High-Capacity, Free-Space Quantum Key Distribution Based on Spatial and Polarization Encoding

Robert W. Boyd
The Institute of Optics and Department of Physics and Astronomy
University of Rochester

Alan E. Willner
Department of Electrical Engineering
University of Southern California

Glenn A. Tyler
the Optical Sciences Company
Anaheim, California

Presented at the ONR Quantum Information Science Review, Arlington Virginia, December 9, 2015. (N00014-15-1-2635)

ARTICLES
PUBLISHED ONLINE: 24 JUNE 2012 | DOI: 10.1038/NPHOTON.2012.138
nature photonics

Terabit free-space data transmission employing orbital angular momentum multiplexing

Jian Wang[1,2]*, Jeng-Yuan Yang[1], Irfan M. Fazal[1], Nisar Ahmed[1], Yan Yan[1], Hao Huang[1], Yongxiong Ren[1], Yang Yue[1], Samuel Dolinar[3], Moshe Tur[4] and Alan E. Willner[1]*

New J. Phys. **17** (2015) 033033 doi:10.1088/1367-2630/17/3/033033

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

PAPER

High-dimensional quantum cryptography with twisted light

Mohammad Mirhosseini[1], Omar S Magaña-Loaiza[1], Malcolm N O'Sullivan[1], Brandon Rodenburg[1], Mehul Malik[1,2], Martin P J Lavery[3], Miles J Padgett[3], Daniel J Gauthier[4] and Robert W Boyd[1,5]

[1] The Institute of Optics, University of Rochester, Rochester, New York 14627, USA
[2] Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria
[3] School of Physics and Astronomy, University of Glasgow, Glasgow, G12 8QQ, UK
[4] Department of Physics, Duke University, Durham, NC 27708 USA
[5] Department of Physics, University of Ottawa, Ottawa ON K1N 6N5, Canada

New Journal of Physics
The open access journal at the forefront of physics
Deutsche Physikalische Gesellschaft DPG | IOP Institute of Physics

Simulating thick atmospheric turbulence in the lab with application to orbital angular momentum communication

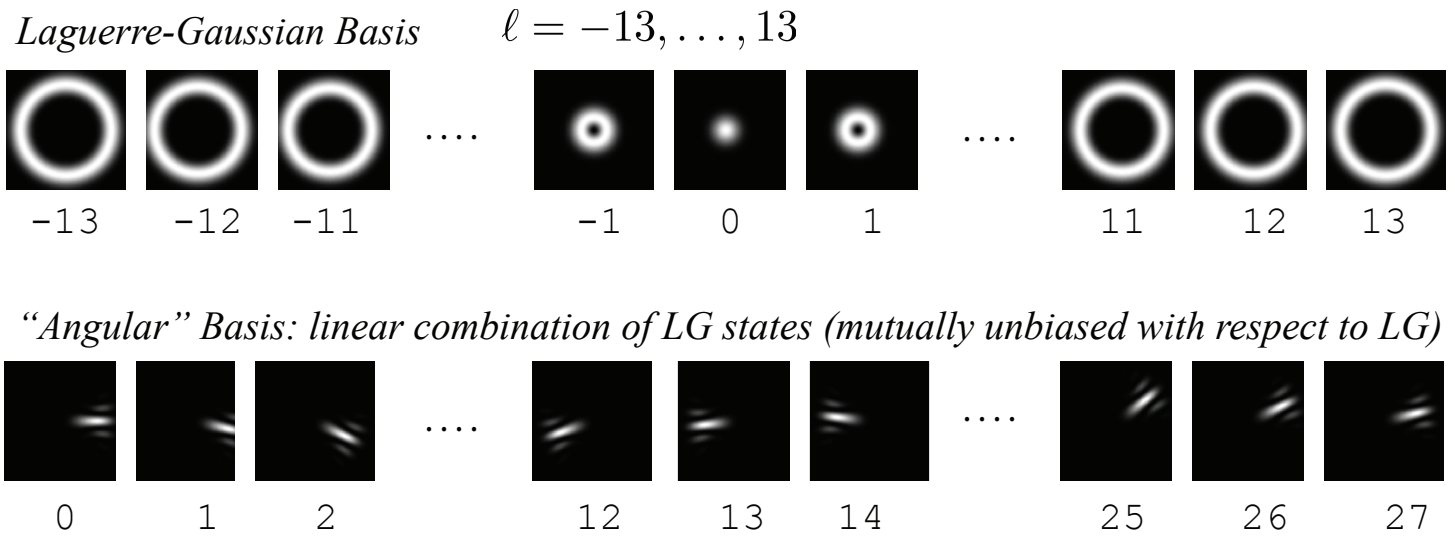
Brandon Rodenburg[1], Mohammad Mirhosseini[1], Mehul Malik[1], Omar S Magaña-Loaiza[1], Michael Yanakas[1], Laura Maher[1], Nicholas K Steinhoff[2], Glenn A Tyler[2] and Robert W Boyd[2,3]

[1] The Institute of Optics, University of Rochester, Rochester, NY 14627, USA
[2] The Optical Sciences Company, 1341 South Sunkist Street, Anaheim, California 92806, USA
[3] Department of Physics, University of Ottawa, Ottawa ON K1N 6N5, Canada
E-mail: Brandon.Rodenburg@gmail.com

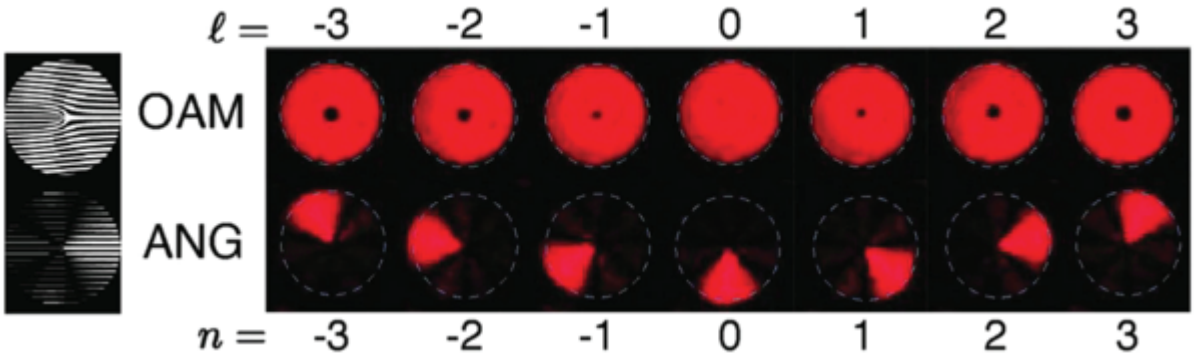
Received 1 October 2013, revised 25 January 2014
Accepted for publication 28 January 2014
Published 19 March 2014
New Journal of Physics **16** (2014) 033020
doi:10.1088/1367-2630/16/3/033020

The OAM-QKD Concept

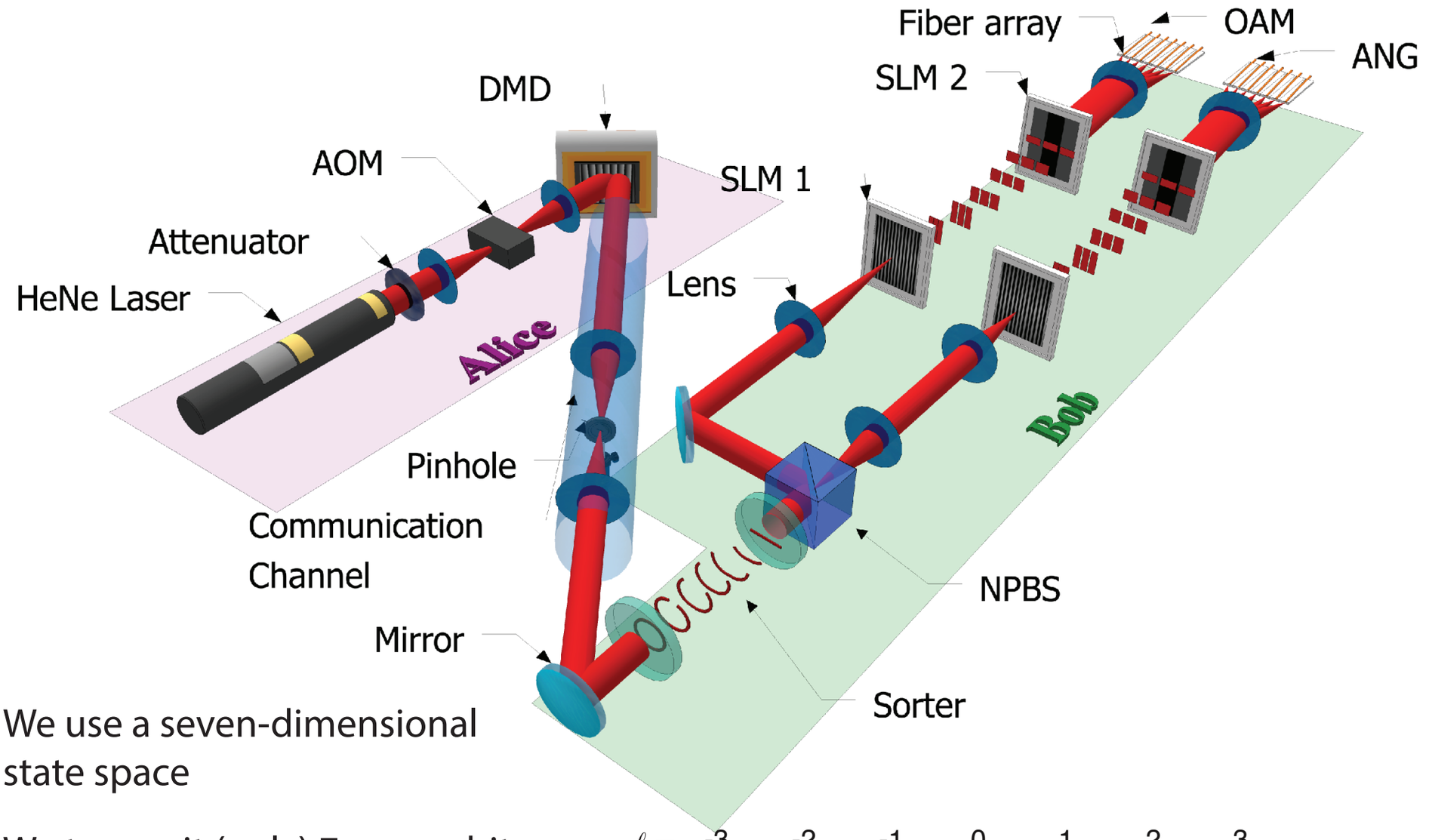
- We encode randomly in one of two mutually unbiased bases



- Our actual implementation (N=7)

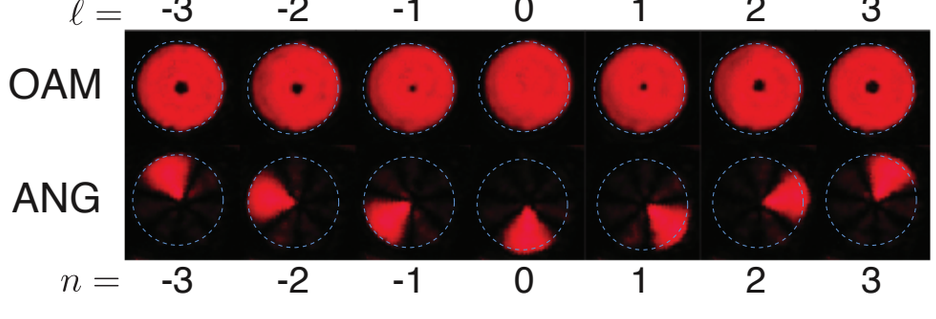


Our Earlier OAM-QKD Implementation



We use a seven-dimensional state space

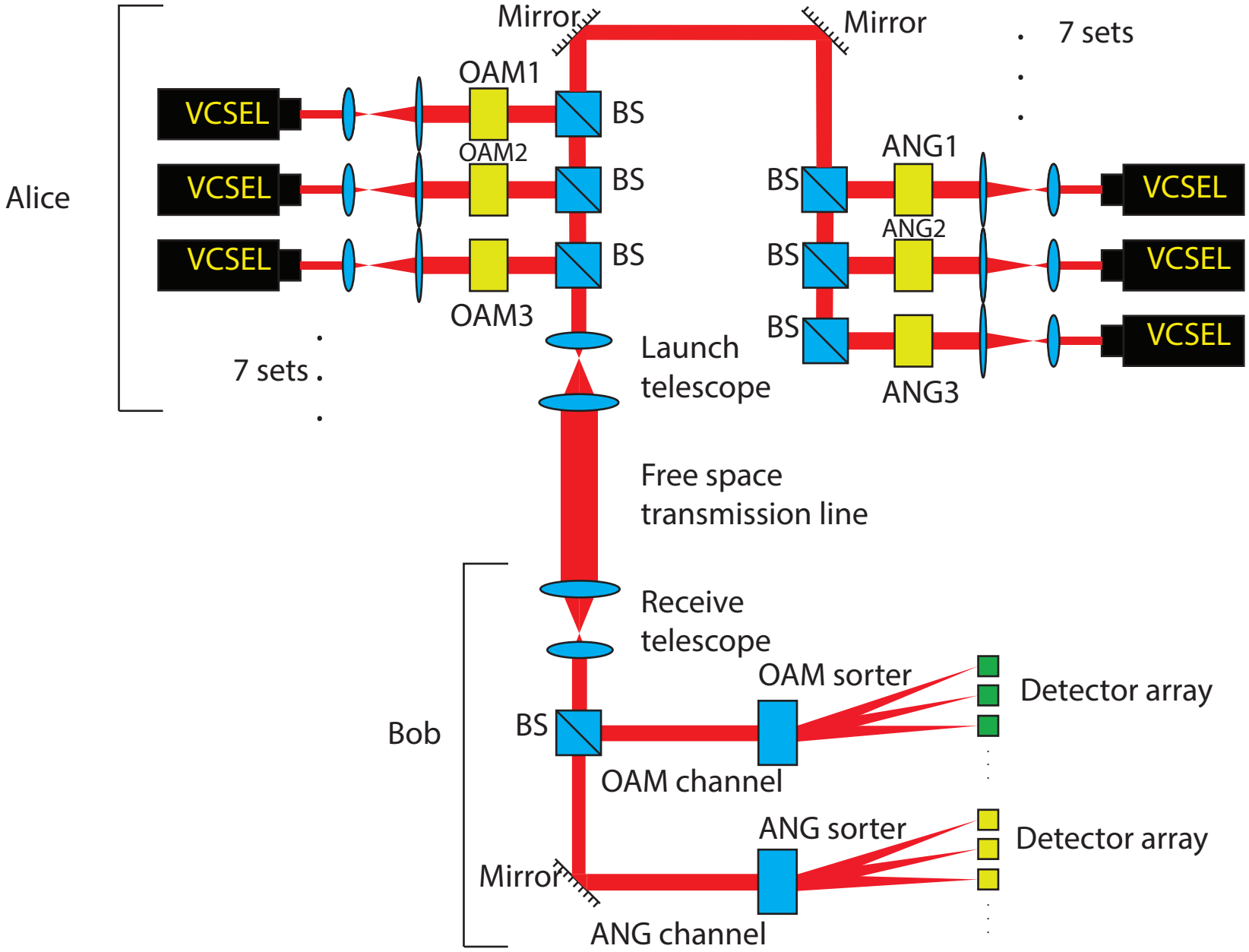
We transmit (only) 7 secure bits per second.



Mirhosseini, Magaña-Loaiza, O'Sullivan, Rodenburg, Malik, Lavery, Padgett, Gauthier and Boyd, New J. Phys. 17, 033033 (2015).

Next Step: gigabit-per-second OAM-based QKD system

- Use direct modulation of laser diode and static holograms to achieve gigabit rates.



Theoretical / Conceptual Issues

What is best strategy?

Assume that we have M OAM states (take M = 9) and assume initially that we will implement 2 MUBs

Do we include all 9 channels in the QKD protocol with N=9?

Or do we implement 3 channels each with N=3?

Or do we implement 9 channels each with of N=1?

Current Thinking:

Data rate is largest for pure multiplexing (9 channels of N=1)

But security can be enhanced by including more states in the QKD protocol

The best tradeoff probably depends on environmental issues such as atmospheric turbulence levels, and can be adjusted in real time.

Further Issues:

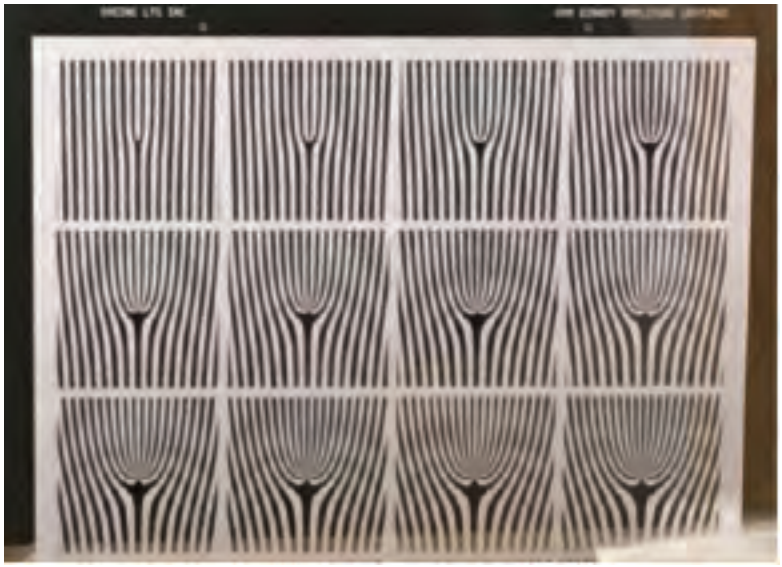
How do this tradeoff change if we implement more MUBs in our protocol?

How do we perform security analysis for finite-length keys

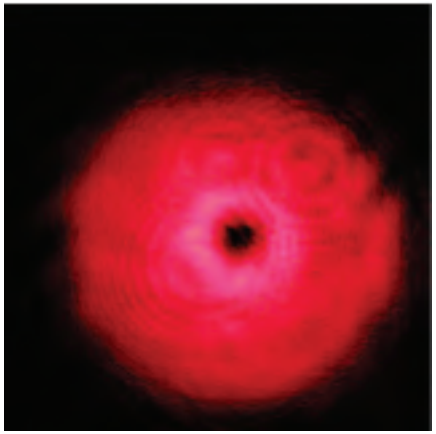
Collaborators: Anne Broadbent, Robert Fickler, and Kamil Bradler, U. Ottawa

Development of Static Holograms

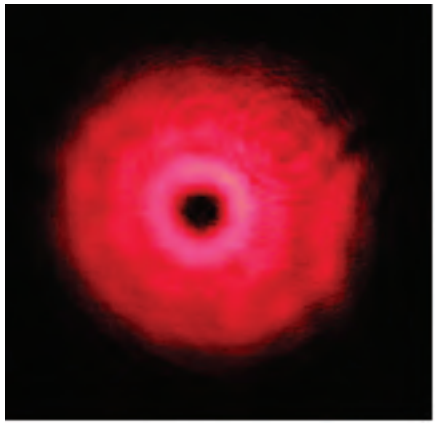
Hologram array



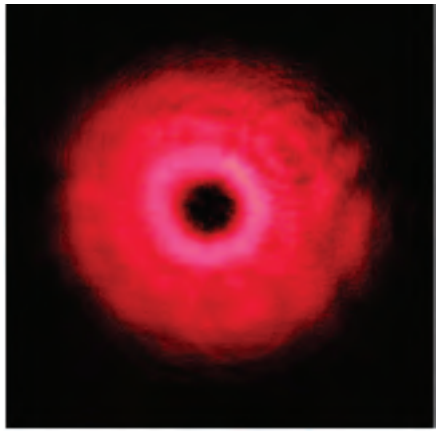
Far-field diffraction patterns



$\ell = 2$



$\ell = 2$

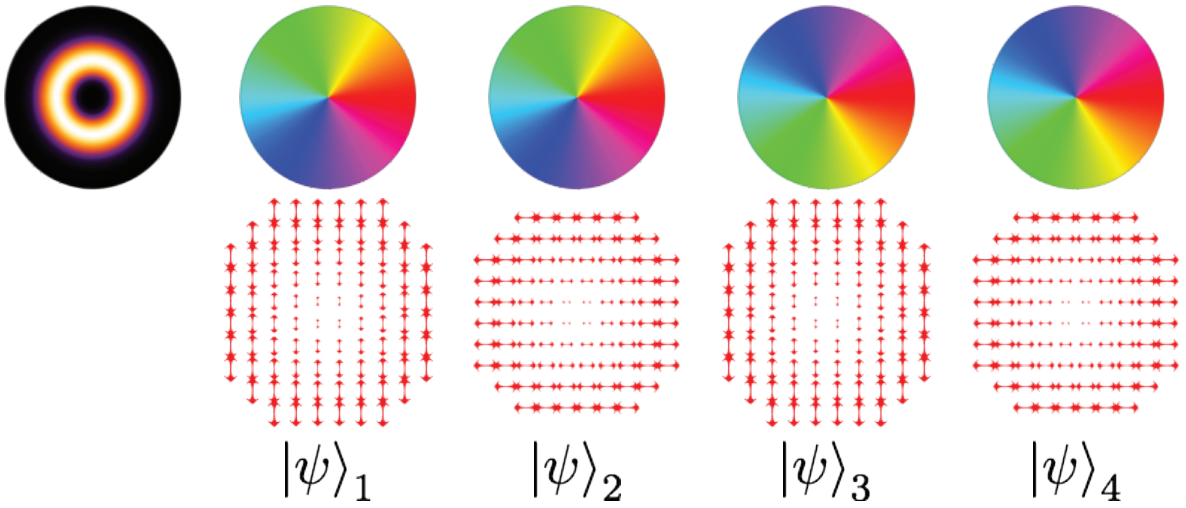


$\ell = 4$

We will simultaneously encode in polarization

- One possibility: use "vector beams"

MUB1



MUB2