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]

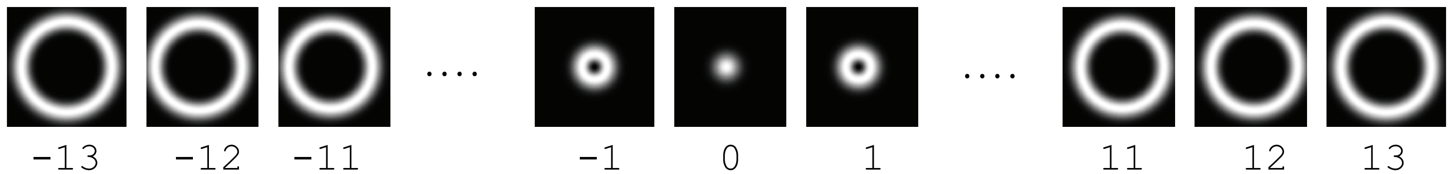
[1] The Institute of Optics, University of Rochester, Rochester, NY 14627, USA
[2] The Optical Sciences Company, 1341 South Sunkist Street, Anaheim, California 92806, USA
[3] Department of Physics, University of Ottawa, Ottawa ON K1N 6N5, Canada
E-mail: Brandon.Rodenburg@gmail.com

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

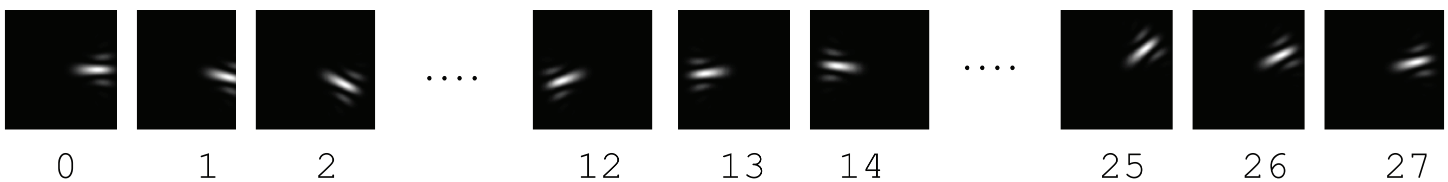
The OAM-QKD Concept

- We encode randomly in one of two mutually unbiased bases

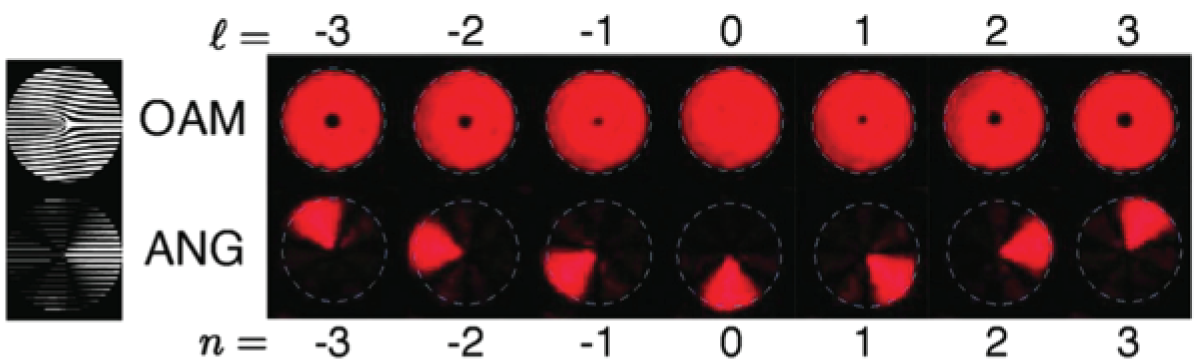
Laguerre-Gaussian Basis $\ell = -13, \ldots, 13$



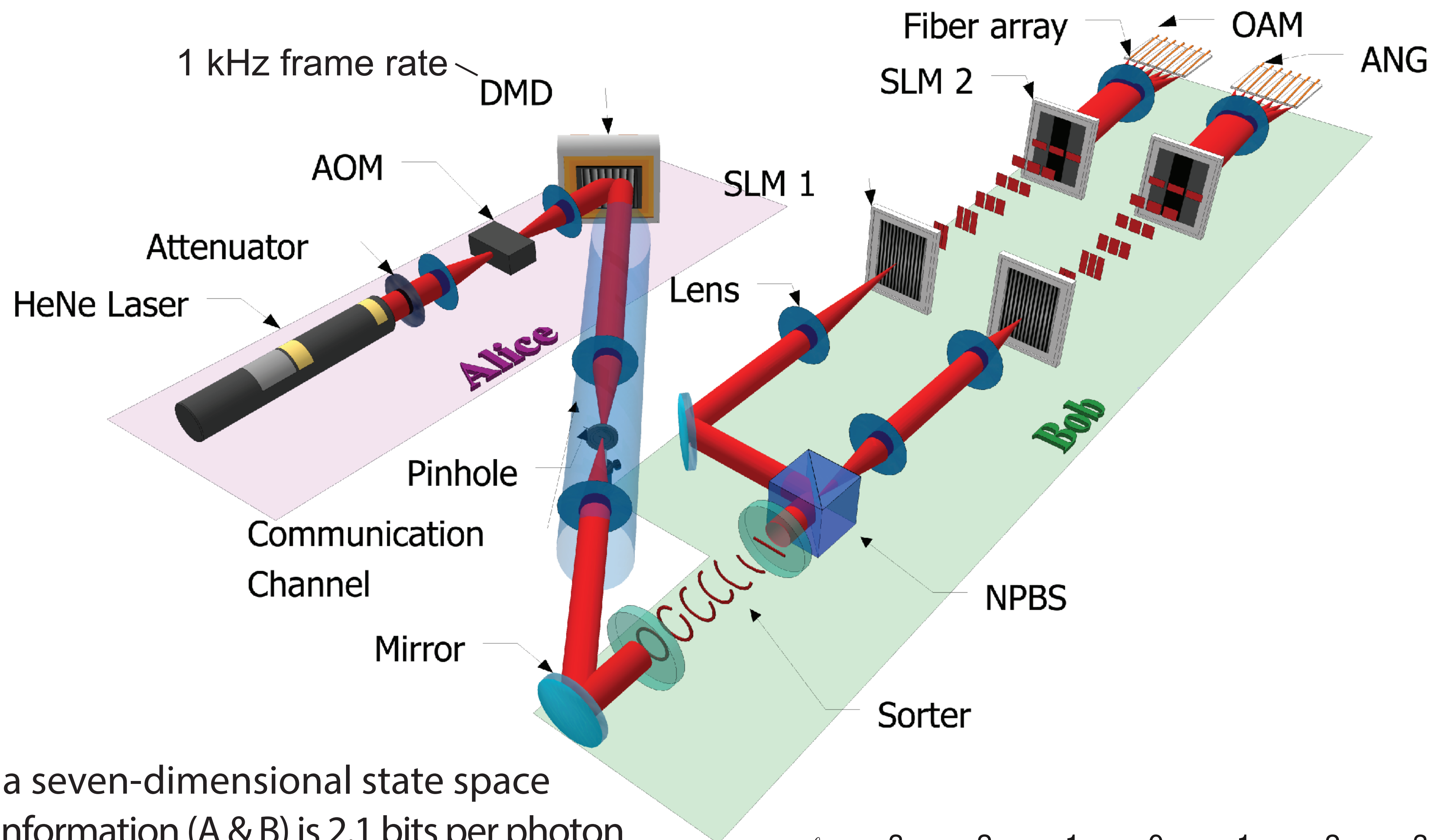
"Angular" Basis: linear combination of LG states (mutually unbiased with respect to LG)



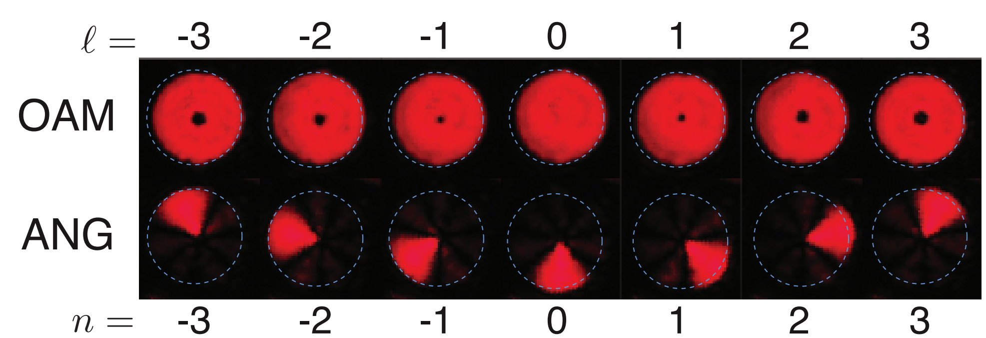
- Our actual implementation (N=7)



Our Earlier OAM-QKD Implementation



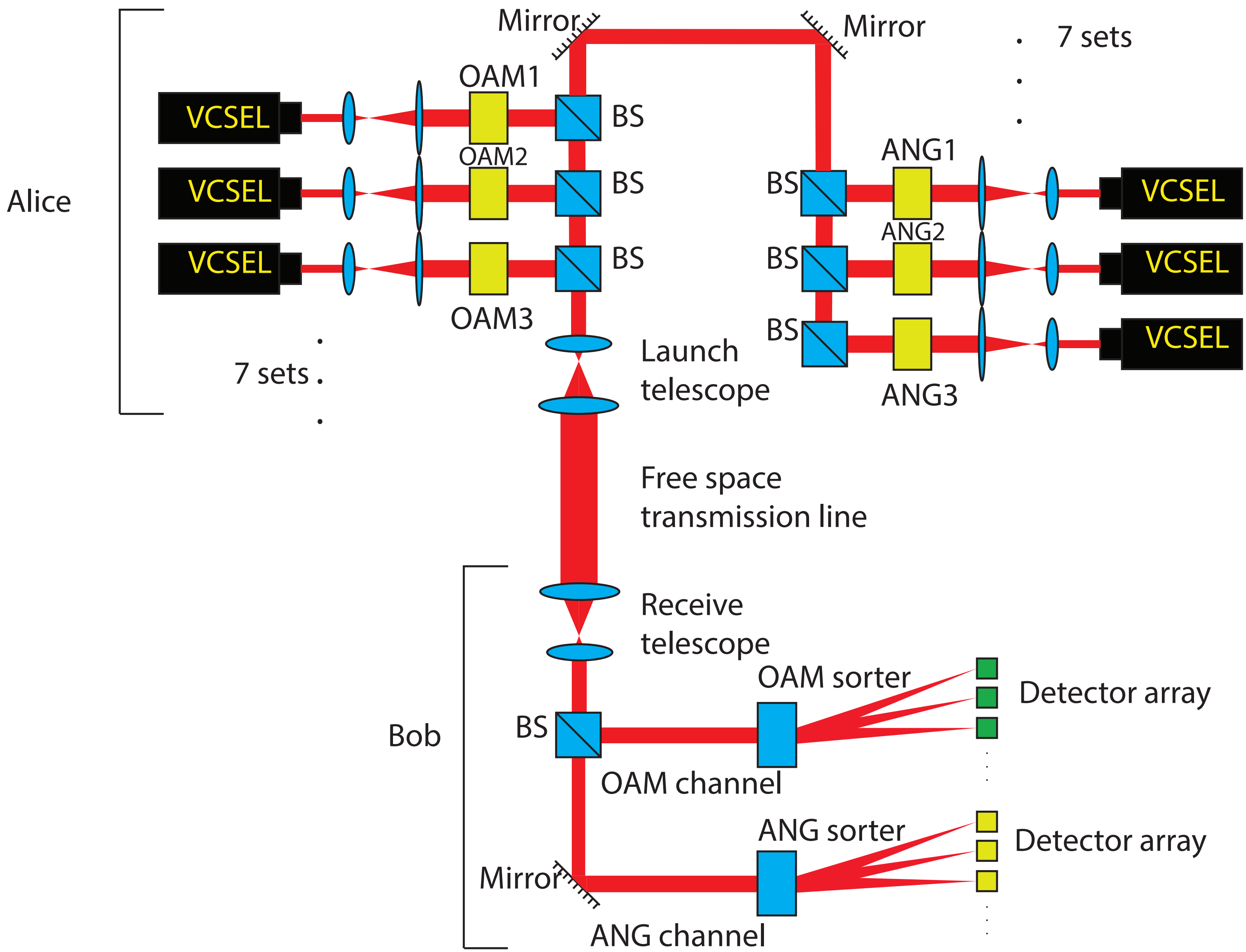
- We use a seven-dimensional state space
- Mutual information (A & B) is 2.1 bits per photon
- Secure transision rate (A & B) is 1.7 bits per photon
- But we transmit only 7 secure bits per second



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:

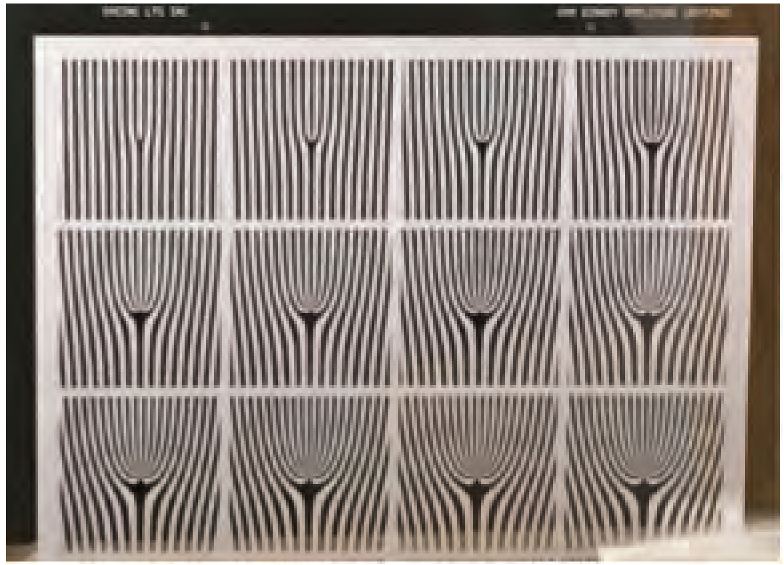
How do this tradeoff change if we implement more MUBs in our protocol?

How do we perform security analysis for finite-length keys

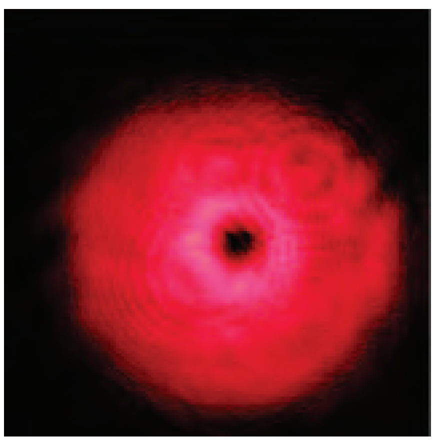
Collaborators: Anne Broadbent, Robert Fickler, and Kamil Bradler, U. Ottawa

Development of Static Holograms

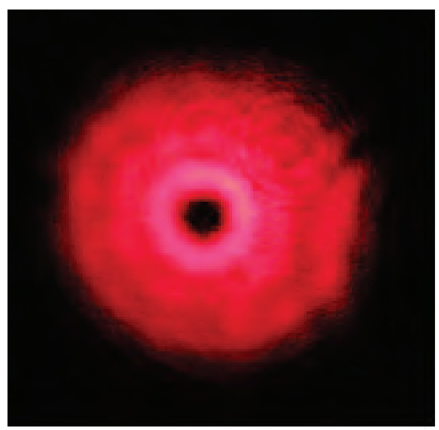
Hologram array



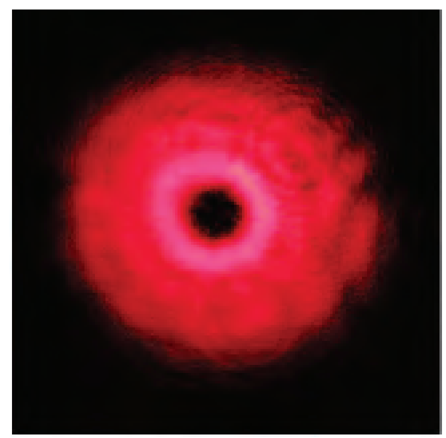
Far-field diffraction patterns



$\ell = 2$



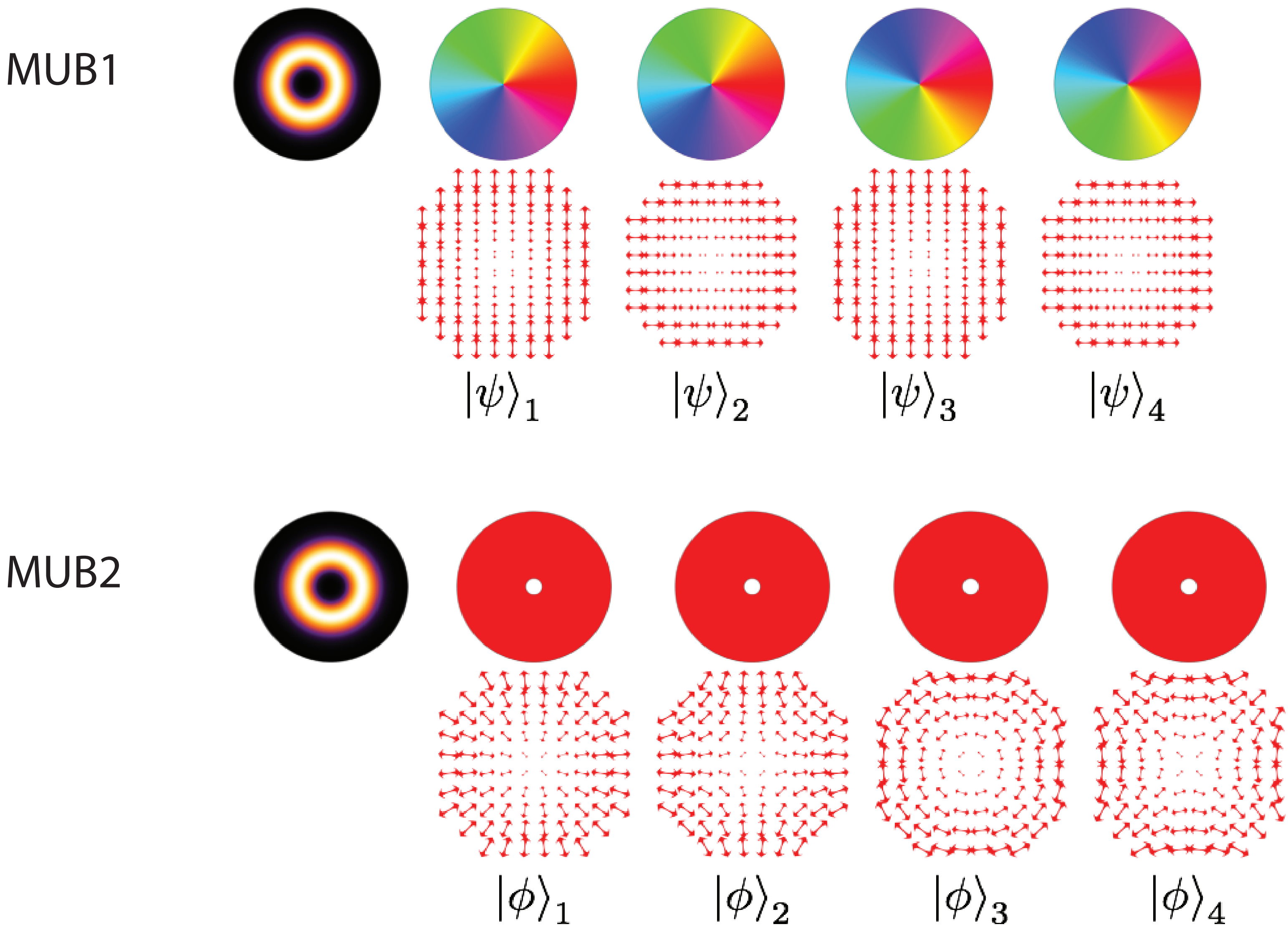
$\ell = 2$



$\ell = 4$

We will simultaneously encode in polarization

- One possibility: use “vector beams”



High Capacity Free Space QKD Based on Spatial and Polarization Encoding: Fast Spatial Mode Encoding

Alan E. Willner, Yongxiong Ren, Cong Liu

Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90089-2565

Plan and Accomplishment

Plan

- We will explore two potential approaches for high-speed (Gbit/s) spatial mode encoding

  1) 1×N optical switch combined with multiple holograms

  2) N parallel VCSELs (with specially design data streams) combined with multiple holograms

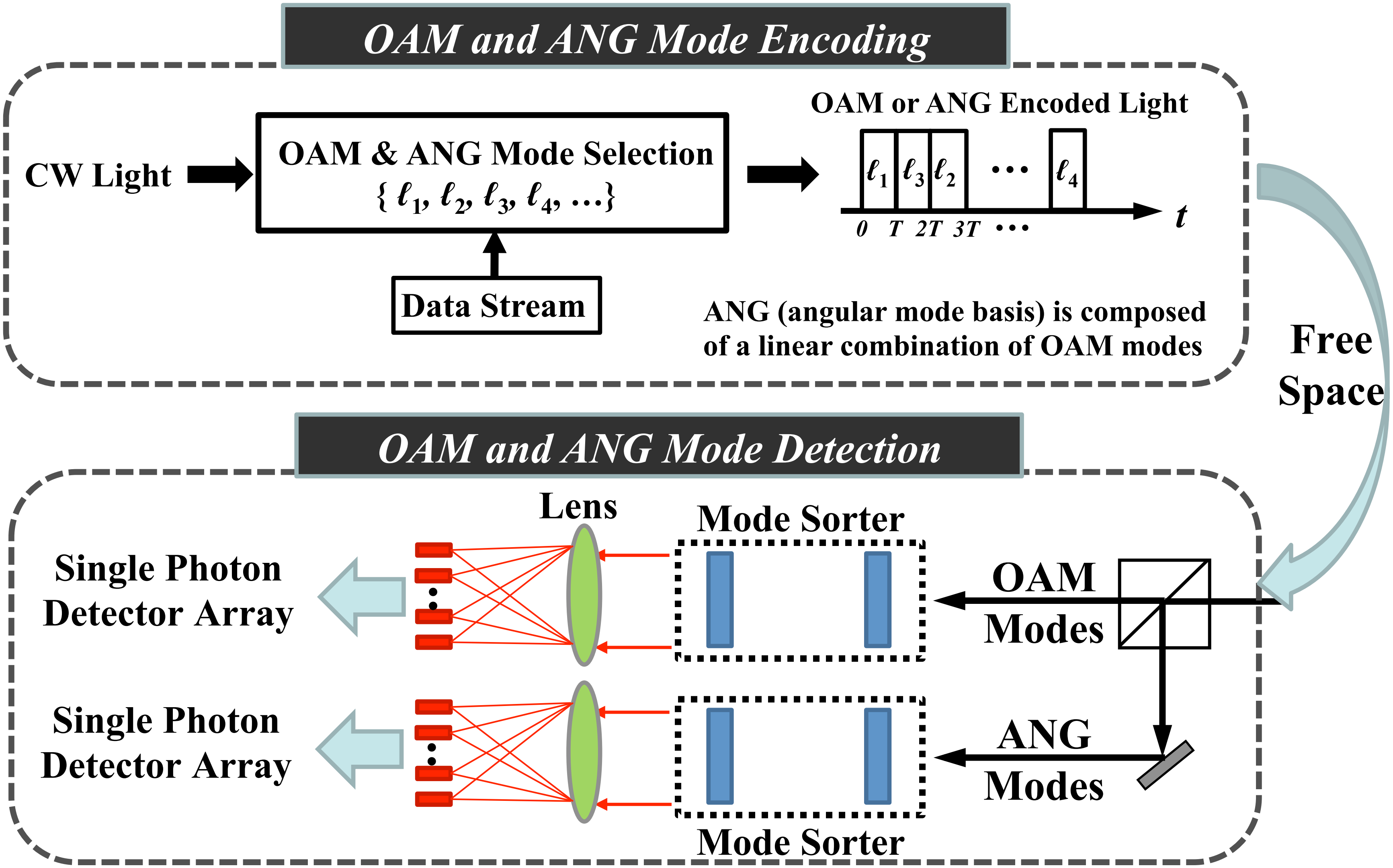
- We will determine an approach to demonstrate a 100 Mbit/s – 1 Gbit/s OAM-based QKD transmitter. We will explore potential limitations and their effects on system security.

Accomplishment

- 20 Gbit/s OAM Encoding: Proof-of-concept experiment in a <u>classical</u> optical link

  - We experimentally demonstrated data encoding at 20 Gbit/s using four possible OAM modes. The influence of mode spacing and time misalignment between modal channels on the switching crosstalk and bit-error-rates was investigated.

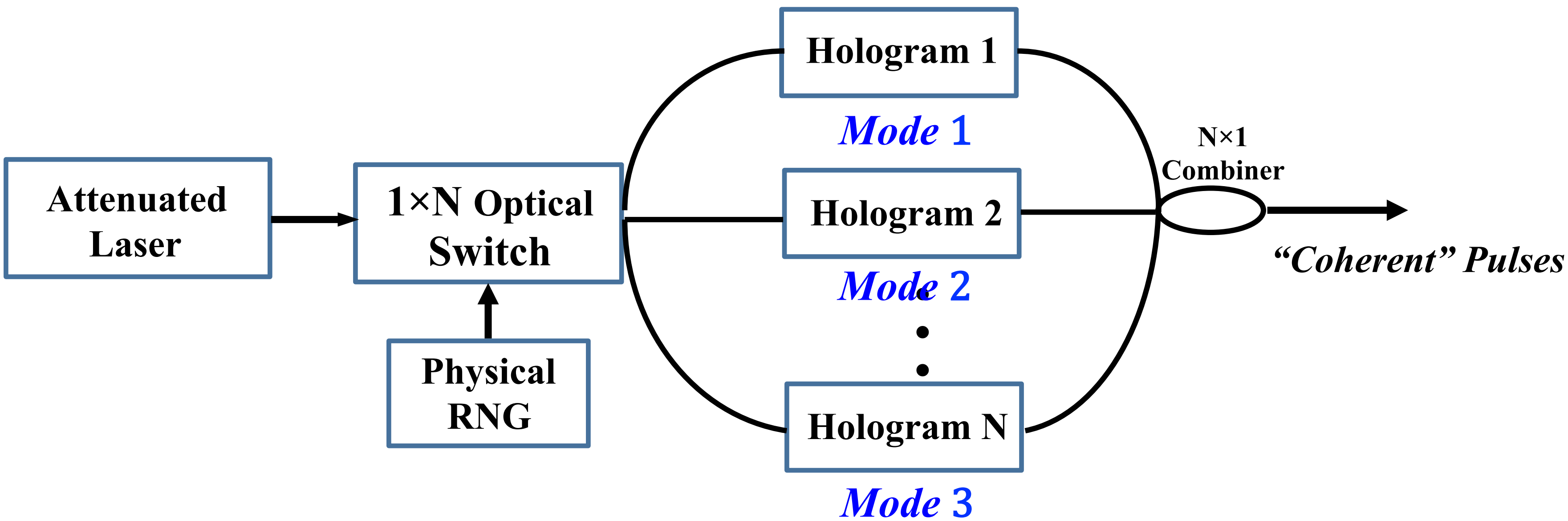
OAM Encoding-Based QKD System



- In theory, we have the following: $\frac{\text{\# of bits info.}}{\text{photon}} = \log_2(\text{\# of possible states})$
- We need a fast spatial mode encoding scheme.

High-speed Spatial Mode Encoding —Scheme 1

- High-speed (Gb/s) spatial mode encoding presents a critical challenge.
- Programmable devices, such as SLMs and digital micromirrors, have limited modulation rates.



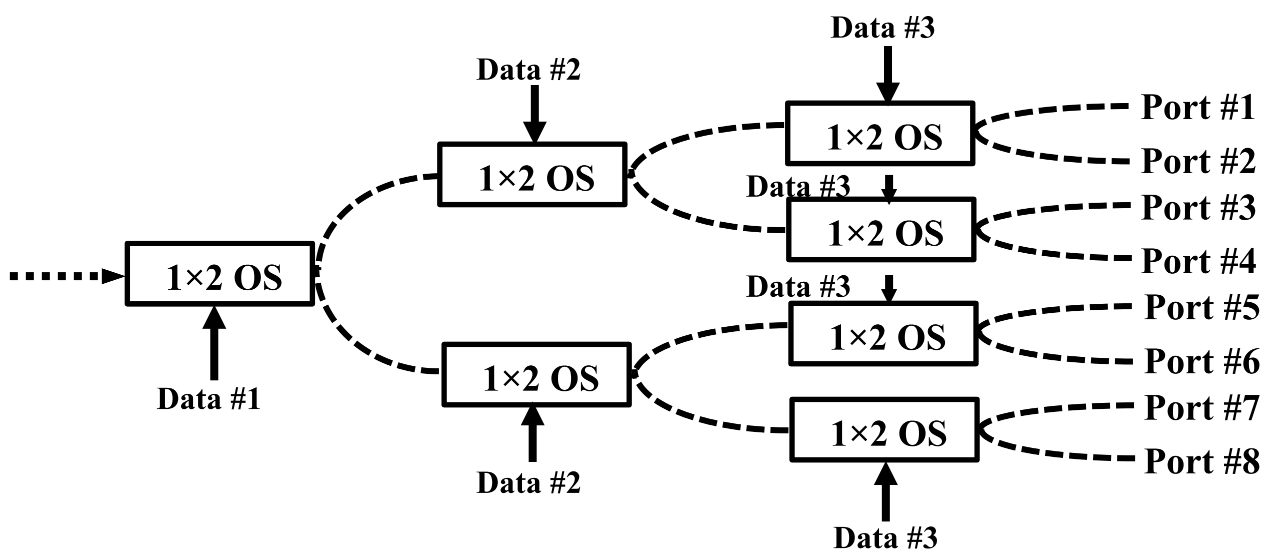
RNG: random number generator

A high-speed 1×*N* optical switch combined with multiple holograms could be potentially used to achieve Gbit/s data encoding

High-speed OAM Encoding — Scheme 1

High-speed 1×*N* Optical Switch

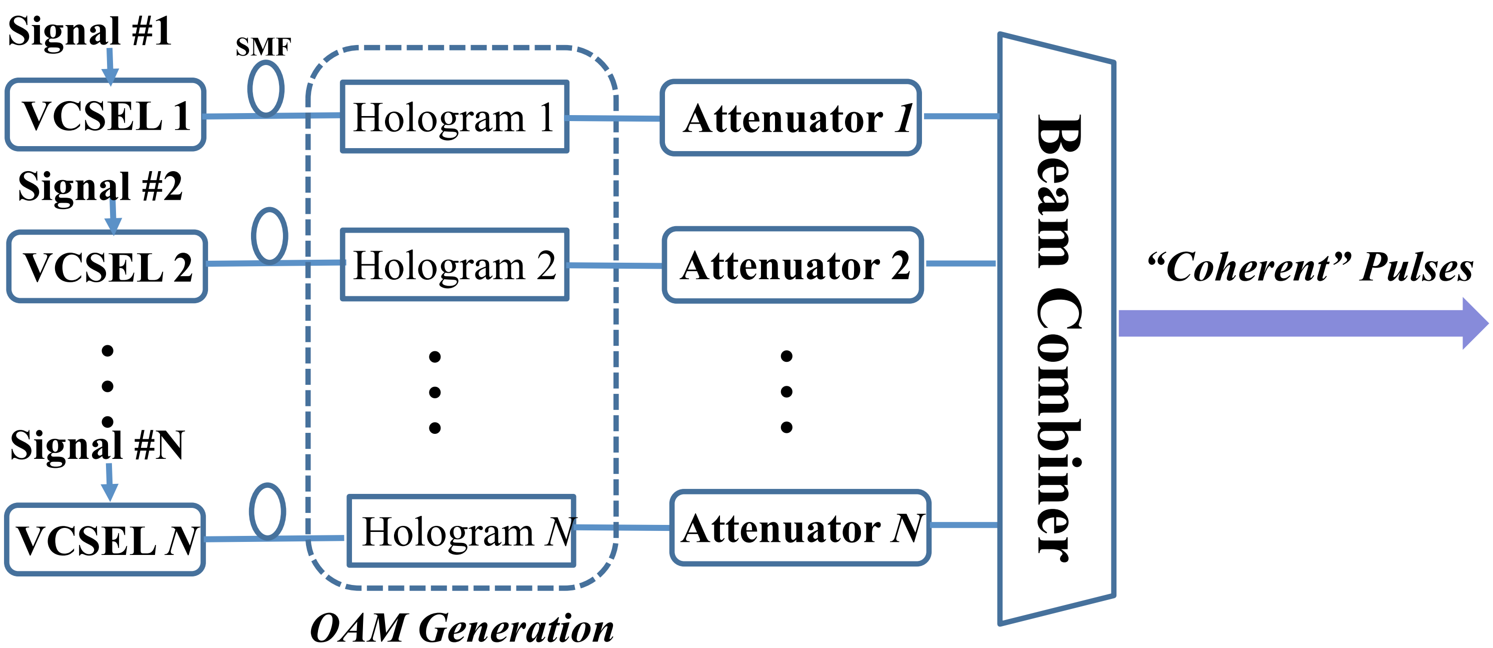
- A 1×*N* GHz optical switch can be built by cascading multiple high-speed 1×2 optical switches.
- For example, seven 1×2 optical switches would be need to built a 1×*8* GHz optical switch



3 independent data streams in total

- This approach can potentially achieve higher speed (such as >10GHz) spatial encoding, but it is not efficiently scalable.

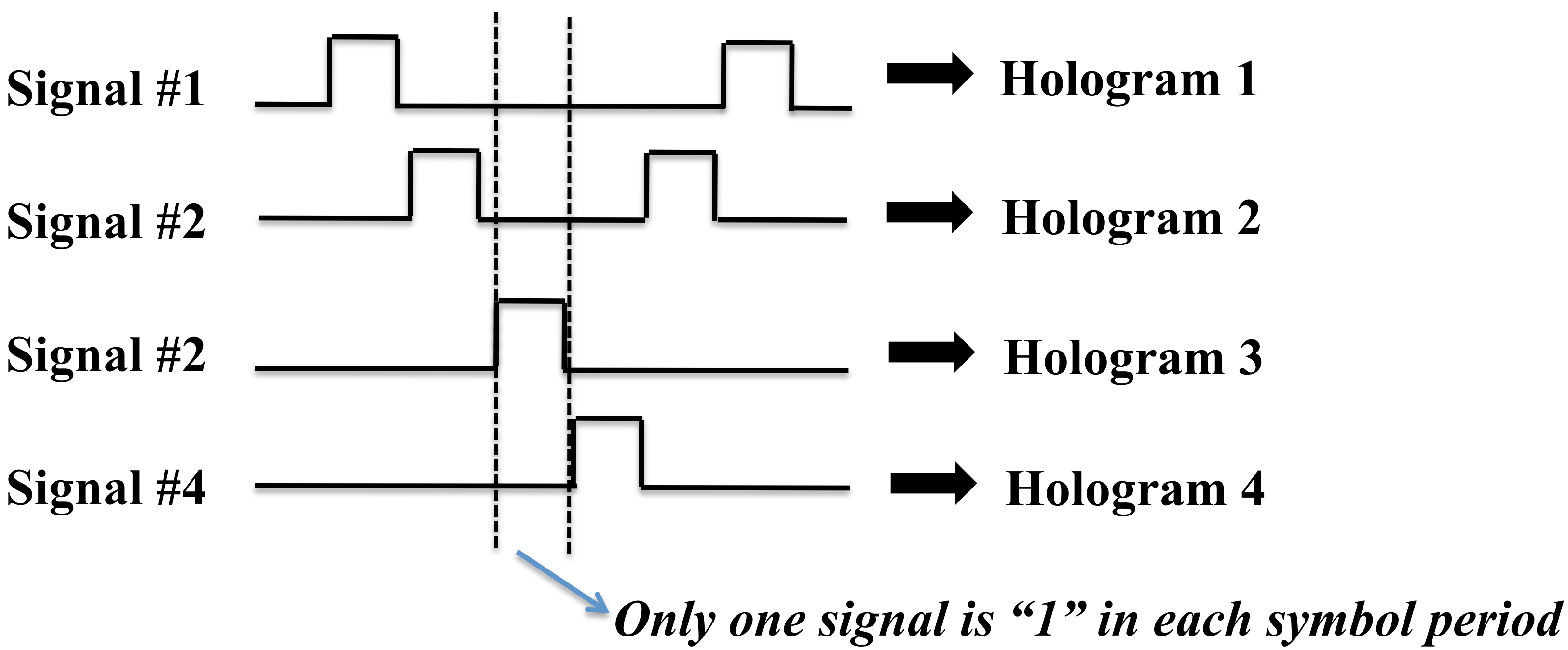
Scheme 2: Parallel VCSELs + Multiple Holograms



- Multiple pairs of {VCSEL + hologram} could be used to generate multiple OAM or ANG modes.
- Each VCSEL can be driven by an independent data signal with a data rate of ~100 Mbit/s.
- By designing the data patterns, we can ensure that only one VCSEL (i.e, only one OAM or ANG mode) is active within each symbol period.

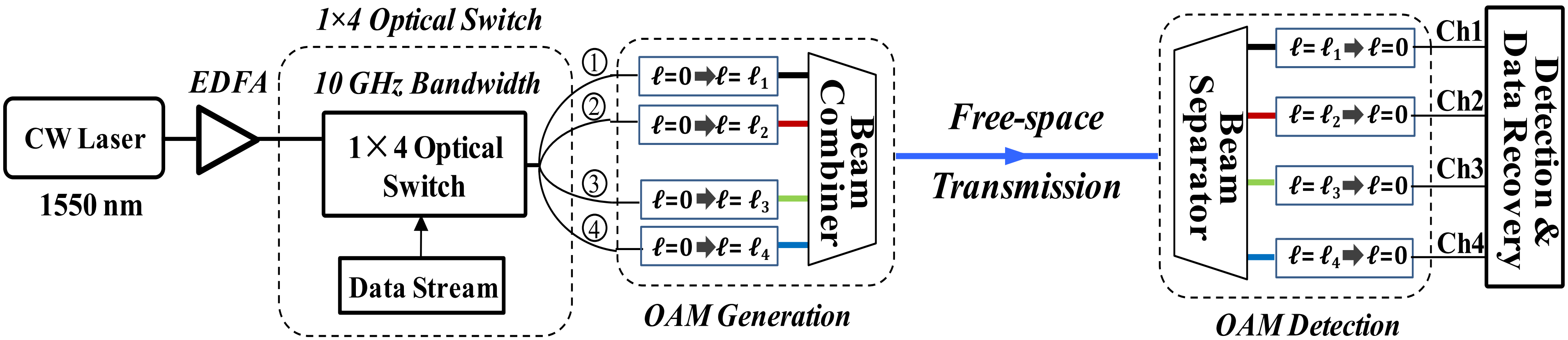
Scheme 2: Parallel VCSELs + Multiple Holograms

The design of data patterns for signals that are fed to VCSELs

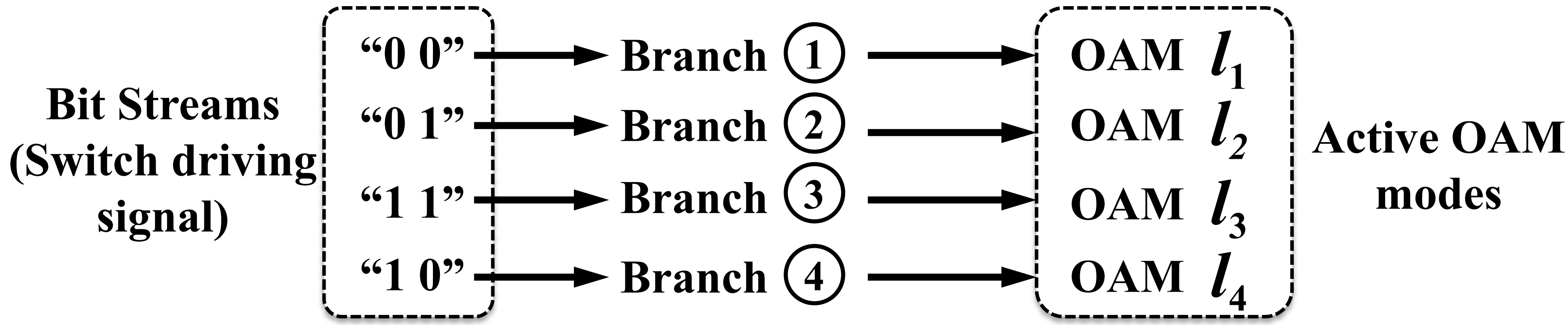


- **Challenges**: the design of data patterns for signal #1-#*N and the* synchronization among all the VCSEL data channels.
- We will explore the influence of using multiple different VCSELs as laser source on the system security and data rate.

20 Gbit/s OAM Encoding — Proof-of-concept Experiment



Mapping Relationship



- The 1×4 optical switch is built by cascading one 2×2 switch with two 2×2 switches, each of which has a 10-GHz switching bandwidth.
- Given that four OAM states are used, 2 bits can be encoded in a symbol period, Therefore, 20 Gbit/s ($10\times\log_2 4$) data rate is achieved.

Optics Letters 2015

20 Gbit/s OAM Encoding — Experiment Setup

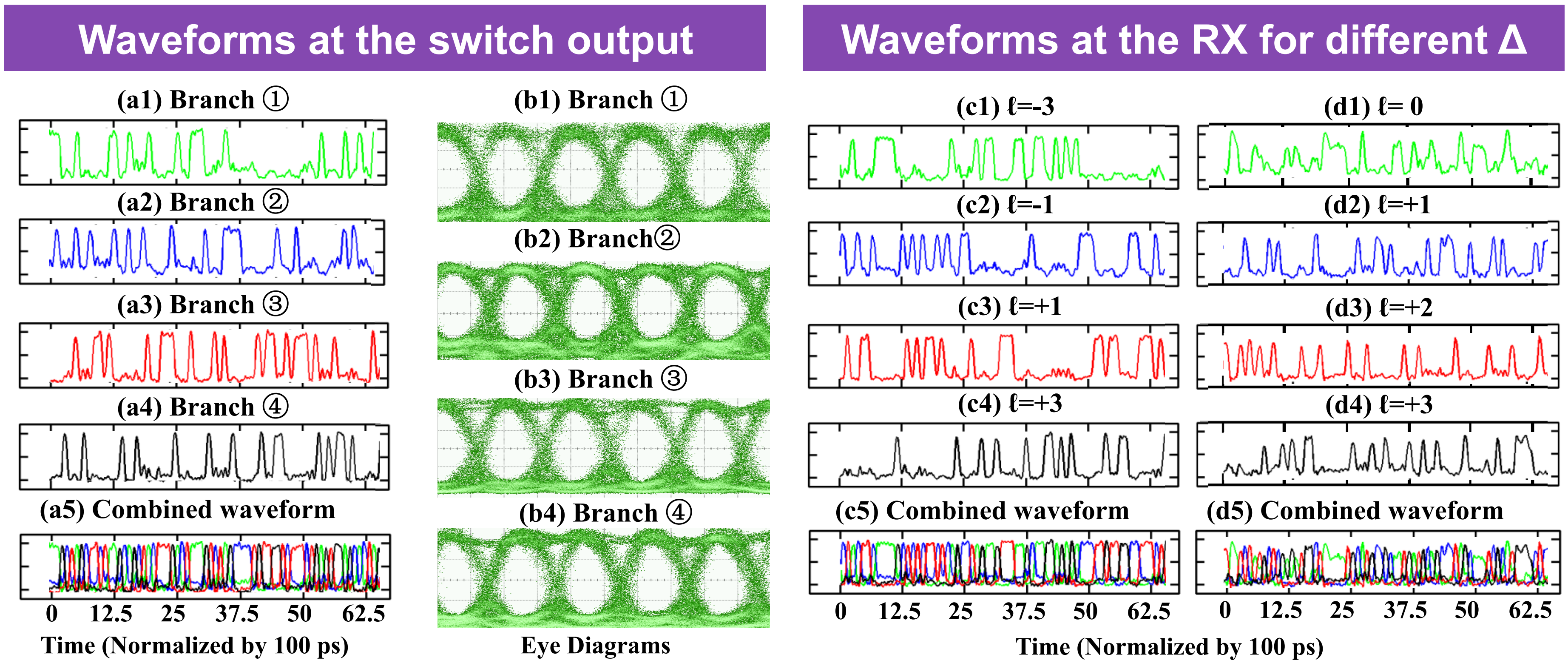
Crosstalk for Different Mode Spacing Δ

Δ=1 (ℓ=0, +1, +2, +3)		Δ=2 (ℓ=-3, -1, +1, +3)		Δ=3 (ℓ=-4, -1, +1, +4)		Δ=4 (-6, -2, +2, +6)	
Mode	**Crosstalk**	**Mode**	**Crosstalk**	**Mode**	**Crosstalk**	**Mode**	**Crosstalk**
ℓ = 0	-11.2 dB	ℓ = -3	-22.5 dB	ℓ = -4	-35.2 dB	ℓ = -6	-36.2 dB
ℓ = +1	-14.0 dB	ℓ = -1	-22.0 dB	ℓ = -1	-19.9 dB	ℓ = -2	-29.4 dB
ℓ = +2	-12.4 dB	ℓ = +1	-18.3 dB	ℓ = +1	-20.8 dB	ℓ = +2	-26.5 dB
ℓ = +3	-12.2 dB	ℓ = +3	-19.4 dB	ℓ = +4	-27.4 dB	ℓ = +6	-27.5 dB

- ❑ The system performance is affected by two kinds of crosstalk: switch-induced crosstalk and OAM intermodal crosstalk.
- ❑ As mode spacing increases, OAM intermodal crosstalk decreases.

Optics Letters 2015

20 Gbit/s OAM Encoding — Experiment Results

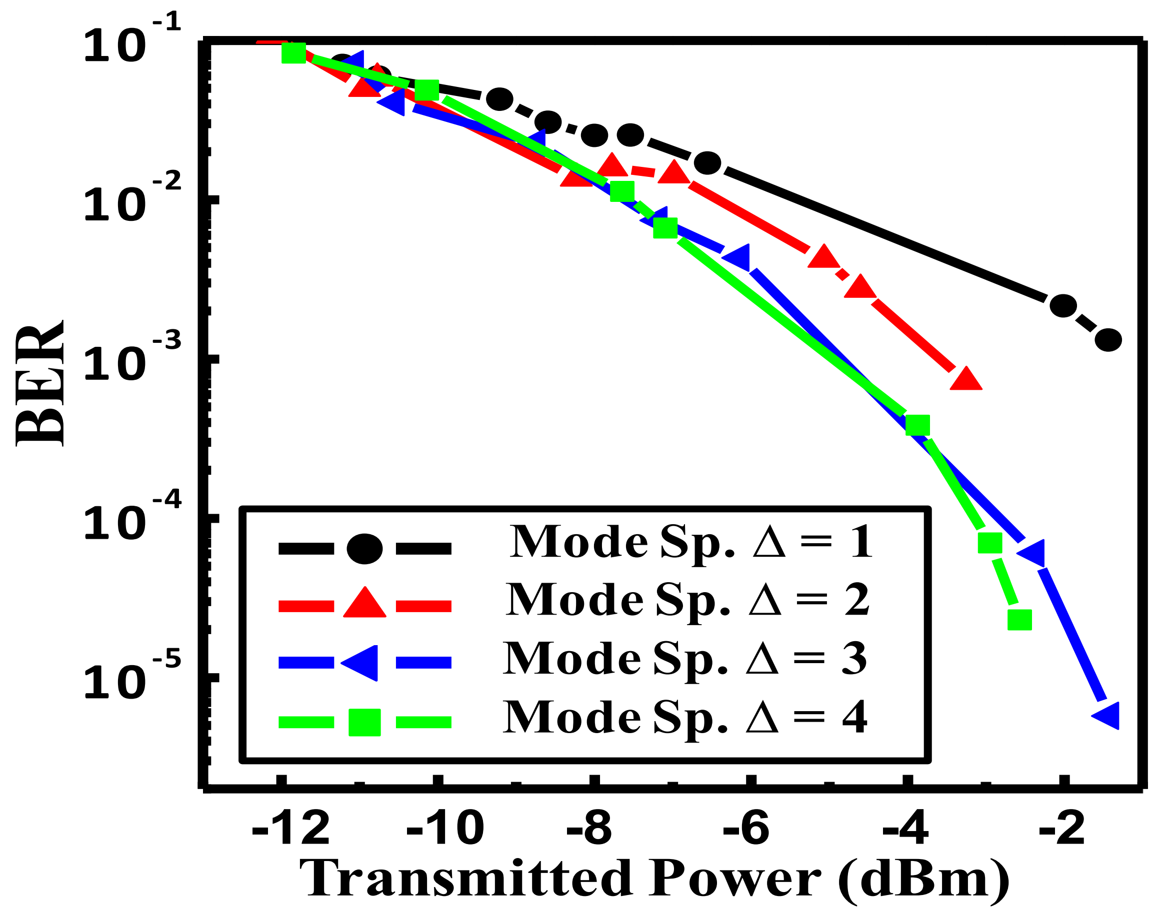


- From the four switch output branches, the combined waveform verifies that light is routed to only one of the branches in each 100-ps period.
- The waveforms when using mode set {-3, -1, +1, +3} exhibit better quality than those when using {0, +1, +2, +3}, due to less OAM intermodal crosstalk.
- By determining which mode is active in each symbol period, the encoded bit information can be recovered.

Optics Letters 2015

20 Gbit/s OAM Encoding — Experiment Results

BER Transmitted Power (measured at switch outputs)



- ❑ The Δ=1 case has worse BER performance due to larger OAM crosstalk.
- ❑ The power penalty of Δ=1 case is estimated to be 3.2 dB with respect to the Δ=3 case at the forward error correction limit of 3.8×10^{-3}.

Optics Letters 2015

The Optical Sciences Company
1341 S. Sunkist St. Anaheim, CA 92806 Phone: (714)772-7668 Fax: (714)772-9870 Email: glenn.a.tyler@tosc.com

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

Atmospheric Considerations

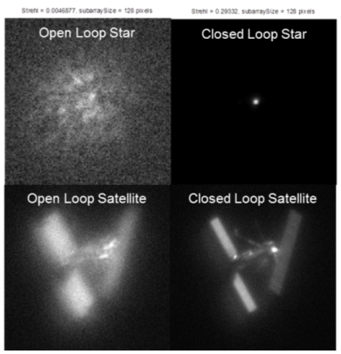
Kick Off Meeting

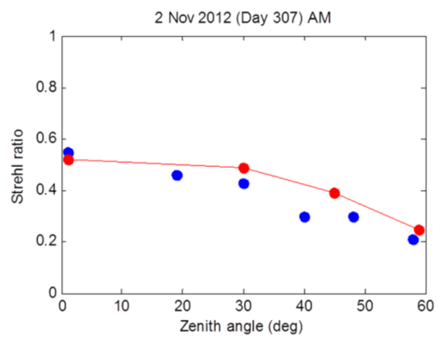
Glenn A. Tyler
Jeffrey L. Vaughn
and
Nicholas K. Steinhoff

9 December 2015

Turbulence Encountered in Navy Engagements Falls into Three Classic Categories

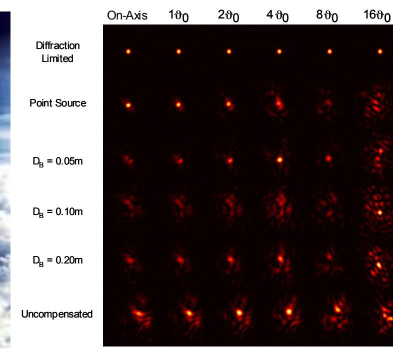
Ordinary Turbulence
(Experimental Data and Hand Analysis for tOSC AMOS Upgrade)

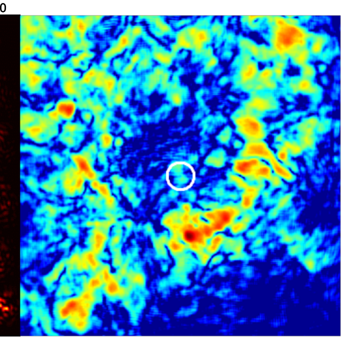




Strong Turbulence
(ABL shot down three missiles)

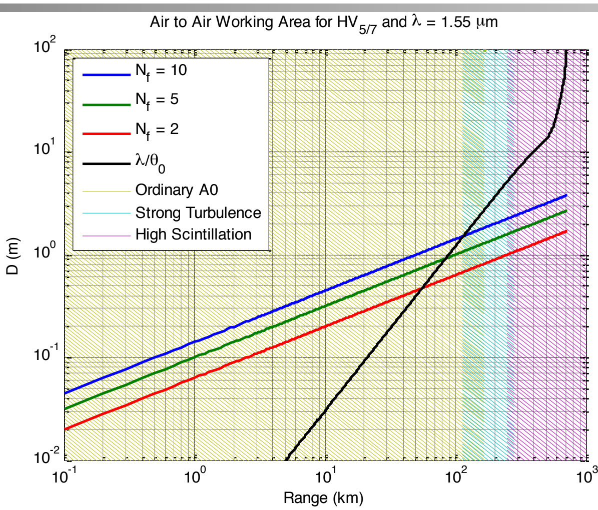
Deep Turbulence
(Left: Anisoplanatism   Right: Irradiance Coupling)

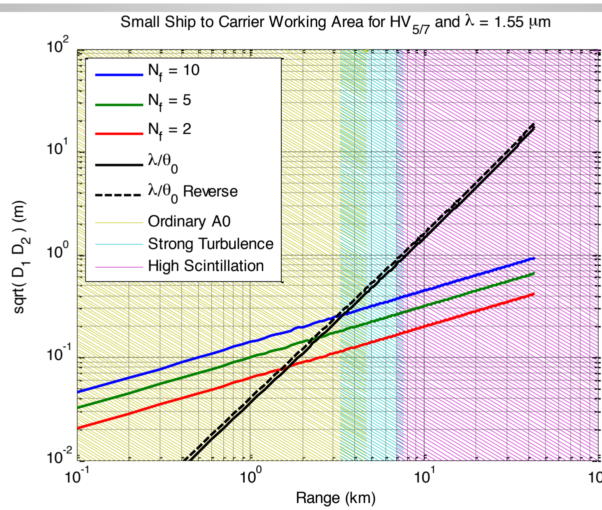


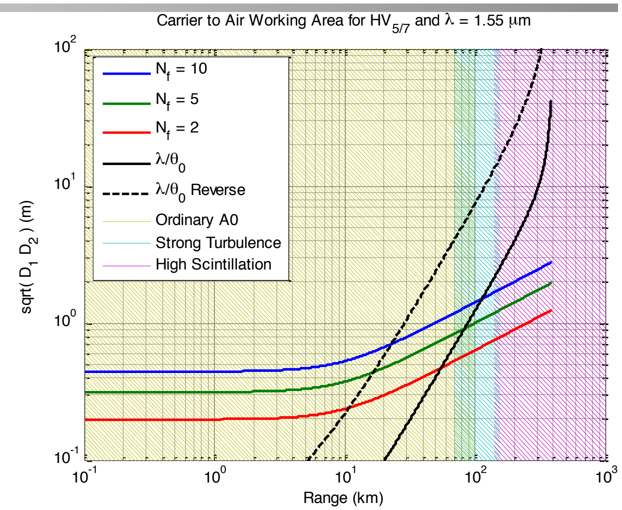


- Ordinary turbulence
  - Encountered in Surveillance and Astronomy
  - First order Rytov theory applies
  - Hand analysis agrees very well with experiment
- Strong turbulence
  - Encountered in relatively weak but long propagation paths
  - First order Rytov Fails, scintillation saturates, onset of branch points
  - Wave optics required and crossvalidated with analysis when appropriate
- Deep turbulence (Strong scintillation and Anisoplanatism)
  - Encountered in tactical applications and horizontal path laser com
  - Rytov number > 1, $\vartheta_0 < \lambda/D$, significant Anisoplanatism, atmospheric guiding
  - Wave Optics crossvalidated with experiment required

Identification of Atmospheric Disturbance Levels for Navy Lasercom Applications







- Three engagements are considered above; Air to Air (10k), Small Ship (20m) to Carrier (60m) and Carrier (60m) to Air (10km)
- The colors indicate the turbulence level (Deep turbulence is below the black lines in the high scintillation region and shows where $D = \lambda/\vartheta_0$)
- To optimize the spatial bandwidth of the propagation link we would like to support a Fresnel number of five indicated by the green lines (the red and blue lines correspond to Fresnel numbers of two and ten, respectively)
- These lines end when the curvature of the earth blocks the beam
- The results illustrate the diameters required and the turbulence levels encountered for the three links of interest
  - Air to Air is Ordinary Turbulence up to about 100km but requires meter class optics
  - Small Ship to Carrier or Carrier to Small Ship requires 30 cm optics at ten kilometers and Deep Turbulence compensation
  - Carrier to Air is ordinary turbulence and requires 30cm optics

High Dimensional MUB States Are Analytically Determined

- In Quantum Communications applications it is desirable to utilize Mutually Unbiased Bases (MUBs)
- The basis vectors are denoted as $|m>$ where m takes on N values
- Each MUB state set has N vectors which in turn are written in terms of the N basis vectors
- The p^{TH} set of MUB States are given by

$$\left|n,p\right\rangle = \sum_{m=1}^{N} A_{pnm}\left|m\right\rangle \quad , \quad A_p^{\dagger}A_p = \tfrac{I}{N}$$

- They satisfy the following relations

$$\left|\left\langle q,m \middle| n,p\right\rangle\right|^2 = \delta_{nm}\delta_{pq} + \tfrac{1-\delta_{pq}}{N}$$

- For N an odd prime there are N+1 MUBs and the expansion coefficients A_{pnm} are given by*

$$A_{pnm} = \begin{cases} \delta_{nm} \quad , & for\ p = 0; \\ \frac{1}{\sqrt{N}} e^{\frac{2\pi i}{N}\left(pn^2+nm\right)}, & otherwise. \end{cases}$$

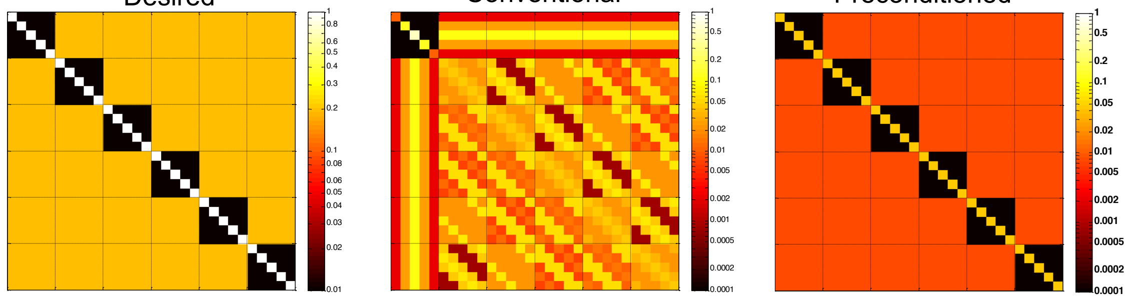
- Note that p=N results in the Fourier kernel
- As a consequence the MUB states have important properties
  - Within each basis the states are orthogonal
  - If the wrong basis is used no information is obtained since all probabilities are equal
- We typically use the basis vectors (p=0) and the Fourier (p=N)
- The basis states have minimum energy loss and are similar to OAM

*I.D. Ivonovic, "Geometrical Description of Quantum State Determination," Journal of Physics A: Mathematical and General, **14** 3241-3245 (1981)

Preconditioned MUB States Based upon Minimum Energy Loss OAM States Address Propagation Issues

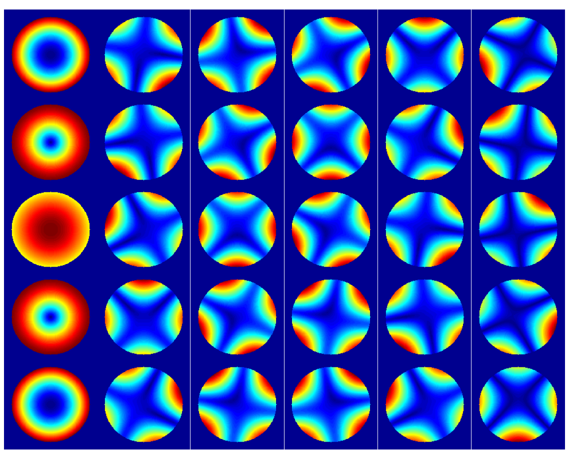
- Transmit Receive Matrix (N_f=1, N=5) exhibits desired character at receiver

Desired Conventional Preconditioned

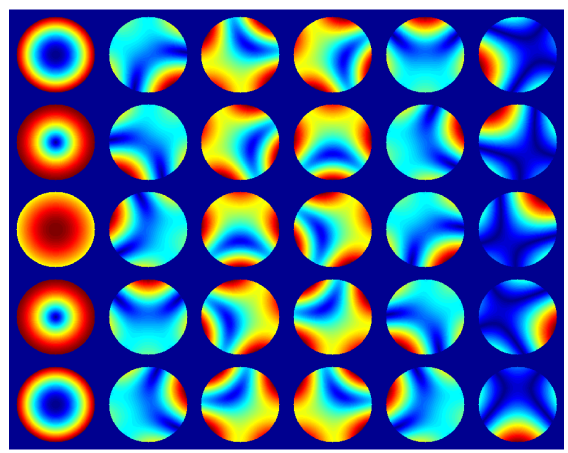


- The preconditioned result includes propagation loses and only differs from desired by a loss factor
- For high dimensions and low Fresnel numbers (N_f=1, N=5) the preconditioned MUB states look quite similar except for the fundamental basis

Transmitted Preconditioned MUB States



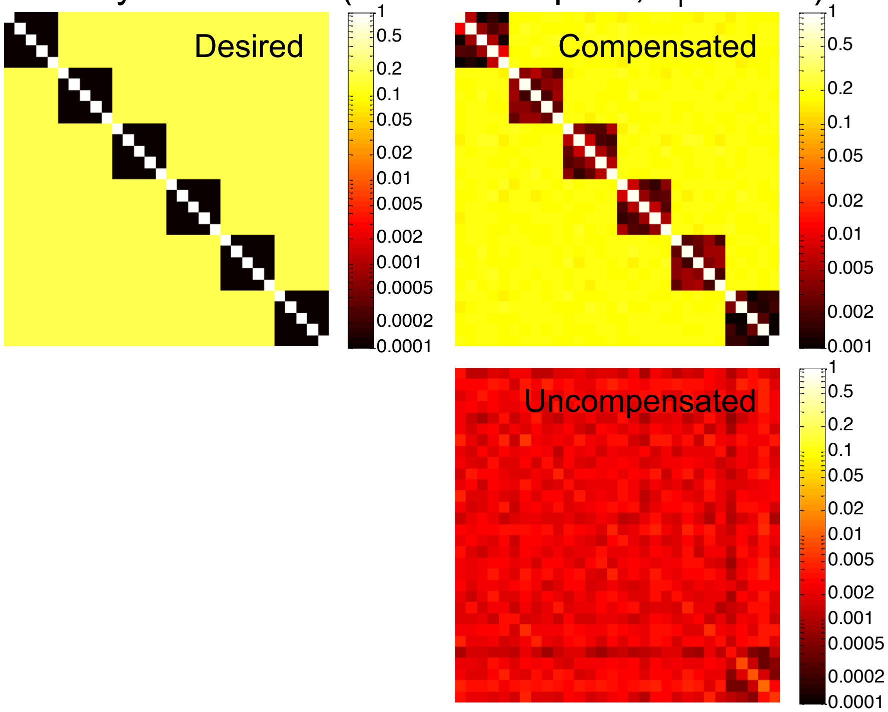
Received MUB States



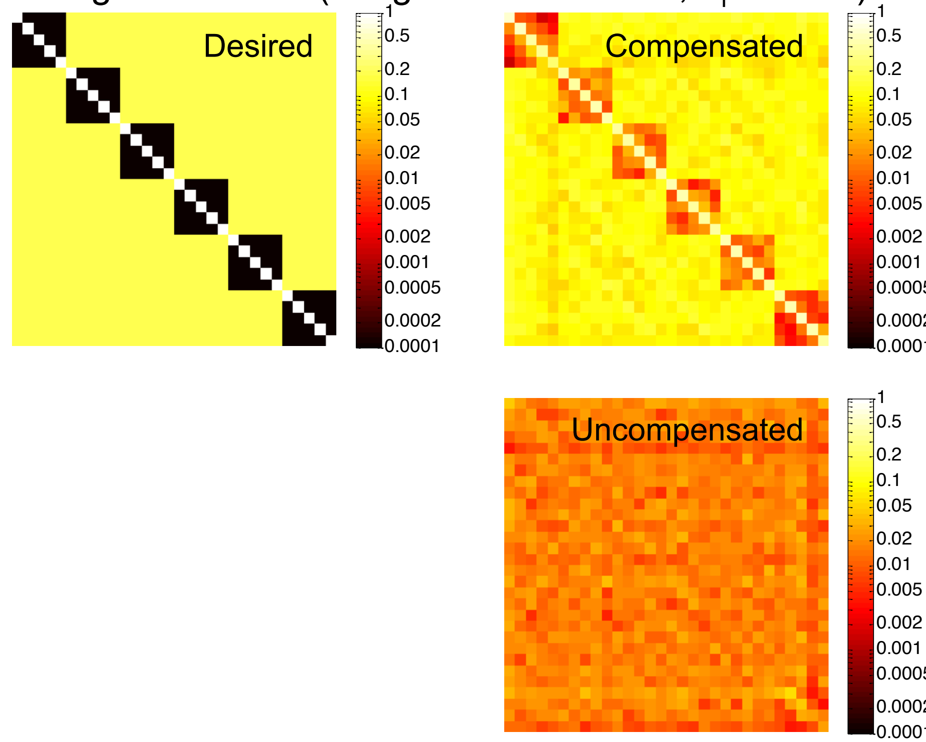
- For low Fresnel Numbers the transmitted and received fields are quite different
- The basis vectors are unaffected because they are already a minimum energy loss state

Ordinary and Strong Turbulence Engagements Are Amenable to AO Enhancement

Ordinary Turbulence (Ground to Space, σ_I^2 = 0.02)



Strong Turbulence (Long Horizontal Path, σ_I^2 = 0.39)

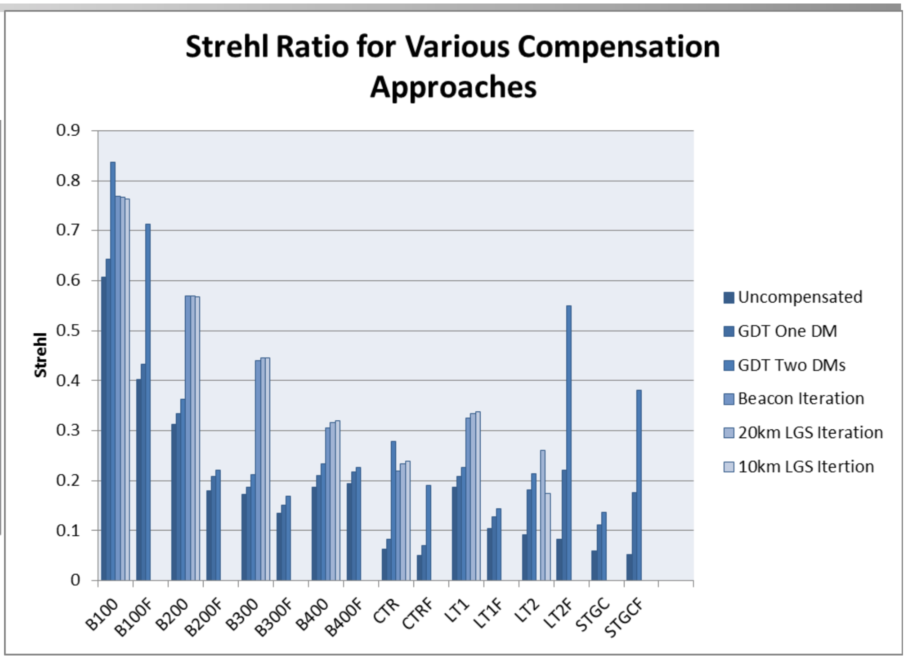


- Both engagements utilize HV57 turbulence with a wavelength of λ = 1.55 μm
- For Ground to Space: L = 350 km represents a LEO propagation at zenith, D_R = 50 cm and D_T = 3.5 m so we have N_f = 2.53
- For Long Horizontal Path: L=20km, altitude = 20m at xmit site and 1600m at receive site, D_R = D_T = 40 cm for N_f = 3.88

The Optical Sciences Company

A Variety of Techniques Have Been Developed for JTO Deep Turbulence Engagements

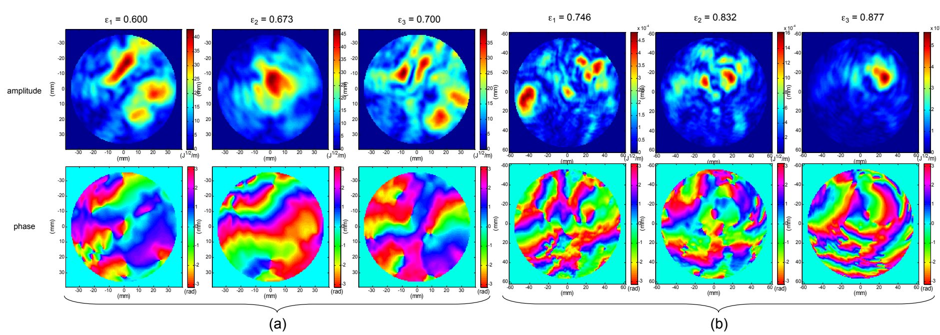
Parameter	Bagnell 100	Bagnell 200	Bagnell 300	Bagnell 400	Carreras Tactical Relay	Low Tactical 1	Low Tactical 2	Duff Strategic
H-observer (km)	8	8	8	8	1.5	4	4	12
H-target (km)	8	8	8	8	0.005	4	4	25
V-observer (m/s)	270	270	270	270	0	100	100	300
V-target (m/s)	1000	1000	1000	1000	10	1000	1000	2000
Range (km)	100	200	300	400	30	180	180	400
Aperture size (m)	0.3	0.3	0.3	0.3	0.3	0.3	1.0	1.5
r_0 (cm)	29.1	20.0	16.7	14.1	12.7	14.4	14.4	15.3
θ_0 (μrad)	0.914	0.314	0.175	0.11	0.259	0.252	0.252	0.287
Rytov (-)	0.202	0.66	1.21	2.12	0.999	1.14	1.14	1.12
Jitter (μrad)	1.49	2.04	2.37	2.73	2.99	2.68	2.68	1.96
Greenwood (Hz)	1770	2570	3050	3610	394	3180	3180	3070
Tyler tracking (Hz)	307	419	485	557	48.6	496	406	388



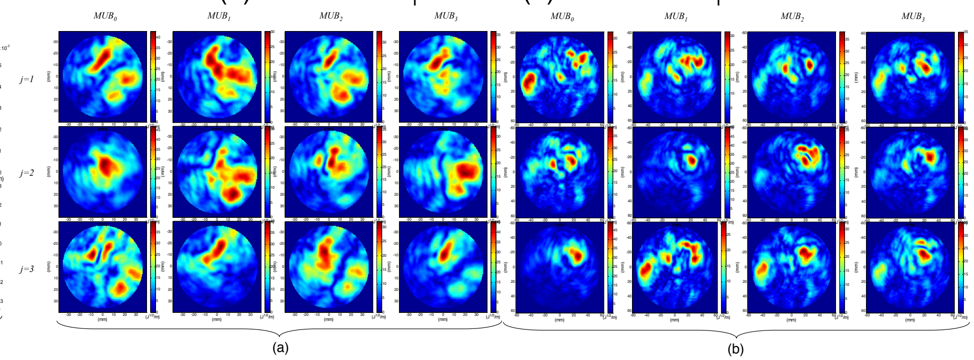
- Compensation techniques for this level of turbulence include multiple DMs, Branch Cut reconstructors, one or more laser guide stars and a variety of iteration approaches
- Gradient Descent Tomography utilizes two DMs and does not require a wavefront sensor
- These and other approaches will be used to address Qcom in Navy Engagements

Preconditioned MUB States in Deep Turbulence

Amplitude and Phase of Minimum Energy Loss Basis for Deep Turbulence
(a) Pertains to N_f = 2 and (b) Pertains to N_f = 5



Preconditioned MUB States for Deep Turbulence
(a) Pertains to N_f = 2 and (b) Pertains to N_f = 5



- In this work it is assumed that the atmosphere is probed to assess its volume characteristics
- The elementary minimum energy loss basis states are found by solving the appropriate Eigen equations
- These state have high efficiencies
- The preconditioned MUB states exploit the scintillation filament structure