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 at the Rochester Astronomy Club Meeting, April 3 2015.

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

Slowing Down the Speed of Light

Robert W. Boyd

The Institute of Optics
and Department of Physics and Astronomy
University of Rochester, Rochester, NY 14627
http://www.optics.rochester.edu

Presented at the Rochester Astronomy Club, April 2, 2004.

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 at the Rochester Astronomy Club Meeting, April 3 2015.

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

Research in Quantum Photonics

Robert Boyd

Canada Excellence Research Chair in Quantum Nonlinear Optics

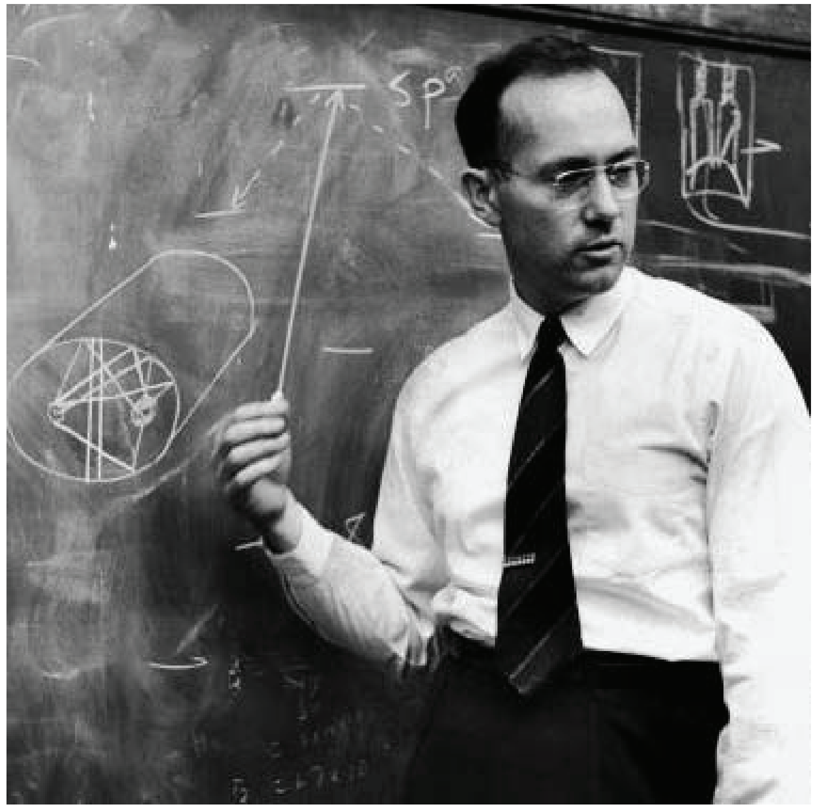
University of Ottawa

Our research interests include:

- Nanophotonics
- Plasmonics
- Photonic crystals
- Photonic device
- Applications of slow and fast light
- Quantum nonlinear optics
- Optical methods for quantum information
- Biophotonics
- Nonlinear optics of atomic vapors
- Optical chirality and structure surfaces

Charles H. Townes

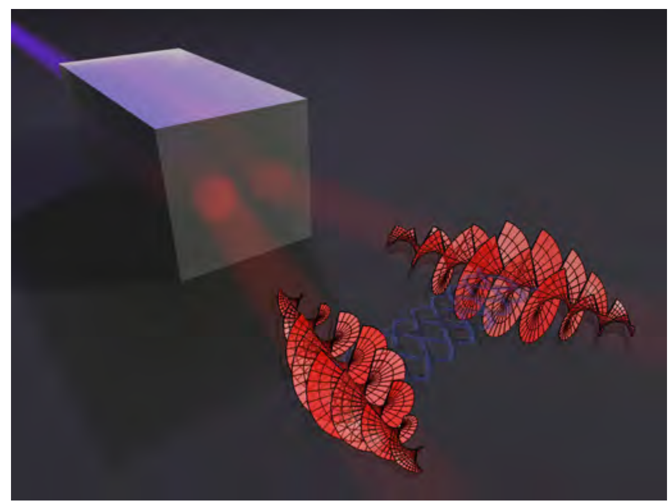
July 28, 1915 to January 27, 2015



- Inventor of the maser and laser
- Nobel Prize, 1964
- Advisor to three US presidents
- Teacher, mentor, and friend

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.

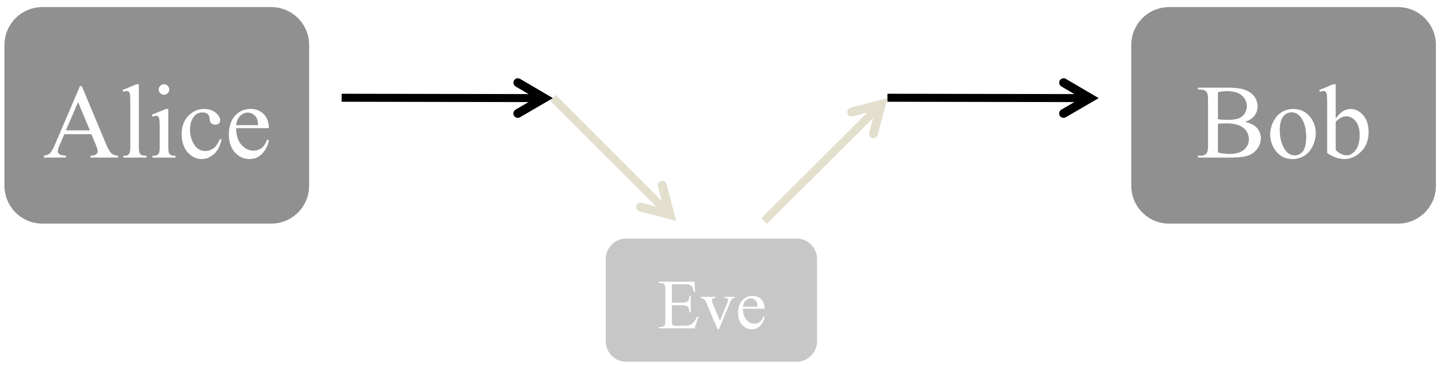


OAM States and Quantum Key Distribution

- The most widely studied protocol is that of Bennett and Brassard (1984), known as the BB84 protocol. It makes use of measurements performed on a single photon, but in more than one set of bases.
- Our work involves an extension of the BB84 protocol by making use of the OAM states of light. One motivation is to increase the data transfer rate by impressing more than one bit per photon.
- Let us begin by reviewing the BB84 protocol.

Secure Communication Using a One-Time Pad

Alice wants to communicate a message to Bob in such a way that no information about the message is leaked to a third party (Eve).



One-Time Pad

Message	A		S	E	C	U	R	E		M	E	S	S	A	G	E
Key	D	Q	Y			G	D	H	X	Z	B	V	S	J	U	E
!"#$%"!"																
Cipher	D	P	P	D	B		U	L	W	K	F	M	J	J		I

completely random

Note that Alice and Bob must share a completely random key unknown to anyone else.

Preparing a Shared One-Time Pad

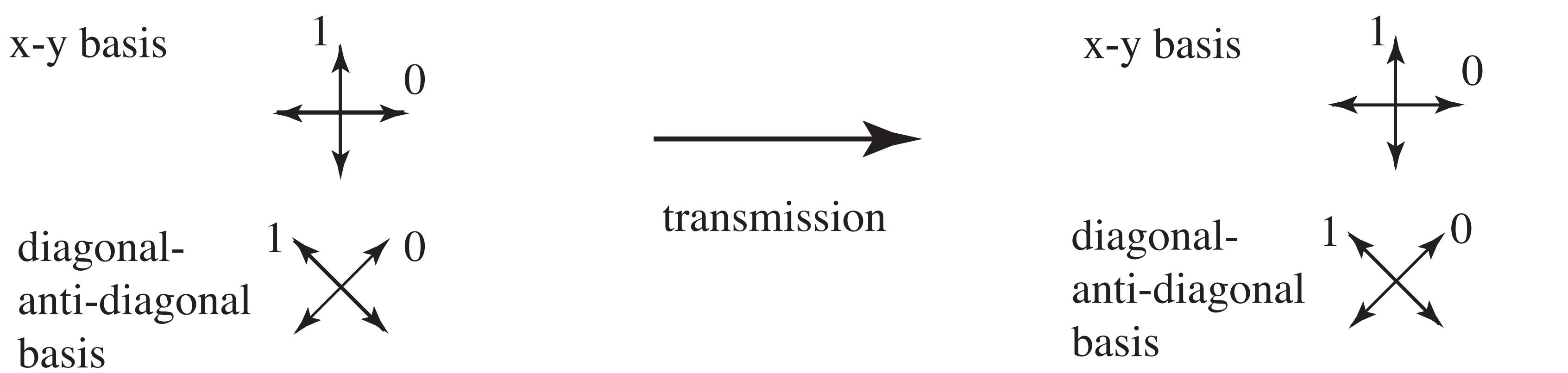
Possible Strategies

- Alice and Bob meet in private and generate a shared string of random numbers
- Alice and Bob have a trusted courier carry the pad from Alice to Bob
- Alice transmits the code to Bob in an entirely secure manner. Security is imposed by the laws of quantum mechanics.
  - This method is known as quantum key distribution (QKD).

The BB84 QKD Protocol – Polarized Light Implementation

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

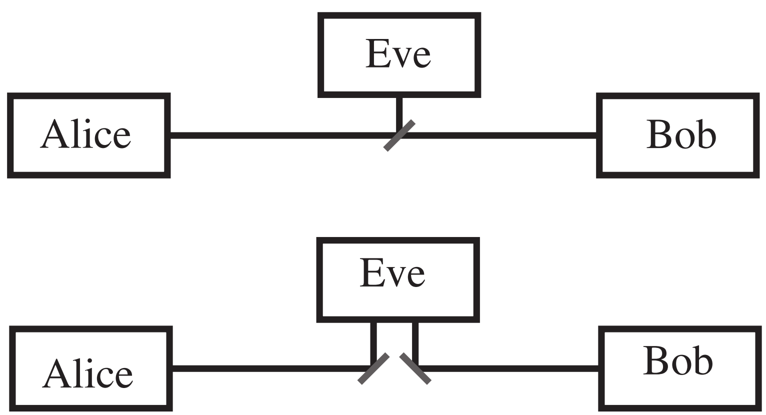
Bob receives in one of two polarization bases, which he choses at random



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.



Quantum Key Distribution

0: $|\updownarrow\rangle$ or $|\nwsearrow\rangle$

1: $|\leftrightarrow\rangle$ or $|\neswarrow\rangle$

Alice			Bob		
Value	Polarizer Setting		Polarizer Setting		Value
0	~~±45~~	$|\nwsearrow\rangle$	~~H/V~~	$|\leftrightarrow\rangle$	1
1	±45	$|\neswarrow\rangle$	±45	$|\neswarrow\rangle$	1
0	H/V	$|\updownarrow\rangle$	H/V	$|\updownarrow\rangle$	0
0	~~H/V~~	$|\updownarrow\rangle$	~~±45~~	$|\nwsearrow\rangle$	0
1	±45	$|\neswarrow\rangle$	±45	$|\neswarrow\rangle$	1

Sifted Key: 101 …

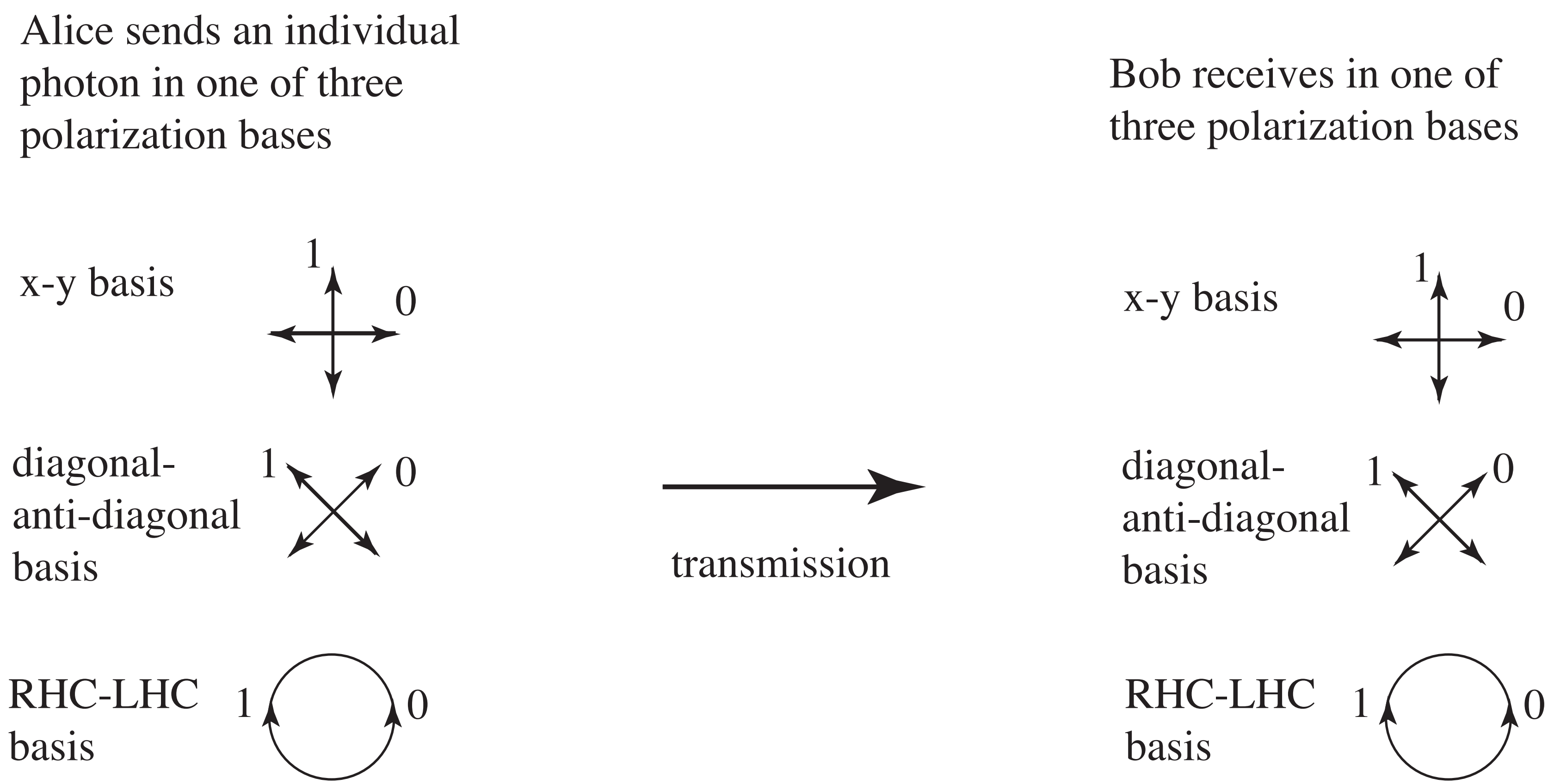
Review of the BB84 Protocol*

Table 2.1. Example of a polarisation protocol. Alice chooses at random a basis ($\oplus$ or $\otimes$) and a bit value (0 or 1), and sends the corresponding polarisation state to Bob. Bob chooses also at random the reception basis, and obtains a given bit. The ensemble of these bits is the raw key. Alice and Bob then tell each other the basis used over the public channel, and keep only the bits corresponding to the same basis. This is the sifted key. They choose at random some of the remaining bits to test for Eve, then discard them. In this case, there are no errors, which indicates that the transmission is secure. The remaining bits form the shared key.

A basis	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$
A bit value	0	1	0	1	1	0	1	0	0	0	0
A sends	|⤢⟩	$\|\leftrightarrow\rangle$	$\|\updownarrow\rangle$	|⤡⟩	$\|\leftrightarrow\rangle$	|⤢⟩	|⤡⟩	$\|\updownarrow\rangle$	|⤢⟩	|⤢⟩	$\|\updownarrow\rangle$
B basis	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\otimes$	$\oplus$	$\oplus$	$\oplus$
B bit	0	1	0	0	1	0	1	1	0	1	0
Same basis?	y	y	n	n	y	y	y	n	n	n	y
A keeps	0	1			1	0	1				0
B keeps	0	1			1	0	1				0
Test Eve?	y	n			y	n	n				n
Key		1				0	1				0

*Dirk Bouwmeester, Artur Ekert and Anton Zeilinger, Eds. **The Physics of Quantum Information**, Springer-Verlag Berlin Heidelberg New York 2000 ISBN 3-540-66778-4 Section 2.3 Quantum Key Distribution with Single Particles pp27-31.

The BB84 QKD Protocol –With Three Bases



- Note that polarization constitutes a two-state system.
- There are three mutually unbiased (MUB) bases for a two-state system.
- Security is increased but data rate is decreased by using all three MUBs.

Quantum Key Distribution

The key should be …

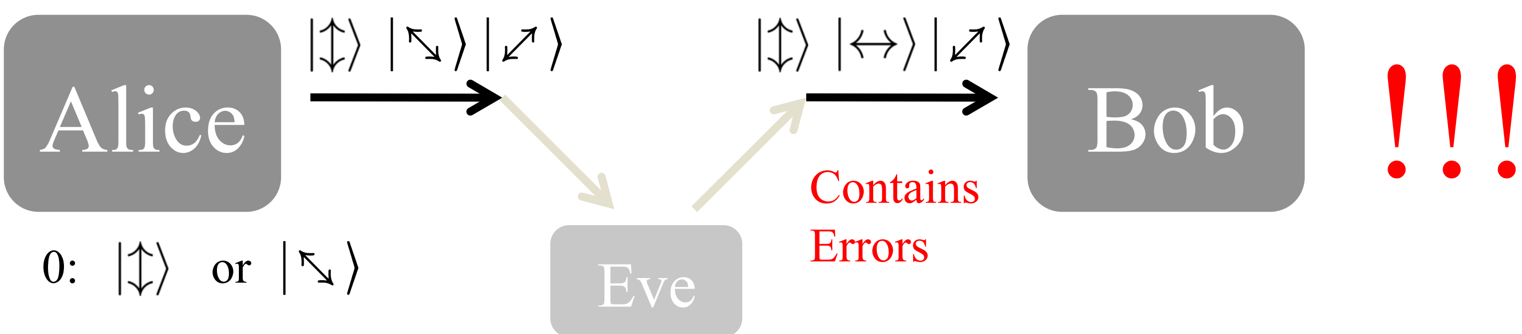
1. Completely random
2. At least as long as the message
3. Known only to Alice and Bob

How?

QKD cannot circumvent eavesdropping but only detect its presence

Idea: Encode information using non-orthogonal quantum states

Wooters and Zurek 1982: non-orthogonal quantum states cannot be copied without errors



0: $|\updownarrow\rangle$ or $|\nwarrow\!\!\!\!\searrow\rangle$

1: $|\leftrightarrow\rangle$ or $|\swarrow\!\!\!\!\nearrow\rangle$

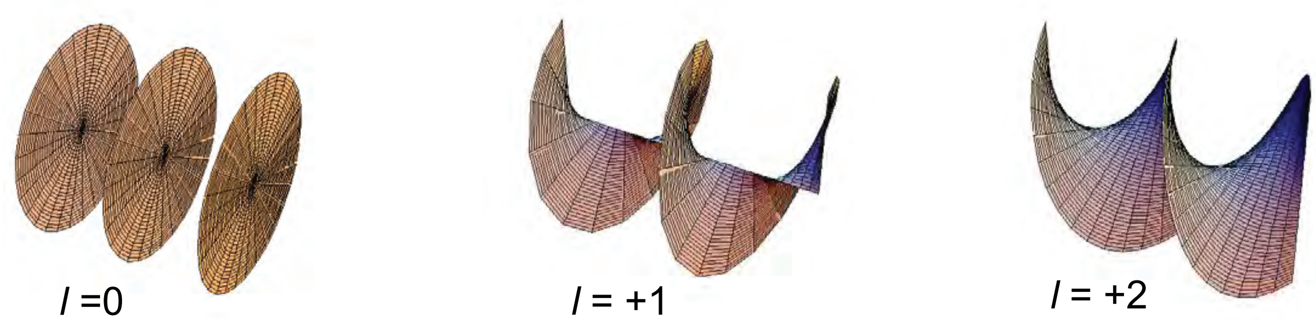
Our Research: BB84 in a High-Dimensional State Space

- 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

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

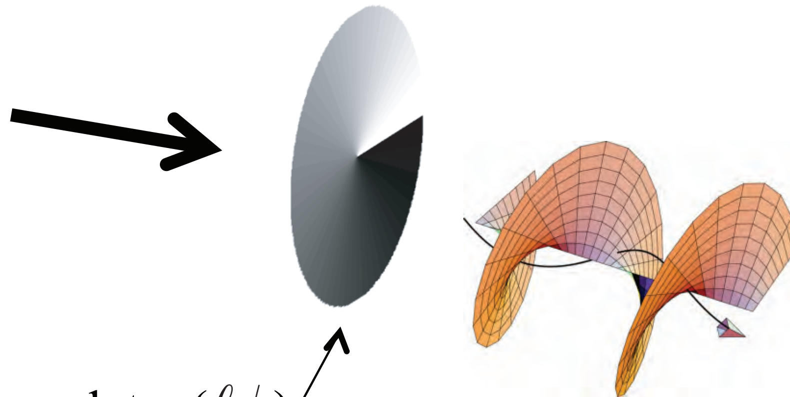
The paraxial wave equation is satisfied by the Laguerre-Gaussian modes, a family of orthogonal modes that have a well defined orbital angular momentum. The field amplitude $LG_p^l(\rho, \phi, z)$ of a normalized Laguerre-Gaussian modes is given by

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

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?

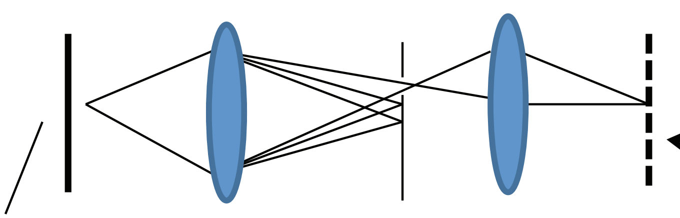
Pass beam through a spiral phase plate



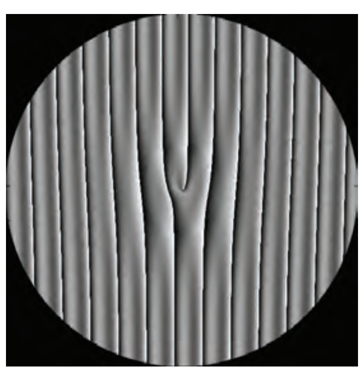
$e^{i\ell\phi}$

Spiral phase plate $(\ell\phi)$

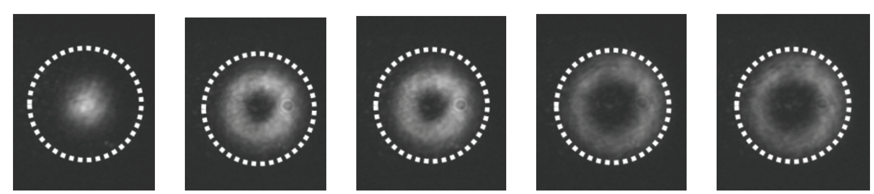
Use a spatial light modulator acting as a computer generated hologram (more versatile)



LG



Laguerre-Gauss



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).

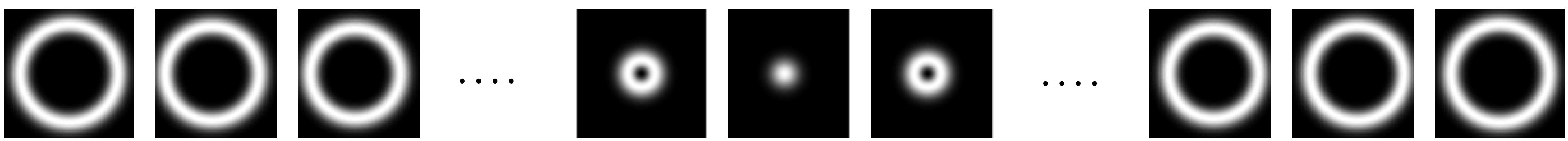
High Capacity QKD Protocol

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).

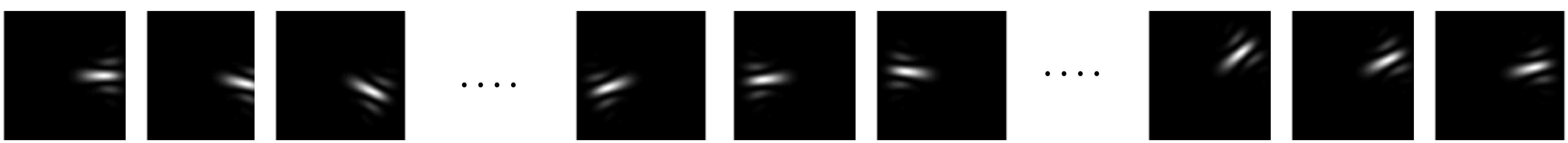
We are developing means to mitigate the influence of atmospheric turbulence

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



0 1 2 12 13 14 25 26 27

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

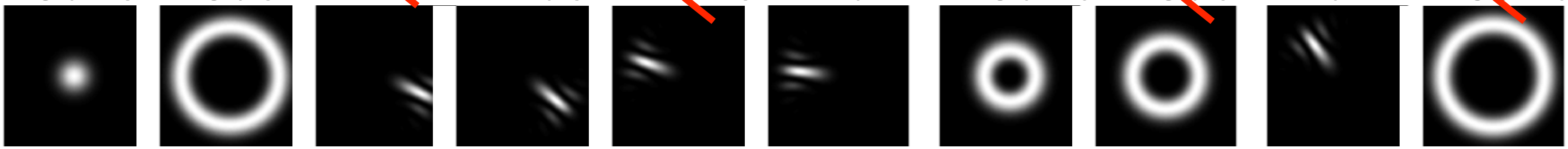


0 1 2 12 13 14 25 26 27

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

Protocol

Alice	LG:13	LG:3	~~AB:2~~	AB:3	~~AB:15~~	AB:14	LG:16	~~LG:8~~	AB:24	~~LG:26~~
Bob	LG	LG	~~LG~~	AB	~~LG~~	AB	LG	~~AB~~	AB	~~AB~~
Result	13	3	~~15~~	3	~~15~~	14	16	~~17~~	24	~~10~~



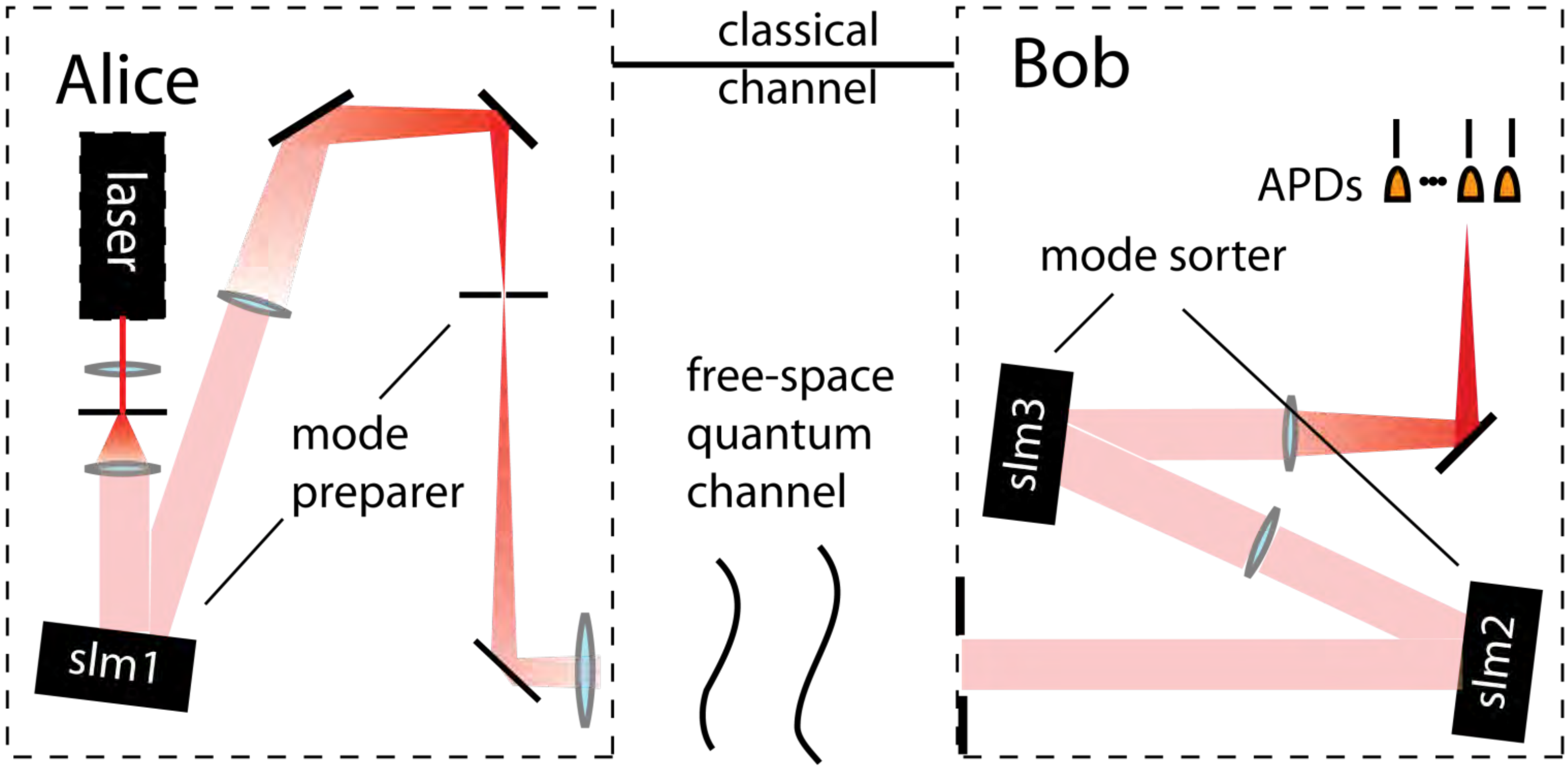
Sifted Key 13 3 3 14 16 24 … ← in principle contains no errors unless eavesdropper is present.

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

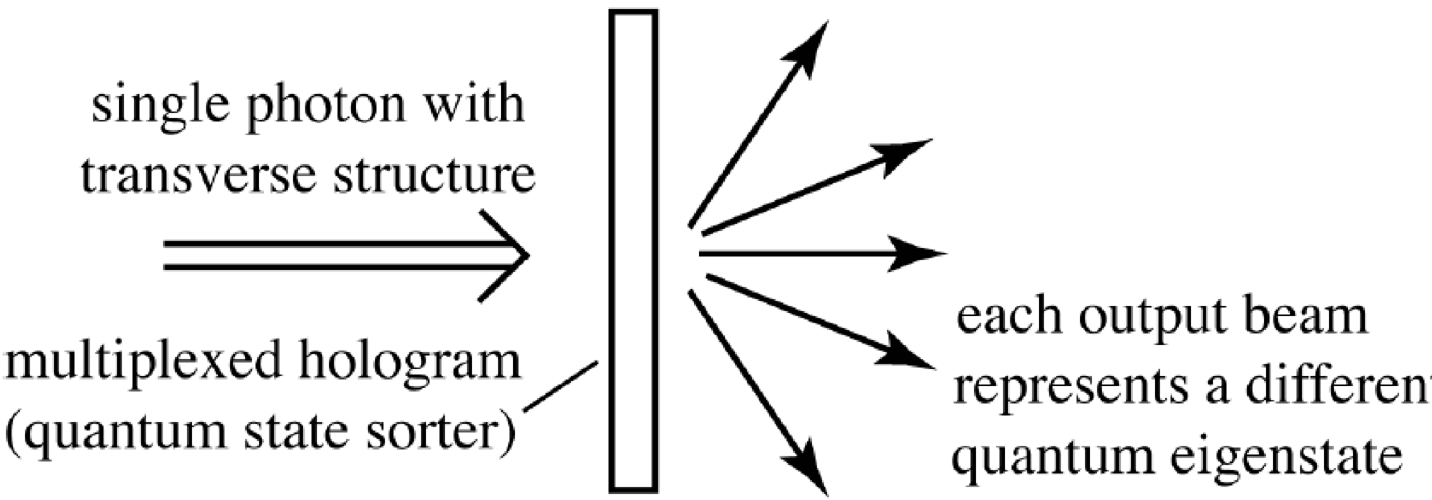
Modified BB84 as discussed

Challenges

1. State Preparation
2. State Detection
3. Turbulence

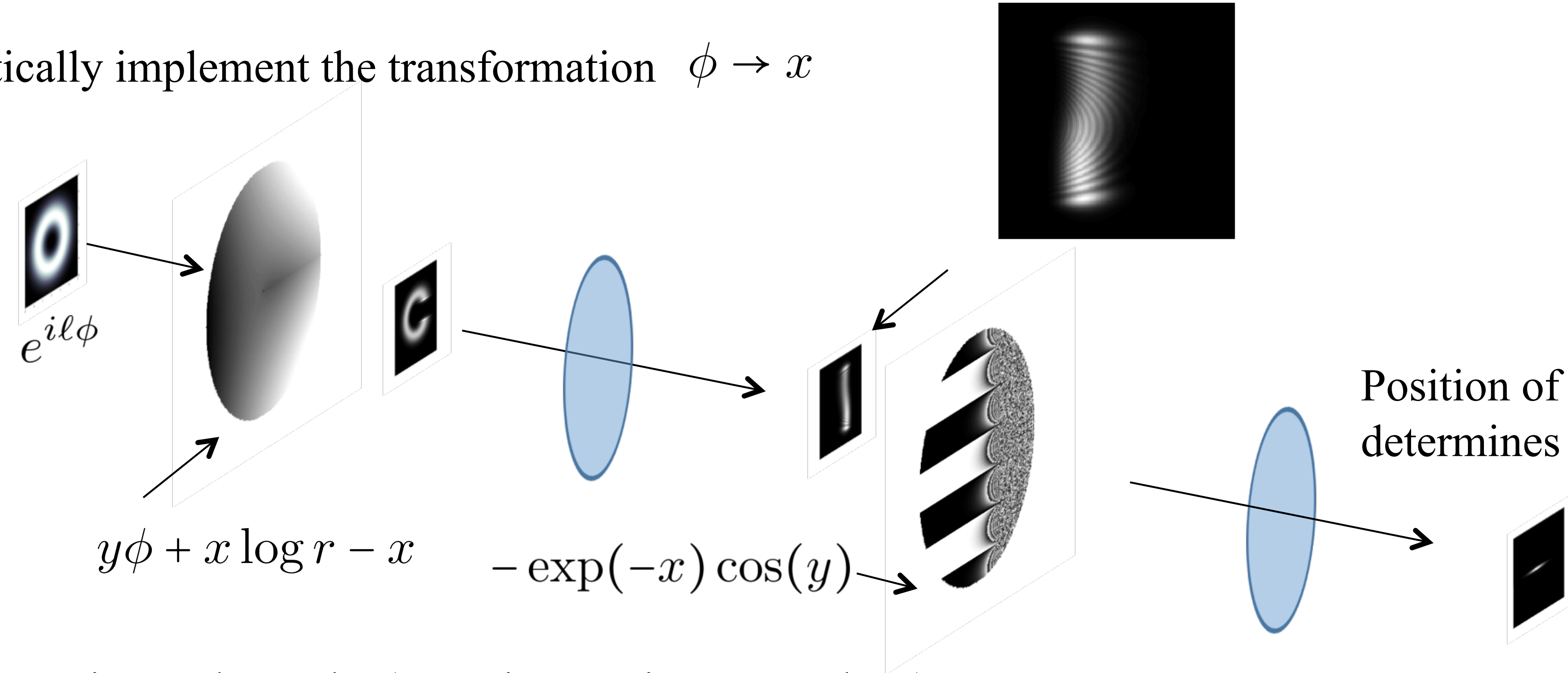
Mode Sorting

A mode sorter

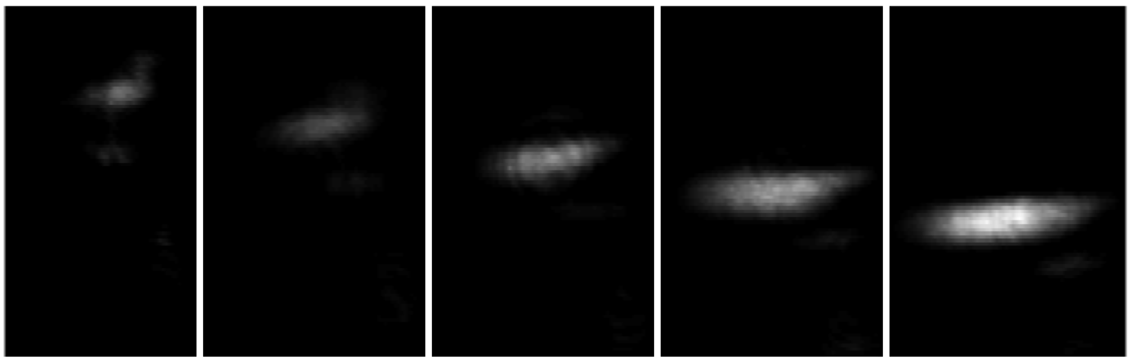


Sorting OAM using Phase Unwrapping

Optically implement the transformation $\phi \to x$



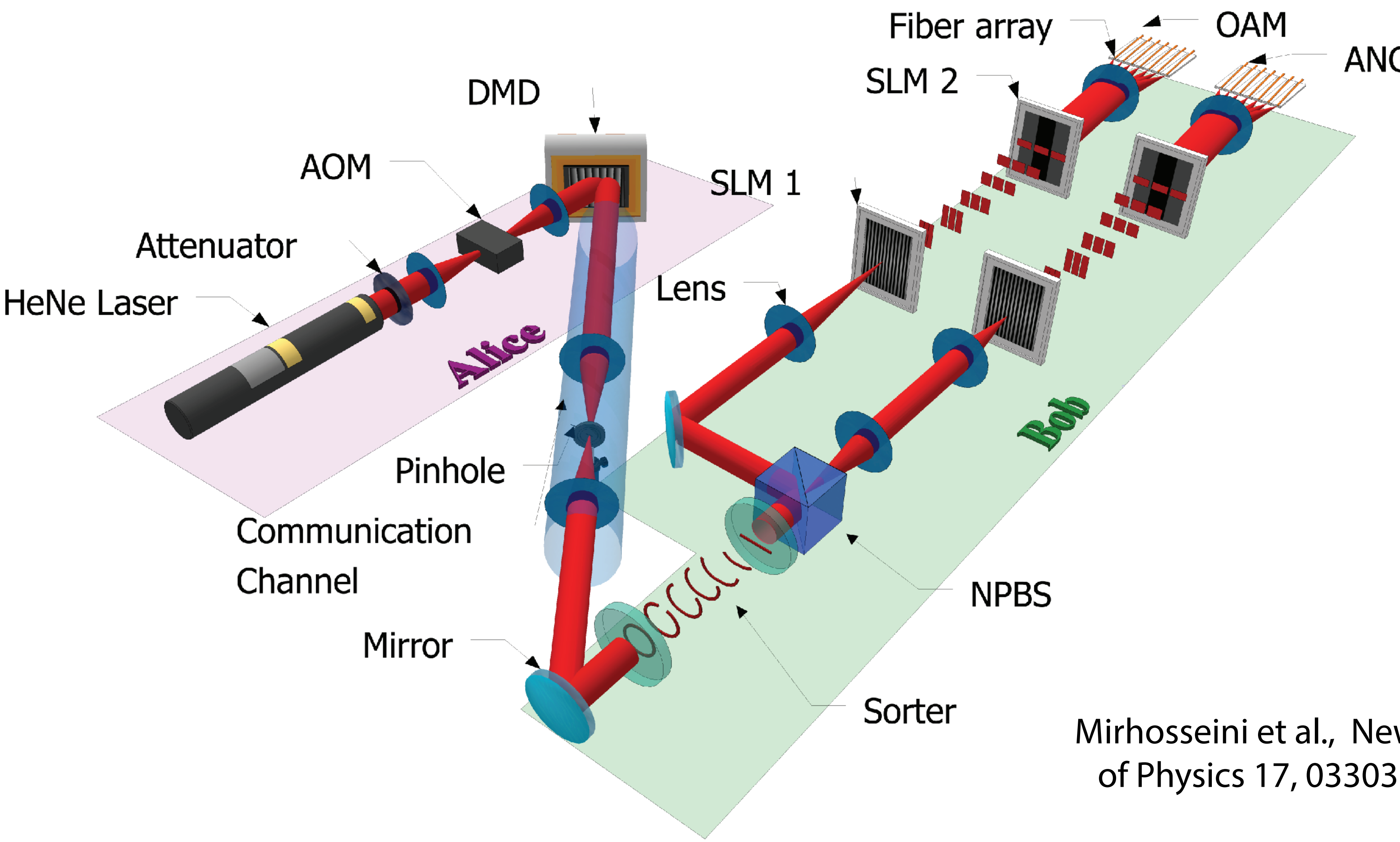
Experimental Results (CCD images in output plane)



- Can also sort angular position states.
- Limited by the overlap of neighboring states.

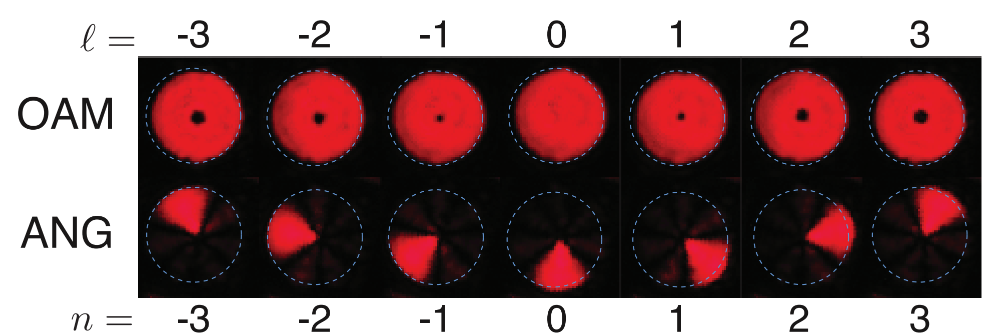
*Berkhout *et al.* *PRL* **105,** 153601 (2010).
O. Bryngdahl, *J. Opt. Soc. Am.* **64**, 1092 (1974).

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	Bob
063133602132045444456141026645 545050363603025261643215524164 230146602513401613222451551026	063033601132021444456141026645 545022353603025261643215524164 230146602515403613422451551026

Error Correction

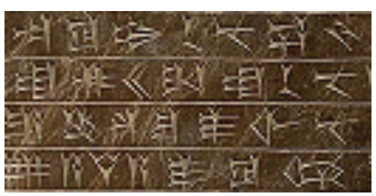
0000 0100 0111 0100 0101 0001 1100 0010 1100 1001 0010 0100 1101 0001 0000 0001 0011 0100 0000 0100 0010 0001 0001 0011 0000 0101 0010 0111 1000 0101 1101 0011 0001 1001 1011 0101 0000 0100 0111 0100 0011 0110 0101 0000 1101 0101 0010 1111 1010 1111 0010 1000

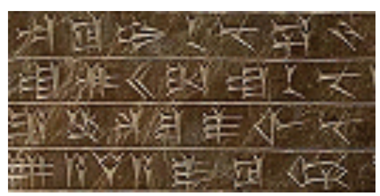
Privacy Amplification

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

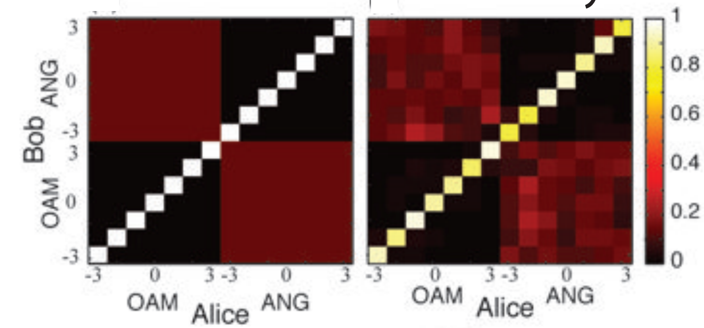
Alice Encrypts

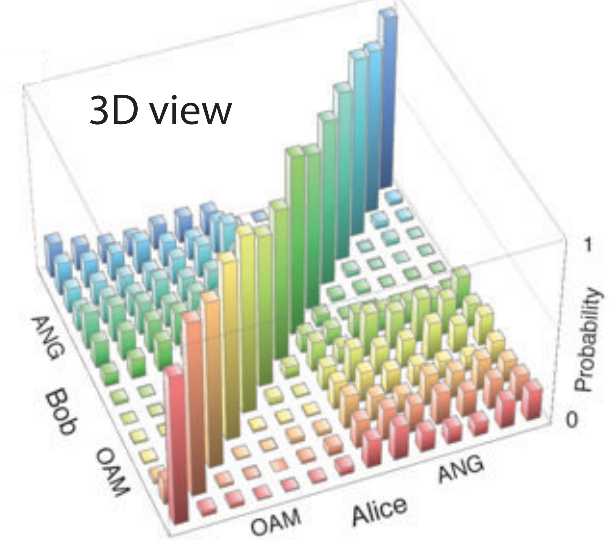
Bob Decrypts



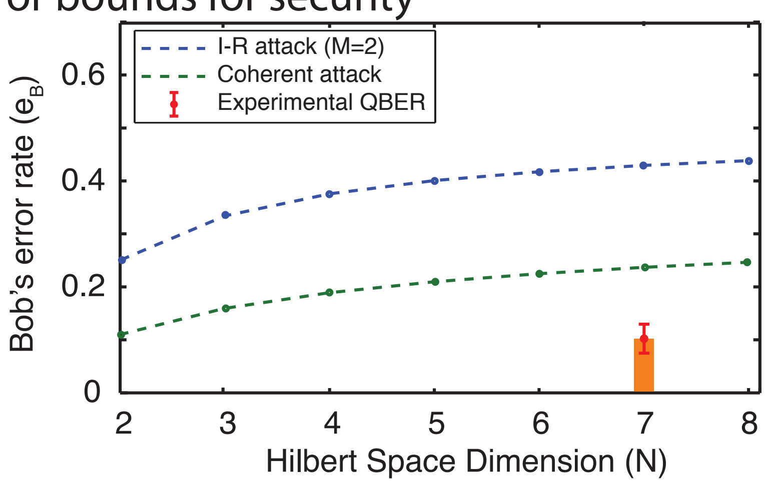


cross-talk matrices





- error bounds for security



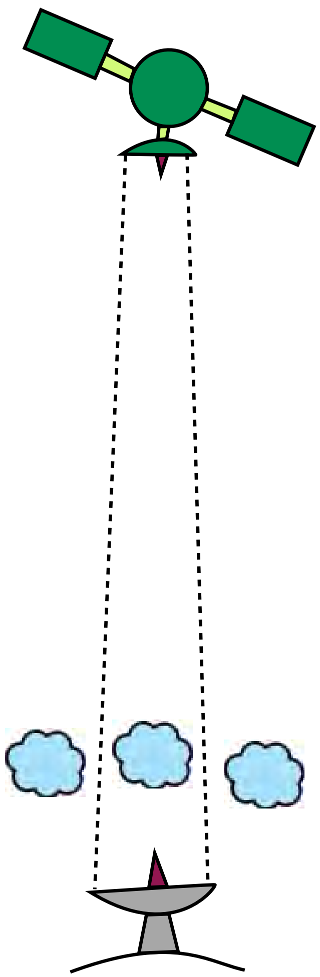
We use a 7-letter alphabet, and achieve a channel capacity of 2.1 bits per sifted photon.

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.

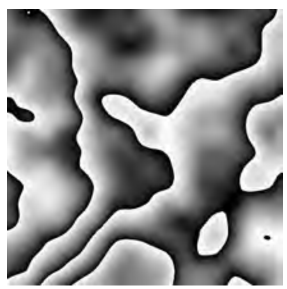
Nonetheless, our error rate is adequately low to provide full security,

Turbulence and Adaptive Optics

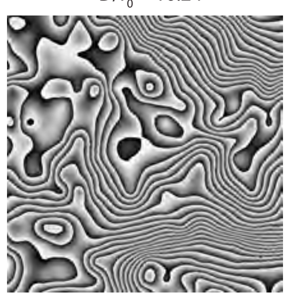
Atmospheric Turbulence Model



D/r_0 = 5.12

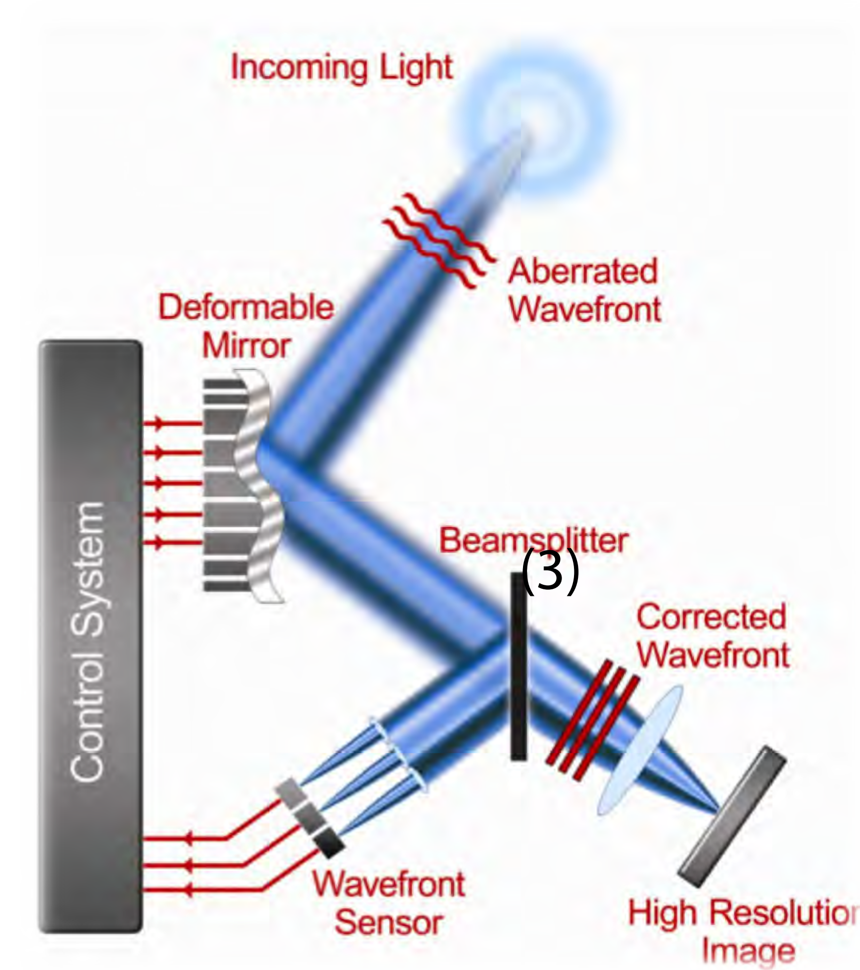


D/r_0 = 10.24

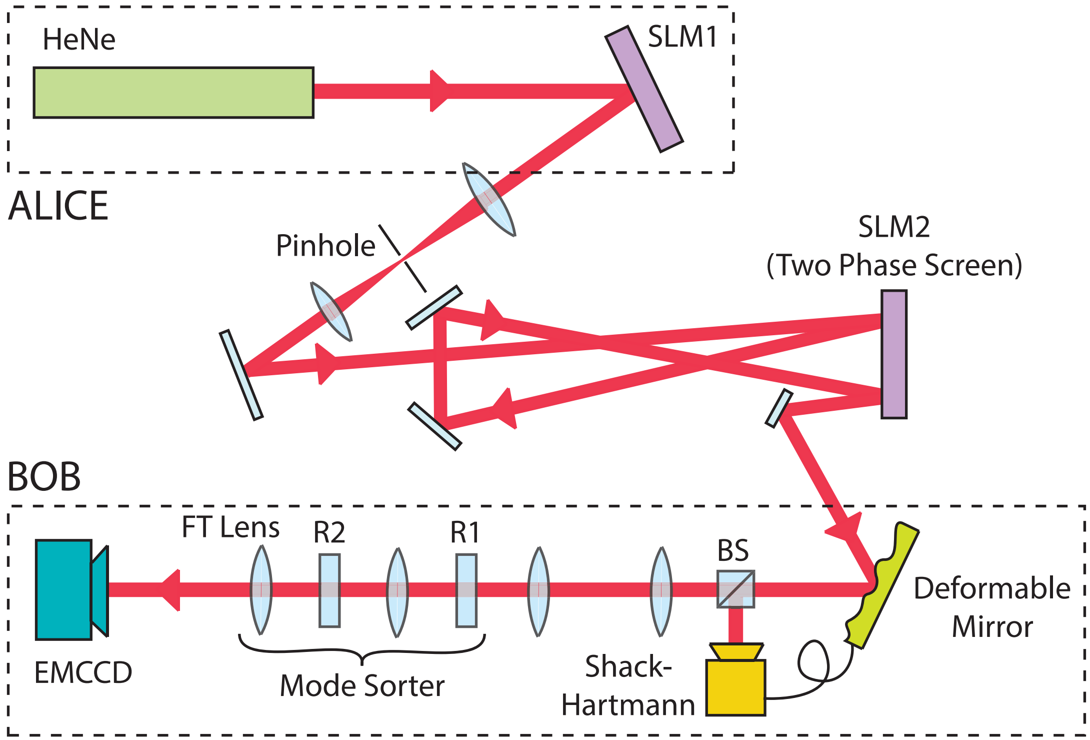


D/r_0 = 102.4

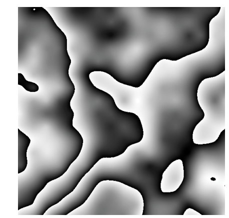
Our Adaptive Optics System

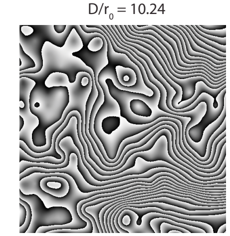


Turbulence and Adaptive Optics




$D/r_0 = 5.12$


$D/r_0 = 10.24$

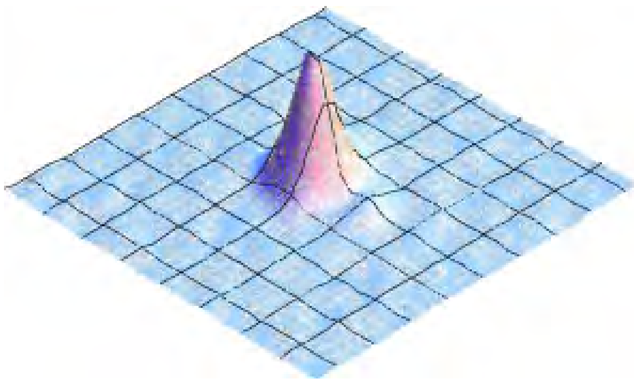

$D/r_0 = 102.4$

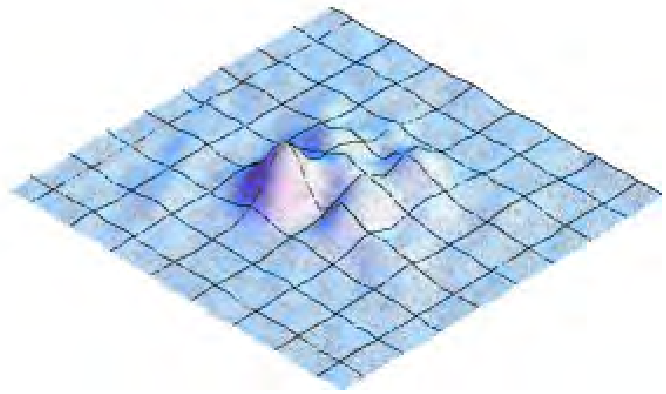
- We have found that we can adequately model thick hoizontal turlulence (10-20 km) using just two phase screens.
- We have also found that conventional adaptive optics methods can be used to mitigate the influence of turlulence.

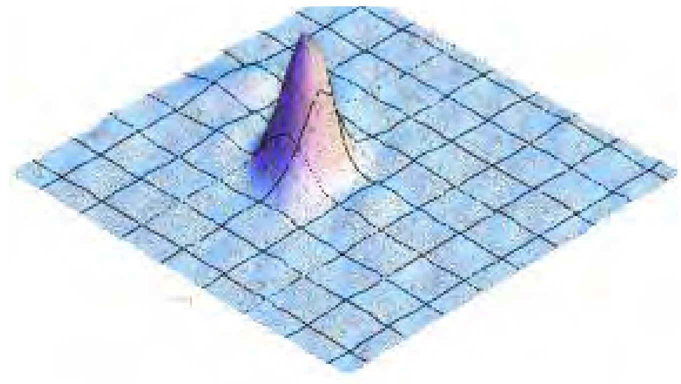
Improved QKD Performance Using Adaptive Optics

Before turbulence | After turbulence | After adaptive optics correction

- focal plane distribution

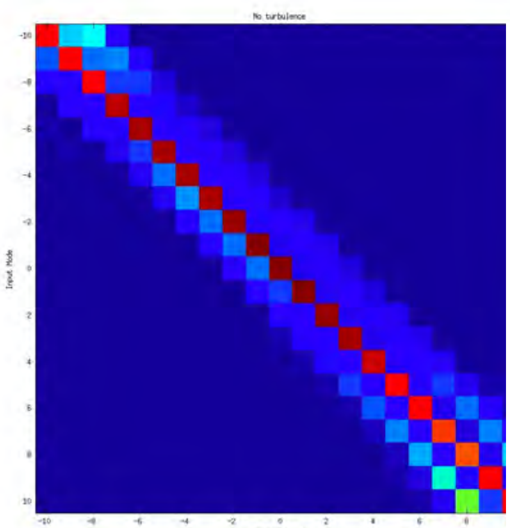




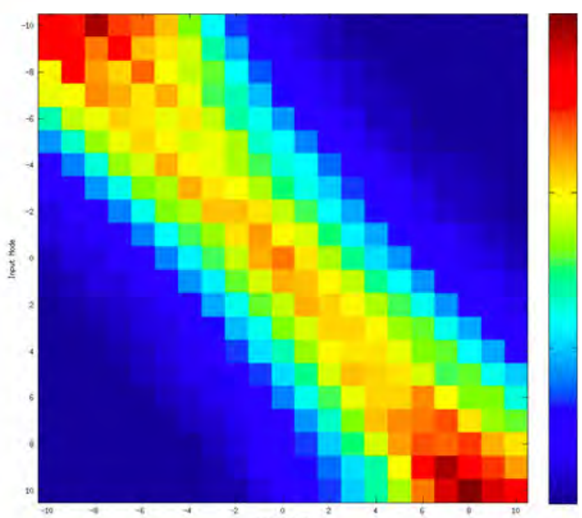


- OAM cross talk

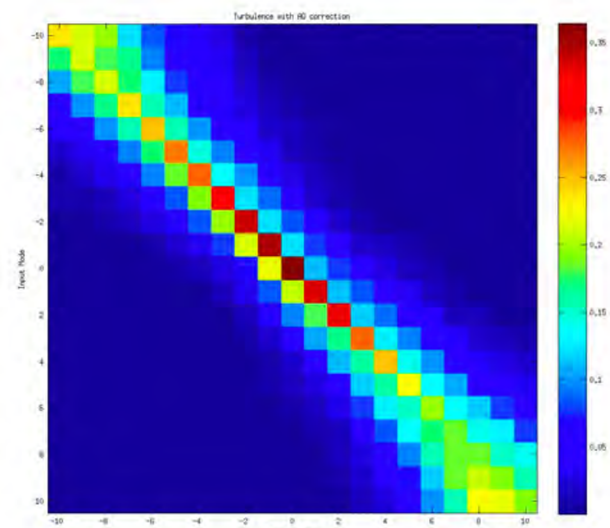
input mode



output mode



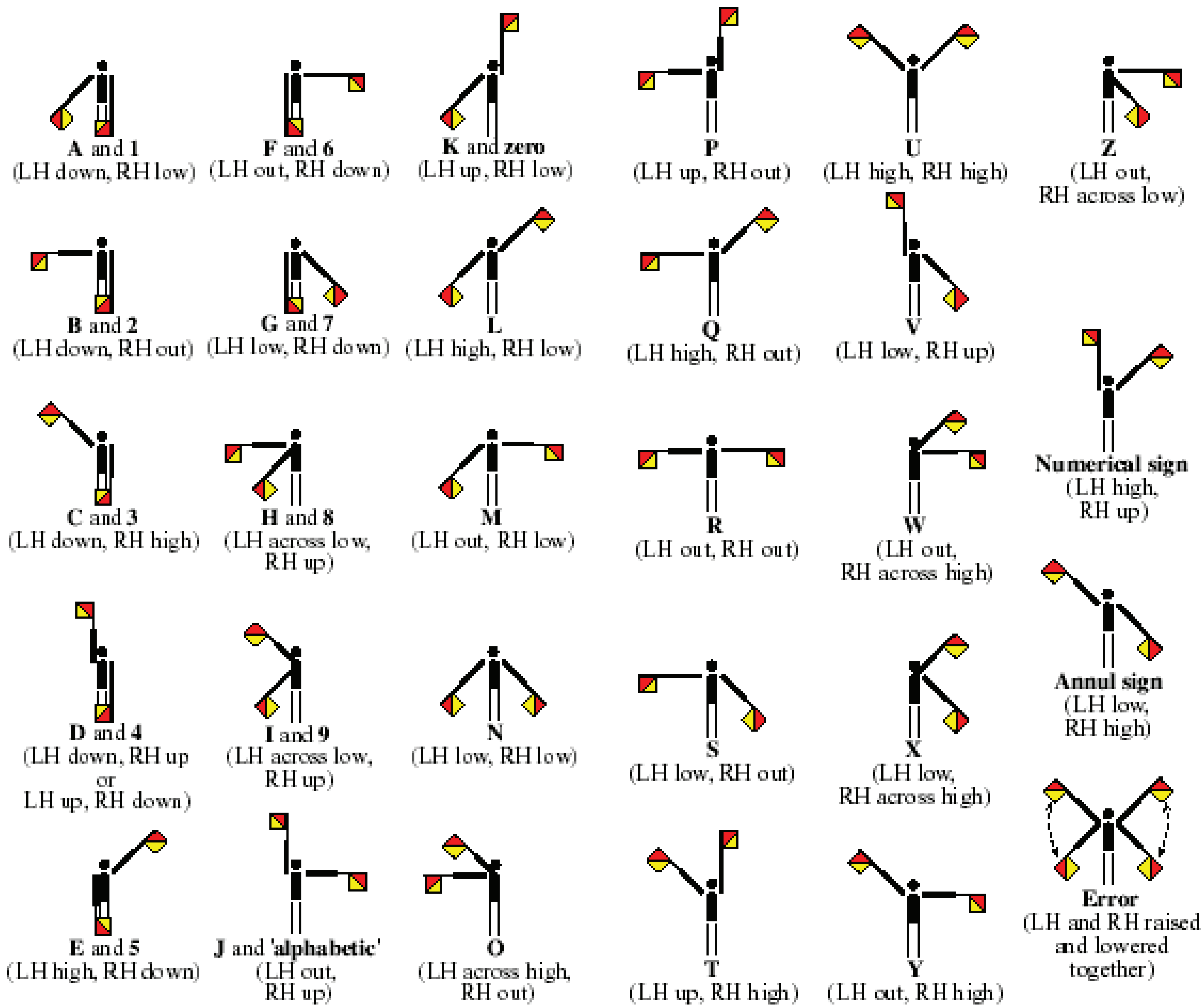
output mode



output mode

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

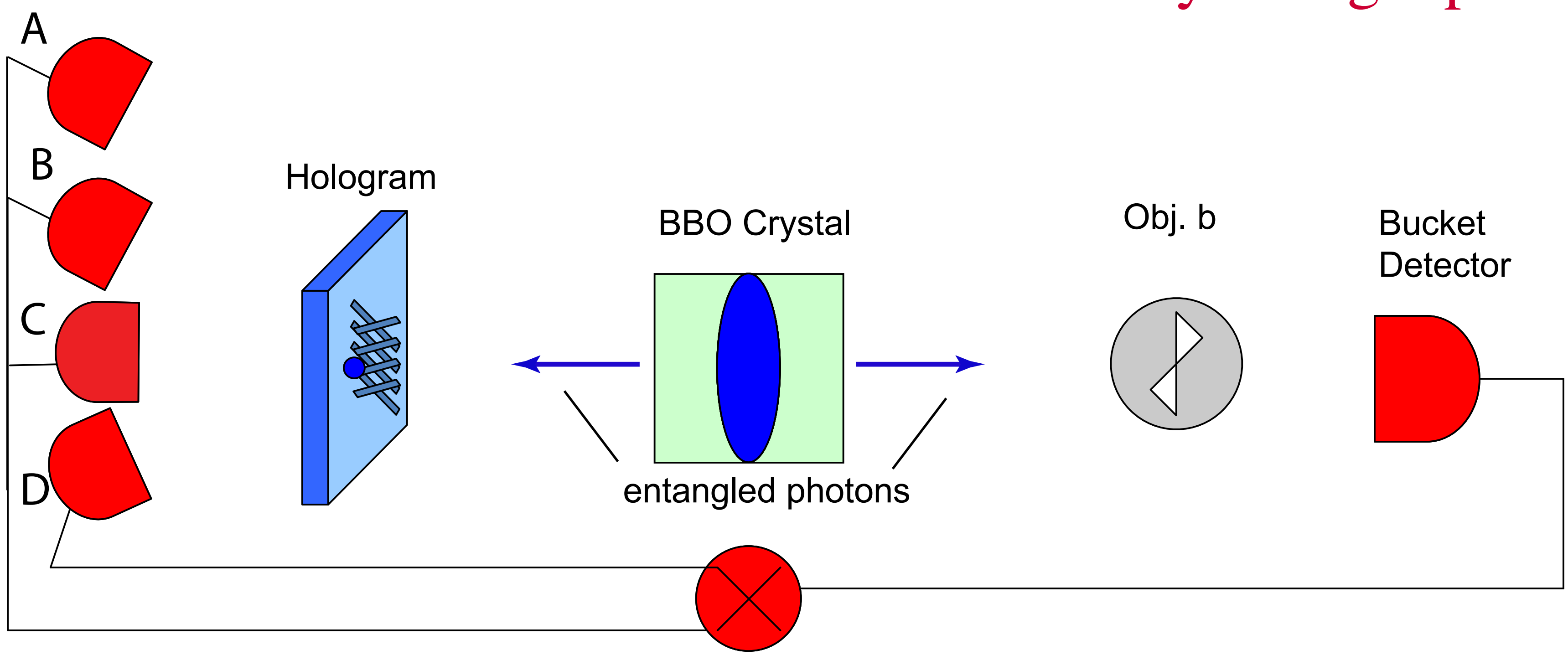
Free-Space Optical Telecommunication based on Transverse Field Structures



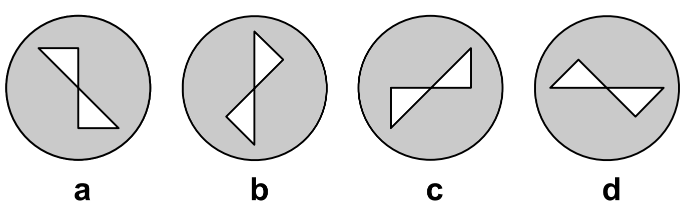
some additional work in quantum technologies

Single-Photon Coincidence Imaging

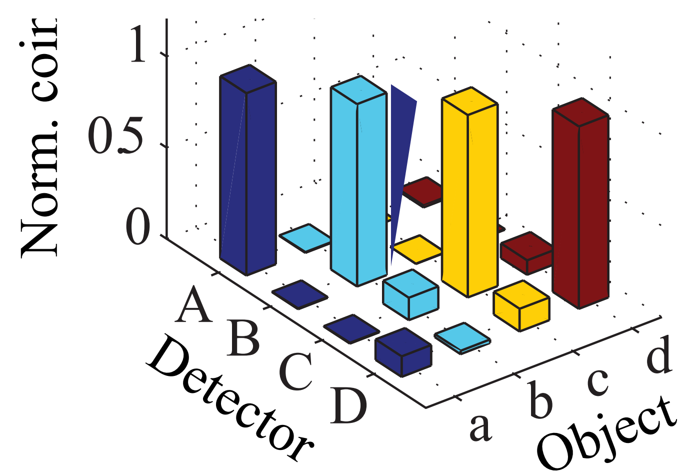
How much information can be carried by a single photon?



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



coincidence count rate

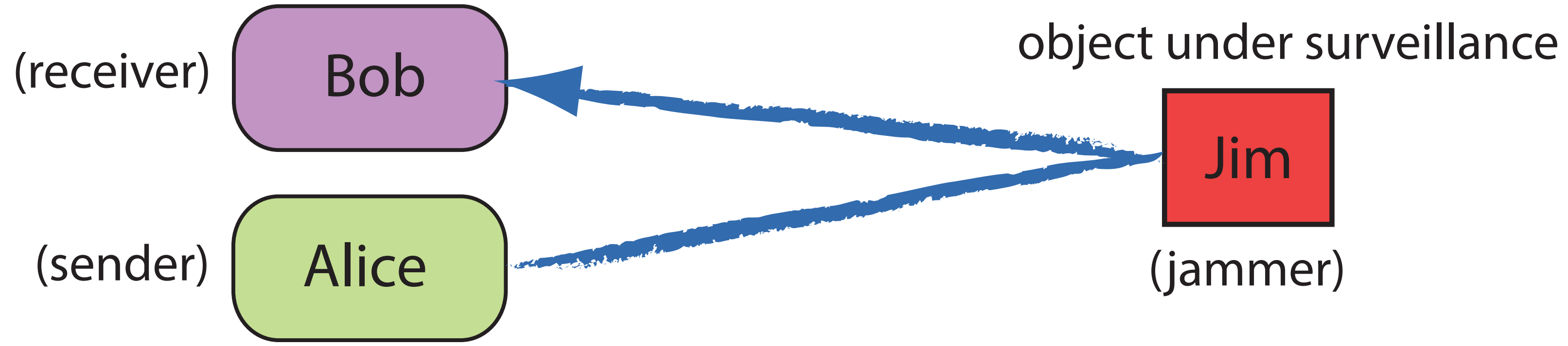


Malik, Shin, O'Sullivan. Zerom, and Boyd, Phys. Rev. Lett. 104, 163602 (2010).

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



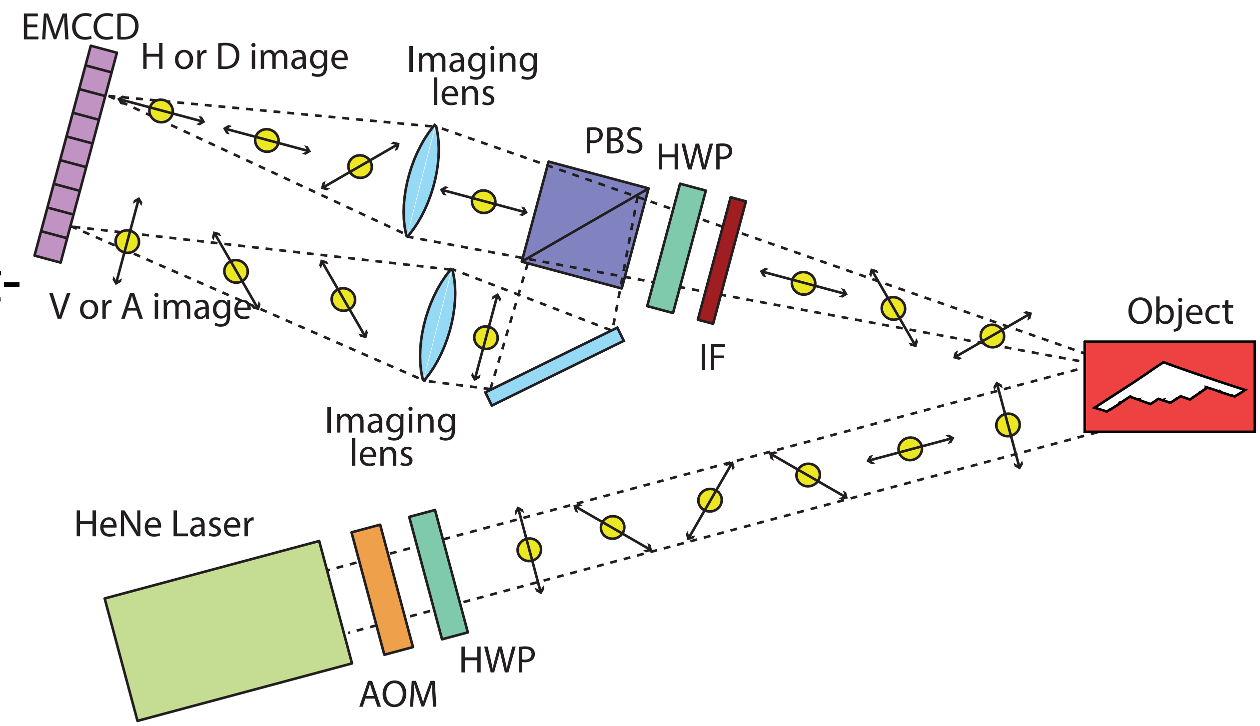
- Photon <u>polarization</u> used for security, photon <u>position and time</u> for surveillance

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

Secure Quantum Surveillance

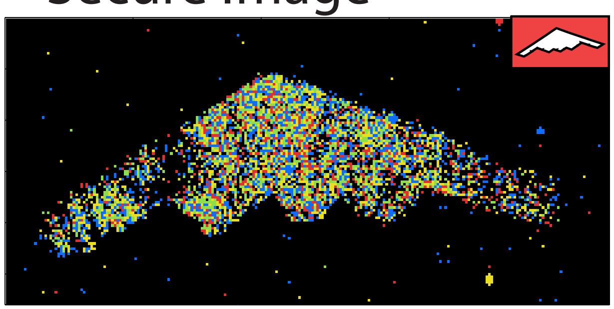
How do we know that what we are looking at is "real"?

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



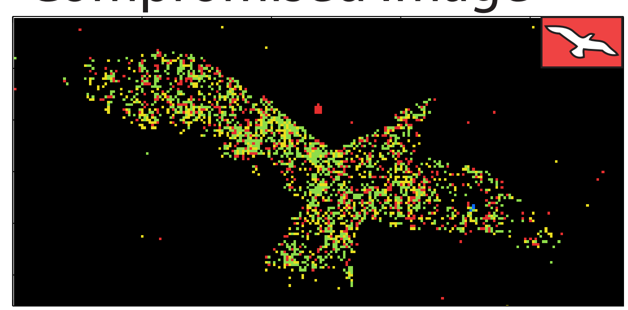
- Results

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

MailOnline 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.

Thank you for your attention!