High Capacity Quantum Cryptography Carrying more than One Bit Per Photon

Robert W. Boyd
Institute of Optics and Department of Physics and Astronomy
University of Rochester
Rochester, NY 14627 USA
boyd@optics.rochester.edu

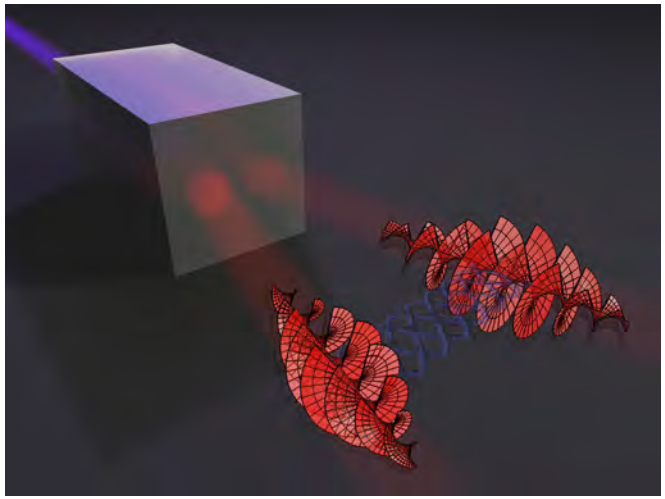
Presented to the US Air Force Scientific Advisory Board (SAB) studying "Utility of Quantum Systems for the Air Force," March 25, 2015.

Use of Quantum States for Secure Optical Communication

- The celebrated BB84 protocol for quantum key distribution (QKD) transmits one bit of information per received photon

- We have built a QKD system that can carry more than one bit per photon.
  - Note that in traditional telecom, one uses many photons per bit!

- Our procedure is to encode using beams that carry orbital angular momentum (OAM), such as the Laguerre-Gauss states, which reside in an infinite dimensional Hilbert space.

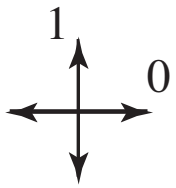


The BB84 QKD Protocol – Polarized Light Implementation

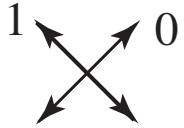
Alice sends an individual photon in one of two polarization bases, chosen at random

Bob receives in one of two polarization bases, which he choses at random

x-y basis

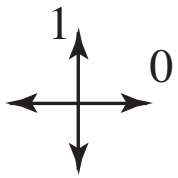


diagonal-anti-diagonal basis

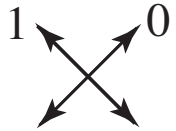


transmission

x-y basis



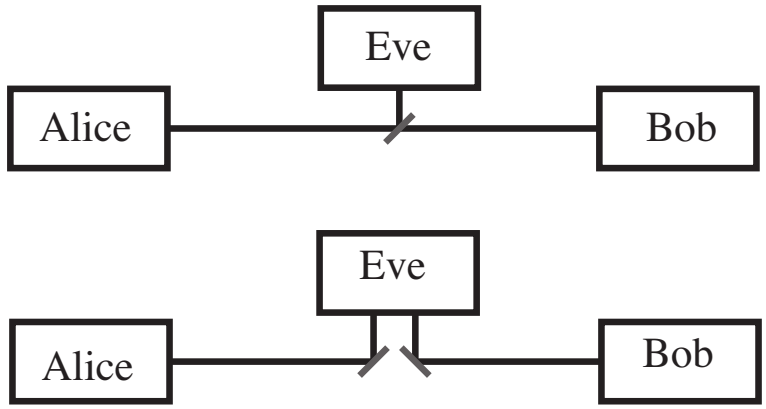
diagonal-anti-diagonal basis



After sending the entire string of numbers that constitutes the key, Alice and Bob openly divulge the basis that they used for each measurement. If they chose different bases, they discard the result of that measurement. (The remaining data is known as sifted data.)

Why Is This Protocol Secure?

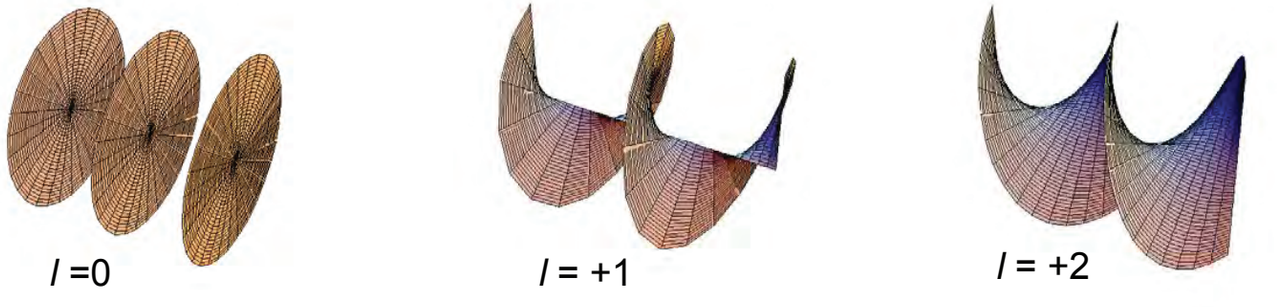
- Suppose that an eavesdropper (Eve) intercepts the transmission. Since only one photon was transmitted, Bob will know that the message was intercepted, because he does not receive Alice's photon.
- To avoid divulging her presence in such an obvious manner, Eve can resend the photon after she intercepts it. But Eve has no guarantee that she will be sending the photon in the same basis as that used by Alice. And if she choses wrong, Alice and Bob will realize that there is a problem.



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.)

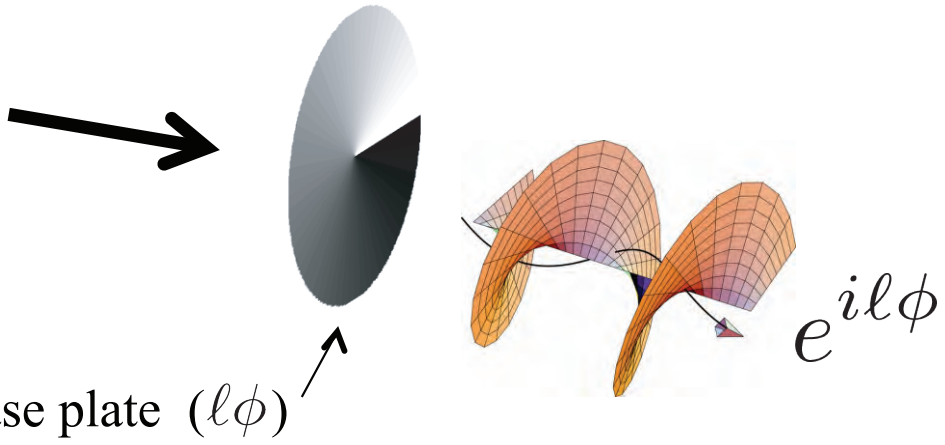
Phase-front structure of some OAM states



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

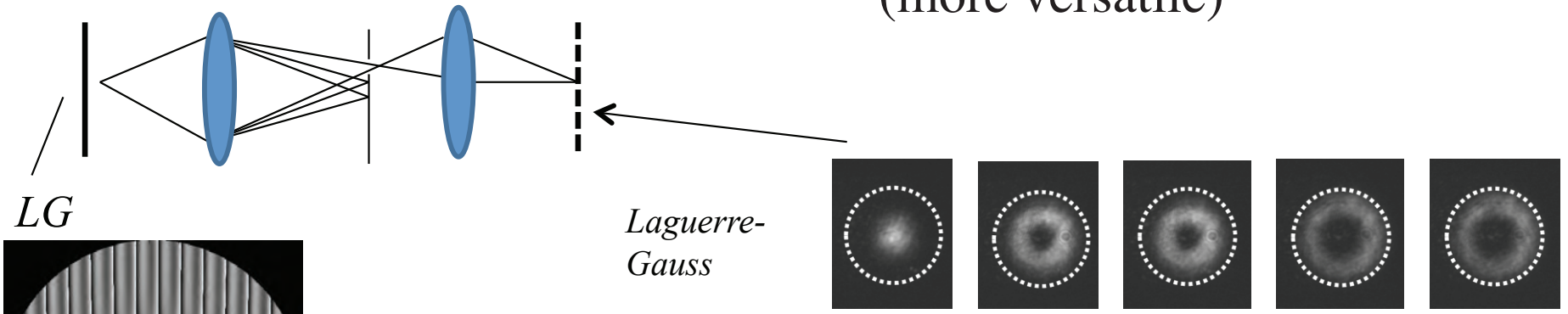
How to create a beam carrying orbital angular momentum?

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).

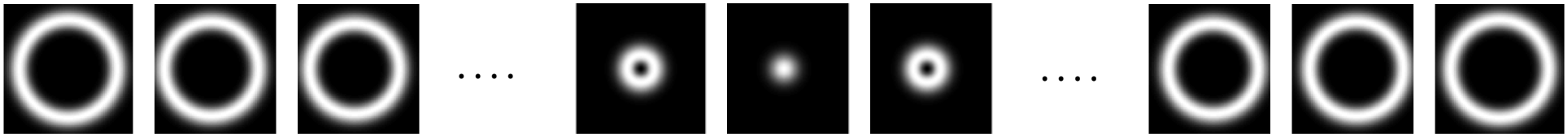
High Capacity QKD Protocol

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).

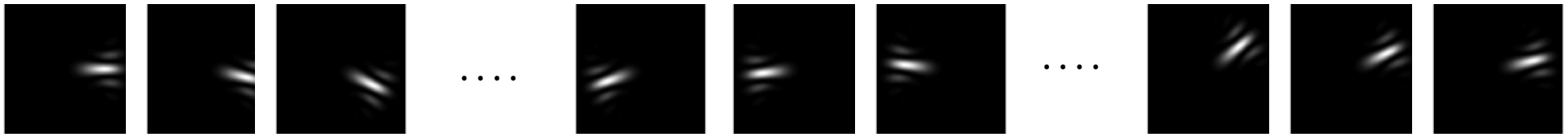
We are developing means to mitigate the influence of atmospheric turbulence

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



0 1 2 12 13 14 25 26 27

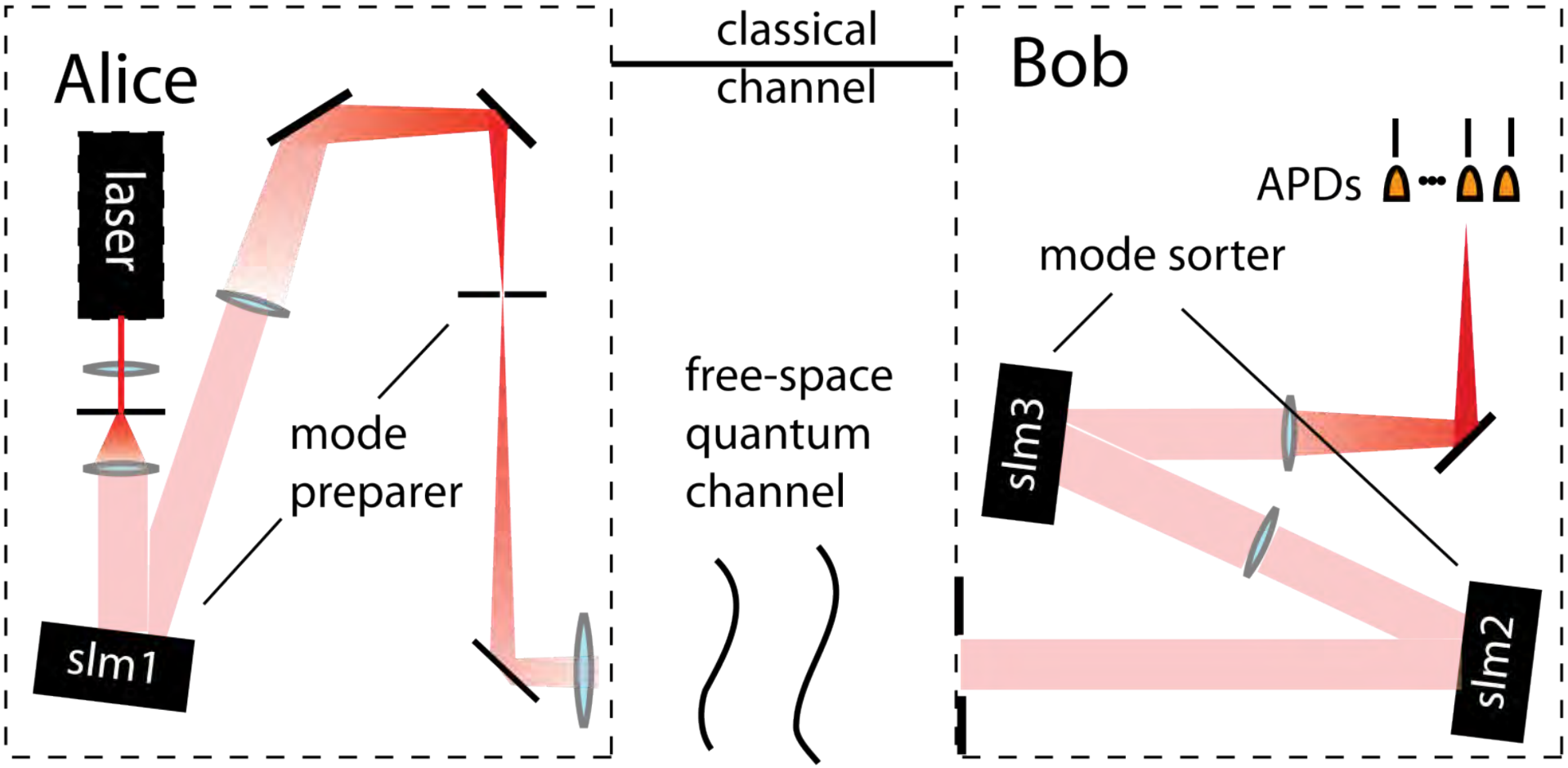
"Angular" Basis (mutually unbiased with respect to LG)



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

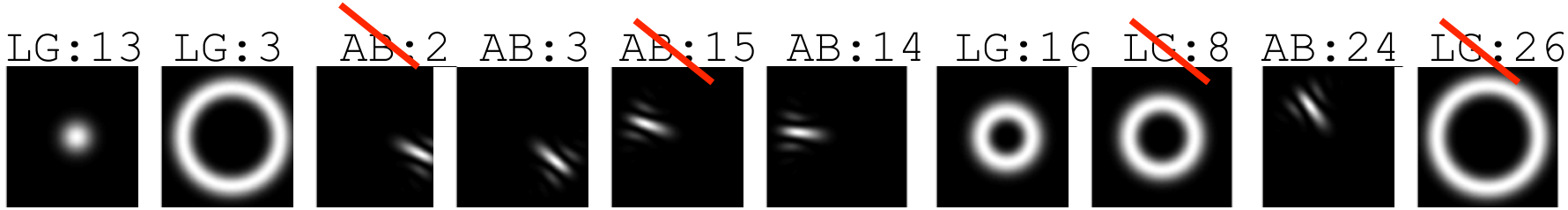
Protocol

Modified BB84 as discussed

Challenges

1. State Preparation
2. State Detection
3. Turbulence

Protocol



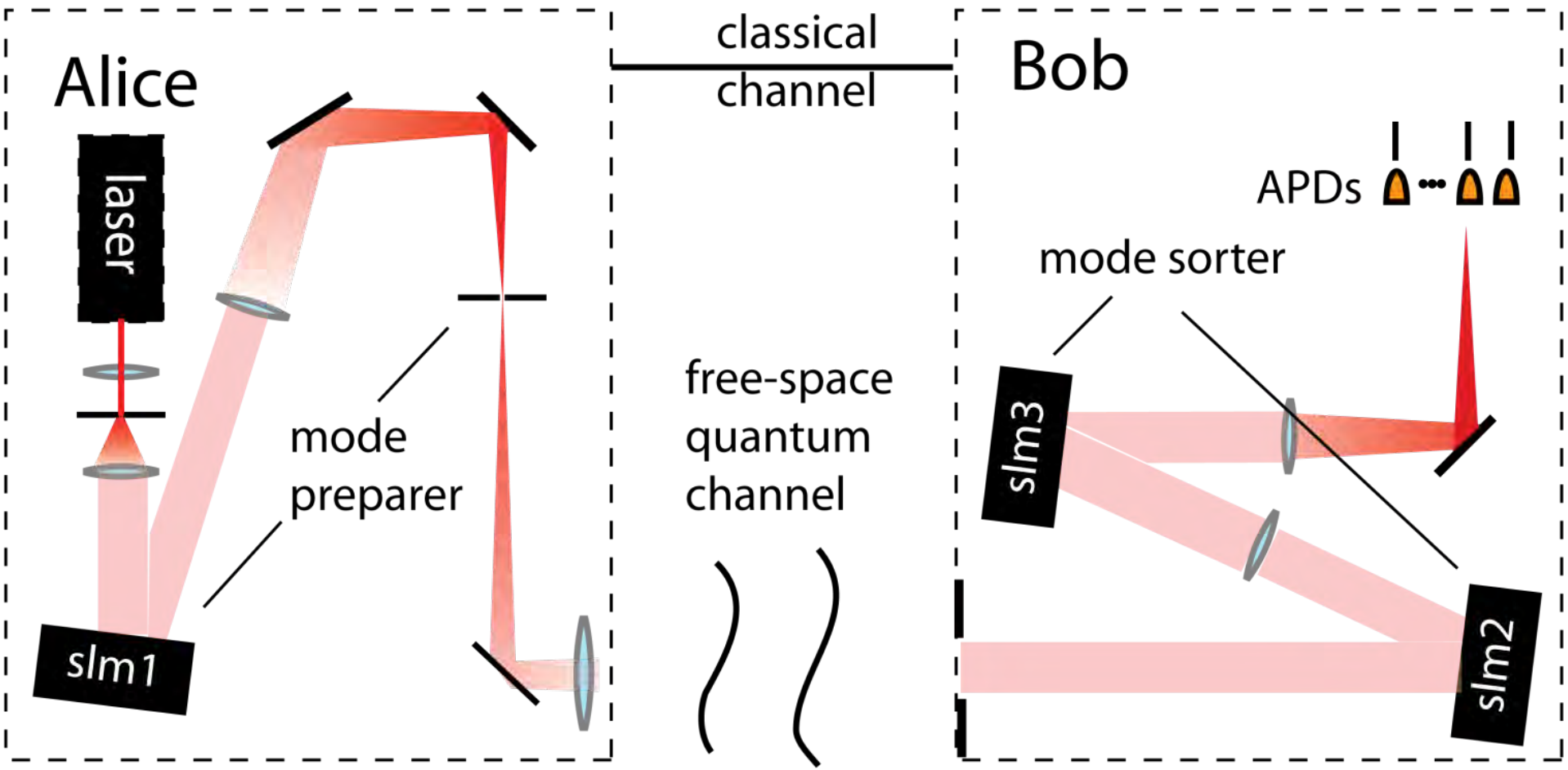
Sifted Key 13 3 3 14 16 24 ... ← in principle contains no errors unless eavesdropper is present.

In any real system, Bob's key will have errors due to system imperfections.

1. Error Correction (Cascade Protocol)
2. Privacy Amplification

Under many conditions, these protocols can be successfully implemented if Alice/Bob share more bits of information than Alice and Eve.

Spatially-Based QKD System



Source

Weak Coherent Light

Heralded Single Photon

Protocol

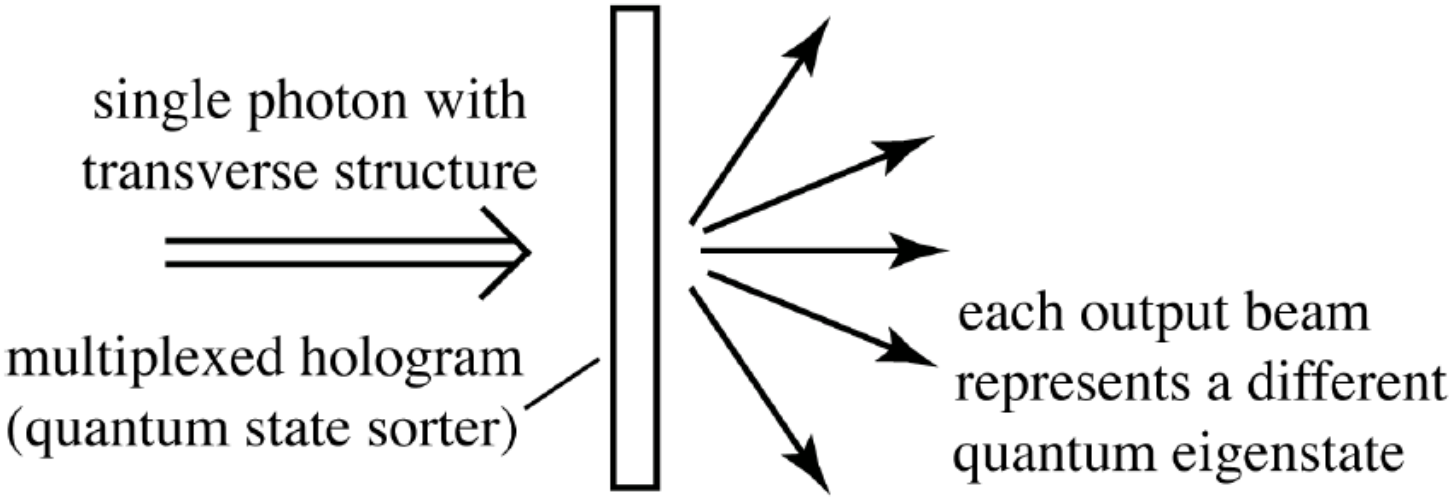
Modified BB84 as discussed

Challenges

1. State Preparation
2. State Detection
3. Turbulence

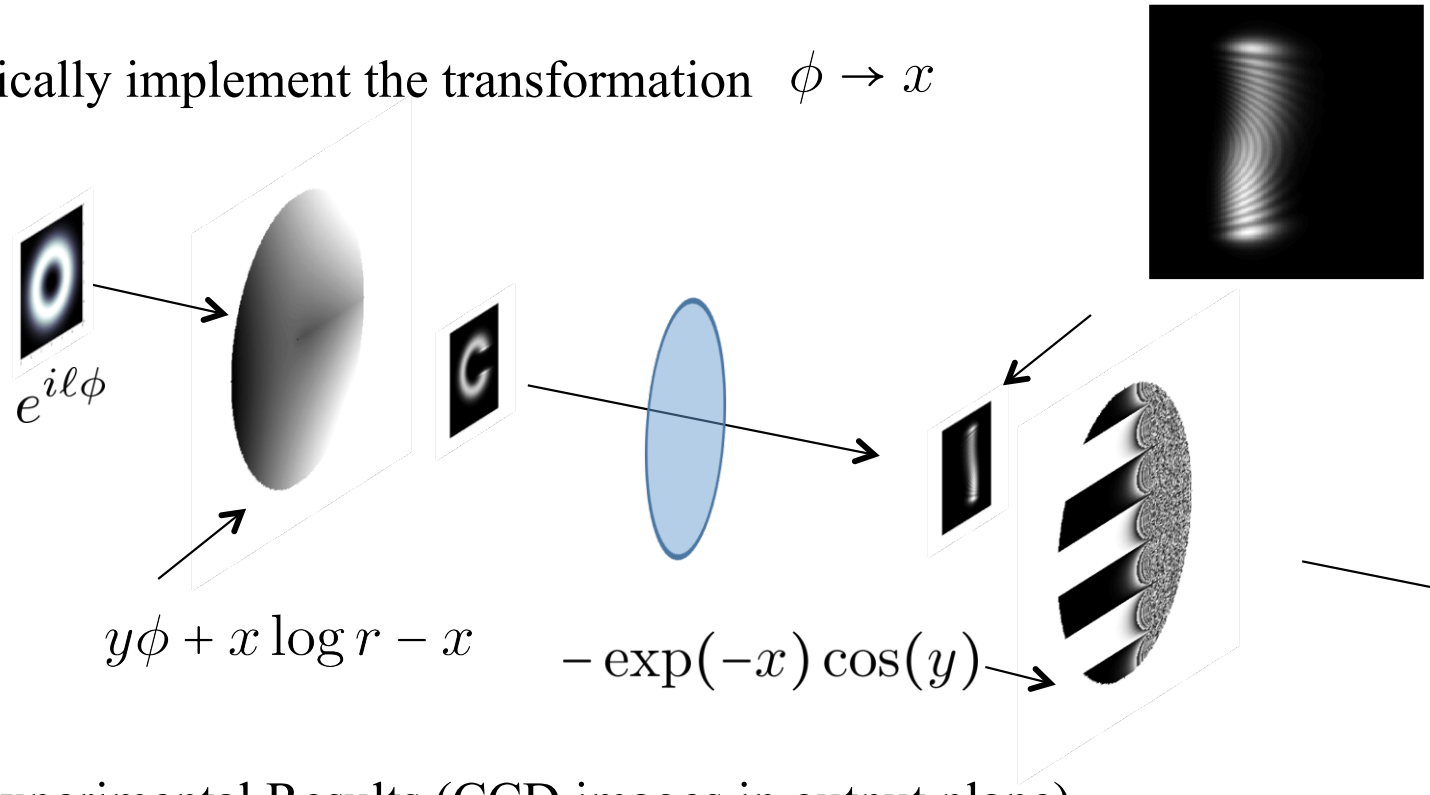
Mode Sorting

A mode sorter

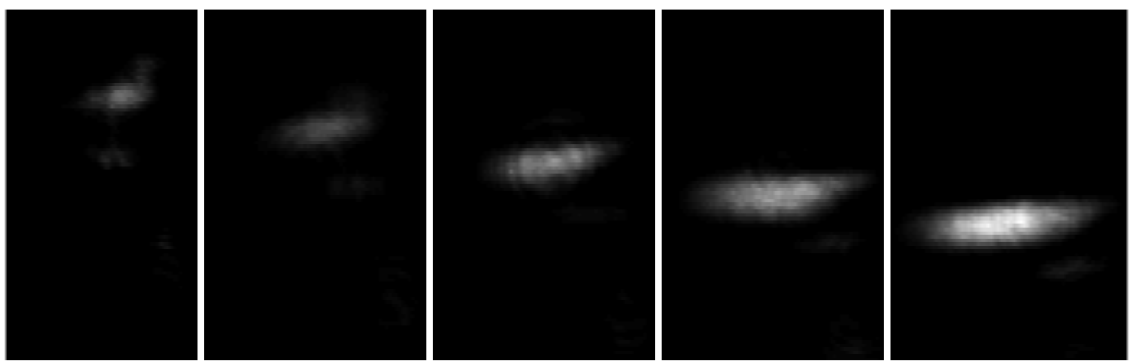


Sorting OAM using Phase Unwrapping

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.

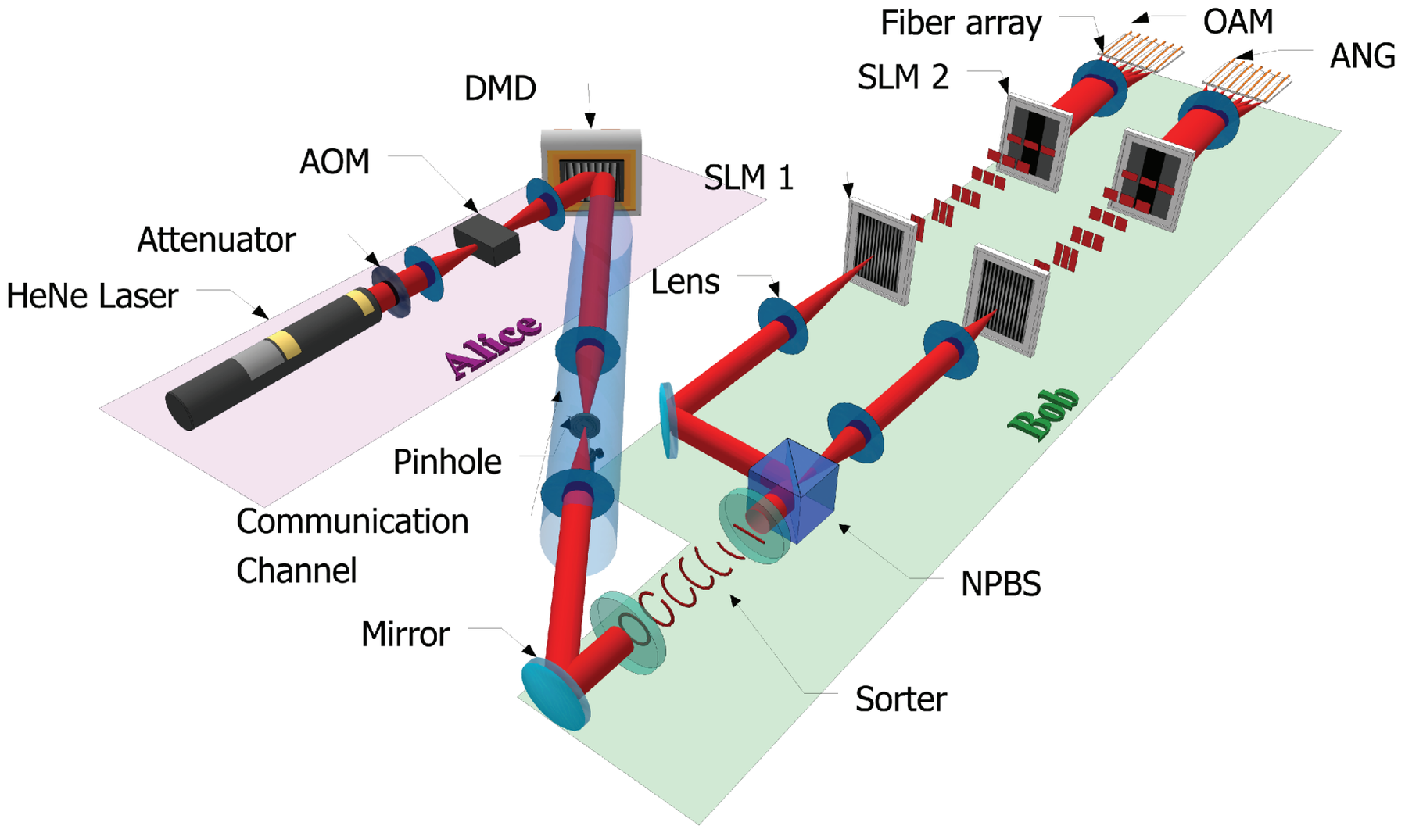
*Berkhout *et al. PRL* **105,** 153601 (2010).

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

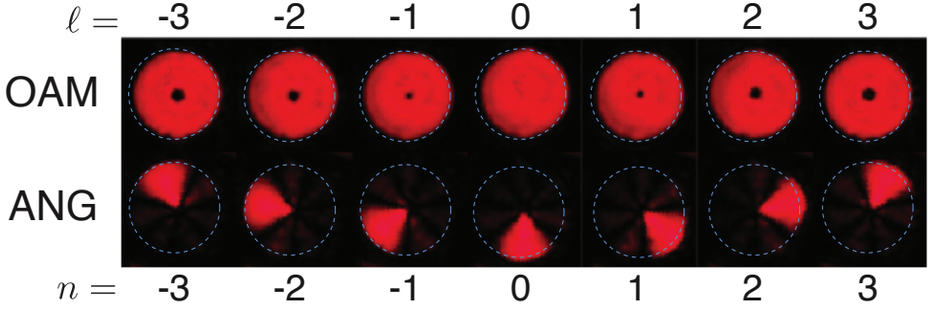
UNIVERSITY of ROCHESTER

Nonlinear Optics Group

Our Laboratory Setup



We use a seven-dimensional state space



Laboratory Results - OAM-Based QKD

Alice

```
0631336021320454444456141026645
5450503636030252616432155241 64
2301466025134016132224515510 26
```

Bob

```
0630336011320214444456141026645
5450223536030252616432155241 64
2301466025154036134224515510 26
```

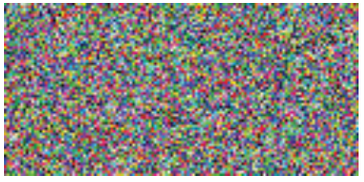
Error Correction

```
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
```

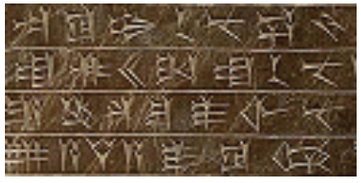
Privacy Amplification

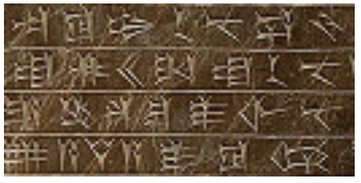
```
0001 0100 1011 1111 1111 1010 1010 0111 1010 1011 1111 0001 0000 1101 1111
1110 1110 1101 1110 0001 0011 1000 0101 1101 1100 0011 0111 1101 0001 1001
0100 0110 1011 0000 0110 1010 1
```

Alice Encrypts

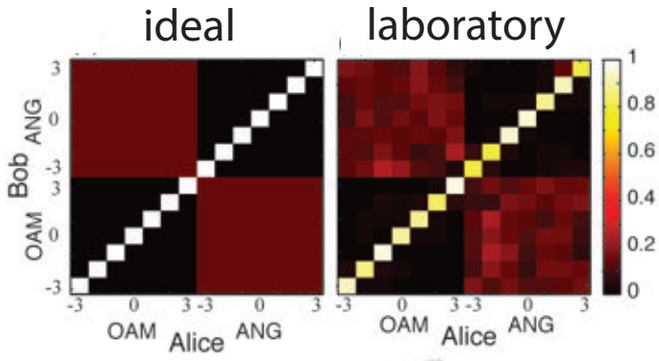


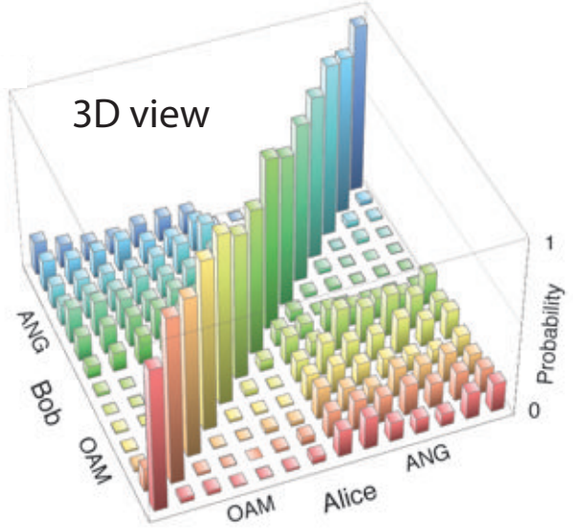
Bob Decrypts



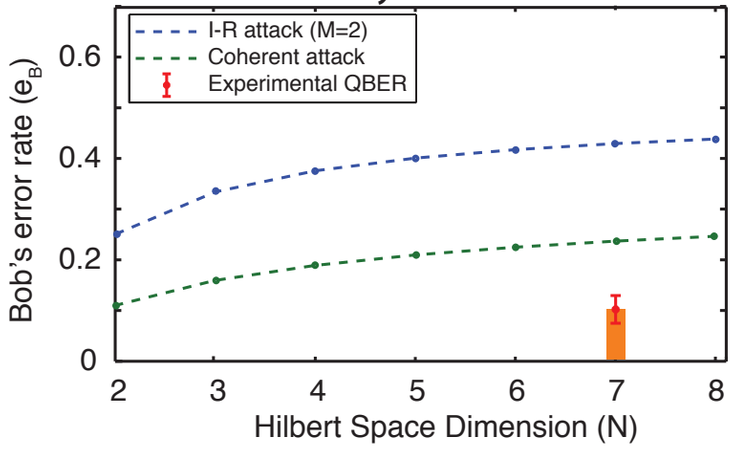


cross-talk matrices





- error bounds for security



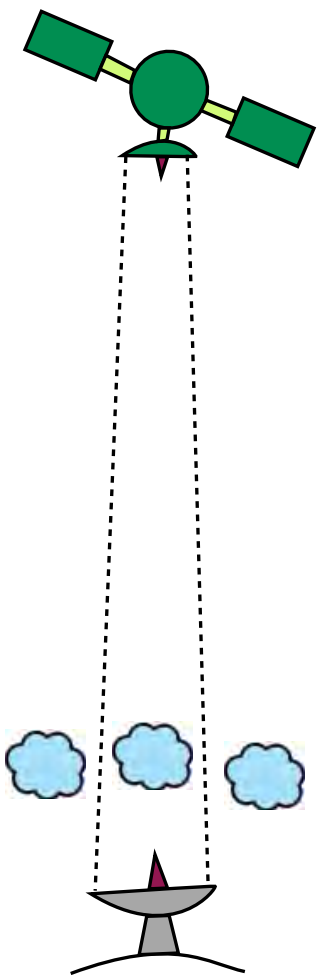
We use a 7-letter alphabet, and achieve a channel capacity of 2.1 bits per sifted photon.

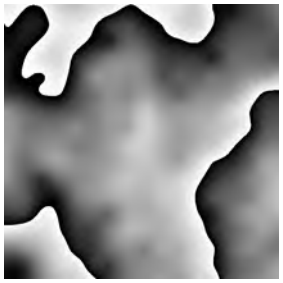
We do not reach the full 2.8 bits per photon for a variety of reasons, including dark counts in our detectors and cross-talk among channels resulting from imperfections in our sorter.

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

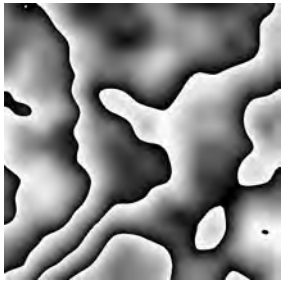
Turbulence and Adaptive Optics

Atmospheric Turbulence Model

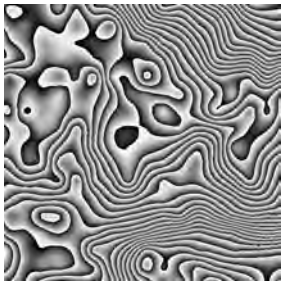




$D/r_0 = 5.12$

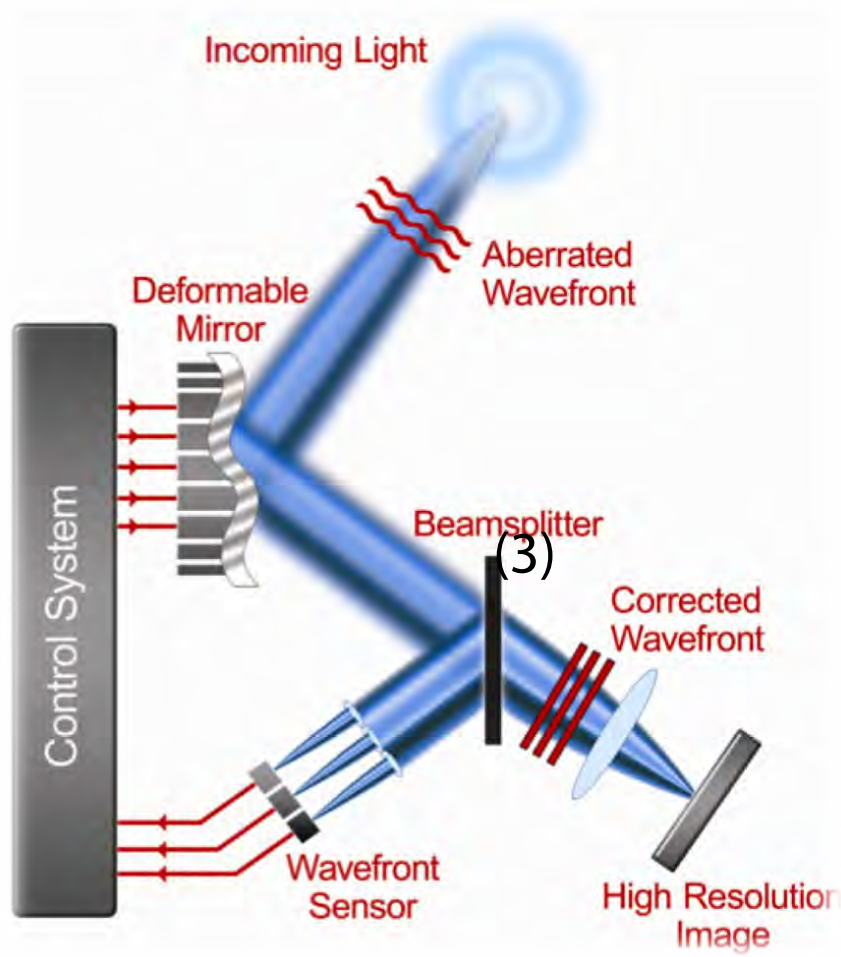


$D/r_0 = 10.24$

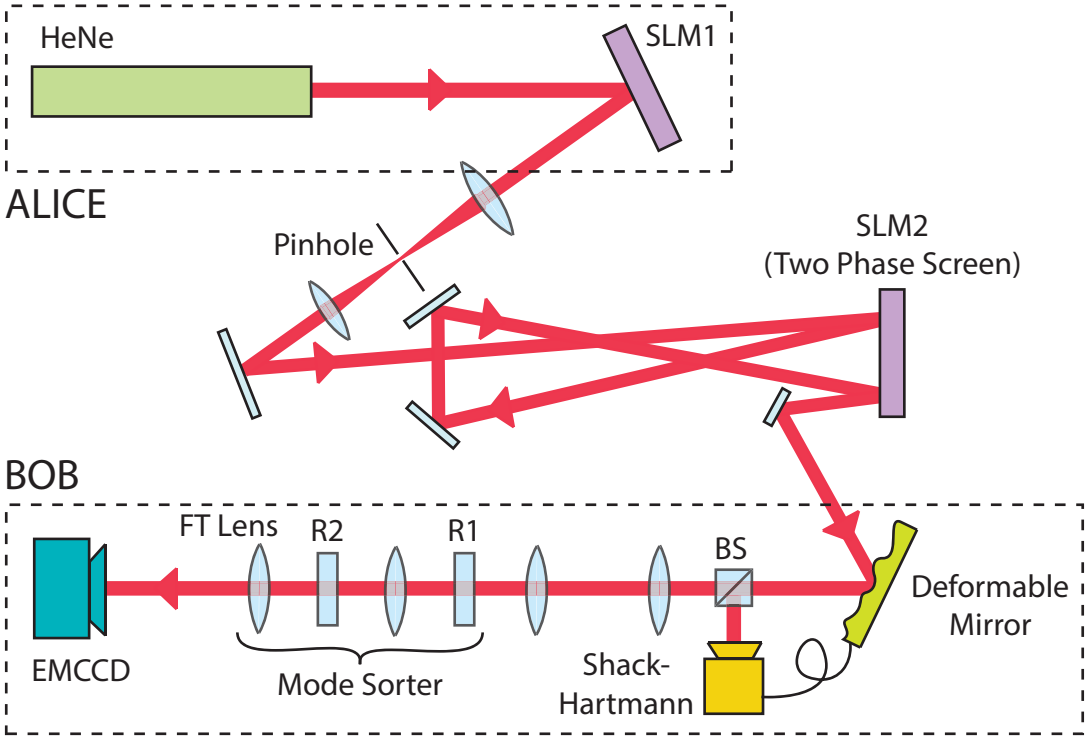


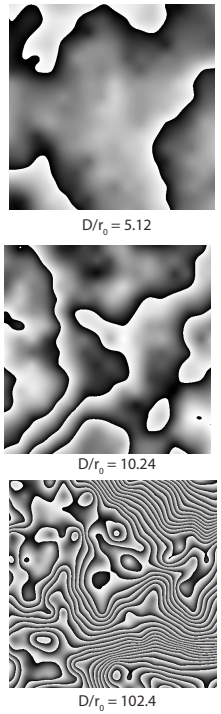
$D/r_0 = 102.4$

Our Adaptive Optics System



Turbulence and Adaptive Optics



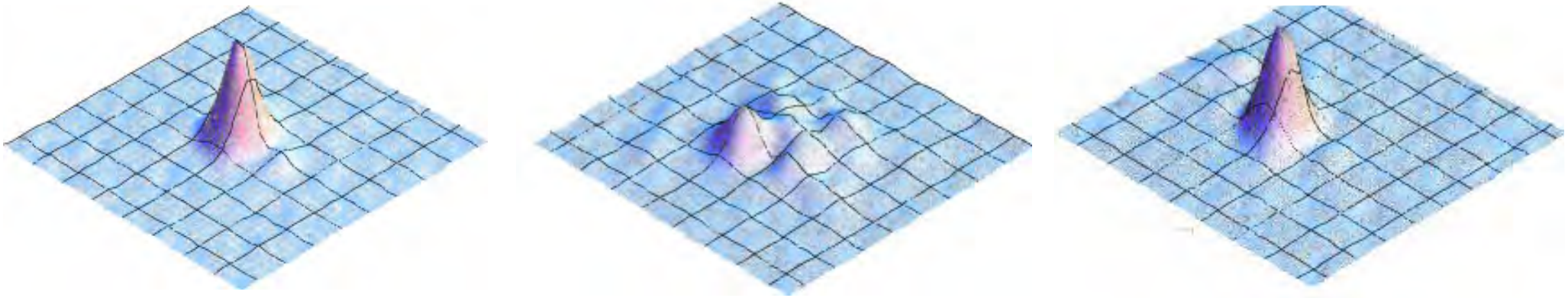


- We have found that we can adequately model thick hoizontal turlulence (10-20 km) using just two phase screens.
- We have also found that conventional adaptive optics methods can be used to mitigate the influence of turlulence.

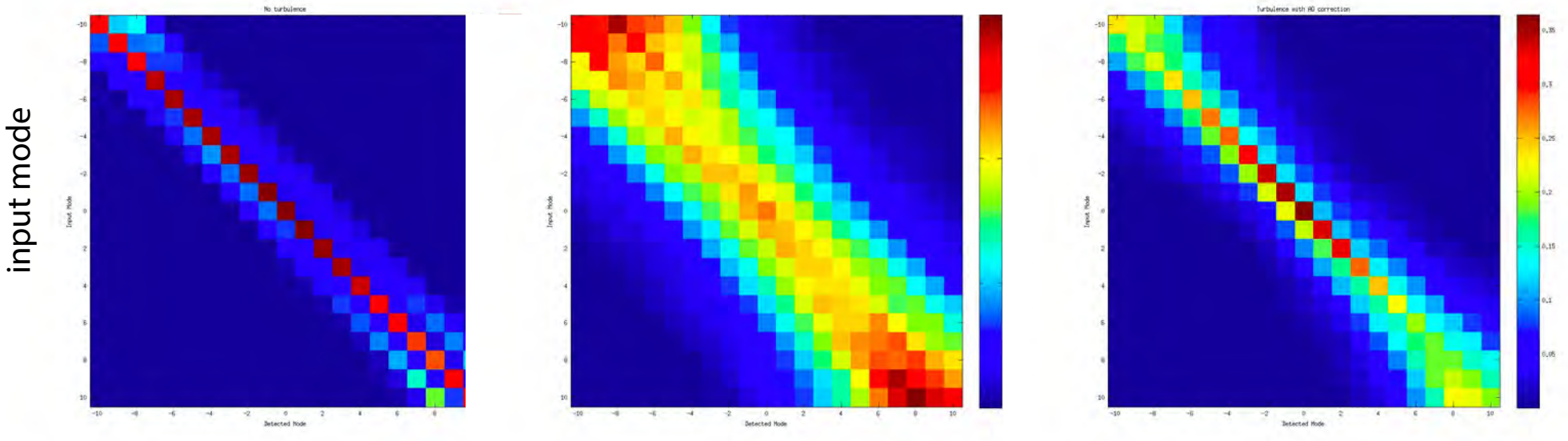
Improved QKD Performance Using Adaptive Optics

Before turbulence | After turbulence | After adaptive optics correction

- focal plane distribution



- OAM cross talk



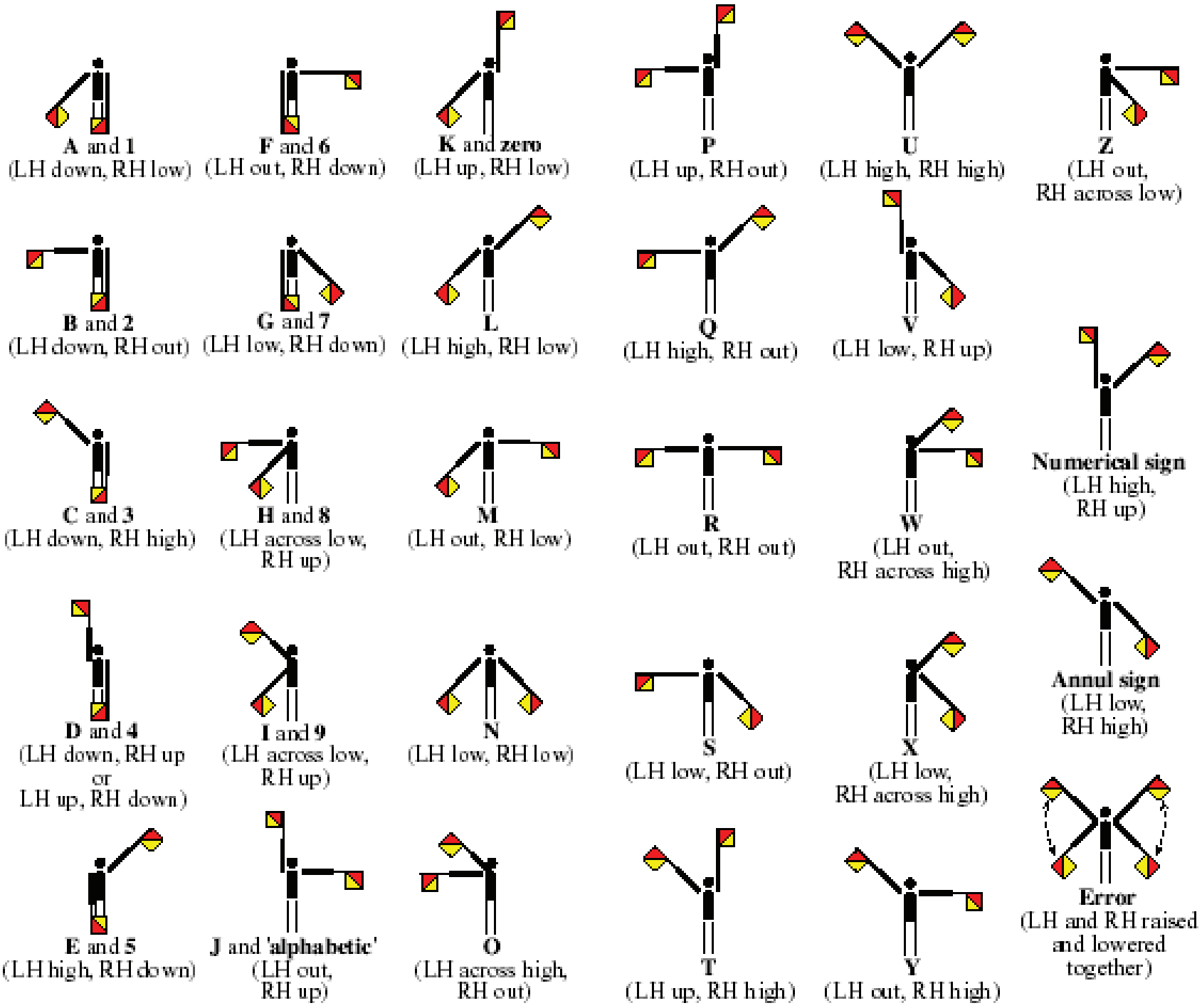
Malik et al., Optics Express 20, 13195 (2012); Rodenburg, et al., Optics Letters 17 3735 (2012).

Status of Effort: High Capacity Quantum Cryptography with More Than One Bit Per Photon

The early stages of this work were funded under a DARPA InPho Program that ended in 2012.

Work on mitigating atmospheric turbulence is being pursued currently as a joint project between University of Rochester and the Optical Sciences Company (Glenn Tyler) under an Air Force contract from Kirtland AFB (Pat Collier).

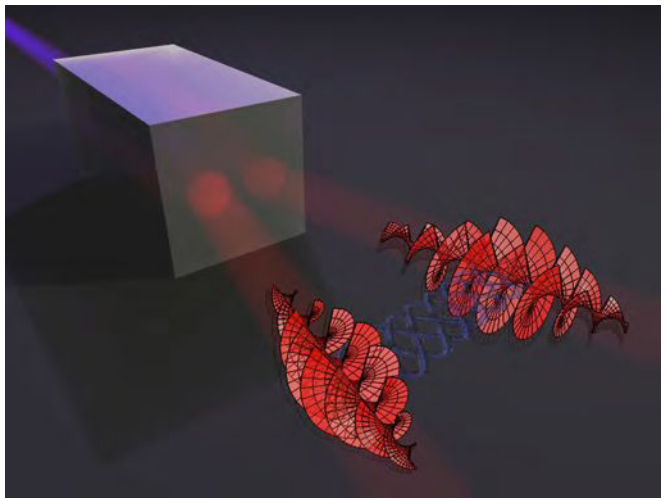
Free-Space Optical Telecommunication based on Transverse Field Structures



some additional work in quantum technologies

Nonlinear Optics, Quantum Imaging, and Quantum Information

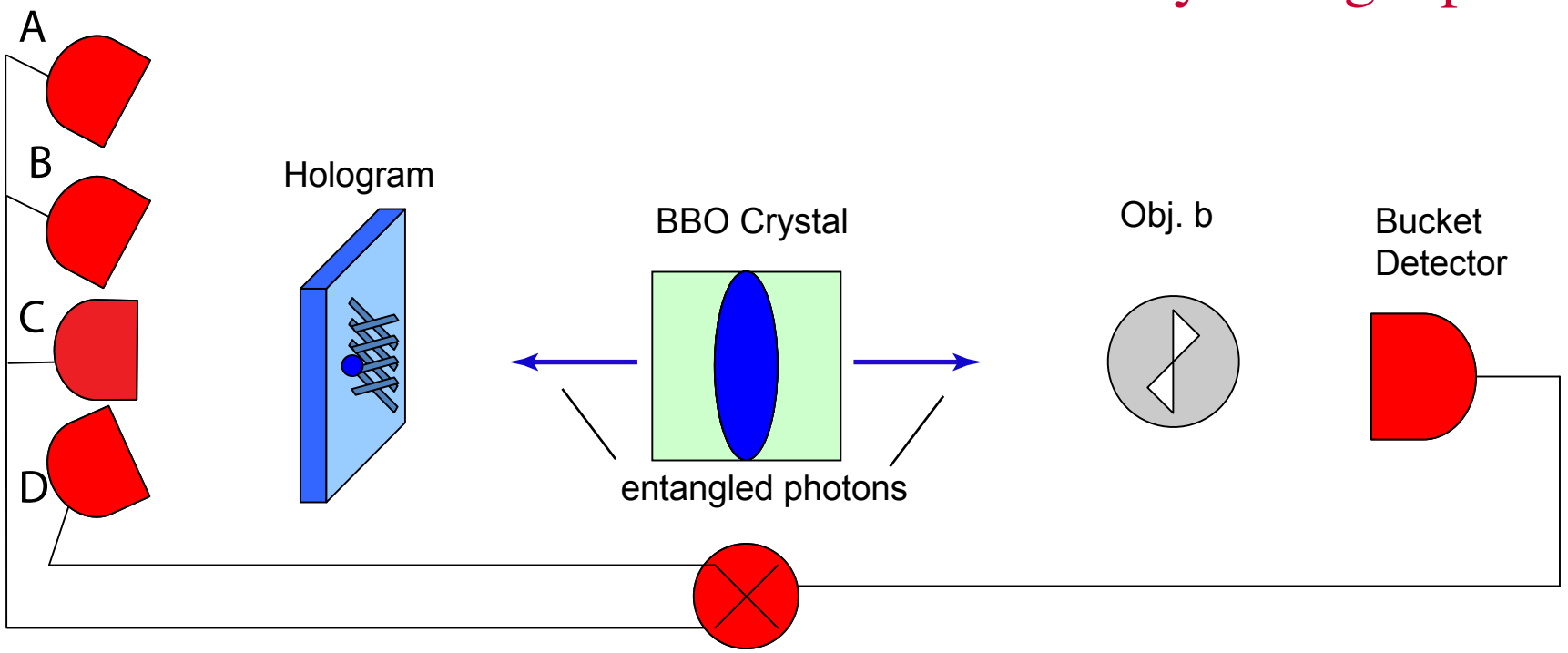
- Use nonlinear optics to create quantum states of light
- Some questions to be addressed
  - Can methods of quantum information be used to perform imaging with higher resolution or sensitivity?
  - How much information can be carried by a single photon?
  - Can we build a QKD system that reliably carries more than one but of information per photon?



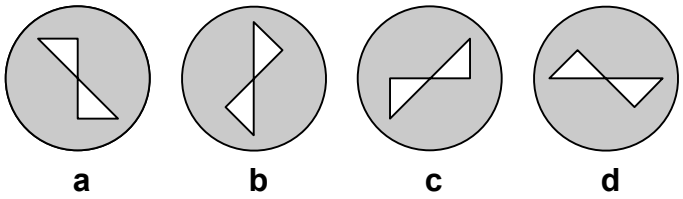
Quantum Correlations in Optical Angle-Orbital Angular Momentum Variables, Leach et al., Science 329, 662 (2010).

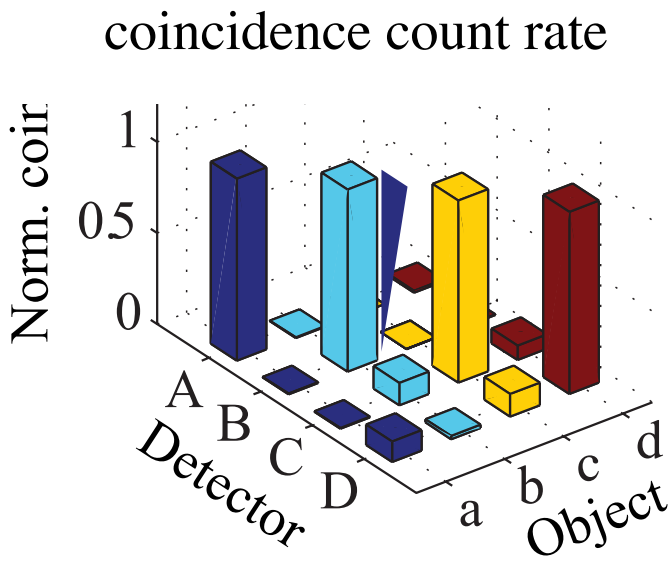
Single-Photon Coincidence Imaging

How much information can be carried by a single photon?



We discriminate among four orthogonal images using single-photon interrogation in a coincidence imaging configuration.



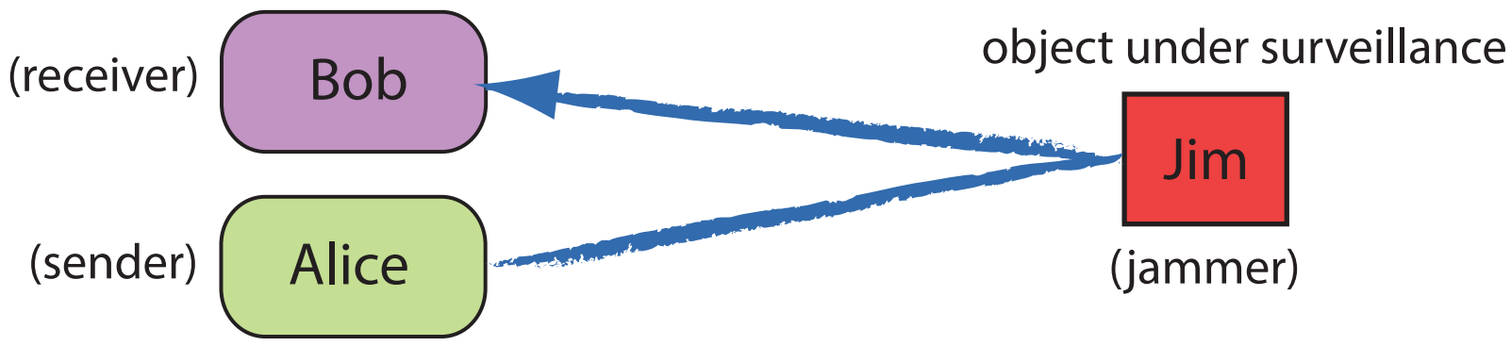


Malik, Shin, O'Sullivan. Zerom, and Boyd, Phys. Rev. Lett. 104, 163602 (2010).

QUANTUM-SECURED SURVEILLANCE

- How do we know that what we are looking at is "real"?
- We use quantum methods to identify "spoofing" by means of an intercept-resend attack
- Conventional quantum communications

- Quantum surveillance



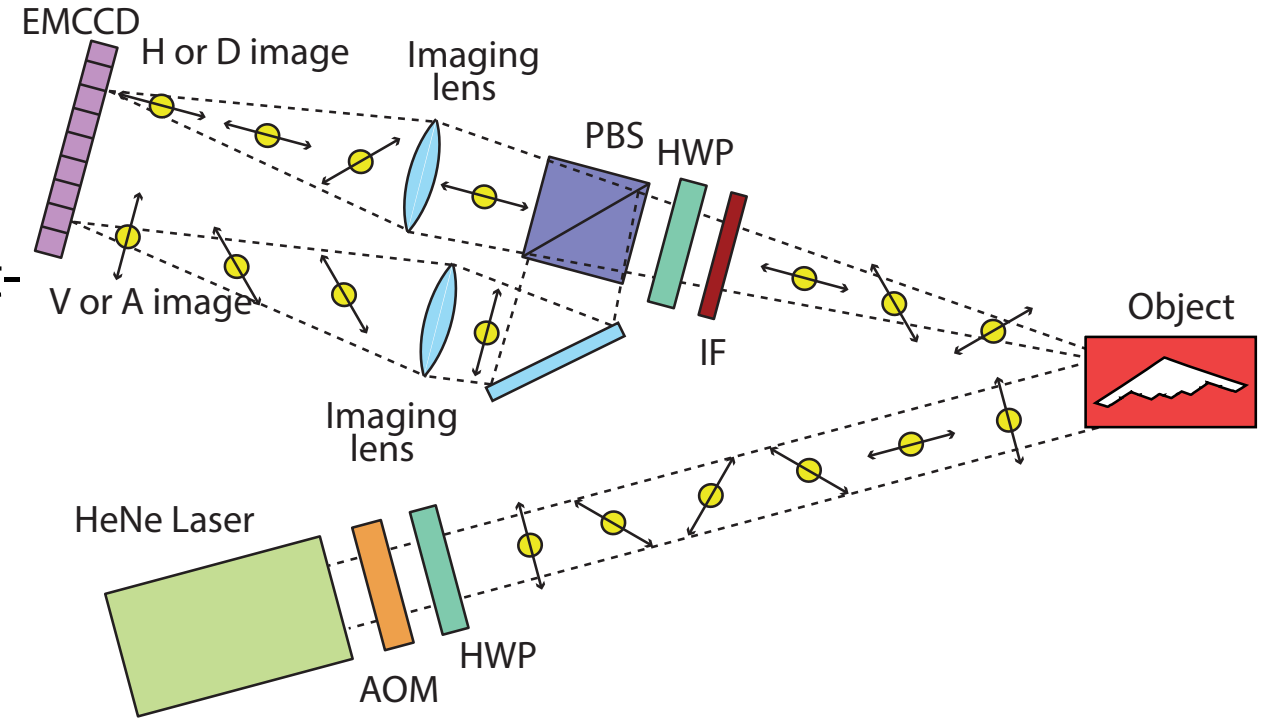
- Photon <u>polarization</u> used for security, photon <u>position and time</u> for surveillance

Malik et. al., APL 101, 241103 (2012)

Secure Quantum Surveillance

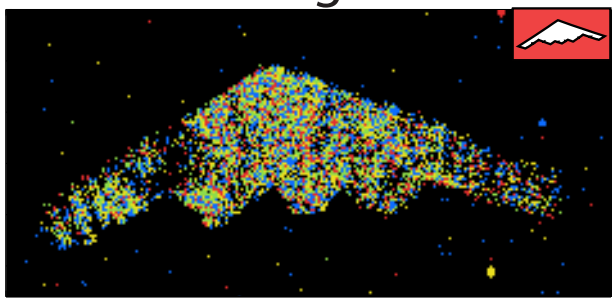
How do we know that what we are looking at is "real"?

- Our procedure provides security against an intercept-resend attack.



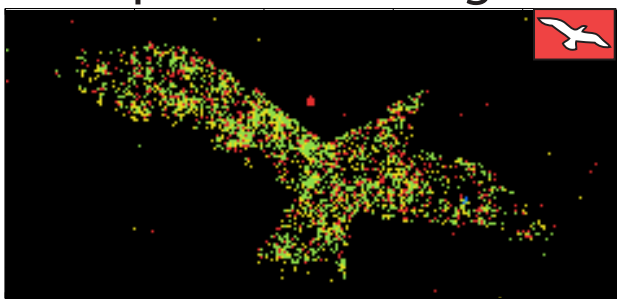
- Results

Secure Image



Total average error = 0.84 % < 25 %
(protocol secure)

Compromised Image



Total average error = 50.44 % > 25 %
(protocol compromised)

Quantum-Secured Imaging, M. Malik, O.S. Magaña-Loaiza, and R.W. Boyd, Appl. Phys. Lett. 101, 241103 (2012).

http://www.technologyreview.com/view/508826/quantum-imaging-technique-heralds-unjammable-aircraft-detection/
http://www.businessinsider.com/quantum-imaging-university-of-rochester-radar-stealth-f-35-fifth-generation-2012-12

MIT Technology Review

Quantum Imaging Technique Heralds Unjammable Aircraft Detection

NewScientist Physics & Math

Warning, speedsters: you can't fool quantum radar

Mail Online Science & Tech

The 'unjammable' quantum radar that could render ALL stealth planes useless

КОМПЬЮЛЕНТА

Квантовая механика как средство радиоэлектронной борьбы

BUSINESS INSIDER

New Imaging System Could Make America's Stealth Technology Obsolete

Robert Johnson | Dec. 18, 2012, 10:33 AM | 17,462 |

The stealth technology of America's fifth-generation jet fighters, the F-22 and the F-35, could be obsolete after a new discovery.

One main goal of fifth-generation aircrafts is to slip through skies over enemy lines without being targeted. It's not invisible, but elusive, and digitally feisty.

The F-35's lineup of electronic tools, work toward that end, by using a variety of sophisticated and devastating radar

This won't be good news to Lockheed Martin and F-35 proponents. It's no secret the F-35 has been hit by its share of problems and cost overruns. Canada just announced its plans to consider other aircraft replace an aging fleet and Australia's delayed their F-35 order so often that delivery Down Under is as distant as it is obscure.

If stealth becomes no longer possible, then a major selling point of the troubled F-35 project will become an expensive waste.

New Journal of Physics
The open access journal for physics

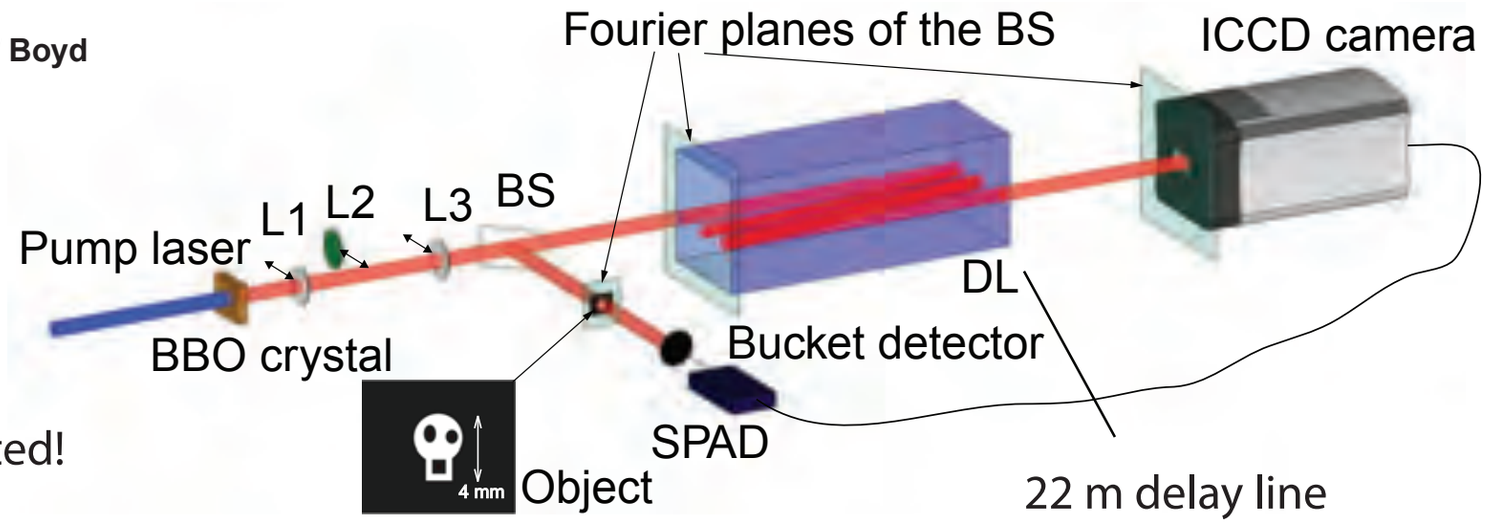
EPR-based ghost imaging using a single-photon-sensitive camera

Reuben S Aspden, Daniel S Tasca , Robert W Boyd and Miles J Padgett

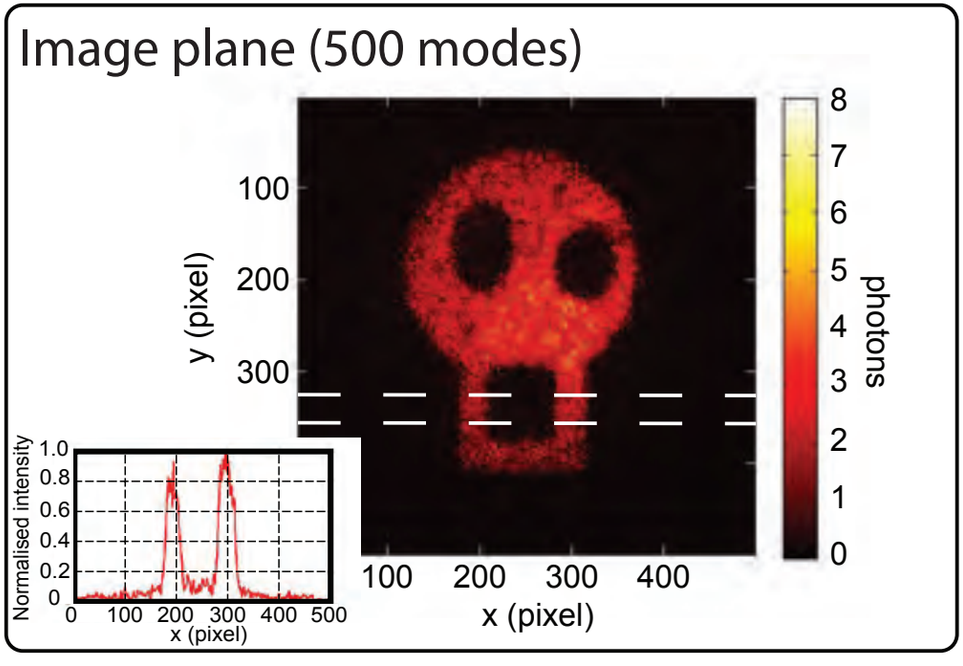
New Journal of Physics **15** (2013) 073032 (11pp)

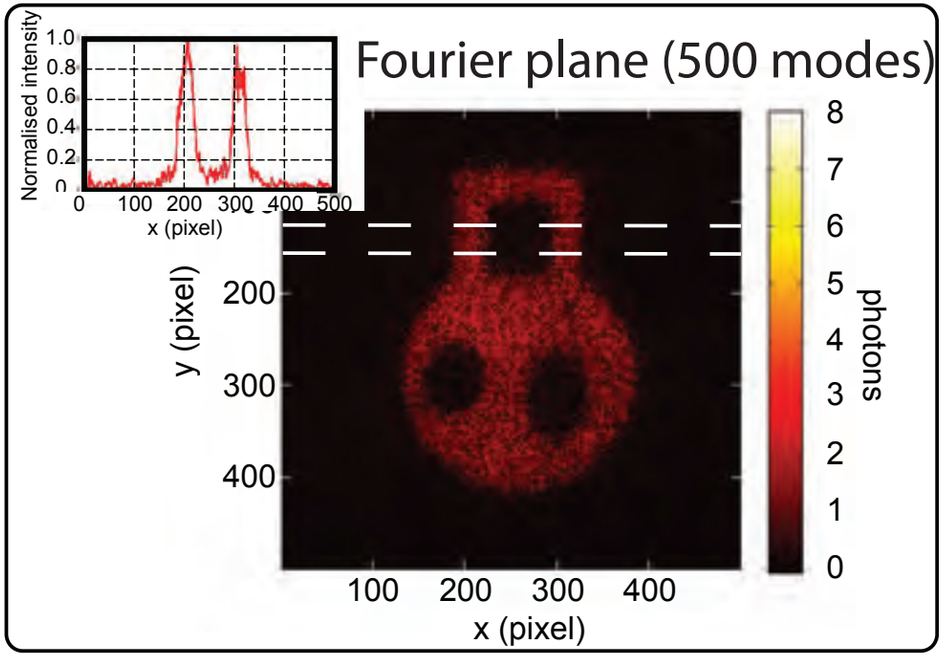
Essentially "ideal" cameras now are available!

When time gated, essentially all background noise is eliminated!



Edgar M P, Tasca D S, Izdebski F, Warburton R E, Leach J, Agnew M, Buller G S, Boyd R W and Padgett M J 2012 Imaging high-dimensional spatial entanglement with a camera Nature Commun. 3 984





Thank you for your attention!