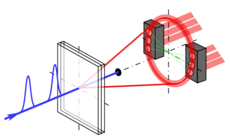
InPho: FSQC Overview

Principal Investigators:

Steve Barnett, Strathclyde, overall system theory
Robert Boyd, Ottawa, Rochester, mode sorting, turbulence mitigation
Daniel Gauthier, Duke, QKD system, detectors, entangled source
Paul Kwiat, Illinois, QKD system, detectors, entangled source, theory
David Miller, Stanford, fundamental limits mode sorters
Miles Padgett, Glasgow, mode sorters, detectors
Glenn Tyler, tOSC, turbulence mitigation

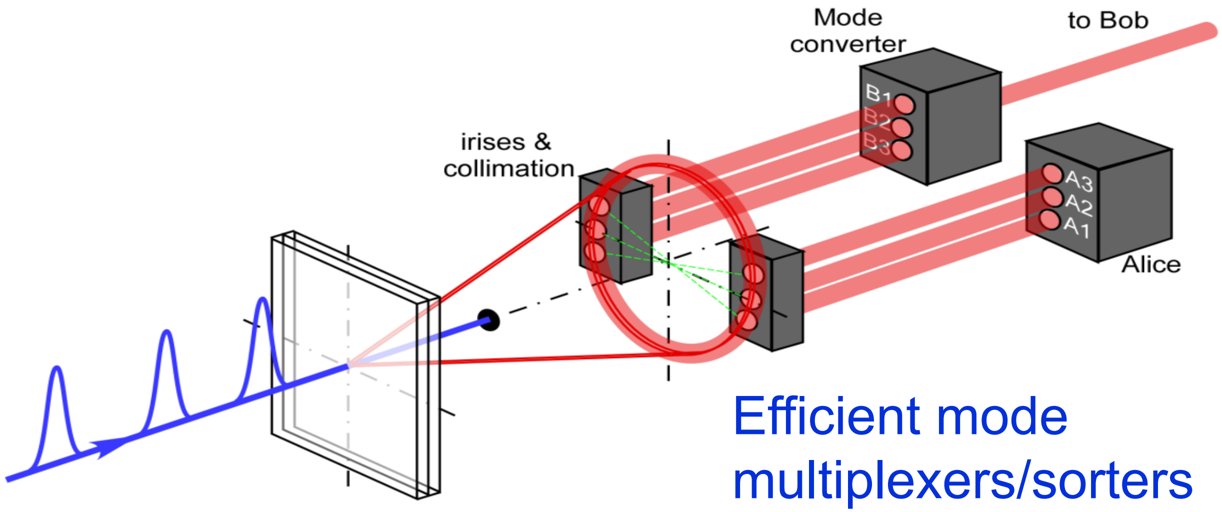
Partners:

Robert Calderbank, Duke, quantum error correction theory
Andrew White, Queensland, mode sorters, detectors, QKD system
Norbert Lutkenhaus, Waterloo, quantum security
Gerard Milburn, Queensland, overall system theory



Project Goal

Goal: Develop a discrete, entanglement-based quantum key distribution (QKD) system to meet program objectives



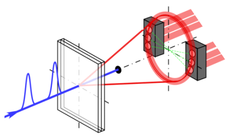
Turbulence mitigation

Low deadtime, efficient, high-speed single-photon-counting detectors

Efficient mode multiplexers/sorters

Trade space of data rate/security

Bright polarization-entangled source



FSQC Concept

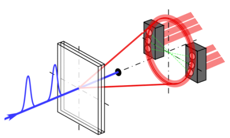
Use hyperentanglement to achieve many bits/photon (bpp) and high secure-key rate: QUANTUM DATA HYPERCUBE

Use polarization, time-bin, spatial mode degrees-of-freedom

Multiplex many independent channels

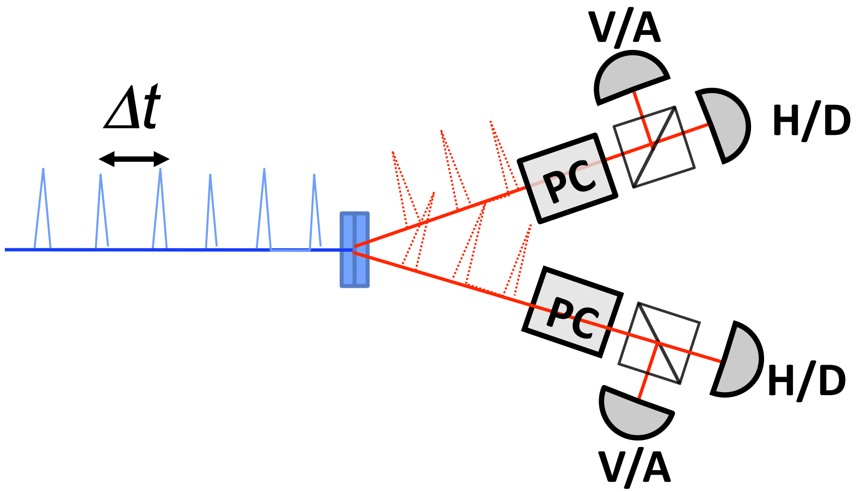
⇨ 1 spatial mode per channel (*e.g.*, orbital angular momentum states (OAM))

Single channel: create mutually-unbaised bases (MUBs) only in polarization, use time bins to achieve bpp



Single Channel

Encode in time, verify security in polarization

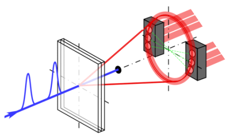


Classical comm channel
2 bits per code length
(+error correction
+ privacy amplification)

$$|\psi\rangle \propto \left(|HH\rangle + |VV\rangle\right) \otimes \left(|t_0 t_0\rangle + |t_1 t_1\rangle + |t_2 t_2\rangle + \ldots + |t_N t_N\rangle\right)$$

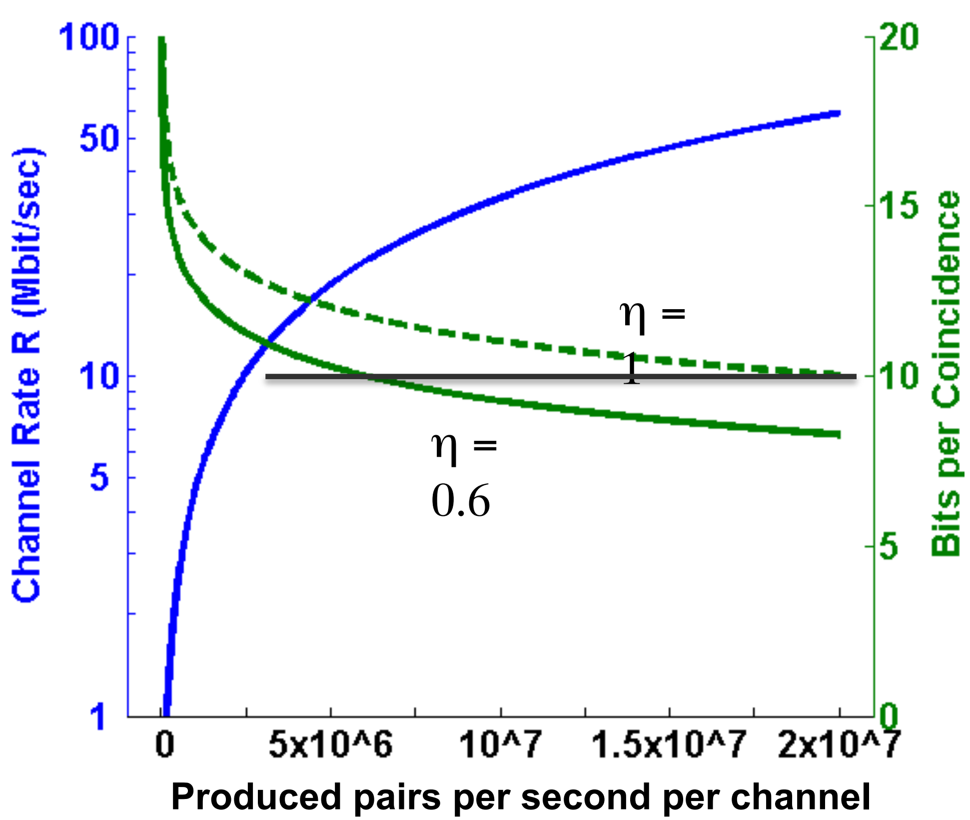
Bin spacing: Δt $\Delta t \sim 130$ ps

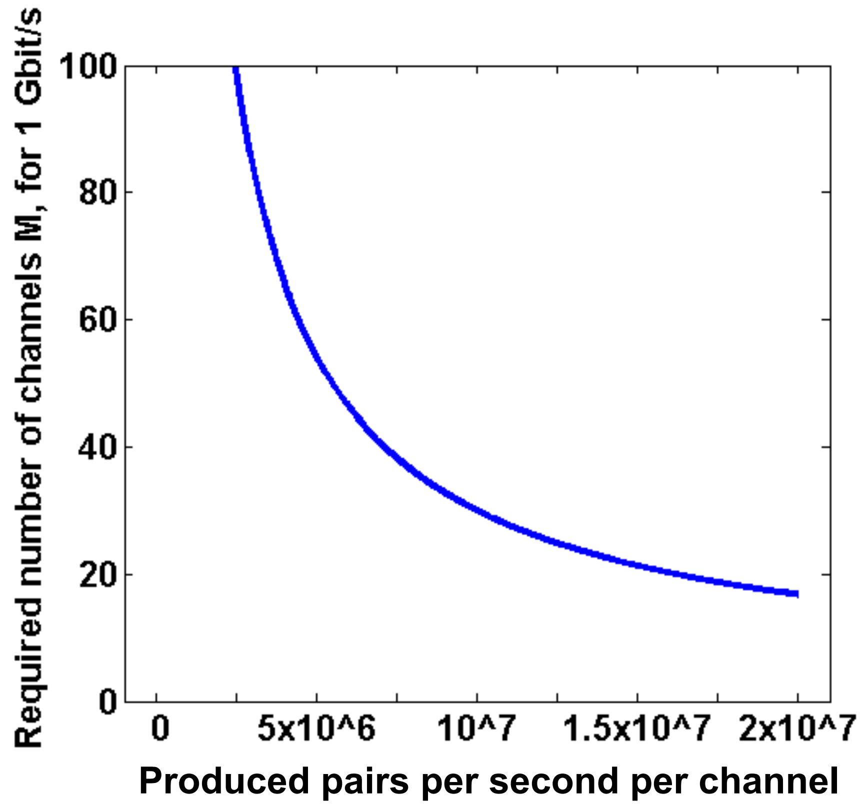
Code "length": $\sim N\Delta t$



bits/photon ~ $\log_2 N$ ⟹ $N \sim 1{,}024$

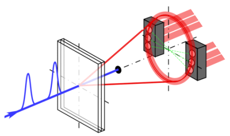
Predicted performance





Trade-off between high count rate and high bits per photon (bpp).

- highest bpp: only send 1 photon per day → ~49 bits/click (but only 1 click/day!)
- highest rate: send at near maximum detector saturation rate → only ~1 bpp
- we can simultaneously satisfy 1Gb/s and 10 bpp, by using multiple channels (10-30, depending on SPDC rate, efficiency, and BER)



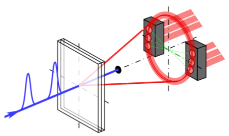
Task 1: QKD Milestones

Year 1	Year 2	Year 3
4 bpp 10 Mbps	4 bpp 100 Mbps	10 bpp 1 Gbps
single channel	*single channel*	

Book keeping of classical channel?

Need to divide bits per photon by ~100?

~1.1 using InPho Classical Com results?



Kwiat and everyone else!

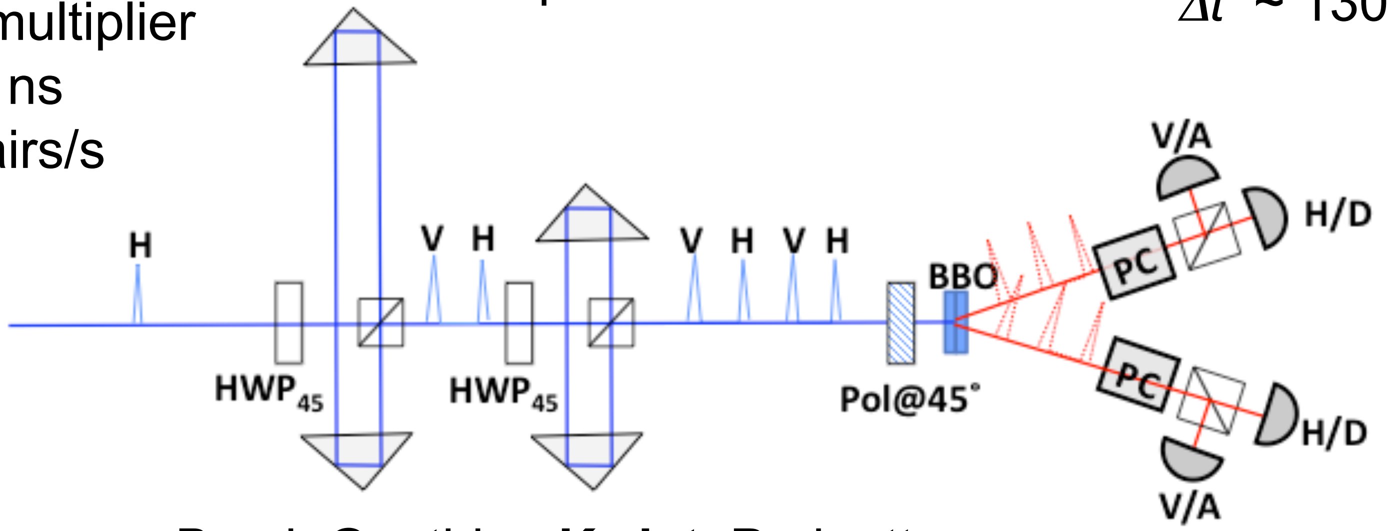
Task 2: Source Development

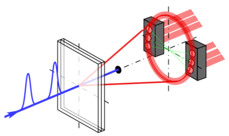
Year 1	Year 2	Year 3
4 bpp 10 Mbps	4 bpp 100 Mbps	10 bpp 1 Gbps

BiBO
High P
Rate multiplier
$\Delta t \sim 1$ ns
10^7 pairs/s

More rate multiplication
10^8 pairs/s

2×10^9 pairs/s
20 channels
$\Delta t \sim 130$ ps





Boyd, Gauthier, **Kwiat**, Padgett

Task 3: Mode Multiplexers/Sorters

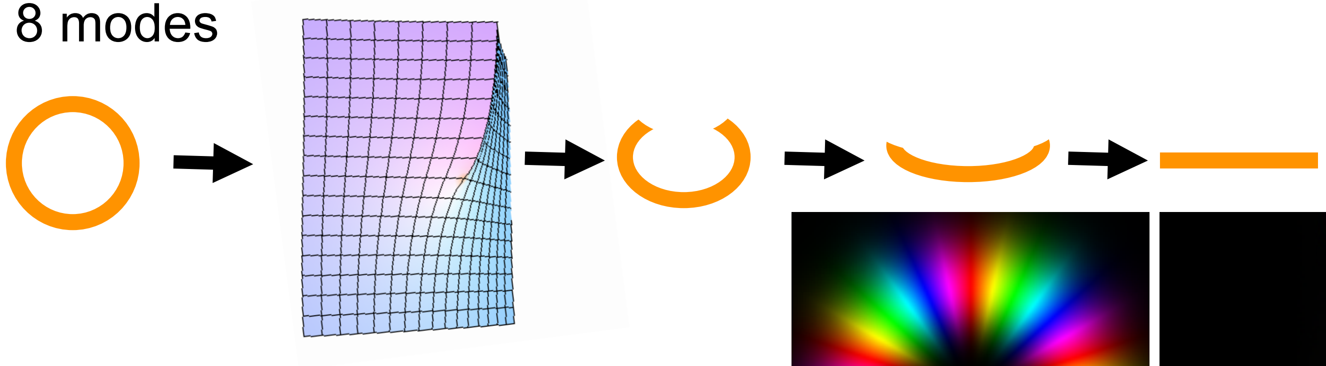
InPho: FSQC

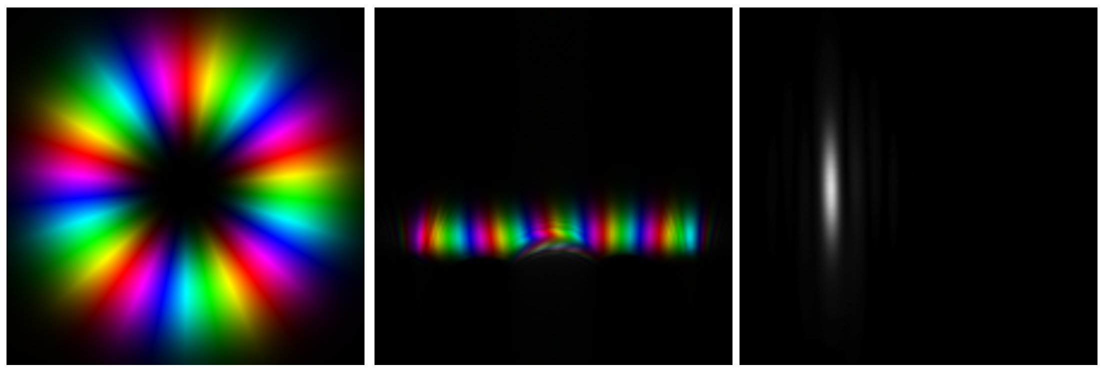
Year 1	Year 2	Year 3
4 bpp 10 Mbps	4 bpp 100 Mbps	10 bpp 1 Gbps

- Demonstrate sorting low-rate QKD testbed
- Thick holograms, other approaches
- 8 modes

- High efficiency sorter
- Fundamental limits
- 32 modes, >80% eff.

- Integrate into high bit rate QKD system
- 64 modes, 70% eff.





Boyd, Miller, Padgett, *White*

Task 4: Detector Development

Year 1	Year 2	Year 3
4 bpp 10 Mbps	4 bpp 100 Mbps	10 bpp 1 Gbps

Year 1:

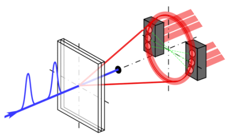
- switching fabric
  w/ high QE detectors
  < 20 ns deadtime
  4-8 detectors
- SiPMTs
- < 250 ps jitter,
  10 element arrays
  > 15% QE

Year 2:

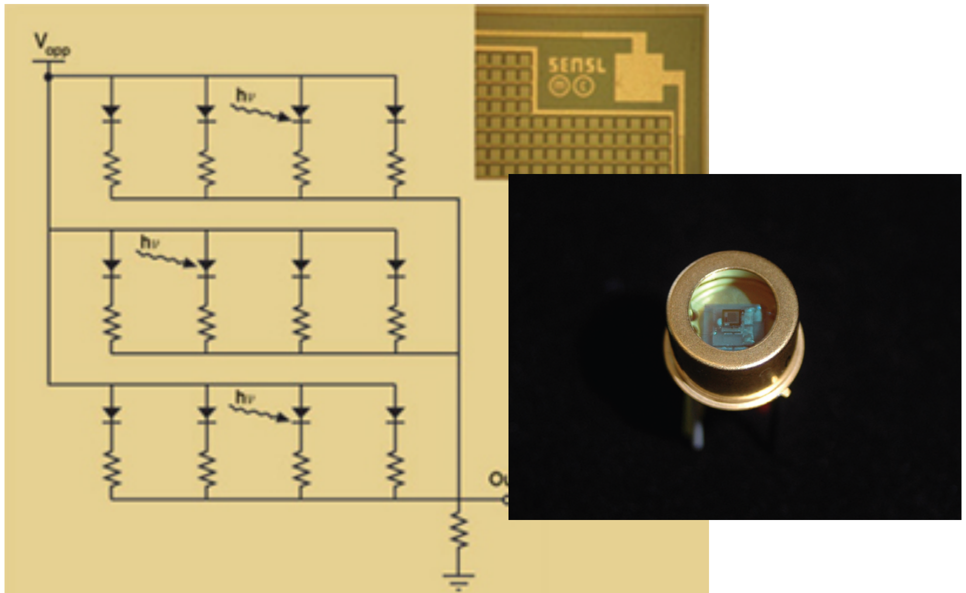
-100 element array
- >35% QE
- < 250 ps jitter

Year 3:

- < 130 ps jitter
- additional arrays



Gauthier, Kwiat



Task 5: Turbulence Mitigation

Year 1

4 bpp
10 Mbps

- Identify minimum energy loss states
- Generate minimum energy loss states

Year 2

4 bpp
100 Mbps

- Investigate spatial entanglement
- Predistorted MUBs
- Optimum aperture sizes
- State-dependent loss
- Test in low-rate QKD testbed, > 5 bpp

Year 3

10 bpp
1 Gbps

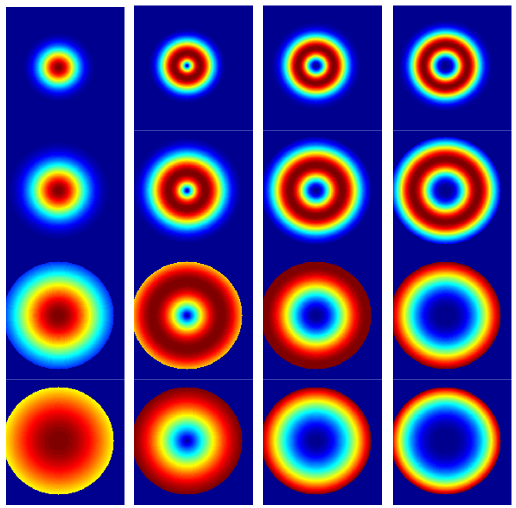
- Test in low-rate QKD testbed w/ turbulence cells

$N_f=10$

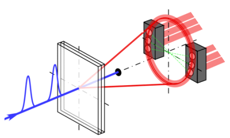
$N_f=5$

$N_f=2$

$N_f=1$



minimum energy loss states



Boyd, **Tyler**

Task 6: Theoretical analysis of security

Year 1

4 bpp
10 Mbps

- Optimum error correction method for large Hilbert space
- What attacks will break us?

Year 2

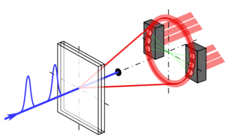
4 bpp
100 Mbps

- Optimum Hilbert space dimension, # MUBs
- Trade space of security, bbp, bps
- Security compromised by state-dependent loss?

Year 3

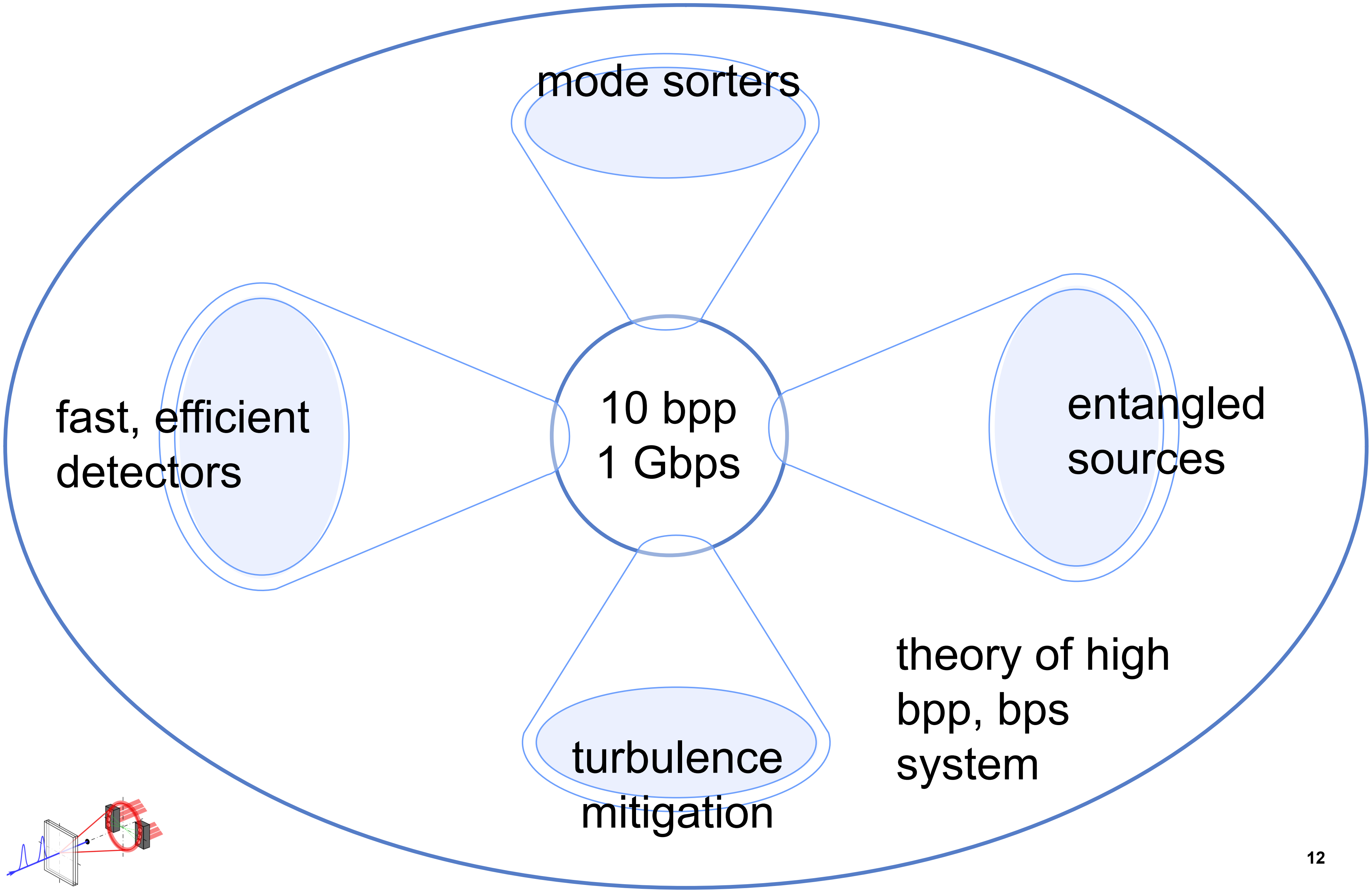
10 bpp
1 Gbps

- Identify system with absolute security
- Decoy states to improve security



Barnett, *Calderbank*, Kwiat, *Lutkenhaus*, *Milburn*, Tyler

Summary Overview



Team Interactions

Interactions via Social Media

Hourly Tweets

Daily Videos

System Details & Components

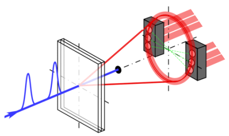
1. Central concept, expanded
2. Laser and pulse multiplexer
3. Down-conversion source
4. Detectors
   - switched, optimized APDs
   - array detectors

---

5. Multi-channels → spatial multiplexing
6. AOM mode sorters, turbulence

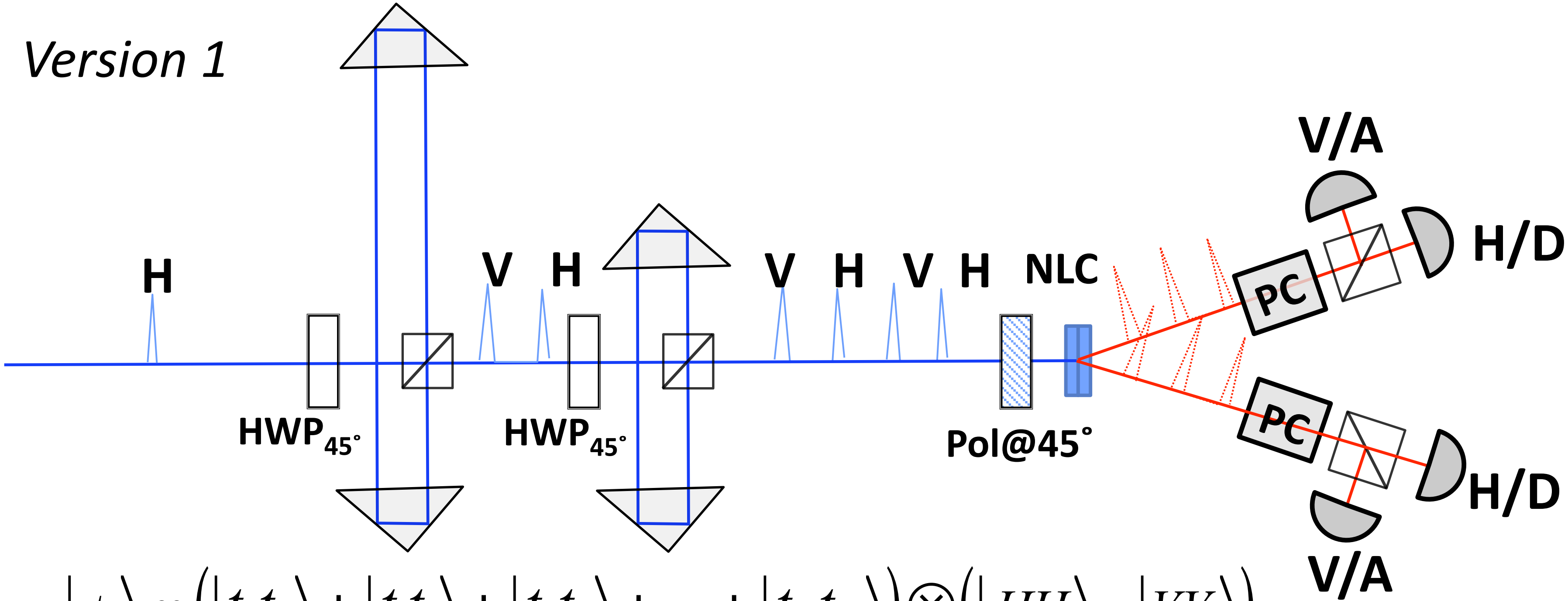
---

7. Eavesdropping, security
8. Open theoretical questions



Central Concept: Encode in time, verify in polarization

Version 1

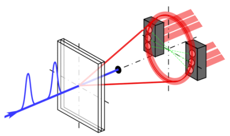


$$|\psi\rangle \propto \left(|t_0t_0\rangle + |t_1t_1\rangle + |t_2t_2\rangle + \ldots + |t_Nt_N\rangle\right) \otimes \left(|HH\rangle + |VV\rangle\right)$$

Alice and Bob use which time bin they detect a photon in to generate multiple bits per click. Get extra bpp from BB84 with polarization.*

They can constantly check for an eavesdropper using the D/A polarization basis (assuming no QND capability for Eve).

Perform standard error detection/correction† and privacy amp.

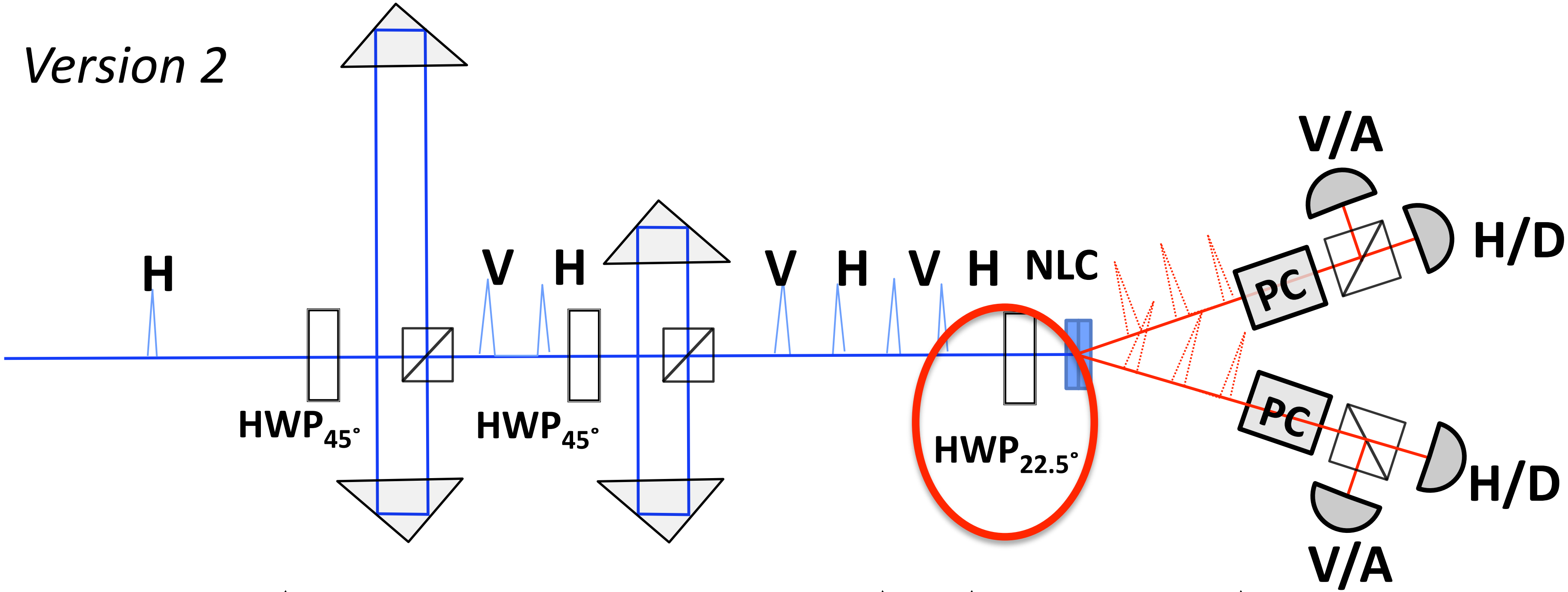


*Ali-Khan, Broadbent, Howell, Phys. Rev. Lett. **98**, 060503 (2007)

† Modified CASCADE

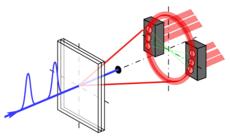
Central Concept: Encode in time, verify in polarization

Version 2



$$|\psi\rangle \propto \left(|t_0 t_0\rangle + |t_2 t_2\rangle + \ldots + |t_{N-1} t_{N-1}\rangle\right) \otimes \left(|HH\rangle + |VV\rangle\right)$$
$$+ \left(|t_1 t_1\rangle + |t_3 t_3\rangle + \ldots + |t_N t_N\rangle\right) \otimes \left(|HH\rangle - |VV\rangle\right)$$

Advantages: No pump power lost, ?harder? to eavesdrop
Disadvantages: Error checking depends on time bin, ???
NOTE: Active basis choice (PC) can be replaced by BS and twice as many detectors.



Pump Laser Source

Paladin Compact 355-4000 by Coherent

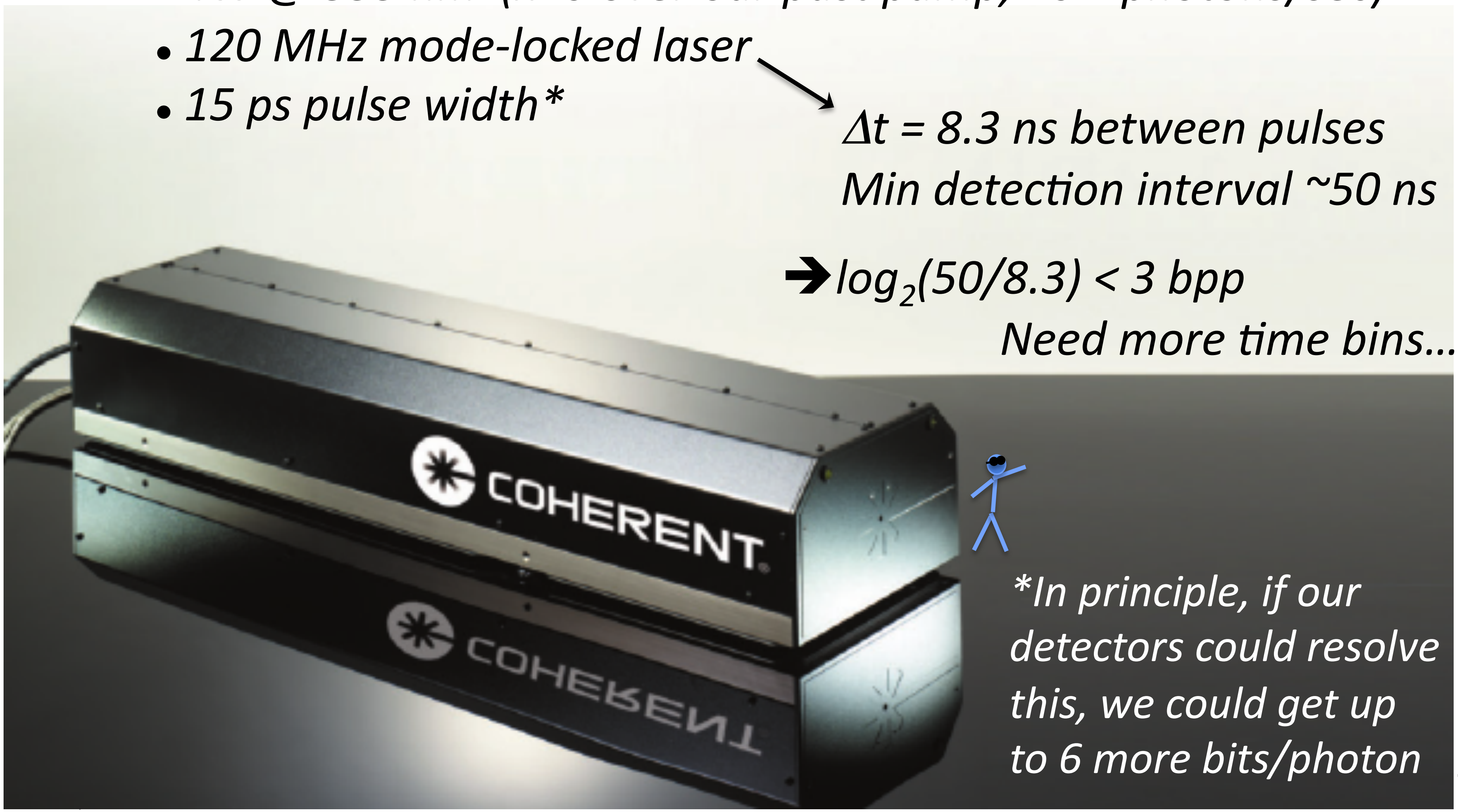
- *4W @ 355 nm (x10 over our past pump, 10^{20} photons/sec)*
- *120 MHz mode-locked laser*
- *15 ps pulse width**

Δt = 8.3 ns between pulses

Min detection interval ~50 ns

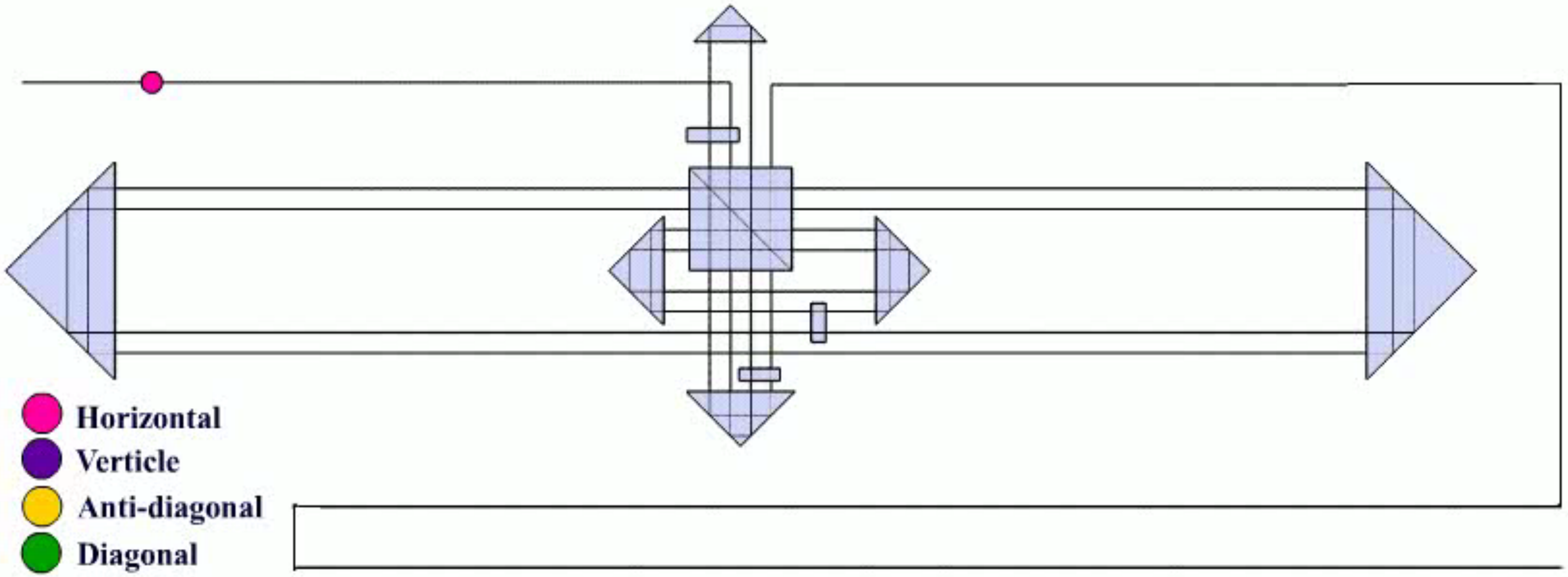
➔ *$\log_2(50/8.3) < 3$ bpp*

Need more time bins…



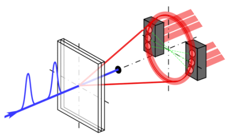
**In principle, if our detectors could resolve this, we could get up to 6 more bits/photon*

Pump Pulse Multiplexer



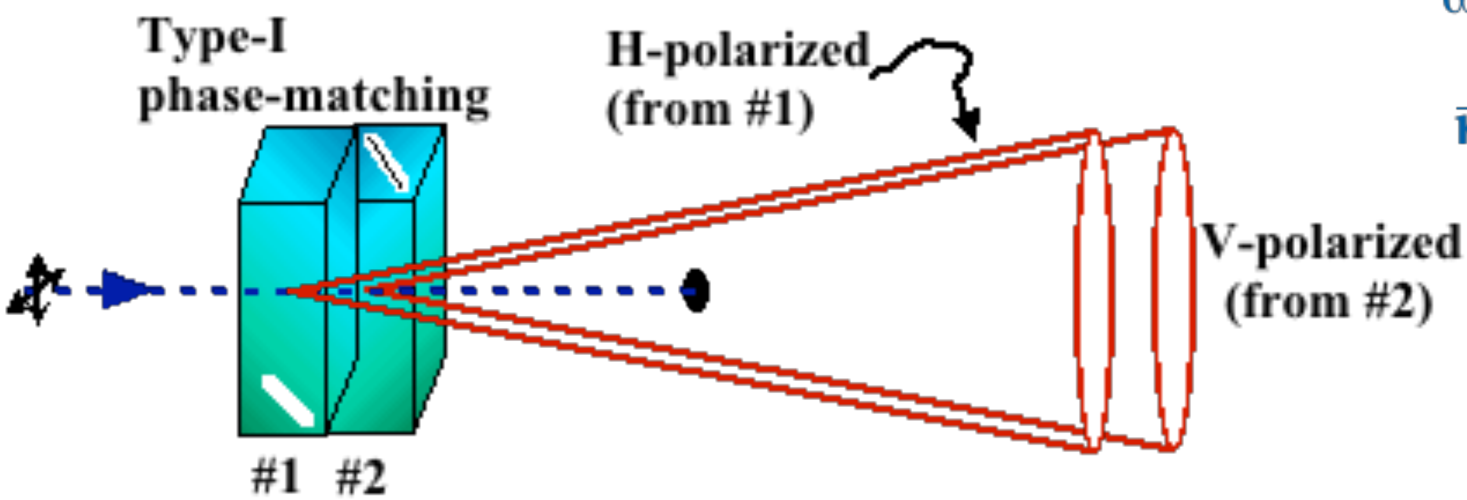
2^4 = 16 system shown; cycles 1-2 and 3-4 perfect "doubles"*

120 MHz (Pump rep rate) x 2^6 = 7.7 GHz (130-ps time bins)



**Phase 1-2 implementations; Phase 3: add two more cycles*

Two-crystal Polarization-Entangled Source



$$\omega_p = \omega_s + \omega_i$$

$$\vec{\kappa}_p = \vec{\kappa}_s + \vec{\kappa}_i$$

PGK et al., PRA **60**, R773 (1999)

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2 + e^{i\varphi}|V\rangle_1|V\rangle_2\right)$$

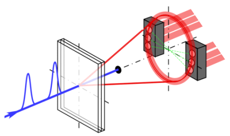
Maximally entangled state

Spatial-compensation: all pairs have same phase ϕ

We detected 2x10^6 pairs/s, with >99%-fidelity entanglement.

→ implied production rate > 2 x 10^{7}s^{-1}

Now: BiBO (3x BBO), up to 10x power → > 10^8 production rate



Opt. Exp. **13**, 8951 (2005)

Detectors: Overview

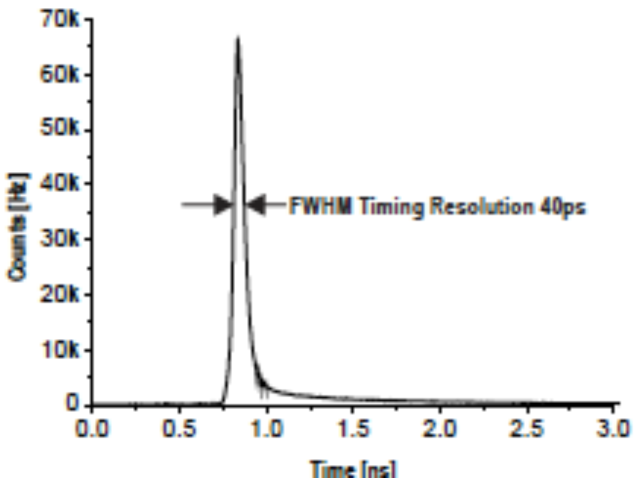
What we want/need:

- *High efficiency (coincidence rate* $\propto \eta^2$*)*
- *Excellent timing jitter (<130 ps, ideally < 15 ps)*
- *Low deadtime/high saturation rate (< 10 ns/>50 MHz)*

What we (traditionally) get:

SPCM
Jitter: 250 ps FWHM
(long tail)
Deadtime: 45 ns
Max count rate > 5 MHz
Efficiency < 65%

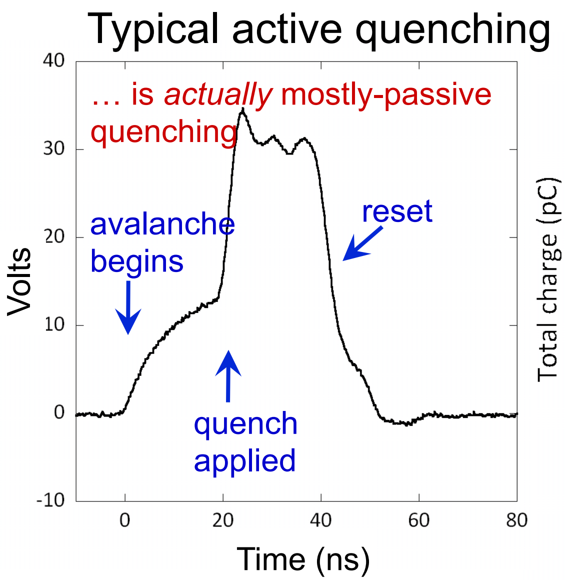
8-channel SPAD module
Jitter: 70 ps FWHM
Deadtime: 50 ns
Max count rate > 5 MHz
Efficiency < 35%

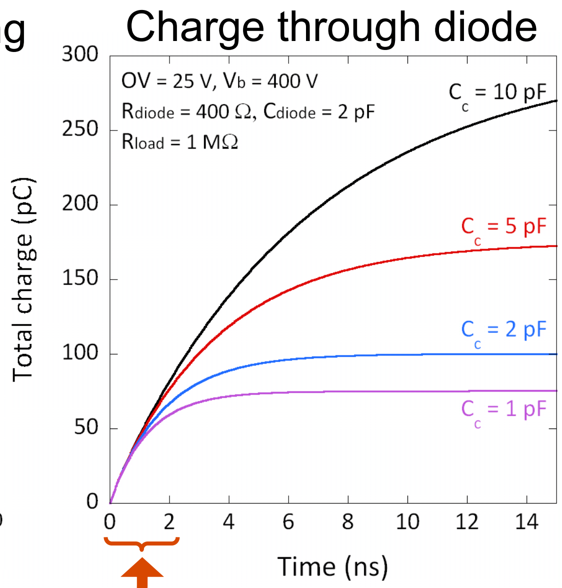


Increasing Count Rates in Thick Si SPADs

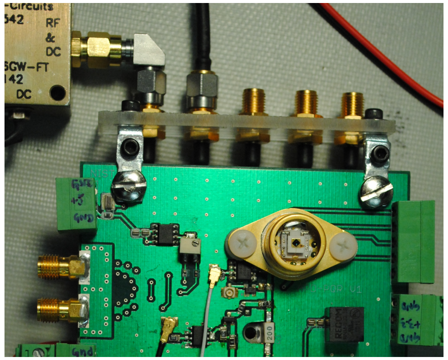
M. Wayne (UIUC)
A. Restelli
J.C. Bienfang

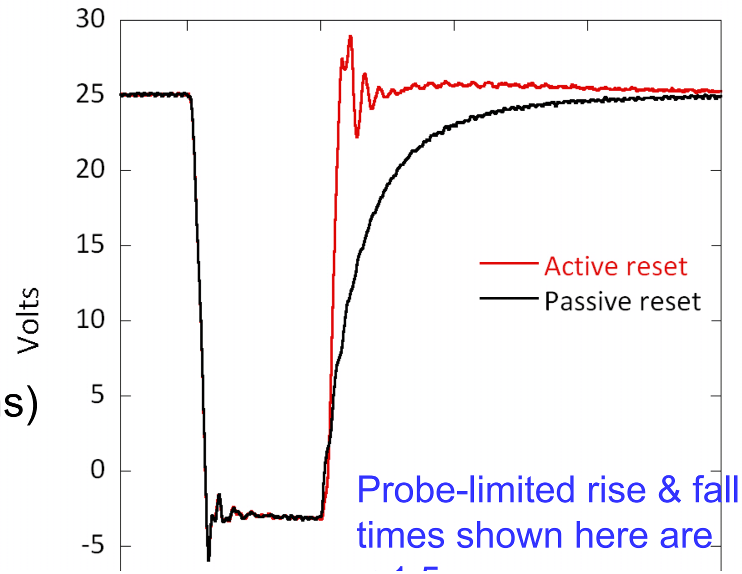
- Afterpulsing is reduced by minimizing the total avalanche charge through diode.
- High-speed electronics to promptly quench & reset Si SPADs.





Want to apply quench here





-Requires both short *signal delays* and *fast edges*

-Gb/s electronics provide < 200 ps delays

-RF power amplifiers provide large slew rates (> 40V/ns)

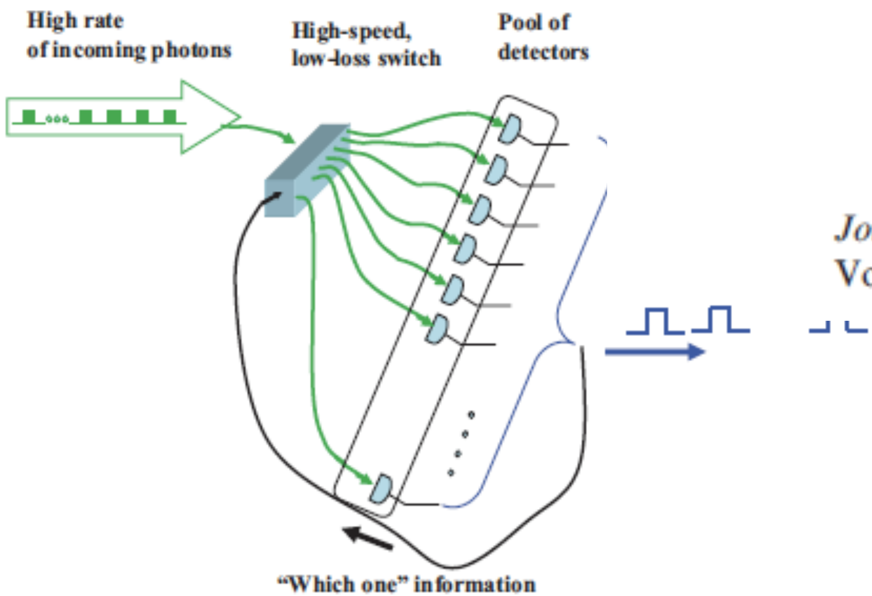
- Virtex-V FPGA provides nanosecond pulse control

- Afterpulse experiment underway

Goal: Reduce 40-ns deadtime → <20 ns

Detectors: How to run APDs faster…

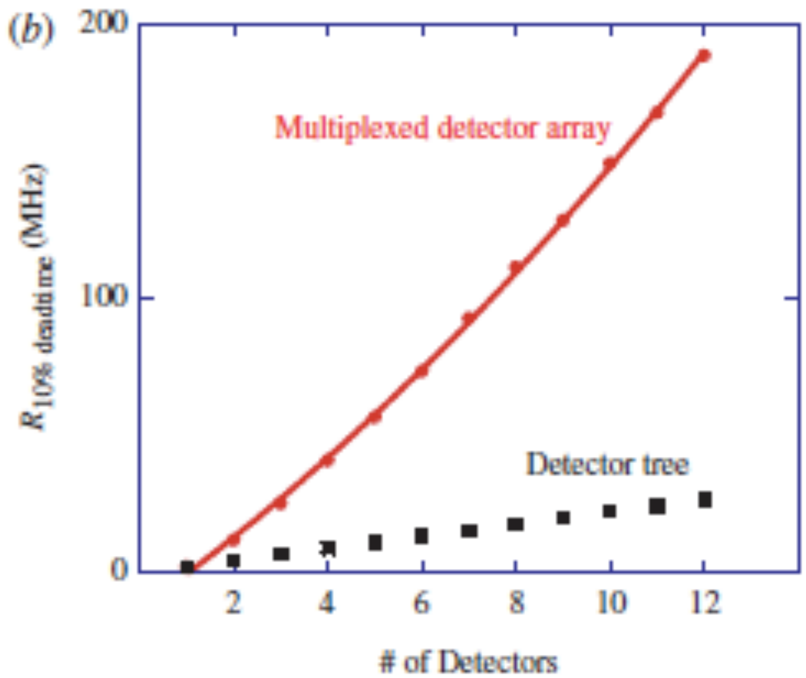
Sequential detection scheme:



Reduced deadtime and higher rate photon-counting detection using a multiplexed detector array

S. A. CASTELLETTO†, I .P. DEGIOVANNI†, V. SCHETTINI† and A. L. MIGDALL*‡

Journal of Modern Optics
Vol. 54, Nos. 2–3, 20 January–15 February 2007, 337–352



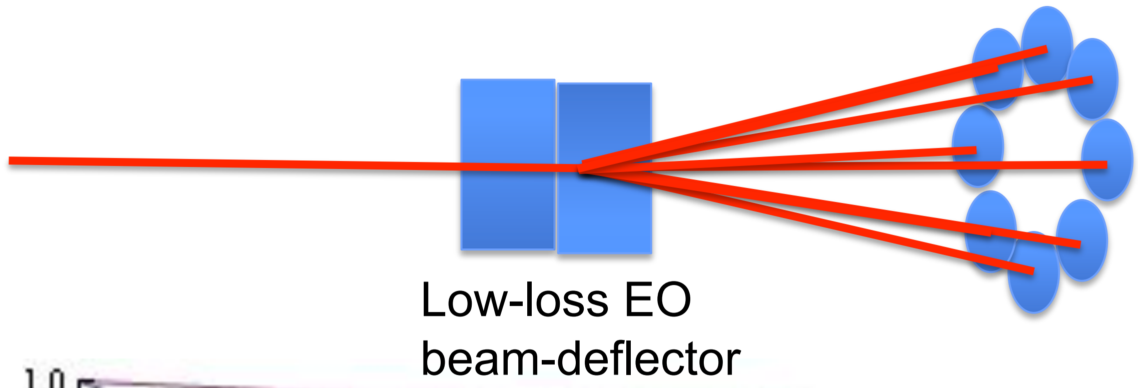
Do much better because no photons go to detector k while it is recovering.

Hard to implement with low loss (need fast "FSO" switch network)…

Detectors: How to run APDs faster…

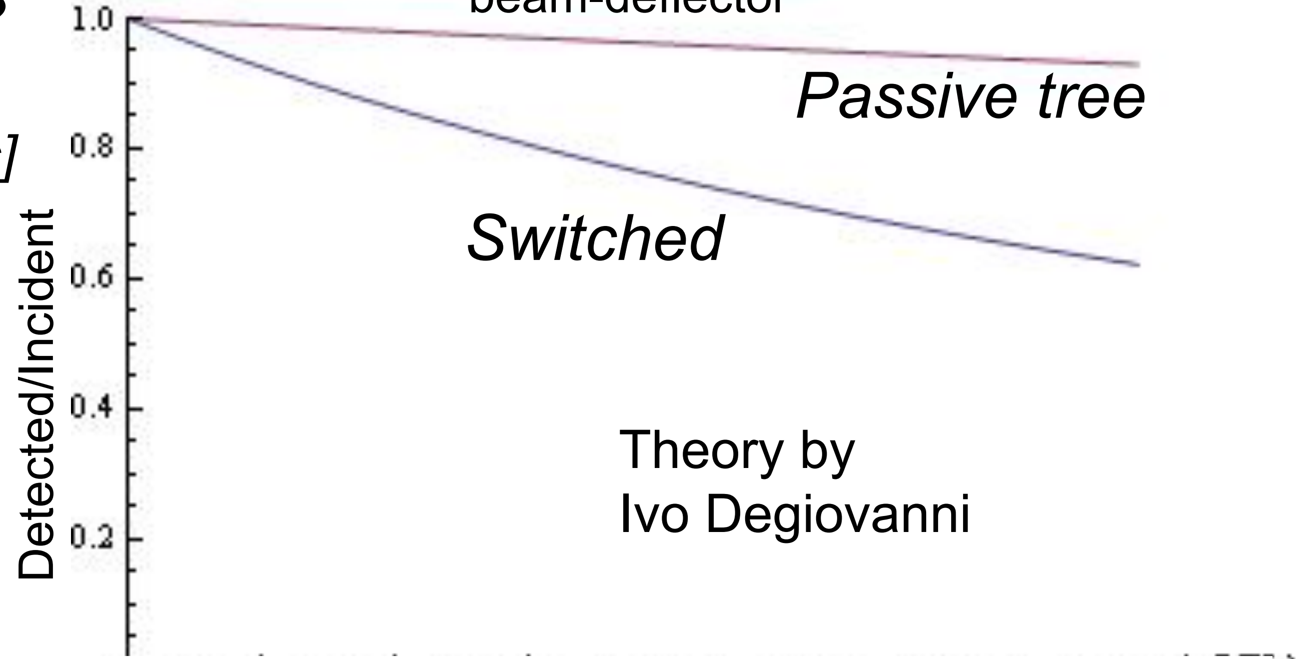
Solution: Periodic sequential detection scheme

Periodic switching is much easier to implement (i.e., no logic).



(How much) does it help?
[assuming 8 detectors, 10 bpp, T_{dead}=40 ns, and Δt = 130ps]

*It **hurts**! Why?*
Because to get 10 bpp, average time between detections = 2^{10} x 130 ps = 133 ns > 3 x 40-ns deadtime

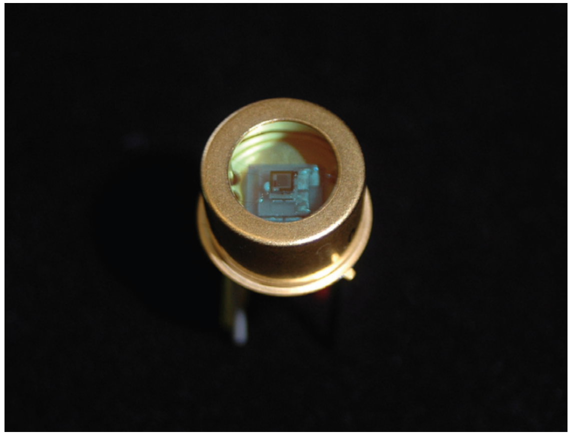


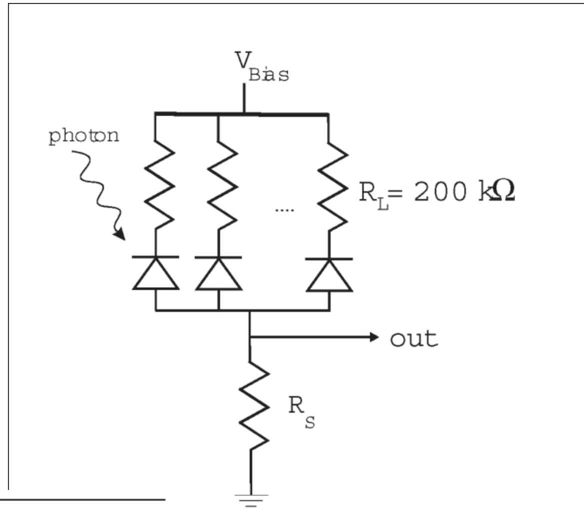
<u>Preliminary</u> conclusion: Passive 'beamsplitter tree' is optimal…

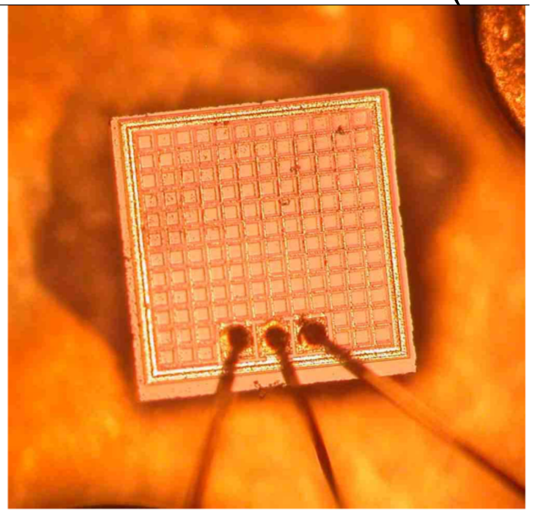
SiPMTs

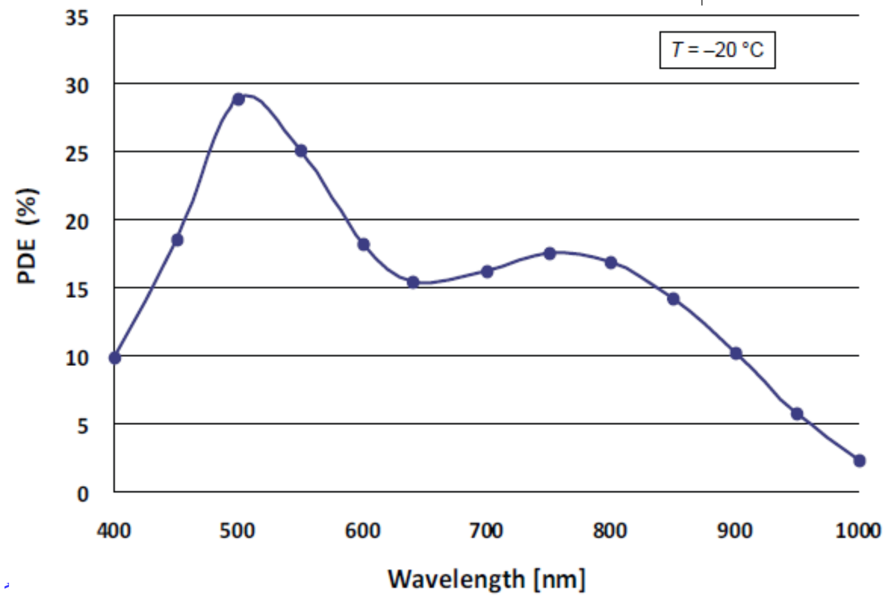
Voxtel "Silicon Photomultiplier"
TE Cooled: SQBF-EK0A (comes in chip form too)

Eraerds *et al.* (2007)







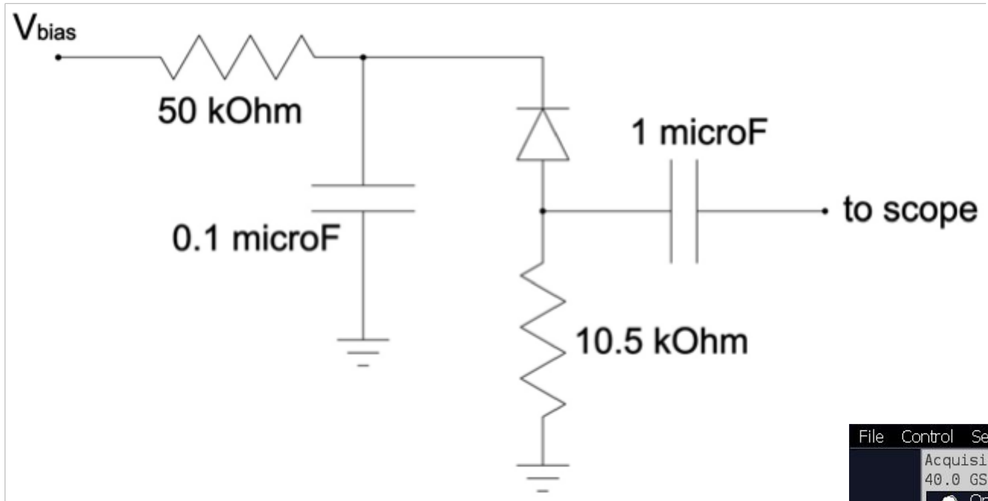


Photon # resolving

~10^6 dcps room temp
~1,000 dcps TEC cooled
~0.1 dcps LN2 cooled

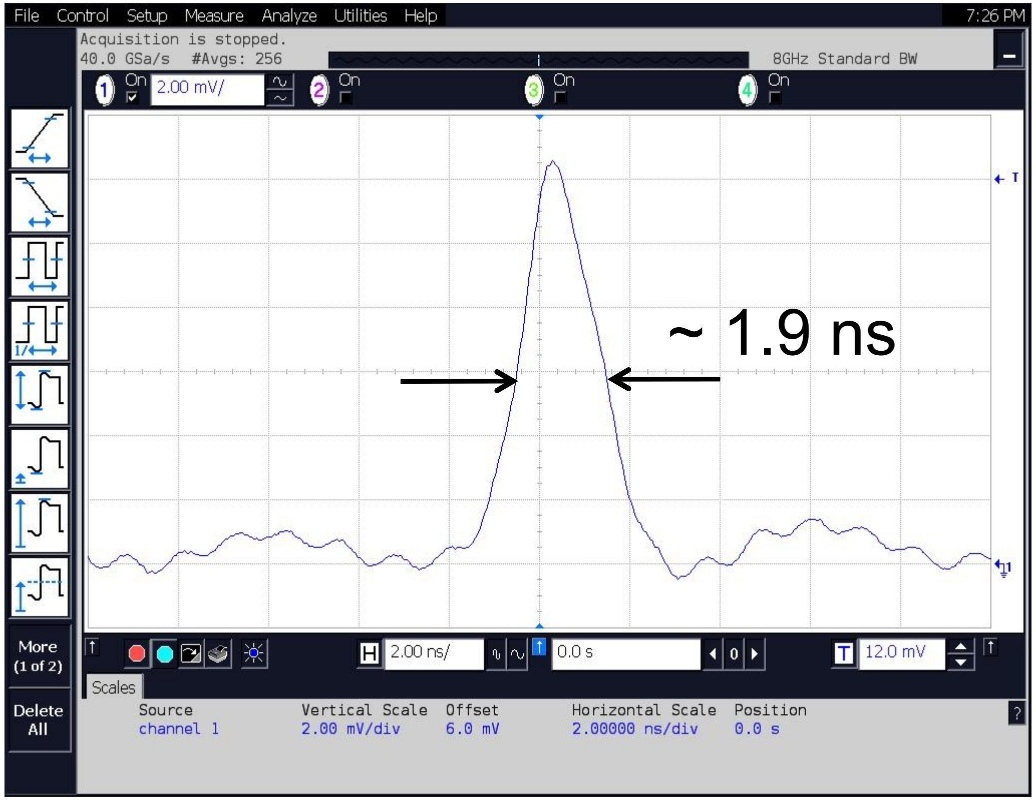
>50% QE soon available (?)

Initial Results with Voxtel Detectors



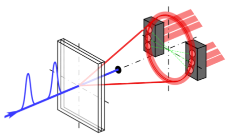
(high-speed layout not used)

single-photon event



Cooled -90˚C below ambient

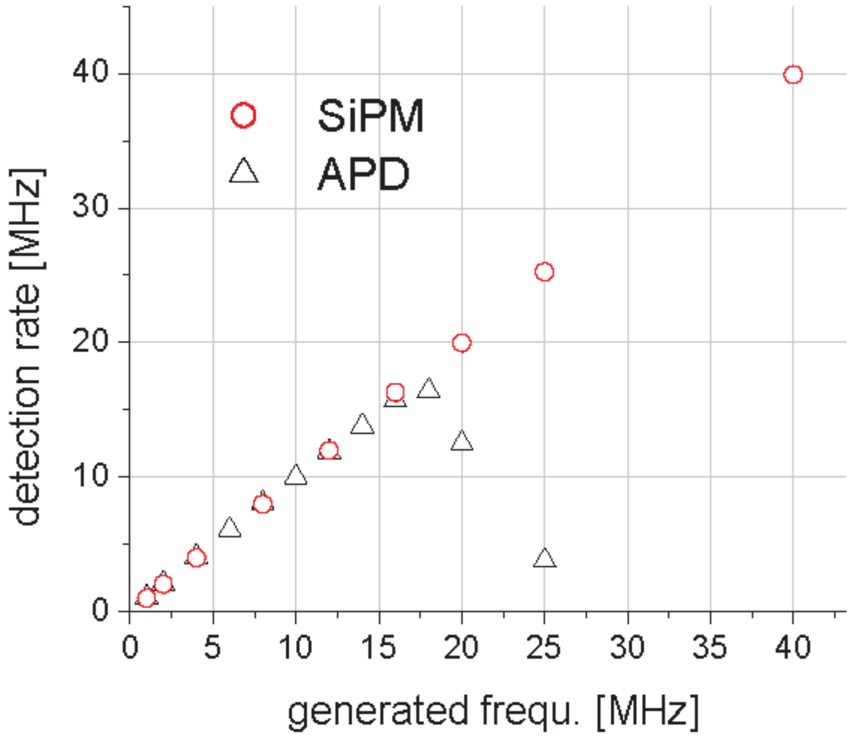
guesstimate 5,000 dcps

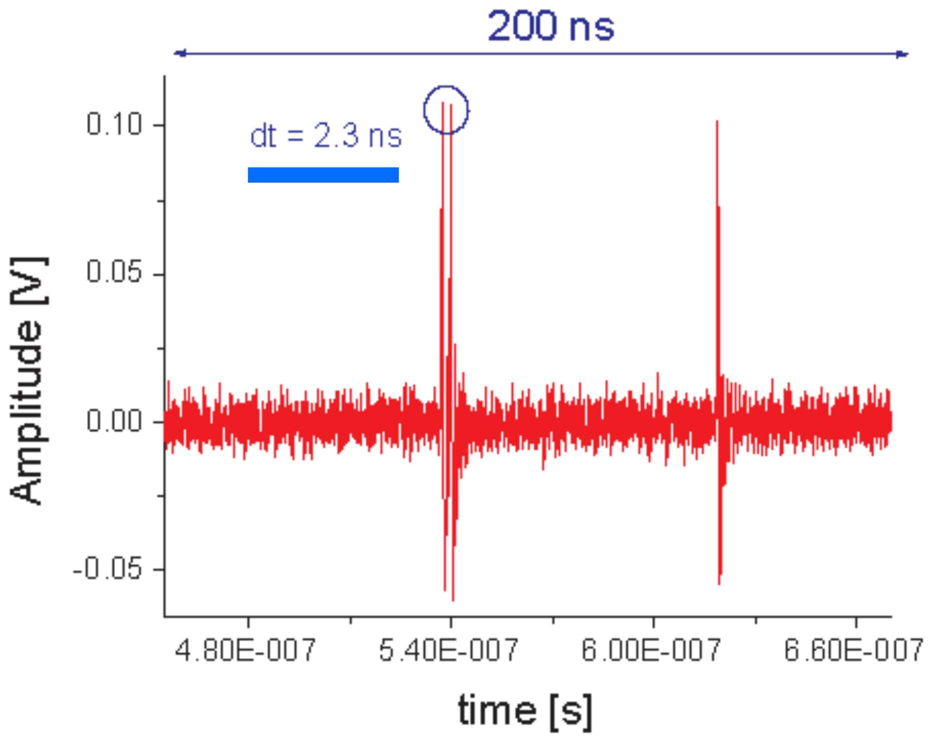


2 ns/div, 2 mV/div

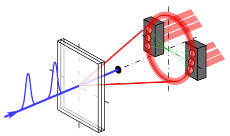
SiPMTs: Demonstrated Characteristics (by different groups)

~ 30-ps timing resolution
(Buzhan, Dolgoshein *et al*. ICFA Instrumentation Bulletin)





weak saturation starts ~150 Mcps

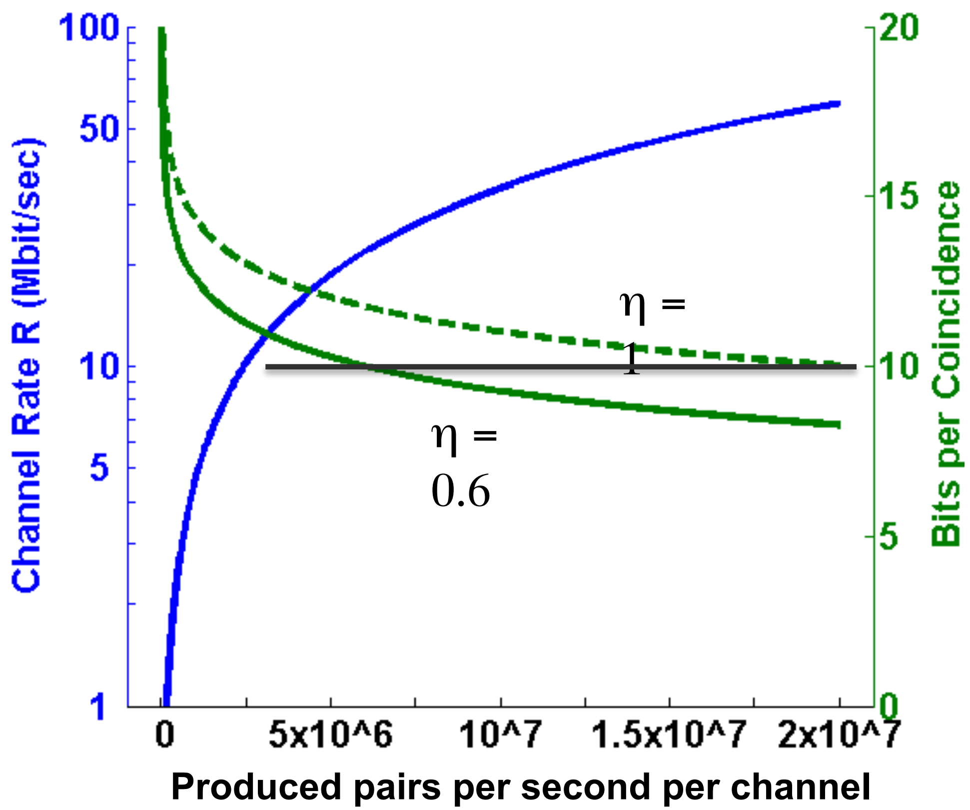


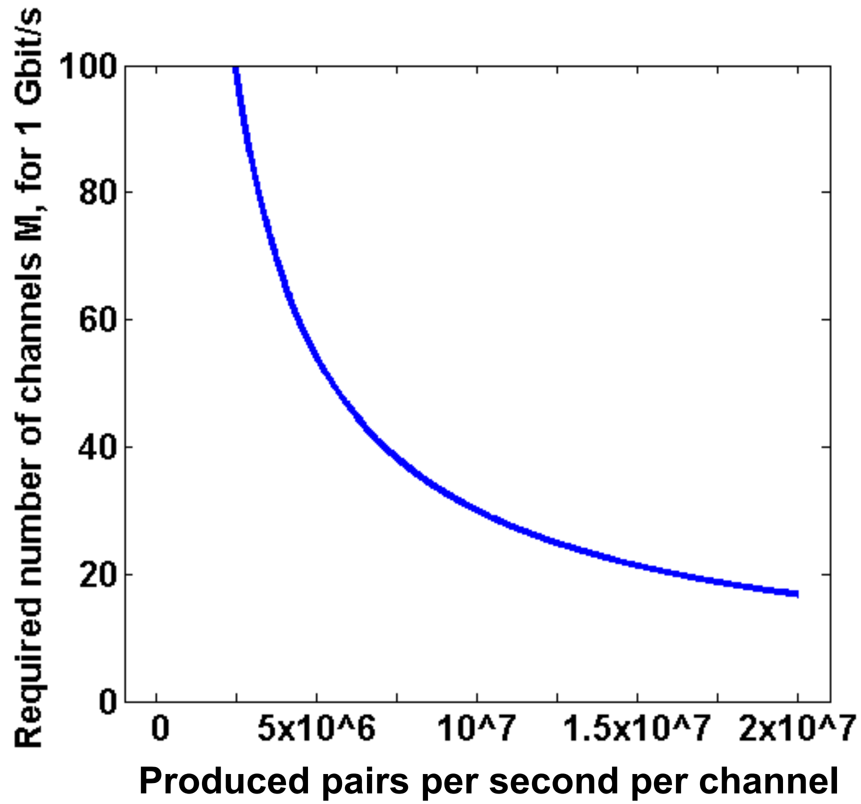
Eraerds, *et al*. (2007).

System Details & Components

1. Central concept, expanded
2. Laser and pulse multiplexer
3. Down-conversion source
4. Detectors
   - switched, optimized APDs
   - array detectors
5. Multi-channels → spatial multiplexing
6. AOM mode sorters, turbulence
7. Eavesdropping, security
8. Open theoretical questions

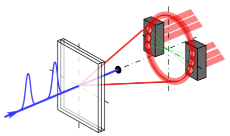
Predicted performance



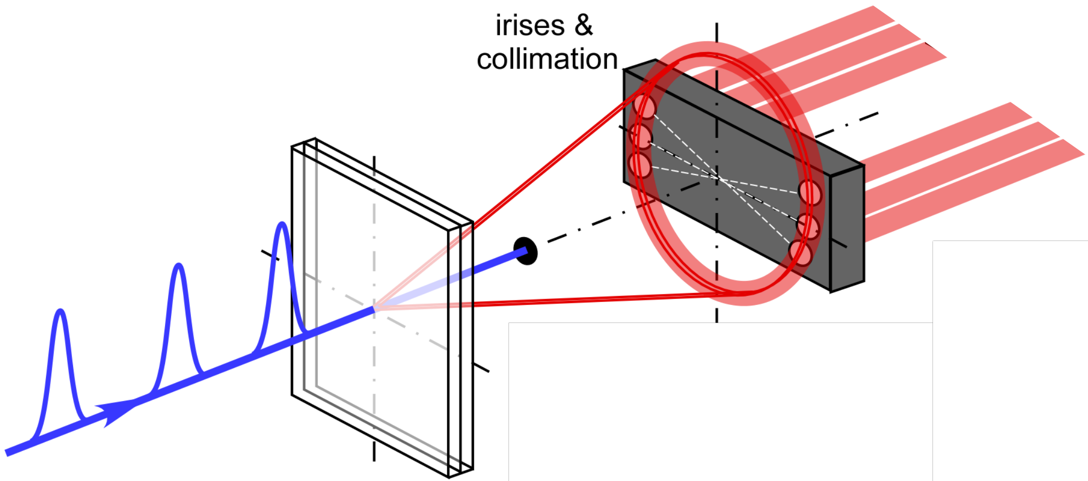


Trade-off between high count rate and high bits per photon (bpp).

- highest bpp: only send 1 photon per day → ~49 bits/click (but only 1 click/day!)
- highest rate: send at near maximum detector saturation rate → only ~1 bpp
- **we can simultaneously satisfy 1Gb/s and 10 bpp, by using multiple channels (10-30, depending on SPDC rate, efficiency, and BER)**



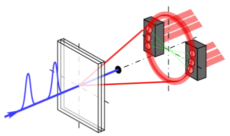
Use spatial modes as independent channels



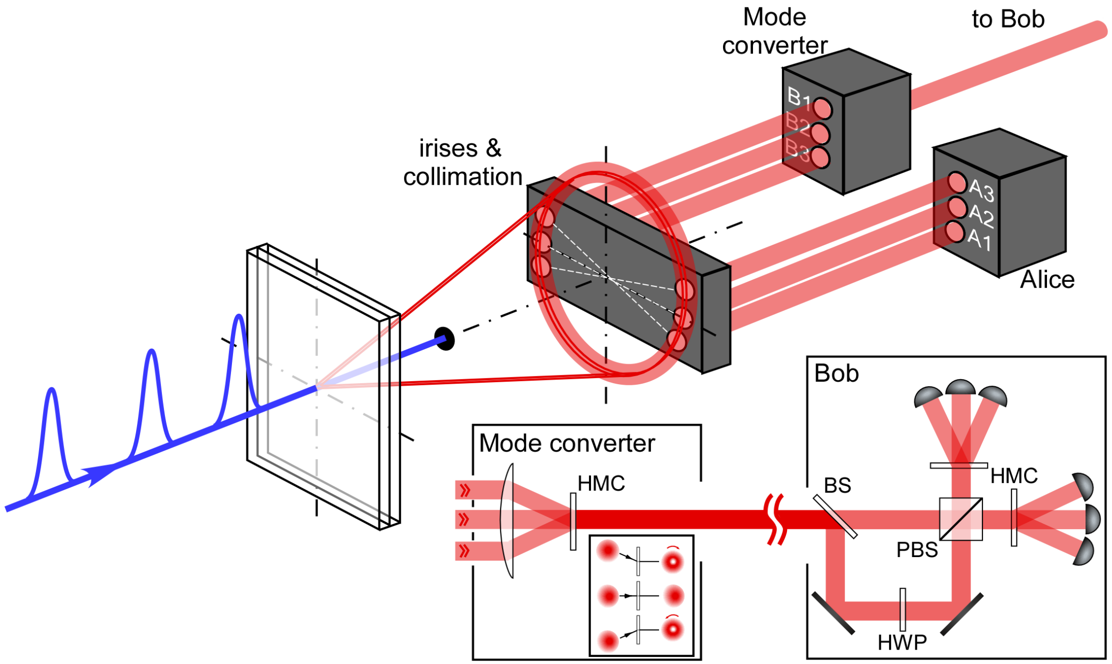
Convert different spatial (gaussian) modes into overlapping OAM-type modes (optimized for turbulence robustness).

Advantages:

- *Potentially simpler optical transmission system*
- *Bob can polarization analyze them all using same setup*



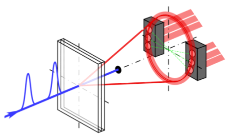
Use spatial modes as independent channels



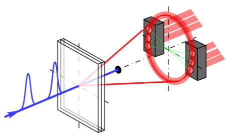
Potential problem: turbulence may 'mix' the channels, i.e., causing crosstalk (?less problematic than if info was encoded using the spatial modes?)

Solutions: *- choose crosstalk-robust states*

- use non-degenerate frequencies for 'adjacent' spatial modes, to further reduce state overlap



Bob Boyd on AOM sorters, turbulence…



Quantum state sorters and spatial mode converters

Need for quantum state sorters and spatial mode converters

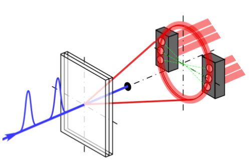
One approach to high-capacity QKD is to encode in the transverse degree of freedom (DoF) of the photon, using, for example states that carry orbital-angular momentum (OAM) such as the Laguerre-Gauss (LG) states.

Crucial Comment: This approach is NOT the baseline approach for our InPho team.

Nonetheless, transverse DOF relevant in two ways:

(1) Use to transmit many quantum channels through the same aperture

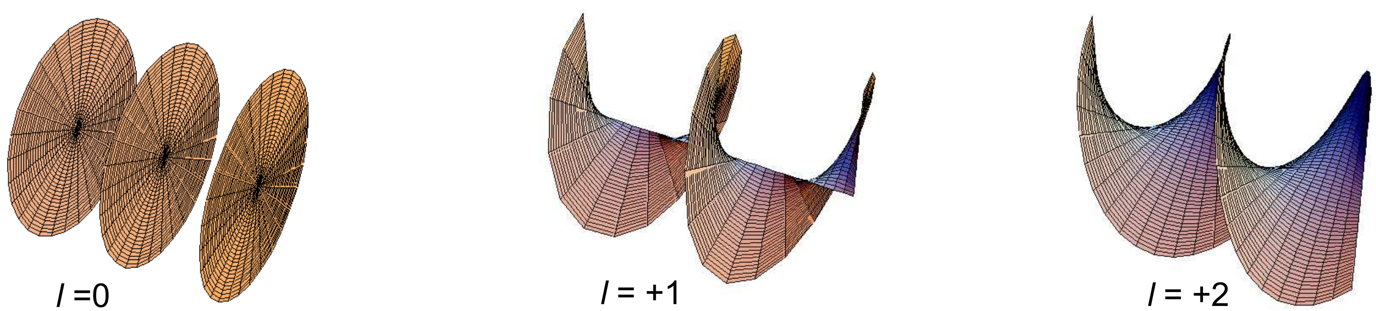
(2) Constitutes an alternative approach that might be exploited in future.



What Are the 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 $\exp(il\phi)$ and carry angular momentum of $l\hbar$ per photon. (Here ϕ is the azimuthal coordinate.)

Phase-front structure of some OAM states



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.

Basic idea (assuming OAM modes for definiteness)

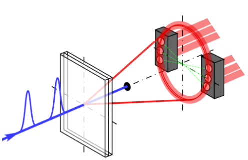
Alice's encoding makes use of OAM

(Generating single photons in an OAM state, if not easy, is at least straightforward)

Bob needs a sorter to separate each input OAM mode into a different output channel

Because Bob has only one photon, he can perform only one measurement in determining what state he has.

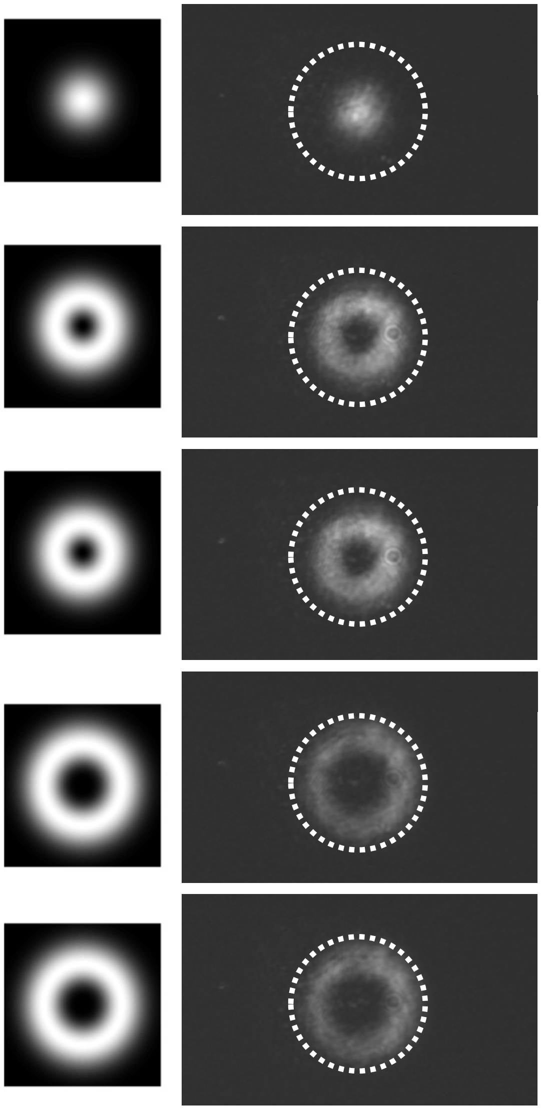
How to do this?



State Generation (d=5)

Basis 1 (LGs)

Theory Experiment



$$LG_{0,0}$$

$$LG_{1,0}$$

$$LG_{-1,0}$$

$$LG_{2,0}$$

$$LG_{-2,0}$$

Basis 2

Experiment Theory

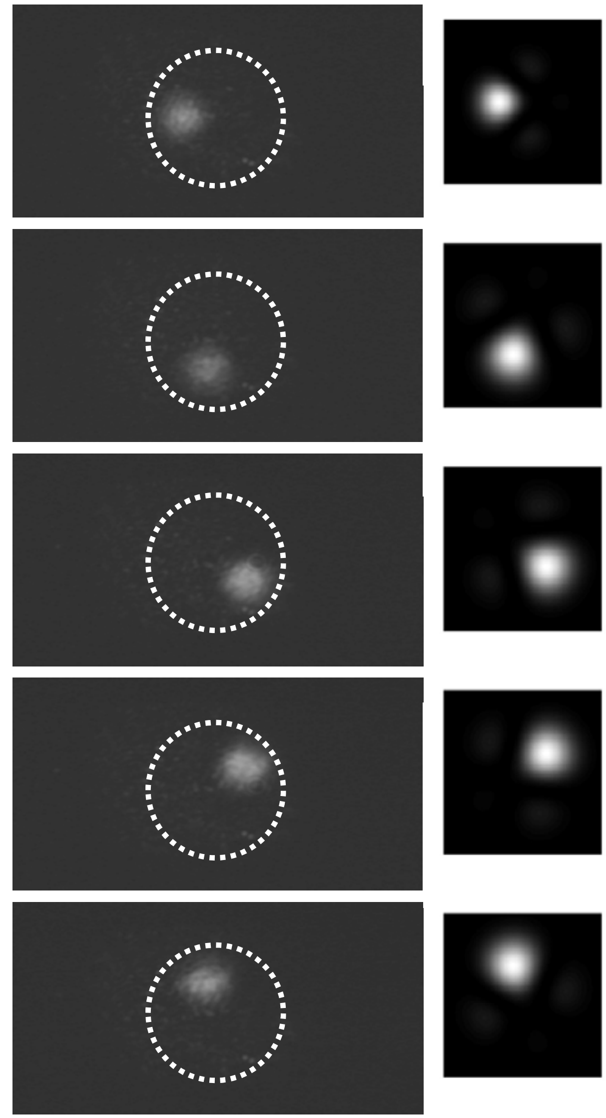
$$\frac{1}{\sqrt{5}}\sum_{l=-2}^{2} LG_{l,0}\, e^{i2\pi l/5}$$

$$\frac{1}{\sqrt{5}}\sum_{l=-2}^{2} LG_{l,0}\, e^{i4\pi l/5}$$

$$\frac{1}{\sqrt{5}}\sum_{l=-2}^{2} LG_{l,0}\, e^{i6\pi l/5}$$

$$\frac{1}{\sqrt{5}}\sum_{l=-2}^{2} LG_{l,0}\, e^{i8\pi l/5}$$

$$\frac{1}{\sqrt{5}}\sum_{l=-2}^{2} LG_{l,0}$$



Basic idea (assuming OAM modes for definiteness)

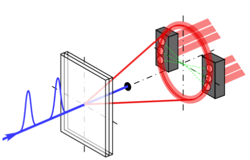
Alice's encoding makes use of OAM

(Generating single photons in an OAM state, if not easy, is at least straightforward)

Bob needs a sorter to separate each input OAM mode into a different output channel

Because Bob has only one photon, he can perform only one measurement in determining what state he has.

How to do this?



How to build a quantum state sorter?

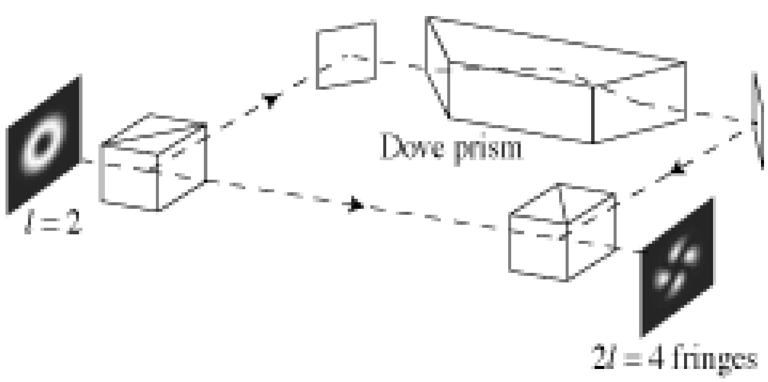
1. Use a thin hologram (widely believed that this will not work)

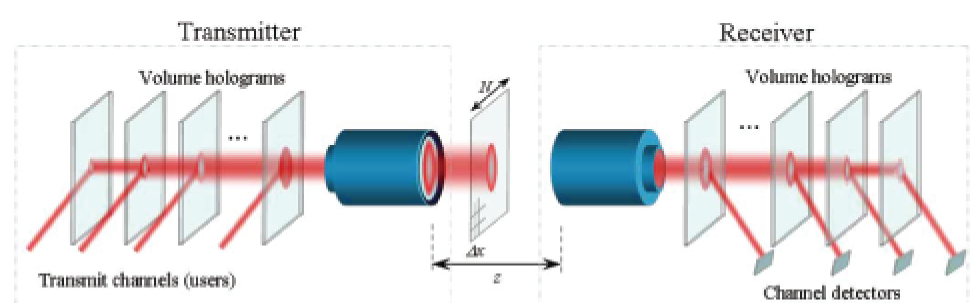
2. Use a thick hologram (seems plausible, but no one has yet made this work)

3. Use a cascade of (d-1) interferometers, each containing a Dove prism

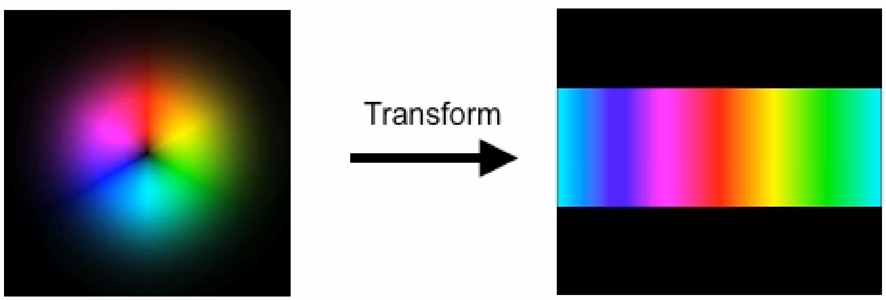
4. Use a diffractive optical element (DOE); inverse problem; what structure?

5. Mode reformatter (Padgett group, PRL in press)
   It works! What are its limitations?





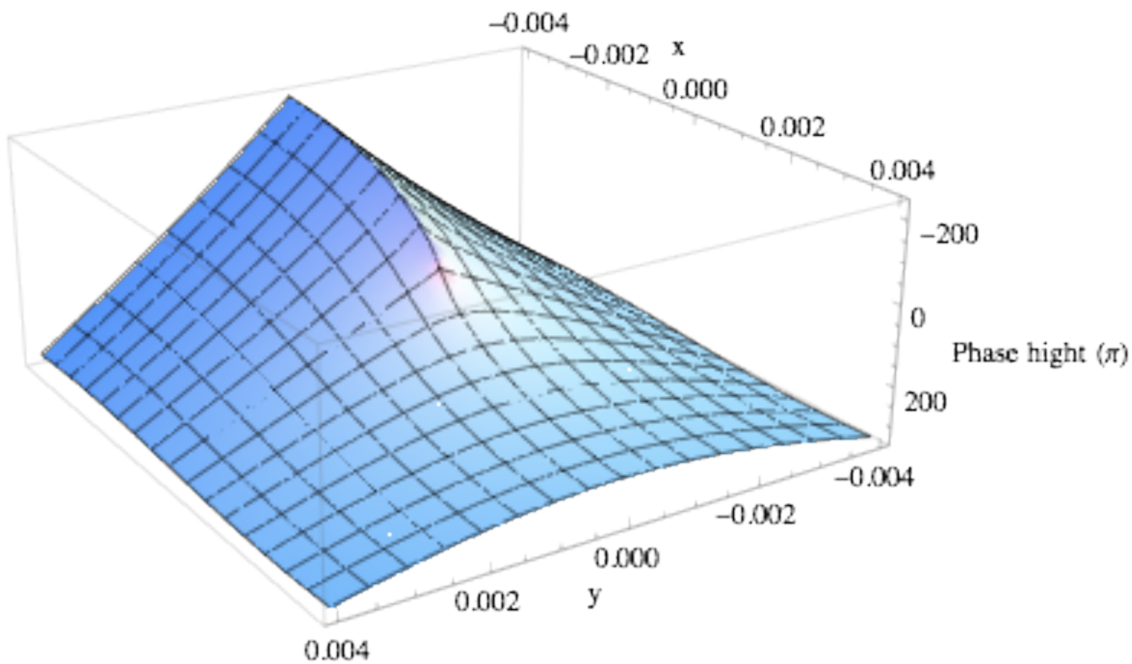
Turbulence-induced channel crosstalk in an orbital angular momentum-multiplexed free-space optical link, J. A. Anguita, M. A. Neifeld, and B. V. Vasic, Applied Optics 47, 2414 (2008).



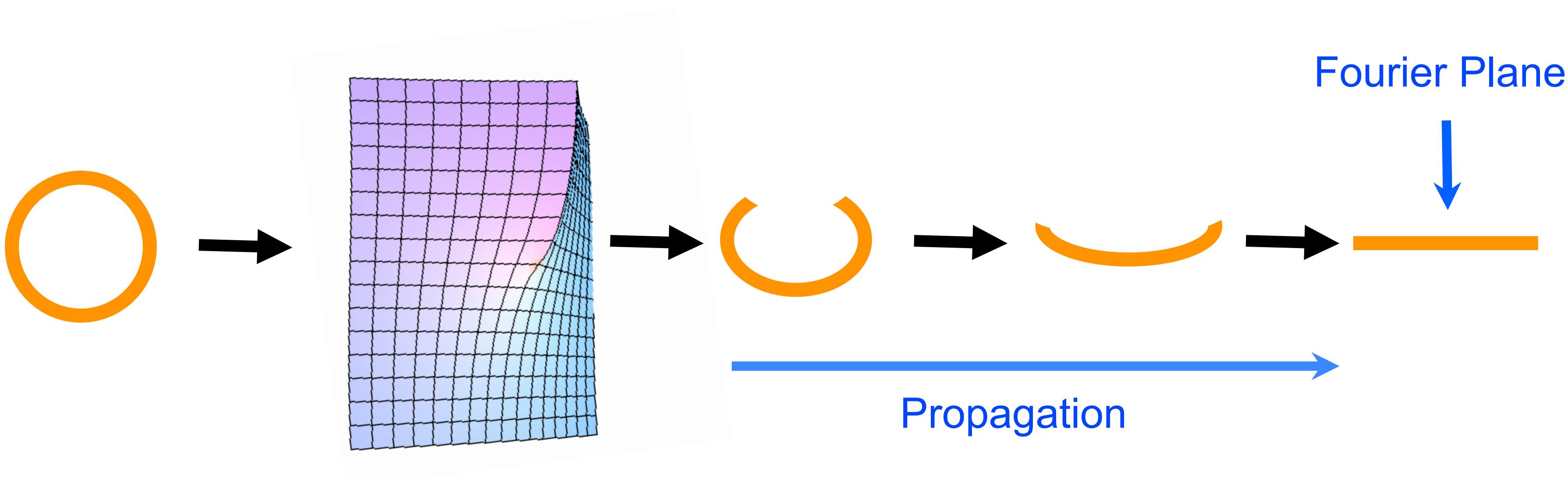
We "unwrap" the azimuthal phase distrubution to form a linear mapping.

Linear maps are easily sorted just using an ordinary lens.

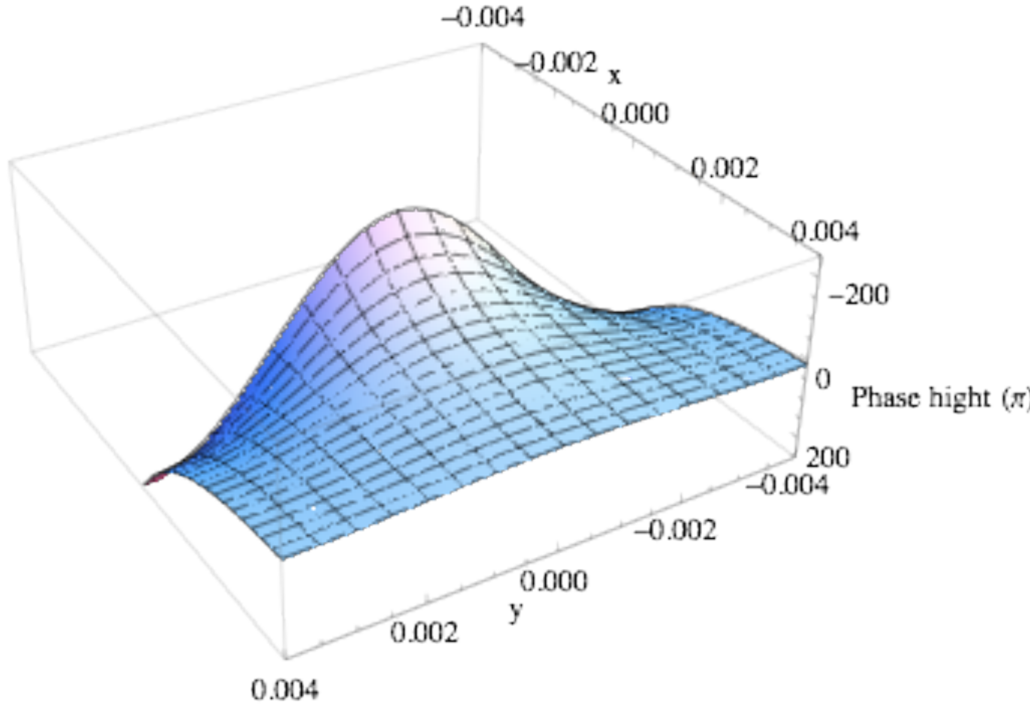
The surface to do this transformation looks like:



$$\phi_1(x,y) = \frac{2\pi a}{\lambda f}\left[y\arctan\left(\frac{y}{x}\right) - x\ln\left(\frac{\sqrt{x^2+y^2}}{b}\right) + x\right]$$


Fourier Plane
Propagation

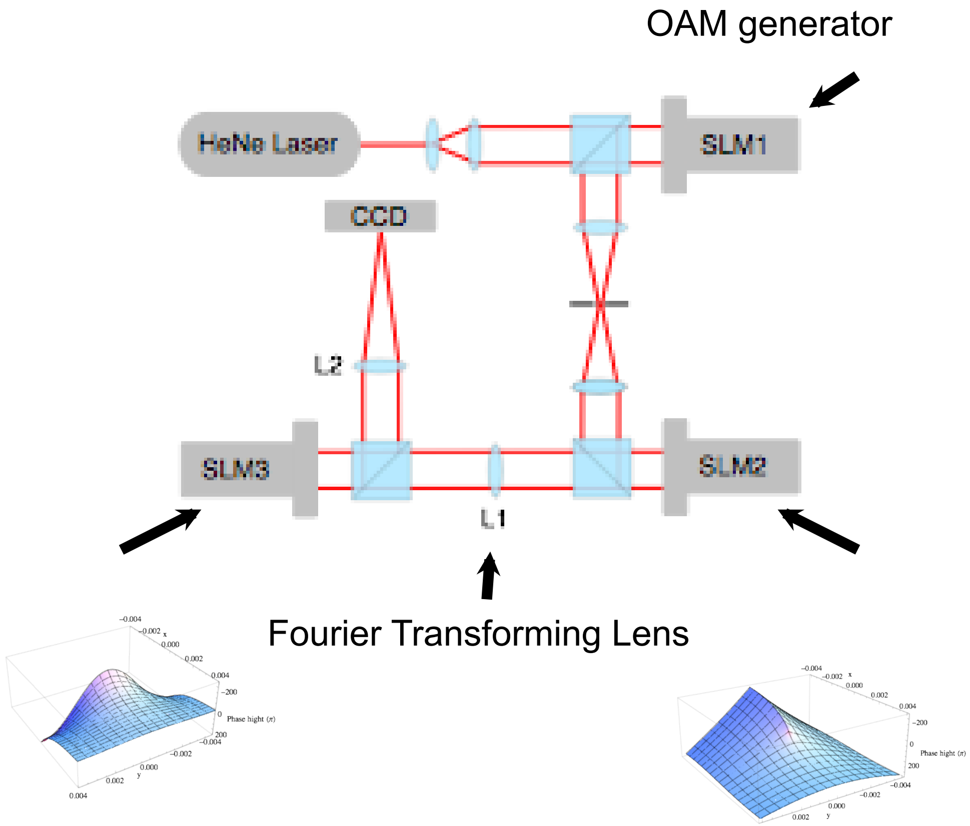
The surface to correct the phase looks like this:

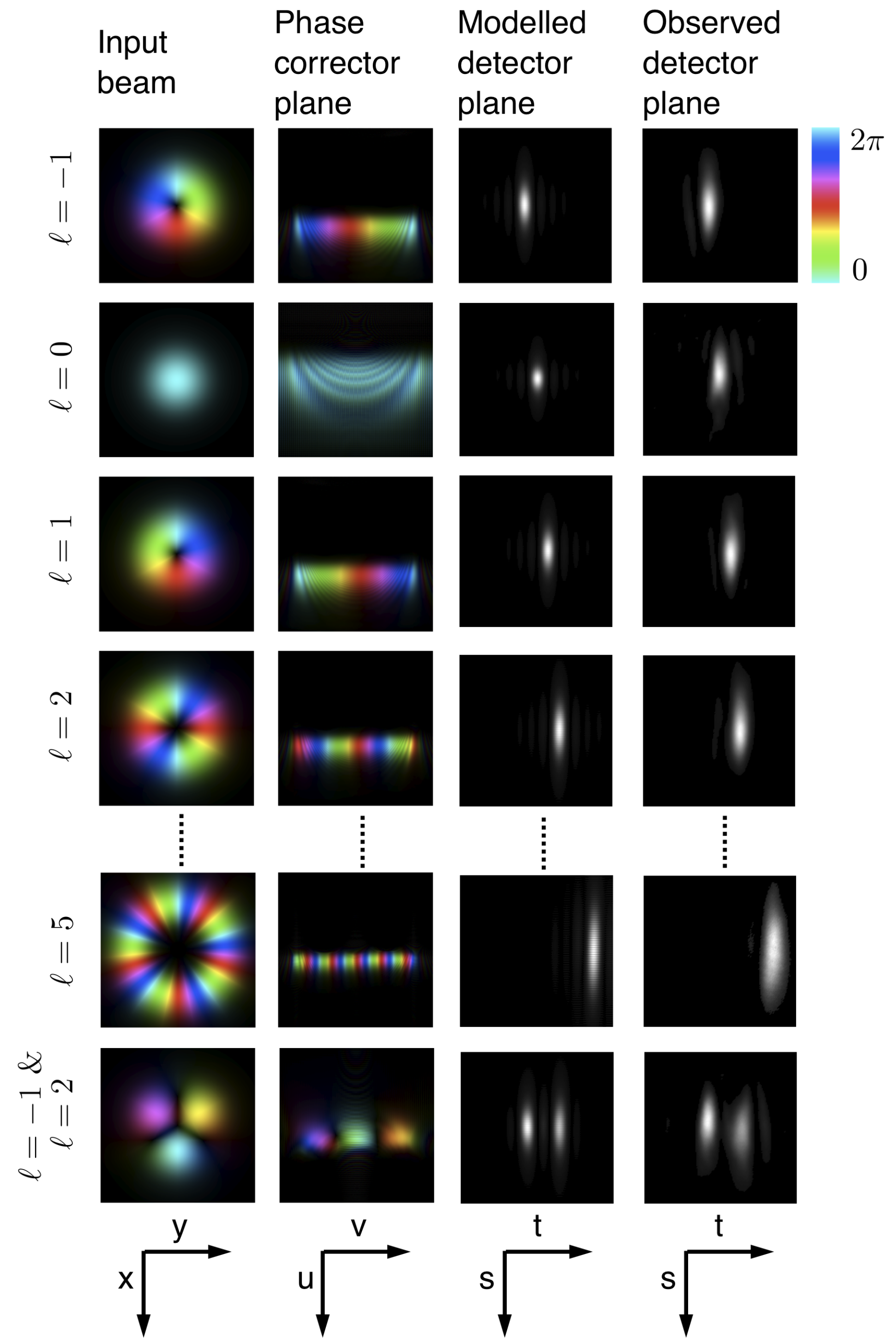


$$\phi_2(u,v) = -\frac{2\pi ab}{\lambda f}\exp\left(-\frac{u}{a}\right)\cos\left(\frac{v}{a}\right).$$

Proof of concept experiment

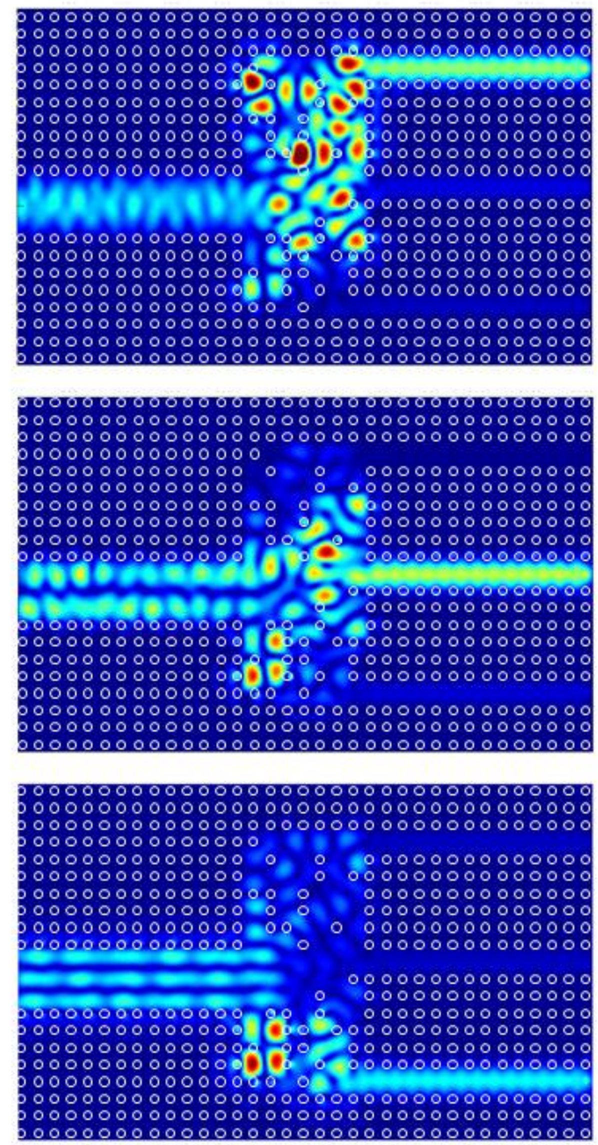
It works!:

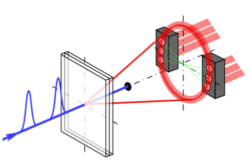




Fundamental limits to mode converters

- **Miller's limit theorem**
  - **provides general limits to the performance of linear optical components based on modal analysis (JOSA B 24, A1 (2007))**
- **Previous work**
  - **Explicit limits for 1D optical structures for**
    - **Pulse dispersive devices, Slow light**
  - **Existence proof design of compact mode converters**
- **Overall work planned on this program includes**
  - **extending previous work to get explicit results for 2D and 3D structures**
    - **explicit limits for monochromatic mode converters**
      - **e.g., limits to thin and thick "holograms"**
- **Future directions include**
  - **Multiple wavelength systems 2D and 3D systems, including**
    - **More restrictive limits for materials that are not themselves dispersive**
    - **Possible pulsed field mode and pulse converters**

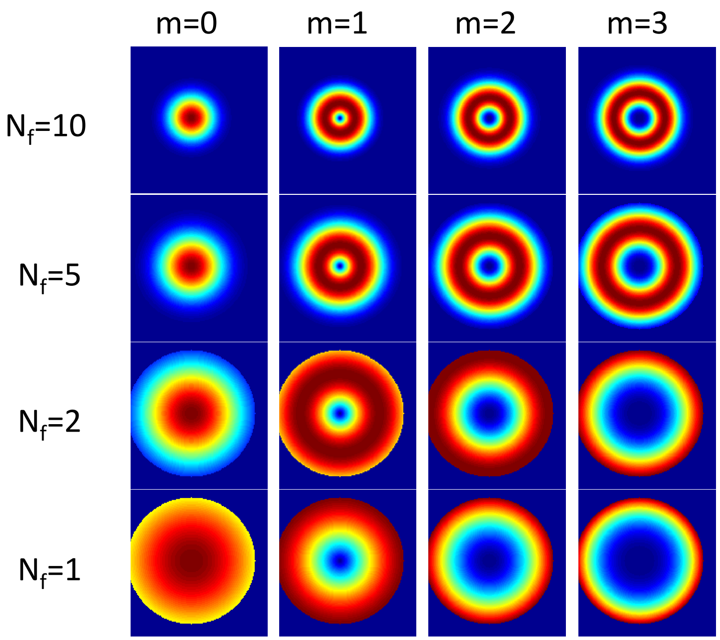


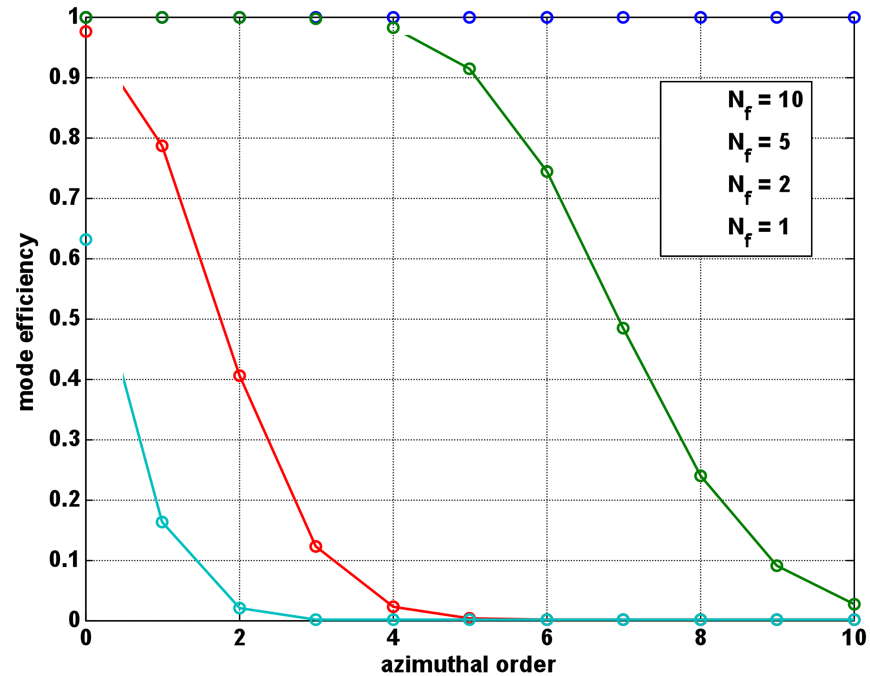


Influence of Atmospheric Turbulence on Quantum Communications: Project Overview

- Near term research concerned with:
  - Baseline Protocol (elementary propagation effects – polarization, dispersion, etc.)
  - Optimum transmission efficiency with minimum energy loss states
  - Entropy and information content associated with a free space propagation link
  - Reduced information content in presence of turbulence
  - Turbulence characteristics associated with horizontal path (SOR 2 mile site)
  - Scintillation and fading probability
- Advanced concepts
  - Preconditioned MUB states with minimum energy loss bases
  - Adaptive Optics (used only if required to sustain link channel capacity)
  - Filament exploitation in deep turbulence
- Experimental considerations
  - Laboratory experiments at U of R, Duke with support from tOSC
  - Field experiments when program is sufficiently mature (tOSC with support from team)
- Our present understanding supports conclusion that 256 time bins and 6 spatial parallel channels (through a single aperture) leads to more than 10 bits per photon in even presence of horizontal path turbulence (without AO)
- Continuing research will address added margin required for security and additional turbulence variability (fading, time varying statistics)

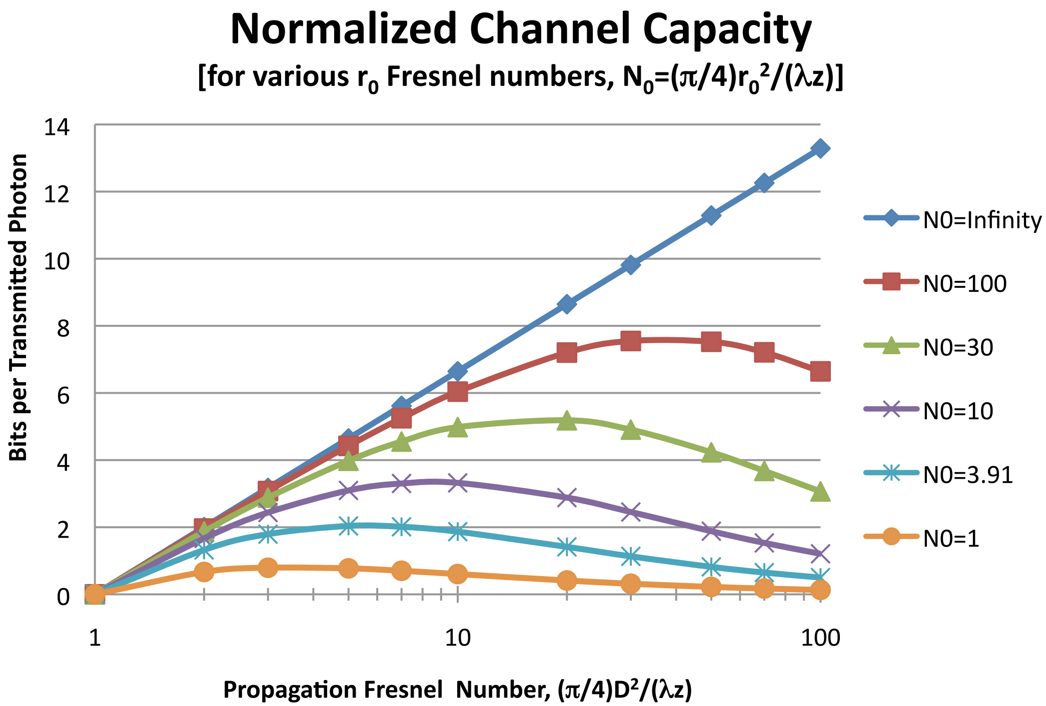
Protocol: Transmit Minimum Energy Loss States





- The minimum energy loss states have the functional form, $F_{nm}(r,\varphi)=f_{nm}(r)\exp(im\varphi)$, where the functional form of is controlled to minimize the energy loss for a propagation link defined by Fresnel number $N_f=(\pi/4)\, D_1 D_2/(\lambda z)$
- The left hand figure illustrates the amplitudes associated with the lowest loss states for each designated m and N_f
- The propagation efficiencies are illustrated in the right figure
- These states have interesting properties
  - They automatically self image as they propagate from transmitter to receiver
  - They are also eigenmodes of a resonator with phase conjugate mirrors
  - In the limit of a large Fresnel number they asymptote to Laguerre Gauss functions
  - In the limit of a small Fresnel number they asymptote to Prolate Spheroidal wave functions
- We also have developed Preconditioned MUB States that use these states as their basis

Normalized Transverse Channel Capacity Significantly Reduced by Atmospheric Turbulence



- For vacuum propagation the normalized channel capacity is (approximately) equal to $\log_2(N_f^2)$
- The number of parallel channels supported by a propagation link is N_f^2
- In the presence of turbulence the effective diameter is r_0 which can significantly limit the information content of the propagation link
- If one attempts to increase the diameter significantly beyond this value, turbulence induced aberrations dominate and further degrade the link
- For a case of interest, consider the SOR Two Mile Site (r_0=0.1m, λ=0.8μm, z=3200m, N_0=3.91)
- The optimum occurs at N_f=5.5 (D=0.12m) resulting in a normalized channel capacity of 2.05 bits per transmitted photon or four parallel channels

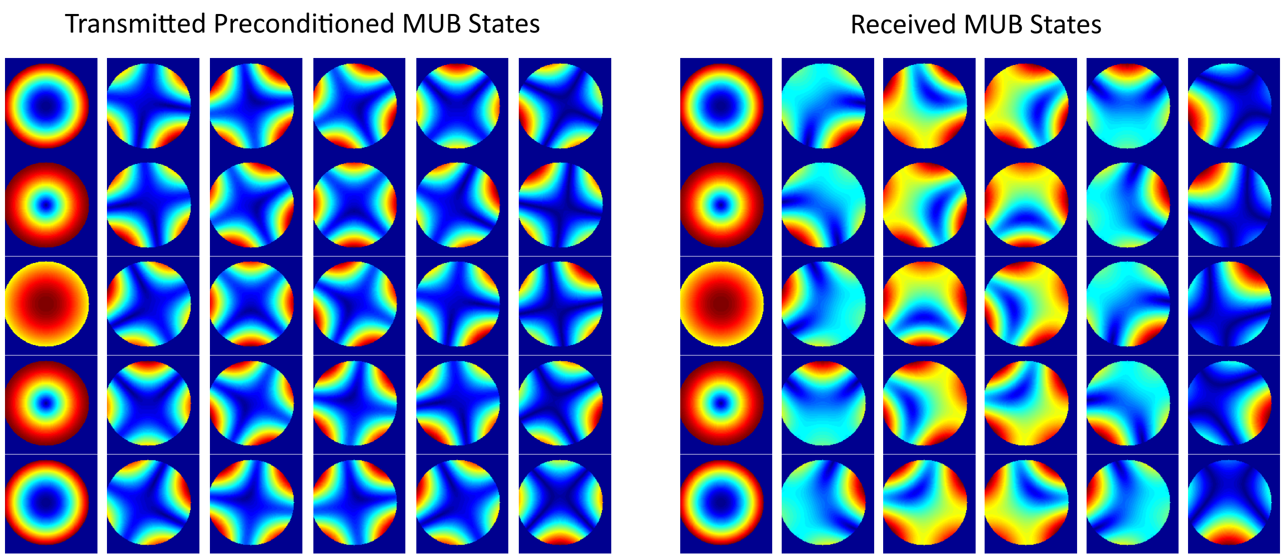
The Optical Sciences Company

The SOR Two Mile Site Provides a Typical Example of a Horizontal Path with Well Known Characteristics

C_n^2	1	2	5	10	20	50	$\times 10^{15}$
r_0	12.7	8.35	4.82	3.18	2.10	1.21	cm
ϑ_0	12.4	8.20	4.73	3.12	2.06	1.19	μrad
Rytov	0.0365	0.0731	0.183	0.365	0.731	1.83	
jitter	2.59	3.77	6.11	8.73	12.4	19.7	μrad
f_G	30.4	46	80	121	183	318	Hz
f_{TG}	5.19	7.56	12.3	17.5	24.9	39.5	Hz
D_{opt}	0.132	0.111	0.095	0.089	0.086	0.084	m
D_{opt}/r_0	1.04	1.33	1.97	2.80	4.09	6.97	
C_{opt}	2.66	1.64	0.744	0.369	0.172	0.059	bits/photon

- DARPA has expressed an interest in assessing quantum communication over a horizontal path
- As an example we consider the SOR Two Mile Site
- The C_n^2 varies from almost as low as 10^{-16} to almost as high as 10^{-13} depending upon time day and time of year
- The above table illustrates the important turbulence parameters for conditions spanning this range (assuming λ=0.8μm, z=3200m)
- We note that as the Rytov number approaches 0.2|1 we experience Branch Points|Deep Turbulence
- We also illustrate the optimum diameter and channel capacity for these conditions

Advanced Concepts: Preconditioned MUB States



- We are developing a new protocol involving Preconditioned MUB States that use the minimum energy loss states as their basis states
- The initial functional form of these state is chosen so that upon propagation the states have the desired MUB character in the receiver plane
- The above figures pertain to a Fresnel number of one and a dimension of five
- For high dimensions and low Fresnel numbers (N_f=1, d=5, b=6), the preconditioned MUB states look quite similar except for the fundamental basis
- 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

But is it secure?

Eve does not have a QND measurement:

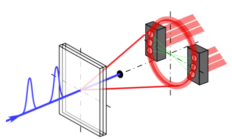
- *Eve has to absorb the photon to measure its timeslot.*
- *She can send Bob a fresh photon in the correct timeslot*, but she cannot mimic the QM correlations of the expected Bell state.*
- *Standard QKD error correction + priv. amplification should apply.§*

Eve does *have a QND measurement†:*

- *Need to measure in an appropriate MUB*

$$\left|\theta_m\right\rangle = N^{-1/2}\sum_{n=0}^{N}\exp\left(in\theta_m\right)\left|t_n\right\rangle \qquad \theta_m = \theta_0 + \frac{2\pi m}{N} \qquad \sum_{n=0}^{N}\left|t_n\right\rangle\left|t_n\right\rangle = \sum_{m=0}^{N}\left|\theta_m\right\rangle\left|-\theta_m\right\rangle$$

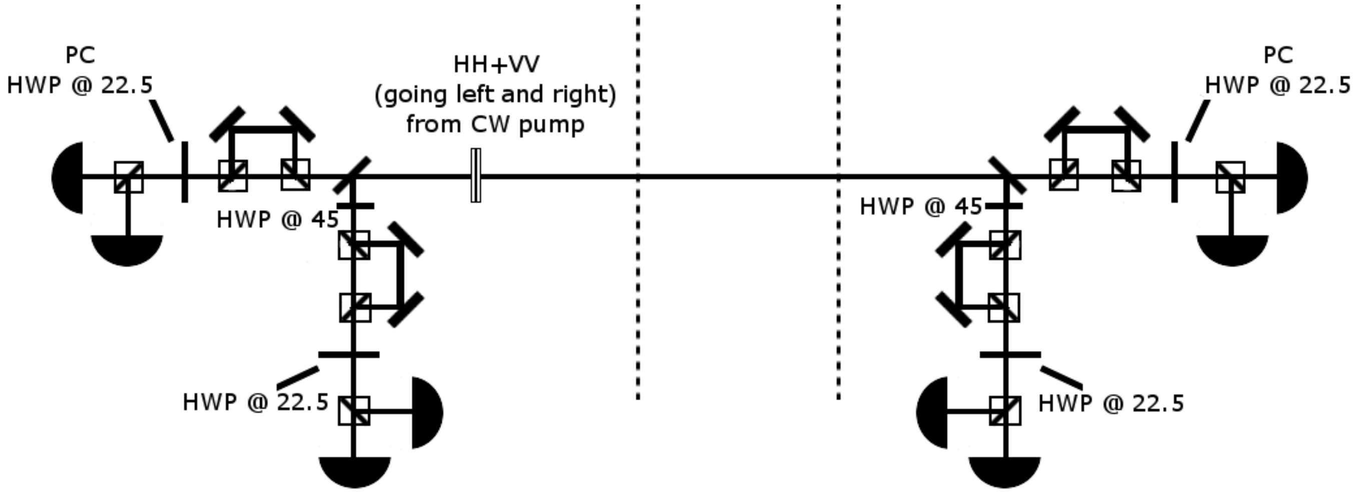
- *Optimal implementation still under consideration…*



* This requires extremely fast processing on her end, to avoid delay…
§ We will need to account for info. released to identify pol. correlations (~1 bit)
† Needs to be polarization-preserving QND!

Temporal MUB measurement

Version 1:



Measure superpositions of adjacent *time bins:*

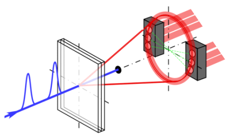
$$\left(\langle t_i| + \langle t_{i+1}|\right)$$

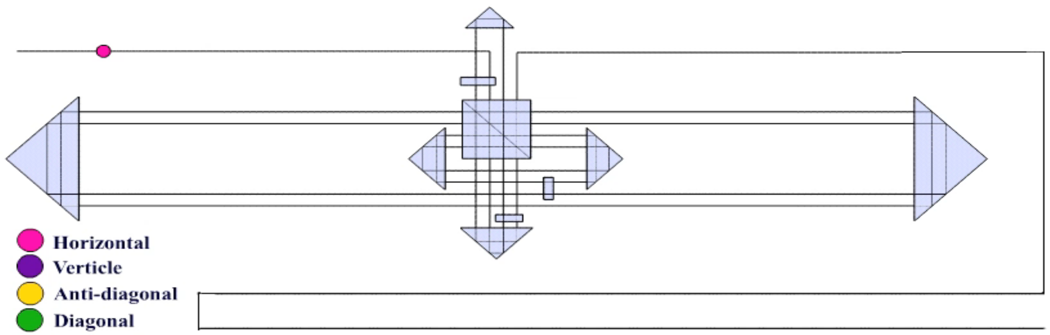
- *"Franson" interference (PGK et al. PRA '90, '93, '96)*
- *~easy to implement; by induction **all** time bins coherent*
- *probably not very eavesdropper sensitive*

Version 2:

Measure superposition of all *time bins:*

$$|\theta_m\rangle = N^{-1/2}\sum_{n=0}^{N}\exp\left(in\theta_m\right)|t_n\rangle$$

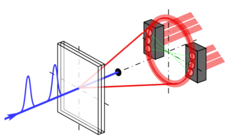




Security concerns

Benefits of time-encoding/polarization checking

- *Polarization checking is easy; can even check* Bell inequalities; *typical error rates quite low, e.g., F > 99%.*
- Every *photon can be used to check for Eve (cf. Ekert protocol)*
- Every *photon contributes to key (cf. BB84 [1/2] or SSP [1/3])*
- *Non-polarization sensitive QND far from realization (best QND measurements to date on microwave photons [Haroche, Martinis])*
- *Errors in time-bin not assumed to be from Eve—her measurements needn't disrupt timing at all [if she can implement an unnoticed delay; likely hard in FSO path (since system is timed to <150 ps)]*
    - *Do not have to account for x5 overhead to account for Priv. Amp. (due to* timing *errors).*
    - *Just need usual classical error detection/correction*
- But *one pol. error means Eve could know* all *bits for that photon*
    - *e.g., 1% BER → Eve looked at ~4% of the photons (and knows their bits completely) → input to Privacy Amplification.*



Security concerns: 'Bit-forcing'

If we only verify polarization, we may be susceptible to "bit-forcing":

Eve blocks the channel for some time bins

→ eliminates possible bit choices, gains information

But the cost to Eve is high:

To force m of N possible bits (2^N bins), Eve must block $N(1-0.5^m)$

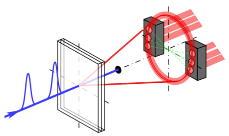
E.g., to determine 1 bit out of 10, she must block half of the bins

to determine 5 bits out of 10, she must block 97%.

This intrusion can certainly be detected, e.g., using decoy pulses with different amplitudes.*

Open questions:

- *What's the most efficient (per photon) decoy encoding?*
- *What is the optimal implementation of temporal MUB?*
- *What is the impact of hyper-entanglement on security?*
- *What is the optimal encoding in DOFs (q-dits vs channels)?*



*H.-K. Lo, X. Ma, and K. Chen. PRL **94**, 230504 (2005)