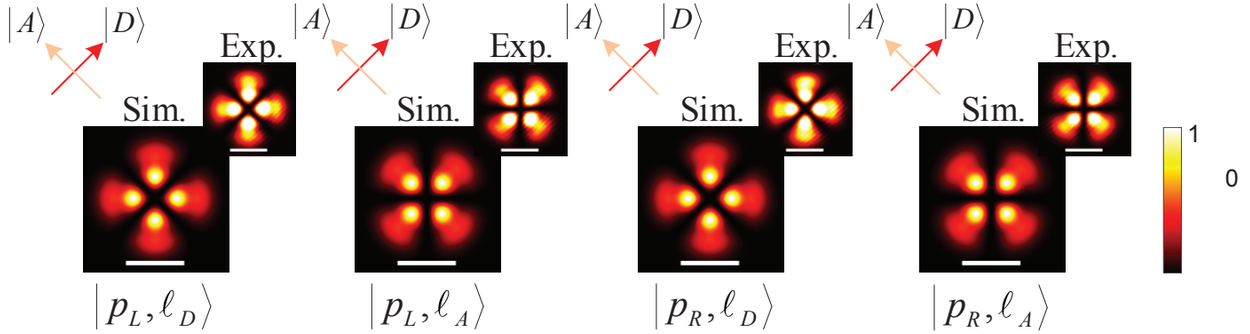
Yiyu Zhou,[1,*] Mohammad Mirhosseini,[1,†] Stone Oliver,[1,2] Jiapeng Zhao,[1]
Seyed Mohammad Hashemi Rafsanjani,[1,3]
Martin P. J. Lavery,[4] Alan E. Willner,[5] and Robert W. Boyd[1,6,‡]

- Perform QKD in an 8-dimensional state space.
- Encode in the transverse variation of amplitude, phase, and polarization
- Transfer 2.15 bits per detected photon

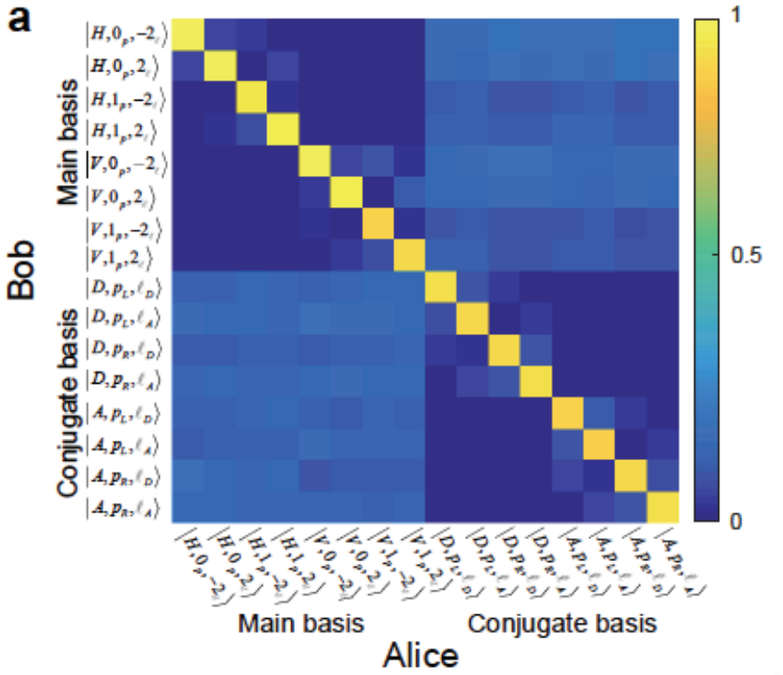
Main basis



Conjugate basis



- Crosstalk matrix



- Secure image transmission

Summary

- New quantum-state sorters for full Laguerre-Gauss determination allow enhanced performance in free-spac quantum communications.

- This technology is useful more generally in advanced imaging by allowing a complex optical field to be decomposed into a complete set of orthogonal modes.