REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
06-10-2015	Final Report	12-Aug-2010 - 30-Jun-2014

4. TITLE AND SUBTITLE
Final Report: Information on a Photon: Free-Space Quantum Communication (InPho: FSQC)

5a. CONTRACT NUMBER
W911NF-10-1-0395

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
0D10BH

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHORS
Daniel J Gauthier

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Duke University
2200 West Main Street
Suite 710
Durham, NC 27705 -4010

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
58495-PH-DRP.92

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
The investigators are developing a free-space quantum communication system that improves both the photon efficiency (long term goal of 10 bits per photon) and communication rate (long term goal of 1 Gbit/s). To achieve these worldrecord results, the system will rely on hyperentanglement in which multiple degrees of freedom (polarization and time/frequency) of the photon are entangled to transmit multiple secret bits per photon and independent communication channels using the transverse spatial degree of freedom will be used to achieve high communication rates. The investigators have achieved a spatial heralding efficiency of >90% in the hyperentangled

15. SUBJECT TERMS
quantum key distribution, entanglement, single-photon detection, high-dimensional Hilbert space, orbital angular momentum of light, atmospheric turbulence, optical mode conversion

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
UU	UU	UU	UU		Daniel Gauthier
					19b. TELEPHONE NUMBER: 919-660-2511

Report Title

Final Report: Information on a Photon: Free-Space Quantum Communication (InPho: FSQC)

ABSTRACT

The investigators are developing a free-space quantum communication system that improves both the photon efficiency (long term goal of 10 bits per photon) and communication rate (long term goal of 1 Gbit/s). To achieve these worldrecord results, the system will rely on hyperentanglement in which multiple degrees of freedom (polarization and time/frequency) of the photon are entangled to transmit multiple secret bits per photon and independent communication channels using the transverse spatial degree of freedom will be used to achieve high communication rates. The investigators have achieved a spatial heralding efficiency of >90% in the hyperentangled source, distributed a quantum key with 8.3 bits/photon at a rate of 67 kbit/s and 2.2 bits/photon at a rate of 12.6 Mbits/s in a single channel, a source brightness of over 100 million photons/s into a single mode, developed single photon counting detectors with >80% quantum efficiency and jitter <120 ps and explored methods for reducing detector after pulsing, evaluated commercial time taggers for the system, devised an improved error correction protocol, improved the performance of a sorter for orbital angular momentum modes, developed a method for arbitrary sorting of spatial modes, assessed the strength of atmospheric turbulence over a 1 km horizontal path, assessed multi-pixel detectors for single-photon counting, and developed new method for securing time bin quantum states.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received	Paper
10/05/2015 50.00	Michael A. Wayne, Alessandro Restelli, Joshua C. Bienfang, Paul G. Kwiat. Afterpulse Reduction Through Prompt Quenching in Silicon Reach-Through Single-Photon Avalanche Diodes, Journal of Lightwave Technology, (11 2014): 4097. doi: 10.1109/JLT.2014.2346736
10/05/2015 90.00	Ryan E. Warburton, Frauke Izdebski, Christian Reimer, Jonathan Leach, David G. Ireland, Miles Padgett, Gerald S. Buller. Single-photon position to time multiplexing using a fiber array, Optics Express, (01 2011): 2670. doi: 10.1364/OE.19.002670
10/05/2015 89.00	Adetunmise C. Dada, Jonathan Leach, Gerald S. Buller, Miles J. Padgett, Erika Andersson. Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities, Nature Physics, (05 2011): 677. doi: 10.1038/nphys1996
10/05/2015 88.00	Gregorius C. G. Berkhout, Martin P. J. Lavery, Miles J. Padgett, Marco W. Beijersbergen. Measuring orbital angular momentum superpositions of light by mode transformation, Optics Letters, (05 2011): 1863. doi: 10.1364/OL.36.001863
10/05/2015 87.00	Martin P J Lavery, Angela Dudley, Andrew Forbes, Johannes Courtial, Miles J Padgett. Robust interferometer for the routing of light beams carrying orbital angular momentum, New Journal of Physics, (09 2011): 93014. doi: 10.1088/1367-2630/13/9/093014
10/05/2015 86.00	J. Leach, R. E. Warburton, D. G. Ireland, F. Izdebski, S. M. Barnett, A. M. Yao, G. S. Buller, M. J. Padgett. Quantum correlations in position, momentum, and intermediate bases for a full optical field of view, Physical Review A, (01 2012): 13827. doi: 10.1103/PhysRevA.85.013827
10/05/2015 85.00	D Giovannini, F M Miatto, J Romero, S M Barnett, J P Woerdman, M J Padgett. Determining the dimensionality of bipartite orbital-angular-momentum entanglement using multi-sector phase masks, New Journal of Physics, (07 2012): 73046. doi: 10.1088/1367-2630/14/7/073046
10/05/2015 84.00	F. M. Miatto, D. Giovannini, J. Romero, S. Franke-Arnold, S. M. Barnett, M. J. Padgett. Bounds and optimisation of orbital angular momentum bandwidths within parametric down-conversion systems, The European Physical Journal D, (07 2012): 178. doi: 10.1140/epjd/e2012-20736-x
10/05/2015 83.00	J Romero, D Giovannini, M G McLaren, E J Galvez, A Forbes, M J Padgett. Orbital angular momentum correlations with a phase-flipped Gaussian mode pump beam, Journal of Optics, (08 2012): 85401. doi: 10.1088/2040-8978/14/8/085401
10/05/2015 82.00	Angela Dudley, Thandeka Mhlanga, Martin Lavery, Andre McDonald, Filippus S. Roux, Miles Padgett, Andrew Forbes. Efficient sorting of Bessel beams, Optics Express, (01 2013): 165. doi: 10.1364/OE.21.000165
10/05/2015 81.00	D. Giovannini, J. Romero, J. Leach, A. Dudley, A. Forbes, M. J. Padgett. Characterization of High-Dimensional Entangled Systems via Mutually Unbiased Measurements, Physical Review Letters, (04 2013): 143601. doi: 10.1103/PhysRevLett.110.143601
10/05/2015 80.00	Mhlambululi Mafu, Angela Dudley, Sandeep Goyal, Daniel Giovannini, Melanie McLaren, Miles J. Padgett, Thomas Konrad, Francesco Petruccione, Norbert Lütkenhaus, Andrew Forbes. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases, Physical Review A, (09 2013): 32305. doi: 10.1103/PhysRevA.88.032305

10/05/2015 79.00 Moshe J. Willner, Hao Huang, Nisar Ahmed, Guodong Xie, Yongxiong Ren, Yan Yan, Martin P. J. Lavery, Miles J. Padgett, Moshe Tur, Alan E. Willner. Reconfigurable orbital angular momentum and polarization manipulation of 100??Gbit/s QPSK data channels,
Optics Letters, (12 2013): 5240. doi: 10.1364/OL.38.005240

10/05/2015 78.00 Yongxiong Ren, Hao Huang, Guodong Xie, Nisar Ahmed, Yan Yan, Baris I. Erkmen, Nivedita Chandrasekaran, Martin P. J. Lavery, Nicholas K. Steinhoff, Moshe Tur, Samuel Dolinar, Mark Neifeld, Miles J. Padgett, Robert W. Boyd, Jeffrey H. Shapiro, Alan E. Willner. Atmospheric turbulence effects on the performance of a free space optical link employing orbital angular momentum multiplexing,
Optics Letters, (10 2013): 4062. doi: 10.1364/OL.38.004062

10/05/2015 77.00 Hao Huang, Guodong Xie, Yan Yan, Nisar Ahmed, Yongxiong Ren, Yang Yue, Dvora Rogawski, Moshe J. Willner, Baris I. Erkmen, Kevin M. Birnbaum, Samuel J. Dolinar, Martin P. J. Lavery, Miles J. Padgett, Moshe Tur, Alan E. Willner. 100 Tbit/s free-space data link enabled by three-dimensional multiplexing of orbital angular momentum, polarization, and wavelength,
Optics Letters, (01 2014): 197. doi: 10.1364/OL.39.000197

10/05/2015 76.00 Hao Huang, Yongxiong Ren, Guodong Xie, Yan Yan, Yang Yue, Nisar Ahmed, Martin P. J. Lavery, Miles J. Padgett, Sam Dolinar, Moshe Tur, Alan E. Willner. Tunable orbital angular momentum mode filter based on optical geometric transformation,
Optics Letters, (03 2014): 1689. doi: 10.1364/OL.39.001689

10/05/2015 73.00 Martin P. J. Lavery, Miles J. Padgett, Stephen M. Barnett, Fiona C. Speirits. Optical angular momentum in a rotating frame,
Optics Letters, (05 2014): 2944. doi: 10.1364/OL.39.002944

10/05/2015 75.00 Reuben S. Aspden, Daniel S. Tasca, Andrew Forbes, Robert W. Boyd, Miles J. Padgett. Experimental demonstration of Klyshko's advanced-wave picture using a coincidence-count based, camera-enabled imaging system,
Journal of Modern Optics, (03 2014): 547. doi: 10.1080/09500340.2014.899645

10/05/2015 74.00 Yongxiong Ren, Guodong Xie, Hao Huang, Changjing Bao, Yan Yan, Nisar Ahmed, Martin P. J. Lavery, Baris I. Erkmen, Samuel Dolinar, Moshe Tur, Mark A. Neifeld, Miles J. Padgett, Robert W. Boyd, Jeffrey H. Shapiro, Alan E. Willner. Adaptive optics compensation of multiple orbital angular momentum beams propagating through emulated atmospheric turbulence,
Optics Letters, (05 2014): 2845. doi: 10.1364/OL.39.002845

10/05/2015 72.00 Megan Agnew, Jonathan Leach, Melanie McLaren, F. Stef Roux, Robert W. Boyd. Tomography of the quantum state of photons entangled in high dimensions,
Physical Review A, (12 2011): 62101. doi: 10.1103/PhysRevA.84.062101

10/05/2015 71.00 M. Agnew, J. Leach, R.W. Boyd. Observation of entanglement witnesses for orbital angular momentum states,
The European Physical Journal D, (06 2012): 156. doi: 10.1140/epjd/e2012-30057-9

10/05/2015 70.00 Mohammad Mirhosseini, Mehul Malik, Zhimin Shi, Robert W. Boyd. Efficient separation of the orbital angular momentum eigenstates of light,
Nature Communications, (11 2013): 2781. doi: 10.1038/ncomms3781

10/05/2015 69.00 Mohammad Mirhosseini, Omar S. Magaña-Loaiza, Changchen Chen, Brandon Rodenburg, Mehul Malik, Robert W. Boyd. Rapid generation of light beams carrying orbital angular momentum,
Optics Express, (12 2013): 30196. doi: 10.1364/OE.21.030196

10/05/2015 68.00 Mehul Malik, Mohammad Mirhosseini, Martin P. J. Lavery, Jonathan Leach, Miles J. Padgett, Robert W. Boyd. Direct measurement of a 27-dimensional orbital-angular-momentum state vector,
Nature Communications, (01 2014): 3115. doi: 10.1038/ncomms4115

10/05/2015 67.00 Ebrahim Karimi, Sebastian A Schulz, Israel De Leon, Hammam Qassim, Jeremy Upham, Robert W Boyd. Generating optical orbital angular momentum at visible wavelengths using a plasmonic metasurface,
Light: Science & Applications, (05 2014): 167. doi: 10.1038/lsa.2014.48

10/05/2015 66.00 Daniel Giovannini, Eliot Bolduc, Nicolas Bent, Filippo M. Miatto, Miles J. Padgett, Robert W. Boyd, Ebrahim Karimi. Exploring the quantum nature of the radial degree of freedom of a photon via Hong-Ou-Mandel interference,
Physical Review A, (01 2014): 13829. doi: 10.1103/PhysRevA.89.013829

10/05/2015 65.00 Hammam Qassim, Filippo M. Miatto, Juan P. Torres, Miles J. Padgett, Ebrahim Karimi, Robert W. Boyd. Limitations to the determination of a Laguerre–Gauss spectrum via projective, phase-flattening measurement,
Journal of the Optical Society of America B, (04 2014): 20. doi: 10.1364/JOSAB.31.000A20

10/05/2015 64.00 Mehul Malik, Justin Dressel, Filippo M. Miatto, Andrew N. Jordan, Robert W. Boyd. : Understanding quantum weak values: Basics and applications,
Reviews of Modern Physics, (03 2014): 307. doi: 10.1103/RevModPhys.86.307

10/05/2015 63.00 Brandon Rodenburg, Robert W. Boyd, Omar S. Magaña-Loaiza, Mohammad Mirhosseini. Amplification of Angular Rotations Using Weak Measurements,
Physical Review Letters, (05 2014): 200401. doi: 10.1103/PhysRevLett.112.200401

10/05/2015 62.00 Omar S Magaña-Loaiza, Nicholas K Steinhoff, Glenn A Tyler, Robert W Boyd, Michael Yanakas, Laura Maher, Brandon Rodenburg, Mohammad Mirhosseini, Mehul Malik. Simulating thick atmospheric turbulence in the lab with application to orbital angular momentum communication,
New Journal of Physics, (03 2014): 33020. doi: 10.1088/1367-2630/16/3/033020

10/05/2015 61.00 Pierre Wahl, Takuo Tanemura, Nathalie Vermeulen, Jürgen Van Erps, David A. B. Miller, Hugo Thienpont. Design of large scale plasmonic nanoslit arrays for arbitrary mode conversion and demultiplexing,
Optics Express, (01 2014): 646. doi: 10.1364/OE.22.000646

10/05/2015 59.00 Thomas Brougham, Stephen M Barnett. Cavity-enabled high-dimensional quantum key distribution,
Journal of Physics B: Atomic, Molecular and Optical Physics, (08 2014): 155501. doi: 10.1088/0953-4075/47/15/155501

10/05/2015 58.00 Thomas Brougham, Stephen M. Barnett. Mutually unbiased measurements for high-dimensional time-bin–based photonic states,
EPL (Europhysics Letters), (11 2013): 30003. doi: 10.1209/0295-5075/104/30003

10/05/2015 56.00 Daniel J. Gauthier, Yu-Po Wong, Hannah E. Guilbert. Observation of elliptical rings in type-I spontaneous parametric downconversion,
Journal of the Optical Society of America B, (09 2015): 2096. doi: 10.1364/JOSAB.32.002096

10/05/2015 55.00 Hannah E. Guilbert, Daniel J. Gauthier. Enhancing Heralding Efficiency and Biphoton Rate in Type-I Spontaneous Parametric Down-Conversion,
IEEE Journal of Selected Topics in Quantum Electronics, (05 2015): 6400610. doi: 10.1109/JSTQE.2014.2375161

10/05/2015 49.00 Ting-Yu Huang, Shiraz Hazrat, Radhika Dirks, Onur Hosten, Stephan Quint, Dickson Thian, Paul G. Kwiat, David Schmid. Adjustable and robust methods for polarization-dependent focusing,
Optics Express, (06 2013): 15538. doi: 10.1364/OE.21.015538

10/05/2015 51.00 Daniel J. Gauthier. Comment on “Generalized grating equation for virtually imaged phased-array spectral dispersers”,
Applied Optics, (11 2012): 8184. doi: 10.1364/AO.51.008184

11/05/2013 20.00 Martin P. J. Lavery, David J. Robertson, Gregorius C. G. Berkhout, Gordon D. Love, Miles J. Padgett, Johannes Courtial. Refractive elements for the measurement of the orbital angular momentum of a single photon,
Optics Express, (01 2012): 0. doi: 10.1364/OE.20.002110

11/05/2013 21.00 Heedeuk Shin, Kam Wai Clifford Chan, Hye Jeong Chang, Robert W. Boyd. Quantum Spatial Superresolution by Optical Centroid Measurements,
Physical Review Letters, (8 2011): 0. doi: 10.1103/PhysRevLett.107.083603

11/05/2013 22.00 F. M. Miatto, T. Brougham, A. M. Yao. Cartesian and polar Schmidt bases for down-converted photons,
The European Physical Journal D, (7 2012): 0. doi: 10.1140/epjd/e2012-30063-y

11/05/2013 23.00 Jonathan Leach, Eliot Bolduc, Daniel J. Gauthier, Robert W. Boyd. Secure information capacity of photons entangled in many dimensions,
Physical Review A, (6 2012): 0. doi: 10.1103/PhysRevA.85.060304

11/05/2013 24.00 G.S. Buller, M.P. Edgar, D.S. Tasca, F. Izdebski, R.E. Warburton, J. Leach, M. Agnew, R.W. Boyd, M.J. Padgett. Imaging high-dimensional spatial entanglement with a camera,
Nature Communications, (8 2012): 0. doi: 10.1038/ncomms1988

11/05/2013 25.00 Mehul Malik, Malcolm O'Sullivan, Brandon Rodenburg, Mohammad Mirhosseini, Jonathan Leach, Martin P. J. Lavery, Miles J. Padgett, Robert W. Boyd. Influence of atmospheric turbulence on optical communications using orbital angular momentum for encoding,
Optics Express, (05 2012): 0. doi: 10.1364/OE.20.013195

11/05/2013 27.00 Martin P J Lavery, David J Robertson, Anna Sponselli, Johannes Courtial, Nicholas K Steinhoff, Glenn A Tyler, Alan E Wilner, Miles J Padgett. Efficient measurement of an optical orbital-angular-momentum spectrum comprising more than 50 states,
New Journal of Physics, (01 2013): 0. doi: 10.1088/1367-2630/15/1/013024

11/05/2013 28.00 Malcolm N. O'Sullivan, Mohammad Mirhosseini, Mehul Malik, Robert W. Boyd. Near-perfect sorting of orbital angular momentum and angular position states of light,
Optics Express, (10 2012): 0. doi: 10.1364/OE.20.024444

11/05/2013 29.00 David A. B. Miller. All linear optical devices are mode converters,
Optics Express, (10 2012): 0. doi: 10.1364/OE.20.023985

11/05/2013 30.00 David A. B. Miller. How complicated must an optical component be?,
Journal of the Optical Society of America A, (01 2013): 0. doi: 10.1364/JOSAA.30.000238

11/05/2013 31.00 David A. B. Miller. Self-aligning universal beam coupler,
Optics Express, (03 2013): 0. doi: 10.1364/OE.21.006360

11/05/2013 32.00 David A. B. Miller. Self-configuring universal linear optical component [Invited],
Photonics Research, (06 2013): 0. doi: 10.1364/PRJ.1.000001

11/05/2013 33.00 Thomas Brougham, Stephen M Barnett, Kevin T McCusker, Paul G Kwiat, Daniel J Gauthier. Security of high-dimensional quantum key distribution protocols using Franson interferometers,
Journal of Physics B: Atomic, Molecular and Optical Physics, (05 2013): 0. doi: 10.1088/0953-4075/46/10/104010

11/05/2013 34.00 Reuben S Aspden, Daniel S Tasca, Robert W Boyd, Miles J Padgett. EPR-based ghost imaging using a single-photon-sensitive camera,
New Journal of Physics, (07 2013): 0. doi: 10.1088/1367-2630/15/7/073032

11/05/2013 35.00 Matthew P. Edgar, Frauke Izdebski, Gerald S. Buller, Miles J. Padgett, Daniel S. Tasca. Optimizing the use of detector arrays for measuring intensity correlations of photon pairs,
Physical Review A, (7 2013): 0. doi: 10.1103/PhysRevA.88.013816

11/05/2013 36.00 M. P. J. Lavery, F. C. Speirits, S. M. Barnett, M. J. Padgett. Detection of a Spinning Object Using Light's Orbital Angular Momentum,
Science, (08 2013): 0. doi: 10.1126/science.1239936

11/05/2013 37.00 Jeff Z. Salvail, Megan Agnew, Allan S. Johnson, Eliot Bolduc, Jonathan Leach, Robert W. Boyd. Full characterization of polarization states of light via direct measurement,
Nature Photonics, (3 2013): 0. doi: 10.1038/nphoton.2013.24

11/05/2013 38.00 Megan Agnew, Jeff Z. Salvail, Jonathan Leach, Robert W. Boyd. Generation of Orbital Angular Momentum Bell States and Their Verification via Accessible Nonlinear Witnesses,
Physical Review Letters, (7 2013): 0. doi: 10.1103/PhysRevLett.111.030402

11/05/2013 39.00 Heedeuk Shin, Omar S. Magaña-Loaiza, Mehul Malik, Malcolm N. O'Sullivan, Robert W. Boyd. Enhancing entangled-state phase estimation by combining classical and quantum protocols,
Optics Express, (01 2013): 0. doi: 10.1364/OE.21.002816

11/05/2013 40.00 Mehul Malik, Sangeeta Murugkar, Jonathan Leach, Robert W. Boyd. Measurement of the orbital-angular-momentum spectrum of fields with partial angular coherence using double-angular-slit interference, Physical Review A, (12 2012): 0. doi: 10.1103/PhysRevA.86.063806

11/05/2013 2.00 Martin P J Lavery, Gregorius C G Berkhout, Johannes Courtial, Miles J Padgett. Measurement of the light orbital angular momentum spectrum using an optical geometric transformation, Journal of Optics, (06 2011): 0. doi: 10.1088/2040-8978/13/6/064006

11/05/2013 4.00 Filippo M. Miatto, Alison M. Yao, Stephen M. Barnett. Full characterization of the quantum spiral bandwidth of entangled biphotons, Physical Review A, (03 2011): 0. doi: 10.1103/PhysRevA.83.033816

11/05/2013 1.00 Alison M Yao. Angular momentum decomposition of entangled photons with an arbitrary pump, New Journal of Physics, (05 2011): 0. doi: 10.1088/1367-2630/13/5/053048

11/05/2013 6.00 Alison M. Yao, Miles J. Padgett. Orbital angular momentum: origins, behavior and applications, Advances in Optics and Photonics, (05 2011): 0. doi: 10.1364/AOP.3.000161

11/05/2013 7.00 Robert W. Boyd, Brandon Rodenburg, Mohammad Mirhosseini, Stephen M. Barnett. Influence of atmospheric turbulence on the propagation of quantum states of light using plane-wave encoding, Optics Express, (09 2011): 0. doi: 10.1364/OE.19.018310

11/05/2013 8.00 Glenn A. Tyler. Spatial bandwidth considerations for optical communication through a free space propagation link, Optics Letters, (11 2011): 0. doi: 10.1364/OL.36.004650

11/05/2013 13.00 Anand Kumar Jha, Girish S. Agarwal, Robert W. Boyd. Supersensitive measurement of angular displacements using entangled photons, Physical Review A, (5 2011): 0. doi: 10.1103/PhysRevA.83.053829

11/05/2013 14.00 Thomas Brougham, Stephen M. Barnett. Information communicated by entangled photon pairs, Physical Review A, (3 2012): 0. doi: 10.1103/PhysRevA.85.032322

11/05/2013 15.00 J. Romero, D. Giovannini, S. Franke-Arnold, S. M. Barnett, M. J. Padgett. Increasing the dimension in high-dimensional two-photon orbital angular momentum entanglement, Physical Review A, (7 2012): 0. doi: 10.1103/PhysRevA.86.012334

11/05/2013 18.00 Anand Kumar Jha, Girish S. Agarwal, Robert W. Boyd. Partial angular coherence and the angular Schmidt spectrum of entangled two-photon fields, Physical Review A, (12 2011): 0. doi: 10.1103/PhysRevA.84.063847

11/05/2013 19.00 F. M. Miatto, H. Lorenzo Pires, S. M. Barnett, M. P. Exter. Spatial Schmidt modes generated in parametric down-conversion, The European Physical Journal D, (10 2012): 0. doi: 10.1140/epjd/e2012-30035-3

11/05/2013 41.00 Melanie McLaren, Megan Agnew, Jonathan Leach, Filippus S. Roux, Miles J. Padgett, Robert W. Boyd, Andrew Forbes. Entangled Bessel-Gaussian beams, Optics Express, (10 2012): 0. doi: 10.1364/OE.20.023589

11/05/2013 43.00 David A. B. Miller. Reconfigurable add-drop multiplexer for spatial modes, Optics Express, (08 2013): 0. doi: 10.1364/OE.21.020220

11/05/2013 44.00 David Miller. Establishing optimal wave communication channels automatically, Journal of Lightwave Technology, (2013): 0. doi: 10.1109/JLT.2013.2278809

11/05/2013 45.00 B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, P. G. Kwiat. Detection-Loophole-Free Test of Quantum Nonlocality, and Applications, Physical Review Letters, (9 2013): 0. doi: 10.1103/PhysRevLett.111.130406

11/05/2013 46.00 Mohammad Mirhosseini, Brandon Rodenburg, Mehul Malik, Robert W. Boyd. Free-space communication through turbulence: a comparison of plane-wave and orbital-angular-momentum encodings,
Journal of Modern Optics, (10 2013): 0. doi: 10.1080/09500340.2013.834084

11/05/2013 47.00 Eliot Bolduc, Nicolas Bent, Enrico Santamato, Ebrahim Karimi, Robert W. Boyd. Exact solution to simultaneous intensity and phase encryption with a single phase-only hologram,
Optics Letters, (09 2013): 0. doi: 10.1364/OL.38.003546

11/05/2013 48.00 Sebastian A. Schulz, Taras Machula, Ebrahim Karimi, Robert W. Boyd. Integrated multi vector vortex beam generator,
Optics Express, (06 2013): 0. doi: 10.1364/OE.21.016130

TOTAL: **75**

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Barnett
1. “Information security: from classical to quantum”, Proc. SPIE 8542, Electro-Optical Remote Sensing, Photonic Technologies, and Applications VI, 85421I, Edinburgh, U.K., November 19, 2012.
2. “Quantum communications with highly entangled photons”, Pecs workshop on Quantum Information and Quantum Optics, Pecs, Hungary, May 28-30, 2012.

Boyd
3. Quantum Aspects of the Transverse Degrees of Freedom of Photons, Presented at the OSA Structured Light in Structured Media Incubator, Washington DC, 29 September – 1 October 2013
4. Ghost Imaging and Quantum Imaging, Presented at the OSA Annual Meeting, Orlando, Florida, October 9, 2013
5. Weak Values and Direct Measurement of the Quantum Wavefunction, Presented at the APS/DLS Laser Science Annual Meeting, Orlando, Florida, October 9, 2013
6. Quantum Aspects of Light Beams Carrying Orbital Angular Momentum, Presented at the VIII Reunión Española de Optoelectrónica, Alcalá de Henares, Madrid, July 10-12, 2013.
7. Quantum Aspects of Light Beams Carrying Orbital Angular Momentum, Presented at International Workshop on "Singularities and Topological Structures of Light," ICTP Trieste. Italy, July 8-12, 2013.
8. Weak Values and Direct Measurement of the Quantum Wavefunction, ICSSUR, Nürnberg, June 24, 2013.
9. Weak Values and Direct Measurement of the Quantum Wavefunction, Presented at CQO/QIM, Rochester, New York, June 16-20, 2013.
10. Nonlinear Photonics (Encompassing nanophotonics and quantum nonlinear optics), presented at the LENS Workshop, Florence Italy, March 12, 2013
11. Multi-bit-per-photon QKD system based on encoding in orbital-angular-momentum states of light, SPIE Photonics West, February 6, 2013.
12. Orbital-Angular-Momentum Encoding for Free Space QKD, Presented at the Symposium on the Physics of Quantum Electronics, Snowbird Utah, January 7, 2013.
13. Encoding Information on Light Fields Using OAM States (Especially Quantum Information), presented at the New York State Center for Complex Light Workshop, CCN, October 22, 2012.
14. The Promise of Quantum Nonlinear Optics, presented at the APS-DLS – OSA Joint Annual Meeting, Rochester, NY, USA, October 16, 2012.
15. Research in Quantum Nonlinear Optics, presented at the IEEE Photonics Conference, San Francisco, September, 26, 2012.
16. Quantum Imaging: Enhanced Image Formation Using Quantum States of Light, presented at the 2012 Karles Invitational Conference on Quantum Information Science and Technology, Naval Research Laboratory Washington, DC 20375, August 27-28, 2012.
17. Quantum Imaging: Enhanced Image Formation Using Quantum States of Light, presented at the 21st International Laser Physics Workshop (LPHYS’12), Calgary, Alberta, Canada, July 23, 2012.
18. Research in Quantum Nonlinear Optics, presented at the Workshop on Novel Ideas in Optics, Purdue University, May 31-June 2, 2012.
19. Nonlinear Optics, Past Successes and Future Challenges, Plenary Talk presented at the Conference on Lasers and Electro-Optics and Quantum Electronics and Laser Science Conference (CLEO: 2012), San Jose, California, May 6-11, 2012.
20. Information in a Photon, Presented at Photonics West, San Francisco, January 25, 2012.
21. High-Order Entanglement for Quantum Information, presented at PQE, Snowbird Utah, January 3, 2012.
22. Promises and Challenges of Ghost Imaging, presented at the OSA Topical Meeting on Signal Recovery and Synthesis, July 11, 2011.
23. Information in a Photon, presented at the First International Workshop on High-Dimensional Entanglement, Como, Italy. June 20-24, 2011.
24. Quantum Imaging: Enhanced Image Formation Using Quantum States of light, Presented at Information Photonics, Ottawa, May 19, 2011.
25. Promises and Challenges in Quantum Nonlinear Optics, Presented at Photonics North, Ottawa, ON, May 16, 2011.
26. Information in a Photon, presented at the Winter Colloquium on the Physics of Quantum Electronics, January 5, 2011.

Gauthier
27. 'Observation of Elliptical Patterns in Type I Spontaneous Parametric Down Conversion', 2013 Frontiers in Optics/Laser Science XXIX (FiO/LS), Orlando FL, Oct. 6 - Oct. 10, 2013.
28. 'Achieving high-rate quantum key distribution by multiplexing orbital angular momentum transverse modes,' 43rd Colloquium on the Physics of Quantum Electronics 2103, Snowbird, Utah, Jan. 7, 2013.
29. 'Quantum Key Distribution Using Hyperentanglement,' Quantum Information and Measurement Conference, Berlin, Germany, Mar. 20, 2012.
30. 'High rate quantum key distribution,' 41st Colloquium on the Physics of Quantum Electronics, Snowbird, UT, Jan. 5, 2011.

Kwiat
31. "Higher-dimensional quantum cryptography", QCrypt 2013, 3rd international conference on quantum cryptography. August 5–9, 2013 in Waterloo, Canada
32. "La Morte de Realismo locale", Paul G. Kwiat, Quantum Information Processing and Communication, Florence, IT, June 30-July 5, 2013.
33. "The Death of Nonlocality", Paul G. Kwiat, Conference on Quantum Information and Quantum Control (CQIQC-V), Fields Institute,

Toronto, Canada, 12 Aug 2013 - 16 Aug 2013
34. "Loopholes -- Be Gone!", Paul Kwiat, Single Photon Workshop 2013, Oak Ridge National Laboratory, October 15-18, 2013
35. "Implementation and Applications of a Loophole-free Test of Quantum Nonlocality", Brad Christensen and Paul Kwiat, Quantum Communications and Photonics, Waikoloa, Hawaii, July 8-10, 2013.
36. "Information Reconciliation in Higher Dimensional Quantum Cryptography", Quantum Information and Measurement 2013, Rochester, New York United States, June 17-20, 2013
37. "The End of Local Realism", Quantum Information and Measurement 2013, Rochester, New York United States, June 17-20, 2013
38. "Advanced Quantum Communication via Hyperentanglement," Quantum Information and Measurement (QIM) 19 March - 21 March 2012, Laser Optics Berlin, Berlin, Germany.
39. "Hyperentanglement: More IS better," 11th Annual Meeting of the Fitzpatrick Institute for Photonics (FIP), Duke University, October 10-11, 2011, Durham, NC.

Miller
40. "Nanometallic concentration for enhanced photodetection," IEEE Photonics conference, Arlington VA, October 13, 2011, Paper ThA1
41. "Device Challenges and Opportunities for Optical Interconnects," (invited tutorial), OSA Frontiers in Optics conference, San Jose, CA, October 18, 2011, Paper FTuV1
42. "Optical Interconnects – Why We Will Have To Use Them," ISSCC, San Francisco, CA, Feb. 20, 2012, Session ES4
43. "Optical Interconnects to Chips," (Invited Tutorial talk), European Conference on Integrated Optics, Sitges, Spain, April 19, 2012
44. "Optical Interconnects to Chips," (Invited Tutorial talk), IEEE International Interconnect Technology Conference, San Jose, June 3, 2012
45. "The Roles of Optics in Information Processing," (Plenary talk), OSA Nonlinear Photonics and Integrated Photonics Research conferences, Colorado Springs, Colorado, June 18, 2012
46. "The Heat Death of Information Processing and Why Interconnects Are More Important Than Logic," Future Trends in Microelectronics 2012, Corsica, June 28, 2012
47. "Why Interconnects Are More Important Than Logic," Royal Society e-Futures Meeting, Royal Society, London, UK, May 14, 2013
48. "Attojoule Optoelectronics?" Royal Society e-Futures Kavli Meeting, Royal Society Kavli Centre, Chicheley Hall, Newport Pagnell, UK, May 16, 2013
49. "Attojoule optoelectronics – why and how," (Plenary talk) IEEE Photonics Society Summer Topical Meetings, Micro- and Nano-Cavity Integrated Photonics, Kona, Hawaii, July 9, 2013, Paper TuA2.1
50. "Requirements and novel devices for optical interconnects," IEEE Photonics Conference, Bellevue, Washington, Sept. 9, 2013
51. "Low-energy optoelectronics for interconnects," (Invited tutorial) OSA Frontiers in Optics, Orlando, Florida, October 8, 2013, Paper FM3B.2
52. "Designing arbitrary optical components without calculations," 9th National Conference on Laser Technology and Optoelectronics and the International Forum on Laser and Optics Technology, Shanghai, China, March 18, 2014
53. "Low energy optoelectronics for interconnects," The Tenth International Nanotechnology Conference on Communications and Cooperation (INC 10), NIST, Gaithersburg, Maryland, May 15, 2014
54. "Limits and opportunities of electrical and optical interconnects," OSA Incubator Nanophotonic Devices: Beyond Classical Limits, Washington, D.C., May 15, 2014
55. "Nanophotonics and Interconnects – Status and Future Directions," 2014 IEEE International Interconnect Technology Conference, May 21, 2014, San Jose, California
56. "Establishing optimal optical channels automatically," OSA Frontiers in Optics, Orlando, Florida, October 7, 2014, Paper FM3B.2

Padgett
57. The nonlinear meeting, Edinburgh, UK, 2014.
58. SPIE Defense and Security, Baltimore, USA, 2014.
59. Quantum Information and Measurement, Berlin, Germany, 2014.
60. Physics of Quantum Electronics, Snowbird, USA, 2014.
61. Plenary Speaker Australia - New Zealand Optics & Photonics, Perth Australia, 2013.
62. Structured Light in Structured Media, OSA Incubator, Washington, USA, 2013.
63. Keynote Speaker, SPIE Security and Defense, Dresden, Germany, 2013.
64. Summer School, New Frontiers on Smart Sensing, Otranto, Italy, 2013.
65. Winter School on Quantum Information Processing, Paraty, Brazil, 2013.
66. Plenary Lecture Physics of Quantum Electronics, Snowbird, USA, 2013.
67. Workshop on Singular Optics, ICTP, Trieste, Italy, 2012.
68. Plenary Lecture Rochester Coherence Conference, Rochester, USA, 2012.
69. Spin-Orbit Interaction for Light and Matter waves, Dresden, Germany, 2012.
70. Plenary Lecture SPIE Photonics West, San Francisco, USA, 2012.
71. National Meeting on Condensed Matter Physics, Águas de Lindóia, Brazil, 2012.
72. Conference on Lasers and Electro Optics, OSA, San Jose, USA, 2012.
73. Workshop on Orbital Angular Momentum and Applications, Vienna, Austria, 2012.
74. SPIE Photonics West, Complex Light, San Francisco, USA, 2012.
75. Physics of Quantum Electronics, Snowbird USA, 2012.

76. "Efficient measurement of orbital angular momentum using refractive optical elements," FIO Oct. 16-21 (2011), San Jose, CA.
77. "Measuring the orbital angular momentum of light with high optical efficiency," ICQI June 6-8, (2011), Ottawa, Canada.
78. "Measuring the orbital angular momentum of light," Invited talk, Photonics West, San Francisco, CA, Jan. 26, 2011.
79. "Sorting optical angular momentum states based on a geometric transformation," Frontiers in Optics 2010, Rochester, NY, Oct. 24, 2010.
80. "Optically efficient separation of orbital angular momentum states," Photon 10, Southampton, UK, Aug. 23-26, 2010.

Number of Presentations: 80.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

<u>Received</u> <u>Paper</u>

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received		Paper
10/05/2015	52.00	Daniel J. Gauthier, Mario Stipcevic. Precise Monte Carlo simulation of single-photon detectors, SPIE Defense, Security, and Sensing. 29-APR-13, Baltimore, Maryland, USA. : ,
10/05/2015	60.00	Stephen M. Barnett, Thomas Brougham. Information security: from classical to quantum, SPIE Security + Defence. 24-SEP-12, Edinburgh, United Kingdom. : ,
10/05/2015	54.00	Kevin T. McCusker, Venkat Chandar, Daniel J. Gauthier, Paul G. Kwiat, Daniel Kumor, Bradley G. Christensen. Information Reconciliation in Higher Dimensional Quantum Cryptography, Quantum Information and Measurement. 19-JUN-13, Rochester, New York. : ,
10/05/2015	53.00	Daniel J. Gauthier, Christoph F. Wildfeuer, Hannah Guilbert, Mario Stipcevic, Bradley G. Christensen, Daniel Kumor, Paul Kwiat, Kevin T. McCusker, Thomas Brougham, Stephen Barnett. Quantum Key Distribution Using Hyperentangled Time-Bin States, Quantum Information and Measurement. 19-JUN-13, Rochester, New York. : ,
10/06/2015	91.00	David A. B. Miller. Separating arbitrary overlapping spatial modes losslessly and without calculations, 2013 IEEE Photonics Society Summer Topical Meeting Series. 08-JUL-13, Waikoloa, HI, USA. : ,
11/05/2013	26.00	Mohammad Mirhosseini, Mehul Malik, Martin Lavery, Jonathan Leach, Miles Padgett, Robert W. Boyd. Photon efficient wavefront sensing using an SLM for polarization-based weak measurements, Frontiers in Optics. , Rochester, NY. : ,
11/05/2013	3.00	Robert Boyd, Heedeuk Shin, Mehul Malik, Colin O'Sullivan, Kam Wai Clifford Chan, Hye Jeong Chang, Daniel J. Gauthier, Anand Jha, Jonathan Leach, Sangeeta Murugkar, Brandon Rodenburg. Applications of Nonlinear Optics in Quantum Imaging and Quantum Communication, Nonlinear Optics: Materials, Fundamentals and Applications. 17-JUL-11, Kauai, Hawaii. : ,
11/05/2013	5.00	Robert W. Boyd, Anand Jha, Mehul Malik, Colin O'Sullivan, Brandon Rodenburg, Daniel J. Gauthier, Zameer U. Hasan, Philip R. Hemmer, Hwang Lee, Charles M. Santori. Quantum key distribution in a high-dimensional state space: exploiting the transverse degree of freedom of the photon, SPIE OPTO. 11-FEB-11, San Francisco, California. : ,
11/05/2013	10.00	Eliot Bolduc, Jonathan Leach, Robert Boyd. The Secure Information Capacity of Photons Entangled in High Dimensions, Quantum Information and Measurement. , Berlin, Germany. : ,
11/05/2013	9.00	Bradley G. Christensen, Kevin T. McCusker, Daniel J. Gauthier, Paul G. Kwiat. High-Speed Quantum Key Distribution Using Hyper-Entangled Photons, CLEO: Applications and Technology. , San Jose, California. : ,
11/05/2013	11.00	Jonathan Leach, Megan Agnew, Melanie McLaren, Stef Roux, Robert Boyd. Quantum State Characterization of High-dimensionally Entangled Photons, Quantum Information and Measurement. , Berlin, Germany. : ,
11/05/2013	12.00	Daniel Gauthier, Hannah Guilbert, Yunhui Zhu, Meizhen Shi, Kevin McCusker, Bradley Christensen, Paul Kwiat, Thomas Brougham, Stephen M. Barnett, Venkat Chandar. Quantum Key Distribution Using Hyperentanglement, Quantum Information and Measurement. , Berlin, Germany. : ,

11/05/2013 16.00 Brandon Rodenburg, Mehul Malik, Malcolm O'Sullivan, Mohammad Mirhosseini, Robert Boyd. Influence of Atmospheric Turbulence on the Performance of a High Dimensional Quantum Key Distribution System using Spatial Mode Encoding,
Quantum Information and Measurement. , Berlin, Germany. : ,

11/05/2013 17.00 Brandon Rodenburg, Mehul Malik, Malcolm O'Sullivan, Mohammad Mirhosseini, Nicholas K. Steinhoff, Glenn A. Tyler, Robert W. Boyd. Influence of thick atmospheric turbulence on the propagation of quantum states of light using spatial mode encoding,
CLEO: Applications and Technology. , San Jose, California. : ,

11/05/2013 42.00 David A. B. Miller. Separating arbitrary overlapping spatial modes losslessly and without calculations,
2013 IEEE Photonics Society Summer Topical Meeting Series. 08-JUL-13, Waikoloa, HI, USA. : ,

TOTAL: **15**

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received Paper

10/05/2015 57.00 Thomas Brougham, Christoph F Wildfeuer, Stephen M Barnett, Daniel J Gauthier. The information of high-dimensional time-bin encoded photons,
arXiv:1506.0442v2 (06 2015)

TOTAL: **1**

Number of Manuscripts:

Books

Received Book

TOTAL:

Received Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Robert Boyd, Canada Excellence Research Chair in Quantum Nonlinear Optics
Robert Boyd, Fellow of the SPIE
Daniel Gauthier, Robert C. Richardson Professorship
David Miller, Fellow of the Electromagnetics Academy
David Miller, Carnegie Millennium Professorship
Miles Padgett, Fellow of the Optical Society of America
Miles Padgett, Fellow of the SPIE
Miles Padgett, Research Fellow of the Royal Society

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Martin Lavery	1.00	
Meizhen Shi	0.78	
Hannah Guilbert	1.00	
Branden Rodenburg	1.00	
Bradley Christensen	1.00	
Kevin McCusker	0.40	
Anand Jha	0.13	
Daniel Giovannini	0.13	
Collin O'Sullivan	1.00	
Mehul Malik	0.13	
Mohammad Mirhosseini	0.78	
Heedueuk Shin	0.13	
Filippo Miatto	0.13	
FTE Equivalent:	**7.61**	
Total Number:	**13**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
Allison Yao	0.10
Christoph Wildfeuer	0.40
Hugo Cavalcante	0.13
Thomas Brougham	0.80
Jonathan Leach	0.50
FTE Equivalent:	**1.93**
Total Number:	**5**

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Steve Barnett	0.08	
Daniel Gauthier	0.08	
Robert Boyd	0.08	
Paul Kwiat	0.08	
David Miller	0.16	Yes
Miles Padgett	0.08	
FTE Equivalent:	**0.56**	
Total Number:	**6**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED	Discipline
Yu-Po Wong	0.20	Physics
Daniel Kumor	0.20	Physics
FTE Equivalent:	**0.40**	
Total Number:	**2**	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 2.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:...... 2.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:...... 2.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):...... 2.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:...... 2.00

Names of Personnel receiving masters degrees

NAME	
Meizhen Shi	
Total Number:	**1**

Names of personnel receiving PHDs

NAME	
Mehul Malik	
Hannah Guilbert	
Kevin McCusker	
Martin Lavery	
Total Number:	**4**

Names of other research staff

NAME	PERCENT_SUPPORTED
Glenn Tyler	0.09
Nicholas Steinhoff	0.28
FTE Equivalent:	**0.37**
Total Number:	**2**

Sub Contractors (DD882)

1 a. Stanford University

1 b. 3160 Porter Drive
Suite 100
Palo Alto CA 943041222

Sub Contractor Numbers (c): 11-DARPA-1021
Patent Clause Number (d-1): 37 CFR 401
Patent Date (d-2):
Work Description (e): Undertake fundamental limits of optical components for transforming the transverse profi
Sub Contract Award Date (f-1): 8/12/10 12:00AM
Sub Contract Est Completion Date(f-2): 6/30/14 12:00AM

---

1 a. Stanford University

1 b. 3160 Porter Drive
Suite 100
Palo Alto CA 943058445

Sub Contractor Numbers (c): 11-DARPA-1021
Patent Clause Number (d-1): 37 CFR 401
Patent Date (d-2):
Work Description (e): Undertake fundamental limits of optical components for transforming the transverse profi
Sub Contract Award Date (f-1): 8/12/10 12:00AM
Sub Contract Est Completion Date(f-2): 6/30/14 12:00AM

---

1 a. the Optical Sciences Company

1 b. 1341 South Sunkist St
PO Box 25309
Anaheim CA 92806

Sub Contractor Numbers (c): 11-DARPA-1023
Patent Clause Number (d-1): 37 CFR 401
Patent Date (d-2):
Work Description (e): Undertake measurements of turbulence on a 1 km horizontal path and develop mitigation
Sub Contract Award Date (f-1): 8/12/10 12:00AM
Sub Contract Est Completion Date(f-2): 11/11/13 12:00AM

---

1 a. University of Rochester

1 b. ORPA
518 Hylan Building
Rochester NY 146270140

Sub Contractor Numbers (c): 11-DARPA-1025
Patent Clause Number (d-1): 37 CFR 401
Patent Date (d-2):
Work Description (e): Develop a quantum key distribution systems based on transverse spatial modes of optical
Sub Contract Award Date (f-1): 8/12/10 12:00AM
Sub Contract Est Completion Date(f-2): 6/30/14 12:00AM

1 a. University of Rochester

1 b. 518 Hylan Bldg.

Rochester NY 146113847

Sub Contractor Numbers (c): 11-DARPA-1025
Patent Clause Number (d-1): 37 CFR 401
Patent Date (d-2):
Work Description (e): Develop a quantum key distribution systems based on transverse spatial modes of optical
Sub Contract Award Date (f-1): 8/12/10 12:00AM
Sub Contract Est Completion Date(f-2): 6/30/14 12:00AM

---

1 a. University of Illinois - Urbana - Champaign

1 b. 1901 S. First St., Suite A

Champaign IL 618207406

Sub Contractor Numbers (c): 11-DARPA-1025
Patent Clause Number (d-1): 37 CFR 401
Patent Date (d-2):
Work Description (e): Develop high-rate quantum key distribution system using high-dimensional encoding
Sub Contract Award Date (f-1): 8/12/10 12:00AM
Sub Contract Est Completion Date(f-2): 6/30/14 12:00AM

---

1 a. University of Illinois - Urbana - Champaign

1 b. 1901 S. First Street, Suita A, MC-68

Champaign IL 618207406

Sub Contractor Numbers (c): 11-DARPA-1025
Patent Clause Number (d-1): 37 CFR 401
Patent Date (d-2):
Work Description (e): Develop high-rate quantum key distribution system using high-dimensional encoding
Sub Contract Award Date (f-1): 8/12/10 12:00AM
Sub Contract Est Completion Date(f-2): 6/30/14 12:00AM

---

1 a. University of Glasgow

1 b. Research Enterprise
10 The Square

Glasgow Scotland G12 8QQ

Sub Contractor Numbers (c): 11-DARPA-1022
Patent Clause Number (d-1): 37 CFR 401
Patent Date (d-2):
Work Description (e): Develop optical systems for sorting spatial modes, investigate high-dimensional quantum
Sub Contract Award Date (f-1): 8/12/10 12:00AM
Sub Contract Est Completion Date(f-2): 6/30/14 12:00AM

---

1 a. University of Strathclyde

1 b. University of Strathclyde

Glaskow

Sub Contractor Numbers (c): 11-DARPA-1022

Patent Clause Number (d-1): 37 CFR 401

Patent Date (d-2):

Work Description (e): Undertake theoretical research on high-dimensional quantum key distribution identifying

Sub Contract Award Date (f-1): 8/12/10 12:00AM

Sub Contract Est Completion Date(f-2): 8/11/13 12:00AM

---

1 a. University of Strathclyde

1 b. University of Strathclyde

106 Rottenrow

Glasgow, G4 0NW UK 00000

Sub Contractor Numbers (c): 11-DARPA-1022

Patent Clause Number (d-1): 37 CFR 401

Patent Date (d-2):

Work Description (e): Undertake theoretical research on high-dimensional quantum key distribution identifying

Sub Contract Award Date (f-1): 8/12/10 12:00AM

Sub Contract Est Completion Date(f-2): 8/11/13 12:00AM

Inventions (DD882)

Scientific Progress

See attached.

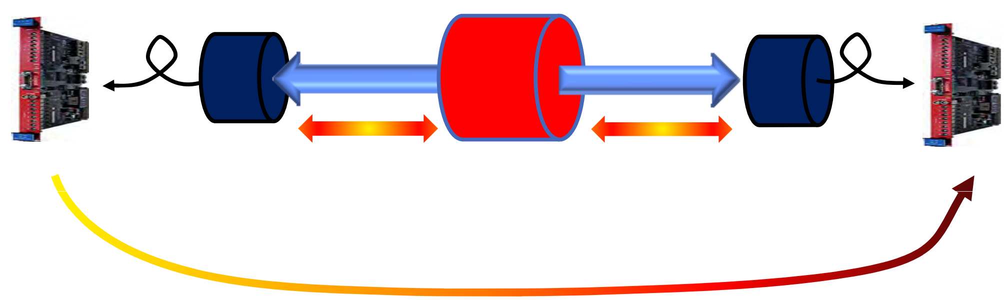
Technology Transfer

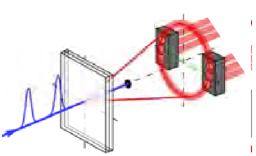
Quantum Key Distribution Using Hyperentanglement

Question: What are the fundamental limits of encoding/decoding information on a photon?

Goal: Develop a free-space, entanglement-based quantum key distribution (QKD) system that achieves >10 bits/photon received and >1 Gb/s

Steve Barnett, Strathclyde, **Robert Boyd**, Ottawa,
Daniel Gauthier, Duke, **Paul Kwiat**, UIUC, **David Miller**, Stanford,
Miles Padgett, Glasgow, **Glenn Tyler**, tOSC
Advisors/Partners:
Venkat Chadra, MIT Lincoln Labs, **Norbert Lütkenhaus**, U. Waterloo
Sae-Woo Nam, NIST



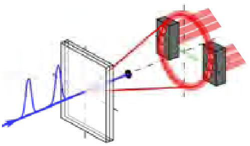


Duke InPho Site Visit, June 6, 2014

Primary Duke InPho Quantum Key Distribution System

Paul Kwiat
University of Illinois, Urbana-Champaign

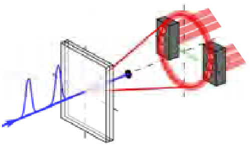
Daniel Gauthier
Duke University

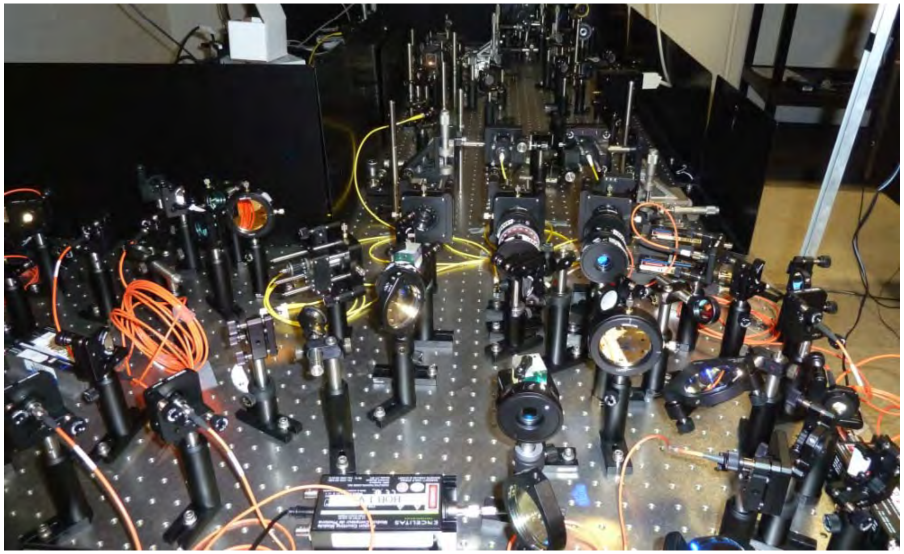


Duke InPho: Free-Space Quantum Key Distribution
Quantum Communication

Accomplishment: **Set up 2-channel hyper-entanglement-based QKD system, with time-bin PPM secured using simultaneous polarization entanglement.**

- Low jitter detectors (average 158-ps FWHM)
- x32 repetition-rate multipliers increase pulse frequency to 3.84 GHz
- Reduced detector deadtime (~25 ns) allows for high saturation
- Still photon-number limited
  - Use few-mode fibers (~x7 brightness)
  - Polarization decoherence issues with few-mode fiber
- Assumes intercept-resend attacks, and no polarization-independent QND measurements

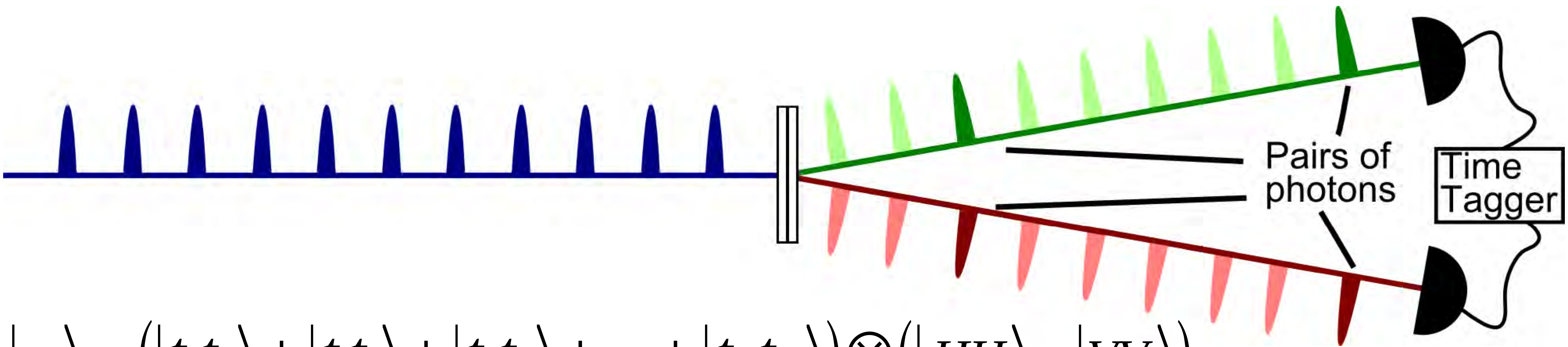




June 2014	Low Power	High Power
Singles	50 kHz	10.1 MHz
Coincidences	8 kHz	2.9 MHz
Average BER	0.4 %	0.9 %
“Secure” bit/coincidence	8.3 bits	**2.2 bits**
“Secure” bit/second	67 kbits	**6.3x2 Mbits 12.6 Mbits**

Hyper-entanglement Secured QKD

Central Concept: Encode in time, verify in polarization



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

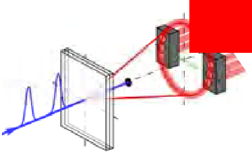
Alice and Bob use which time bin they detect a photon in to generate multiple bits per click, e.g., 1 pair in 1024 bins (2^{10}) → ~10 bits

Get extra 0.5 bpp from BB84 w. polarization.

They can constantly check for an eavesdropper using the polarization DOF (assuming no QND capability for Eve).

Perform NON-standard error detection/correction and privacy amp.

First experiment to use one DOF to secure another.



World-Record Heralding Efficiency

Source Quality:

- $\eta = \eta_{spatial} * \eta_{spectral} * \eta_{optics}$
  $= 0.9 * 0.95 * 0.95 = 0.81$

- Used in detection-loophole-free Bell test

- Visibility in all bases >99.7% using temporal compensation,

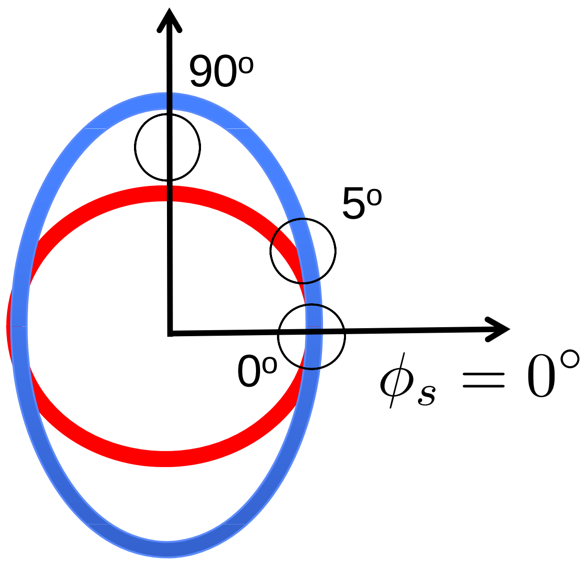
- World-record (?) pair production rate of 30 MHz into a single mode (over a >20 nm bandwidth at 710 nm)

- Other improvements possible (*e.g*., achromatic coupling)

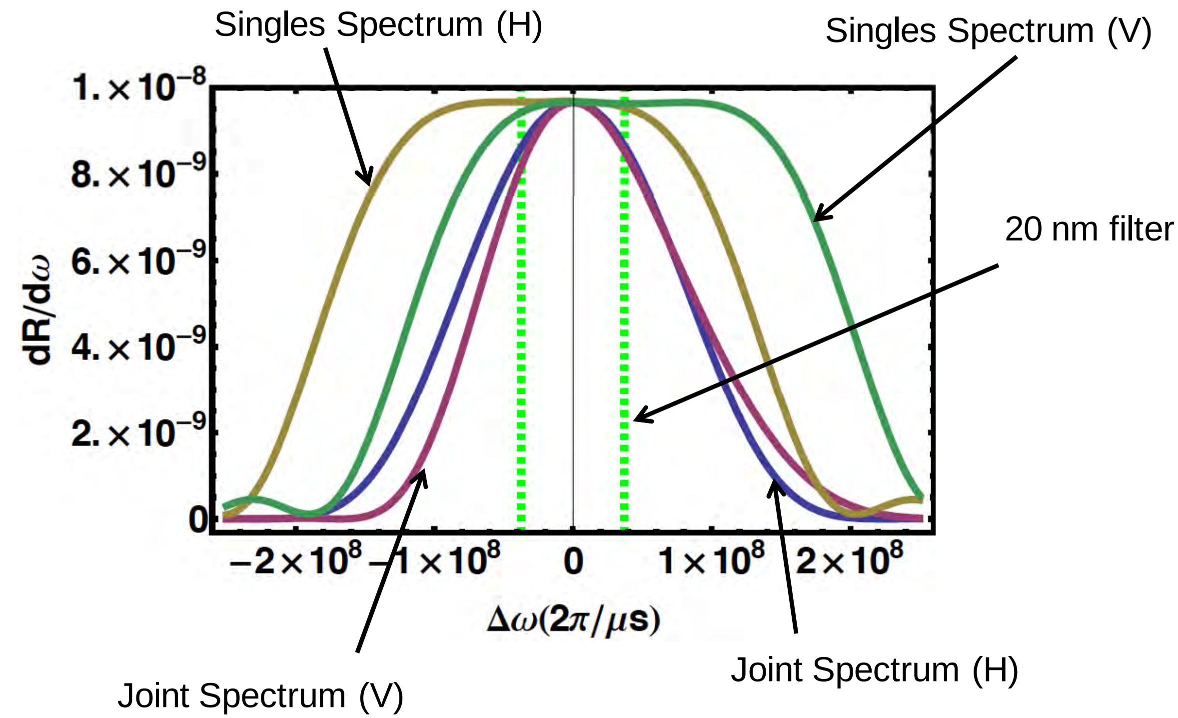
Developed one of the world's best entanglement sources.

Heralding Efficiency for BiBO source

InPho Breakthrough – Develop complete model for coupling bi-photons into single mode fibers. Accounts for elliptical shape of down-conversion ring, spatial-spectral coupling



Note: Eccentricity exaggerated in drawing

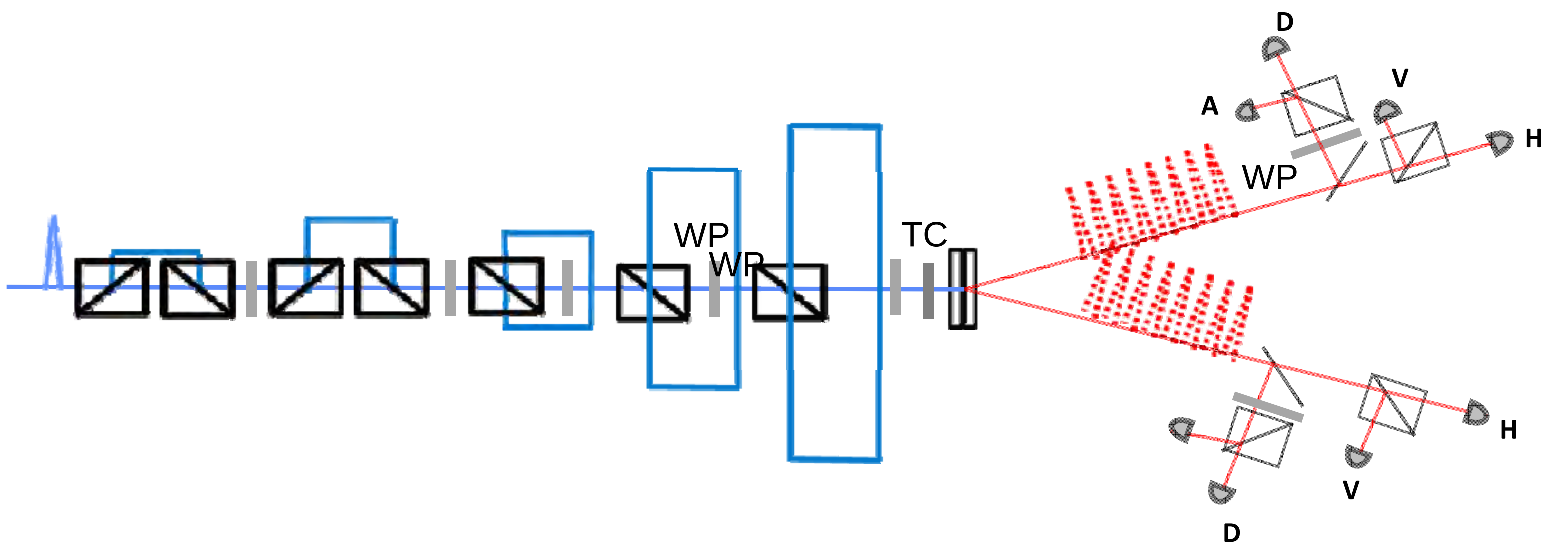


	Visibility	HE (H)	HE (V)
0°	99.986%	96.44%	95.71%
5°	99.982%	95.62%	96.23%
90°	99.971%	96.64%	95.84%

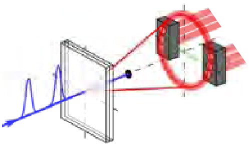
Predicted polarization visibility spatial/spectral heralding efficiency (20 nm bandwidth)

Repetition Rate Multiplication System

Implemented rep-rate multiplication system (x32) to achieve detector-jitter limited system.

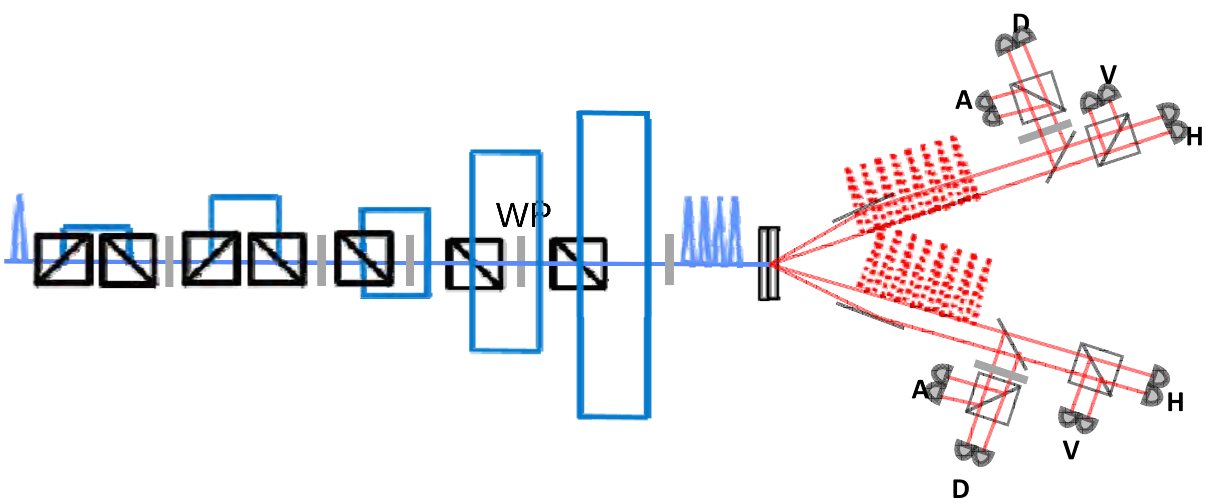


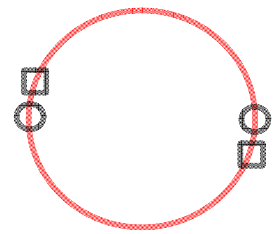
- Repetition-rate multipliers increase pulse frequency from 120 MHz → 3.8 GHz
- Time-bins (~260 ps) comparable to combined detector/time-tagger jitter
- Use spectrum-analyzer and high-speed detector to ~match path lengths (necessary for eventual mutually-unbiased basis checking)



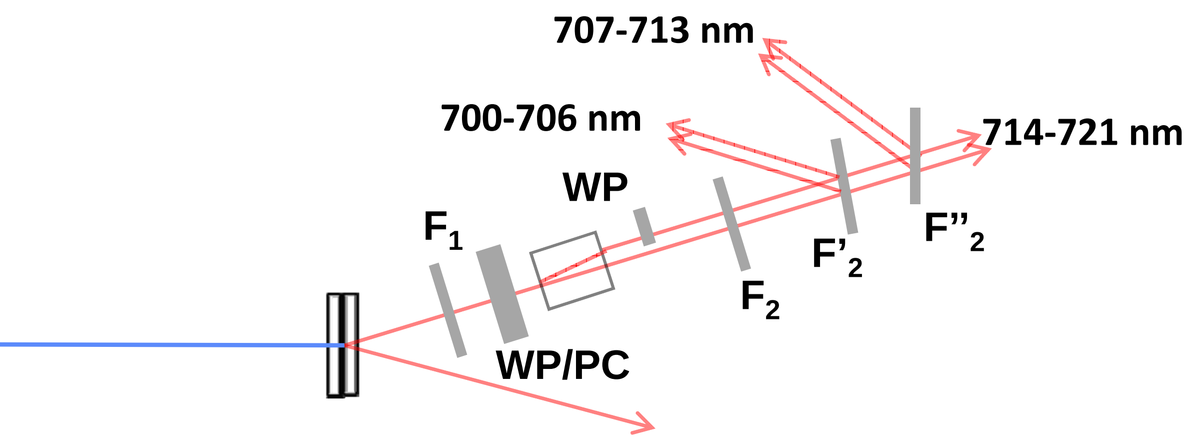
Multiple Spatial/Spectral Channels

Demonstrated/will demonstrate methods to achieve multiple independent spatial and spectral channels

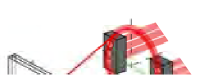




End view of SPDC cone



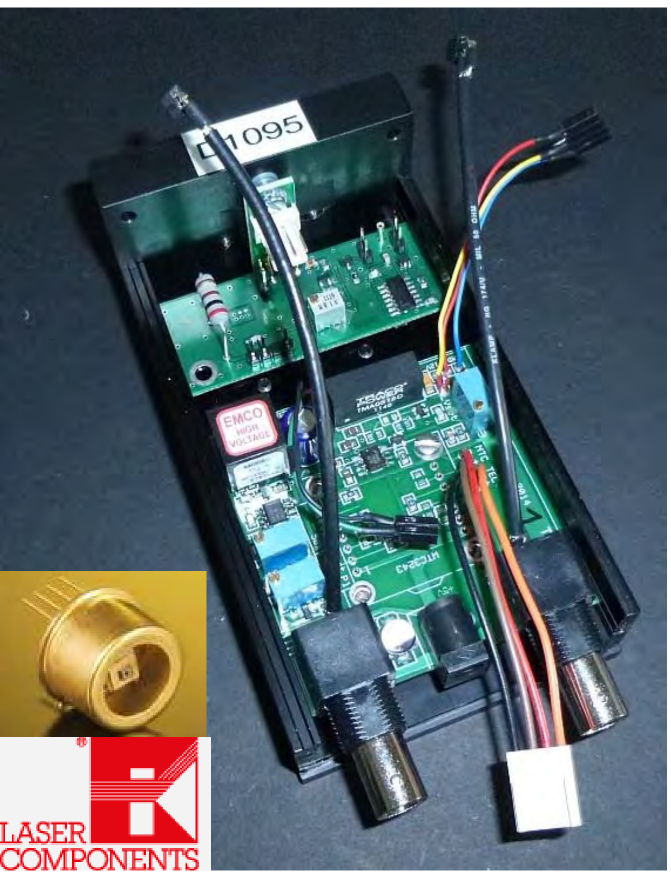
- Up to 10 sets of spatial pairs possible/practical
- Sequential tilted filters allow x3 WDM (~x20 possible)
- Collection into few-mode fiber allows saturation of each channel
- Key rates above ~60 MHz (with 2 spatial channels)
- 10 channels + few-mode iber → >1 GHz key rate!

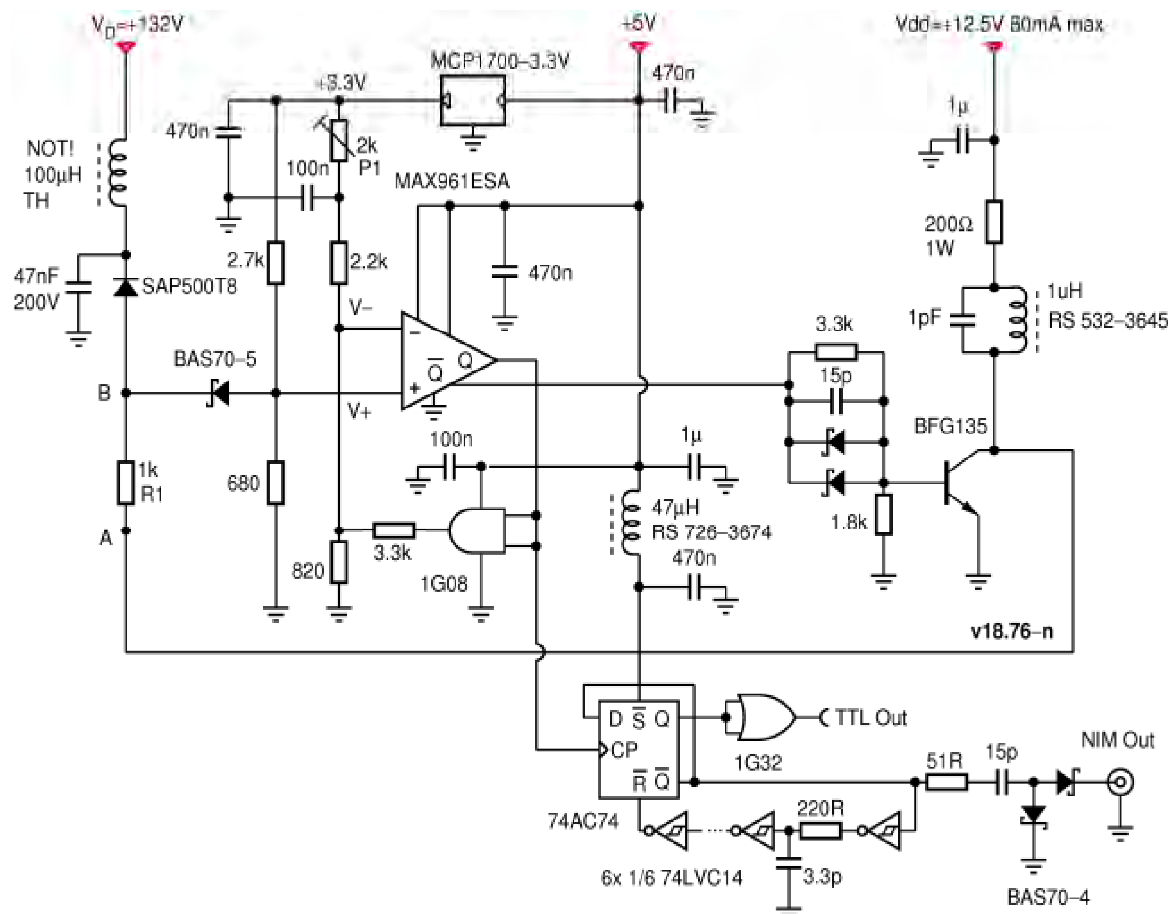


Demonstrate all technologies to achieve milestones!

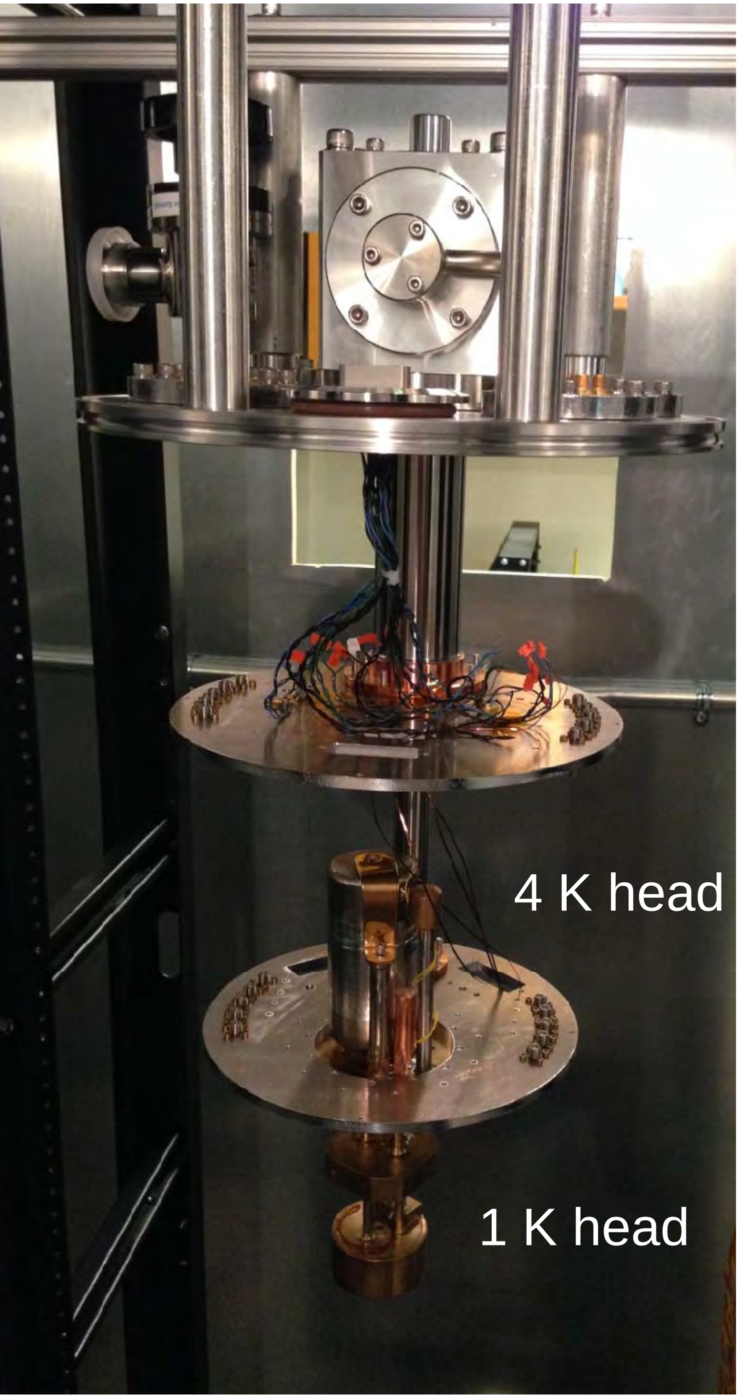
InPho Breakthrough – Develop custom electronics mated with Laser Components SAP-500 SPAD

Quantum Efficiency @ 710 nm: ~70%
Deadtime: 24.5 ns (41 MHz saturation rate)
Jitter: 158 ps average for 15 detectors
Afterpulsing probability: <0.1%
Dark Count Rate: ~3.5 kHz





Superconducting nanowire detectors



InPho Breakthrough – Develop 8 channel SiW superconducting nanowire detectors optimized for 710 nm in collaboration with NIST

Status report (6/4/14): Cryostat constructed, chill-down tests, detectors fabricated, undergoing testing

Anticipated performance:

Quantum Efficiency: >90%
Jitter: 100 ps
Deadtime: <20 ns

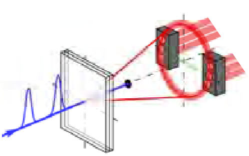
High-Resolution, High-Throughput Timetaggers for Time-Bin QKD

InPho Breakthrough – Assess and qualify time-taggers for time-bin QKD. Developed high-throughput custom time-tagger.

	Agilent	IQC	UIUC/NIST
Max count rate:	80 MHz (20 MHz continuous)	12 MHz	200 MHz (400 MHz possible)
Resolution (jitter):	50 ps (60 ps)	156 ps (180 ps)	50-100 ps (10 ps)
Channels:	6	12	4

- The Agilent timetagger can run up to 80 MHz in “burst mode” where only a few milliseconds of data are taken at a time.

- Custom UIUC/NIST timetagger count rate limited by hard drive write speed. At high rates, less bits per count (currently 32 bits) can be used allowing up to 400 MHz continuous. Resolution limited by the FPGA clock, the current board has a 100 ps resolution. A better board could allow for a 50 ps time bin size.

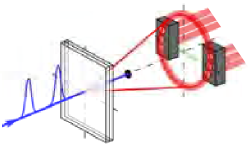


Mutual Information of the quantum key distribution system including error correction, privacy amplification, and security analysis

Steve Barnett
University of Strathclyde/Glasgow University

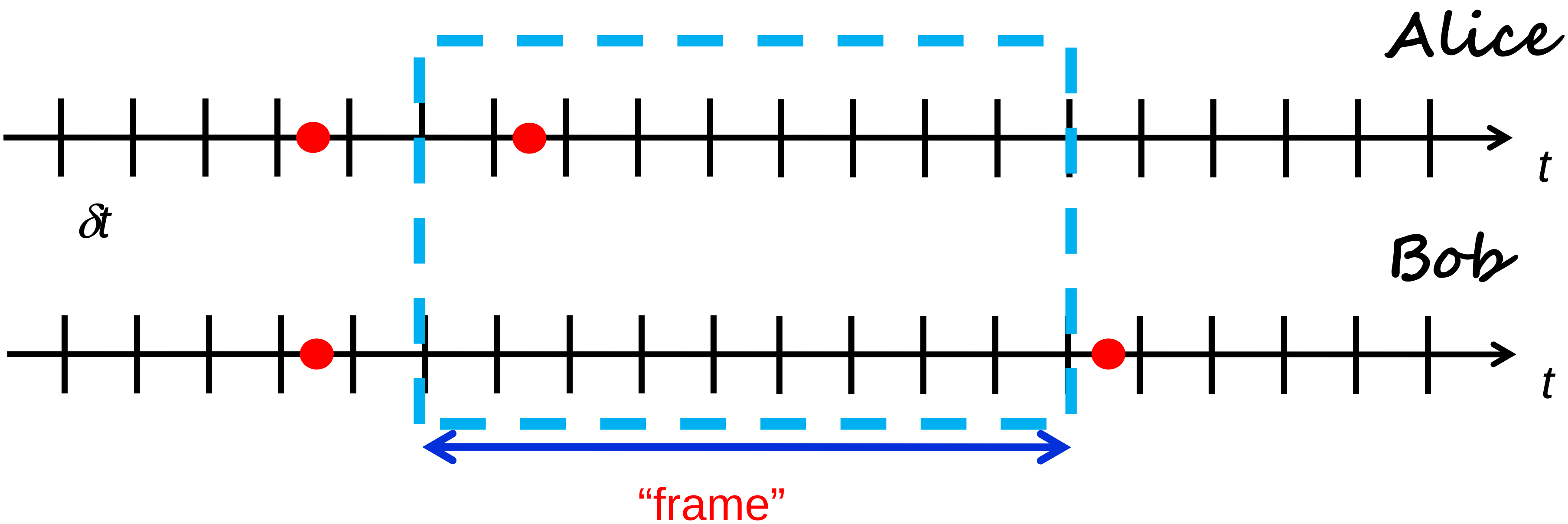
Paul Kwiat
University of Illinois, Urbana-Champaign

Daniel Gauthier
Duke University



The information per photon pair

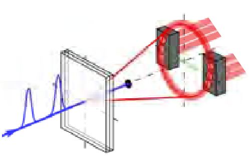
• Number bits / photon depend on errors. Typical errors are ***finite efficiency***, ***channel losses***, ***dark counts, after-pulsing, jitter, etc***.



• *Even* with errors, we can get **>*10 bits per detected photon pair**** [*]*.*

• ***InPho break through*:-** developed new model, takes account of ***frame-encoding, losses, dark counts, jitter, multiple photons in each frame and dead-time***.

• Very general, applies to other high-D QKD setups.

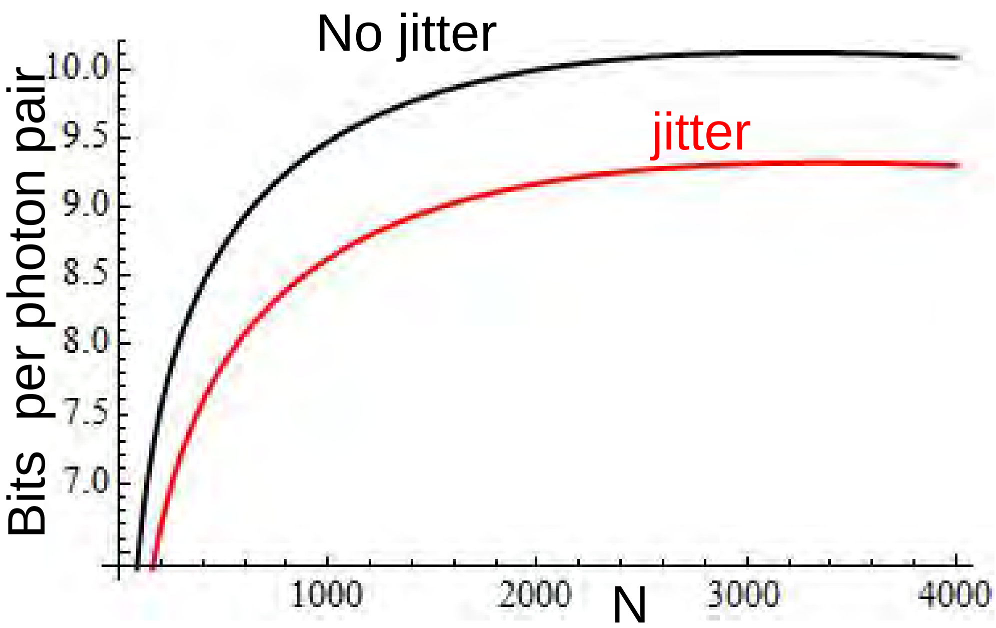


* Brougham & Barnett, PRA **85**, 032322 (2012).

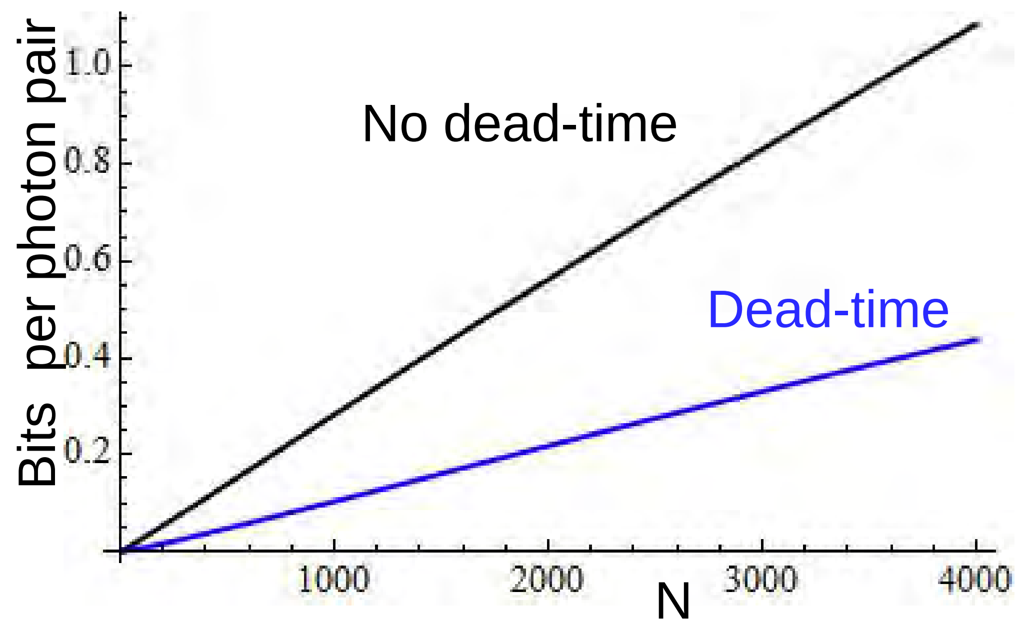
Information in frame-encoded photons

Can optimize frame size, N, in presence of realistic errors

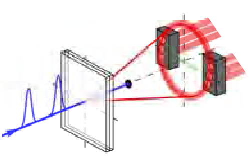
Information in 1,1-frames



Information in 2,2-frames



$\eta = 0.3$, $\lambda = 6.0\text{x}10^{-5}$, Pulse rate = 1ns,
jitter probability = 0.1, Dead-time = 1 time-bin
dark count rate = 300/s, After-pulsing rate = 1000/s



T. Brougham, C. F. Wildfeuer, S. M. Barnett and D. J. Gauthier, manuscript in preparation.

Error Correction

Implemented novel Slepian-Wolf-based error correction (both 'non-binary' and 'binary' levels, to cope with sparse data sets).

A data string is generated with the QKD source

Data String

1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

Current frame size is 16 bins (laser pulses)

The data string is broken into two data strings: an occupancy string and a letter string.

1	0	0	1

Parity Bits

1	0	1	1

5% of the Shannon-limit entropy

We keep 0% of the Shannon-limit entropy.

28% of the entropy is primarily lost due to multi-events per frame

67% of the Shannon-limit entropy

We keep 62% of the Shannon-limit entropy.

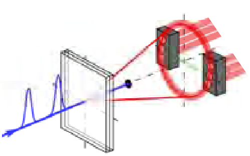
4	3

2	4

Parity Bits

Goes into a non-binary Slepian-Wolf Code

Goes into a binary Slepian-Wolf Code



Detecting Eve and leaked information I

- ***InPho breakthrough*:-** Bound information leaked to Eve for reasonable attacks (not QND). Standard results don't work for our setup.

- **Direct attack**: Eve measures time by making as general a POVM, with constrain that she ***absorbs and possibly re-emits photons***.

- Photons in state $|\psi\rangle \propto \left(|HH\rangle + |VV\rangle\right) \otimes \left[|11\rangle + |22\rangle + \ldots + |dd\rangle\right]$

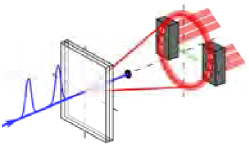
Polarization is *entangled.*

- Eve's attack must disturb polarization (as it is not a QND measurement).

- Detect Eve by checking *polarization correlation* within two mutually unbiased bases.

- Example: η=0.3, λ=5.33x10^{-5} , D.C =300/s and a bit error rate of P_E= 0.02

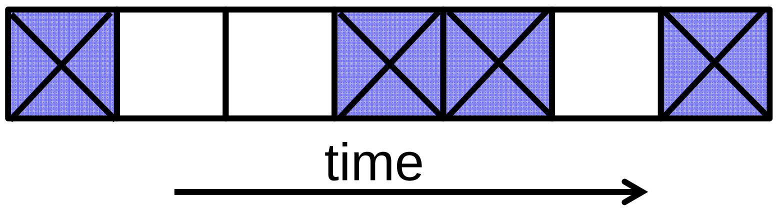
I_{AB} = 10.3 bits / photon pair & I_{Eve} = 0.82 bits / photon pair



Detecting Eve and leaked information II

•**Blocking attack**: Eve randomly blocks several, *non-contiguous,* time-bins.

• Eve knows photons not found in certain time-bins. ***This reduces her uncertainty and thus she gains information.***



• Eve can also ***partially block*** time-bins, reduces probability that photons found within those time-bins.

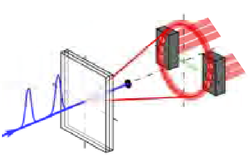
• ***InPho breakthrough*:-** Developed new methods to detect ***sophisticated blocking attacks***

• Detect attacks using ***'decoy' pulses***.

• From detection statistics for pulses, we estimate blocked and partial blocking time-bins.

• Example: η=0.3, λ=5.33x10^{-5} ,D.C =300/s and *fully* blocking ½ of all time-bins

I_{AB} = 10.3 bits / photon pair & I_{Eve} = 0.74 bits / photon pair



• Setup still vulnerable to QND attacks

Security against QND attacks: Franson interferometers

• Franson interferometer secure in the limit of 3-4 bits per photon (8 to16 time-bins), PRL**112**, 120506 (2014).

• ***InPho breakthrough*:-** Showed ***single*** interferometers insecure in **high-dimensions** ~10 bits per photon*. Would need visibility >99.8%.

• ***InPho breakthrough*:-** Developed bounds for Eve's information gain for ***multiple*** interferometers.

• Bounds valid for collective attacks#.

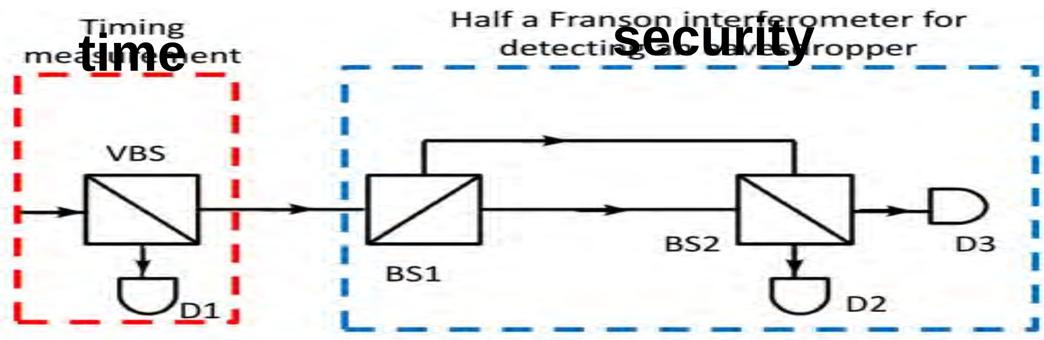
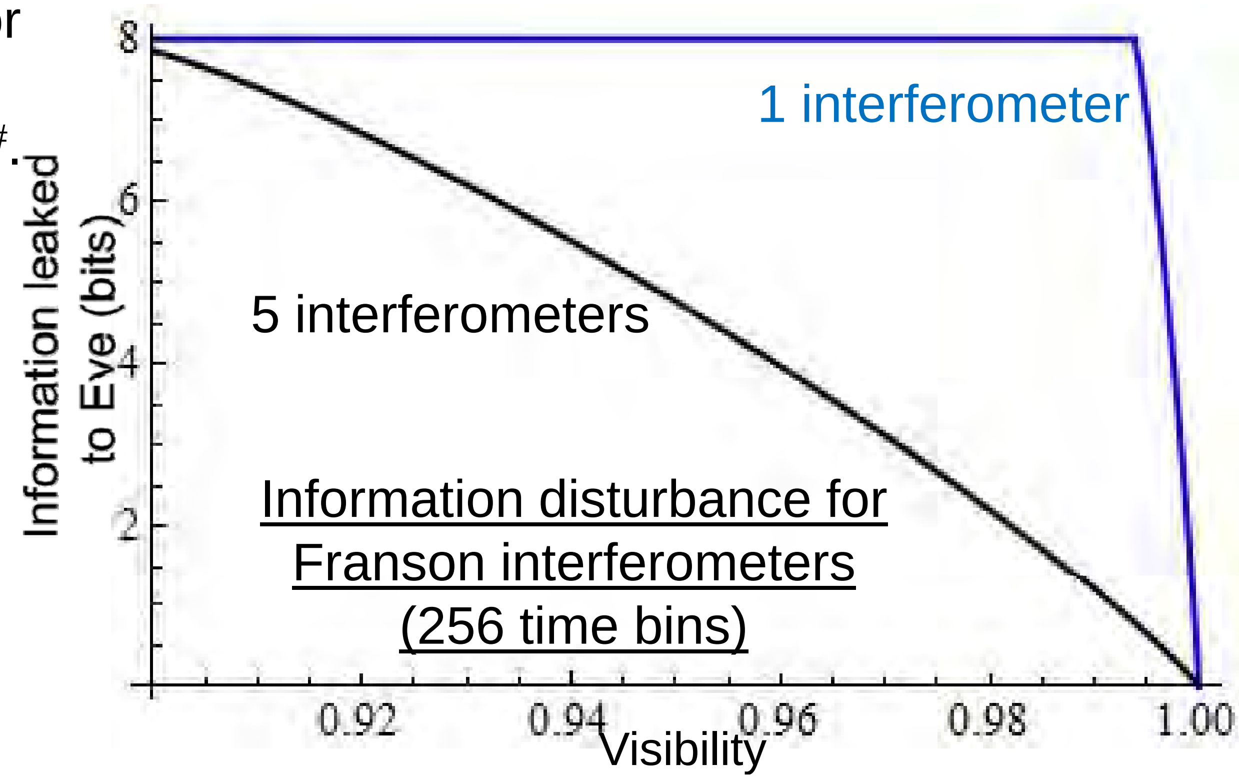
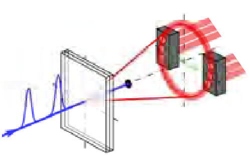


Figure 1. One half of the optical setup that Alice and Bob would each have. VBS is a variable beam splitter, while BS1 and BS2



* J. Phys. B **46**, 104010 (2013).

Manuscript in preparation.



Security against QND attacks: implementing MUBs using a cavity

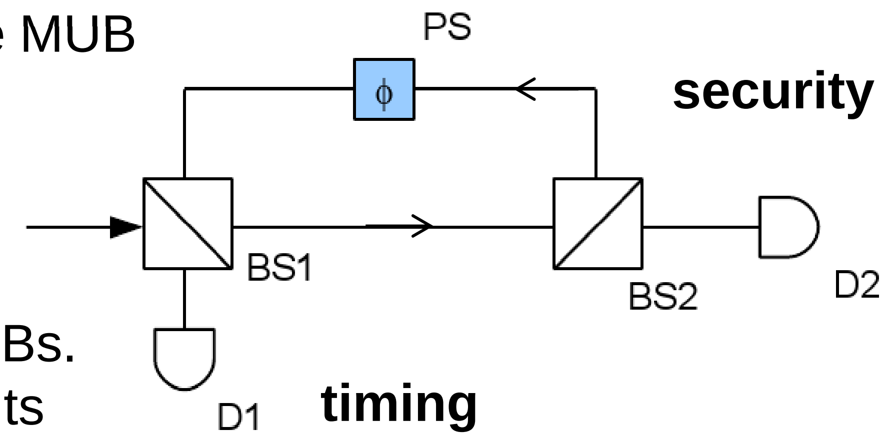
• ***InPho breakthrough*:-** Scheme that uses cavity to project onto ***very high-dimensional*** MUB states.

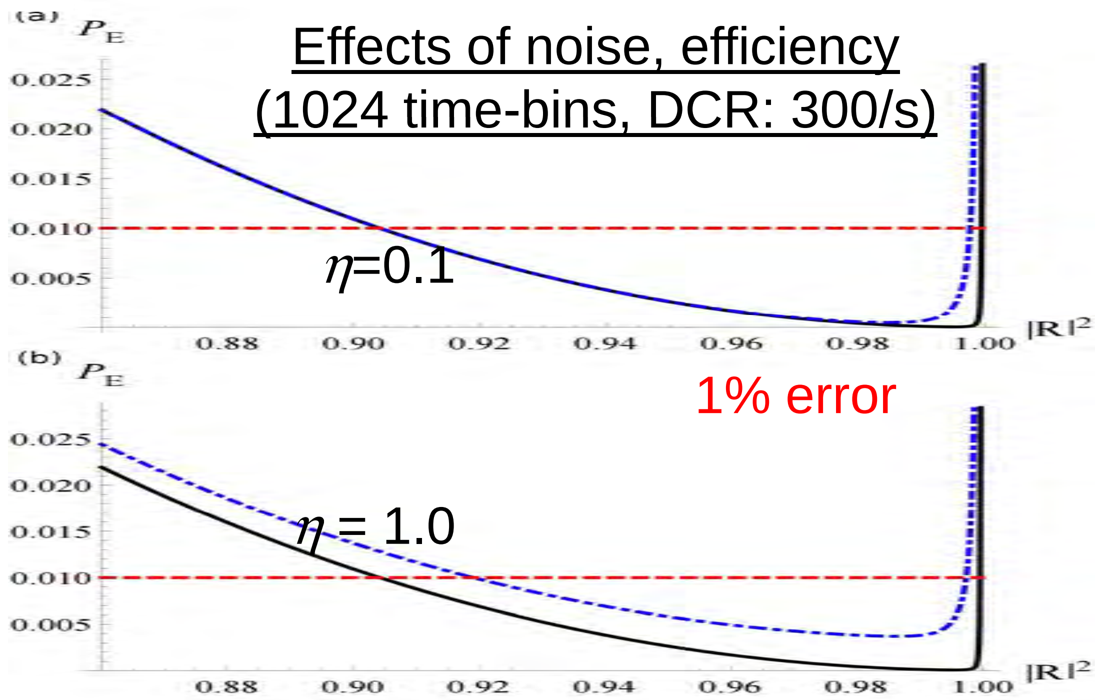
• Detection at D2 is projects onto the approximate MUB state

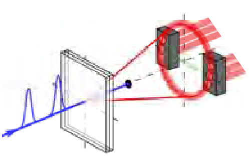
$$\sum_{m=0}^{N-1} |R_1|^m |R_2|^m e^{im(\phi+\pi)} |N-m\rangle \text{ where } R_1 \approx R_2 \approx 1$$

• Different values for ϕ correspond to different MUBs.
• Setup robust to errors for 1024 time-bins (~10 bits per photon pair).

Alice and Bob's setup



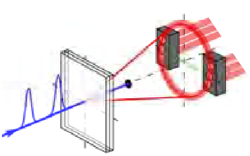




Brougham & Barnett, EPL **104**, 30003 (2013).

Brougham & Barnett, to appear in J. Phys. B

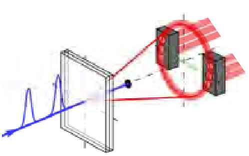
Technological Developments for Quantum Key Distribution Systems using Spatial Modes including Turbulence Mitigation



Generating, Sorting, and Characterizing Orbital Angular Momentum States

Robert Boyd
University of Rochester

Miles Padgett
Glasgow University

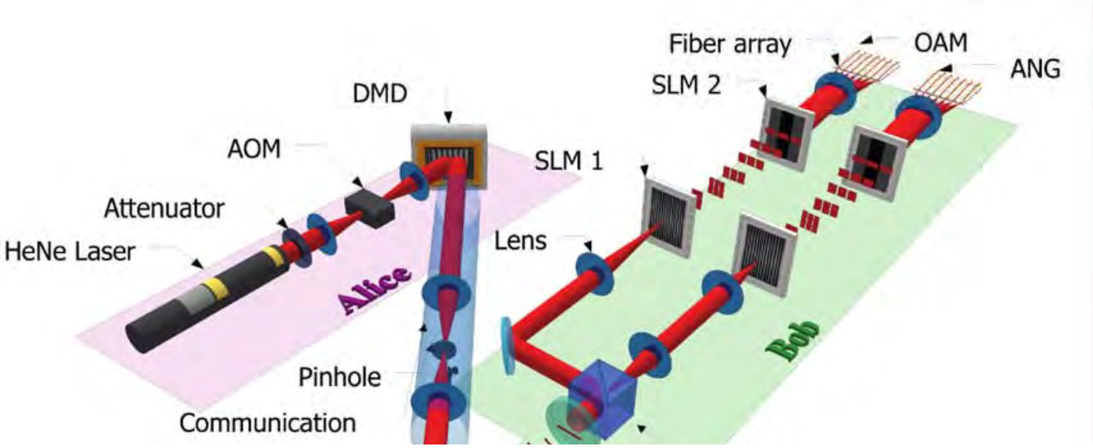


Quantum Cryptography with More Than One Bit Per Photon

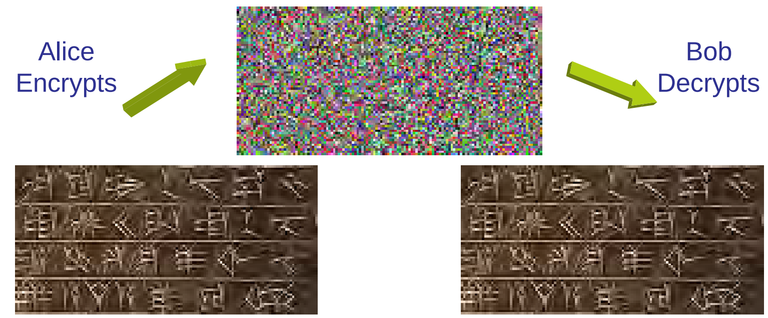
We have constructed a QKD system that can transit more than one bit (2.1 bits at present) per sifted photon.

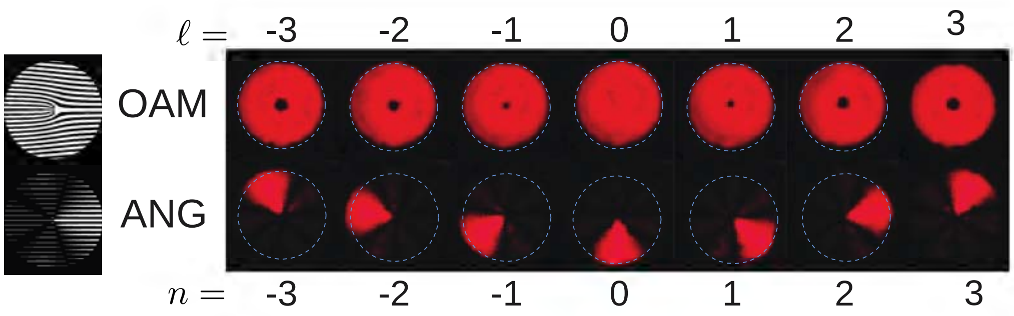
We have demonstated that this system is secure against even coherent attacks

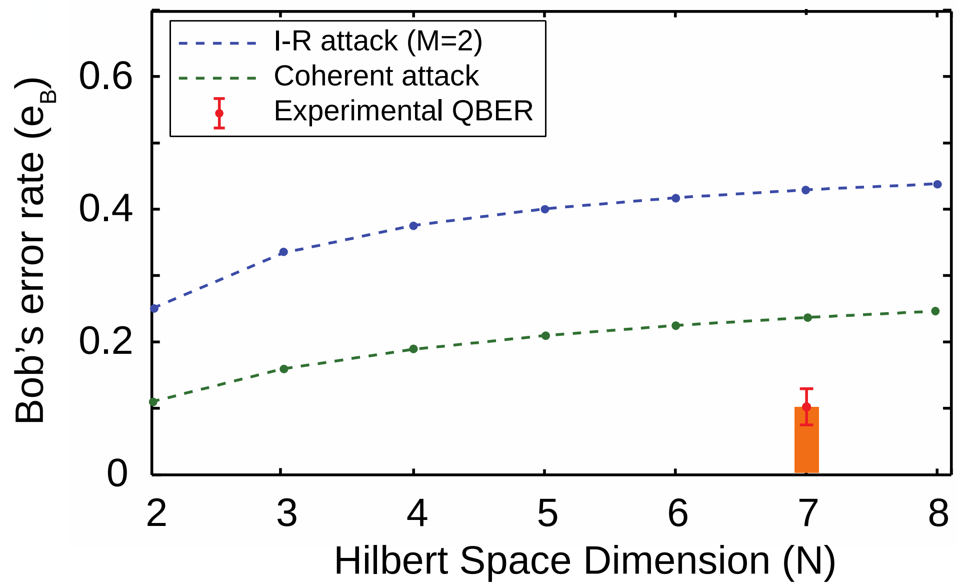
The experimental setup



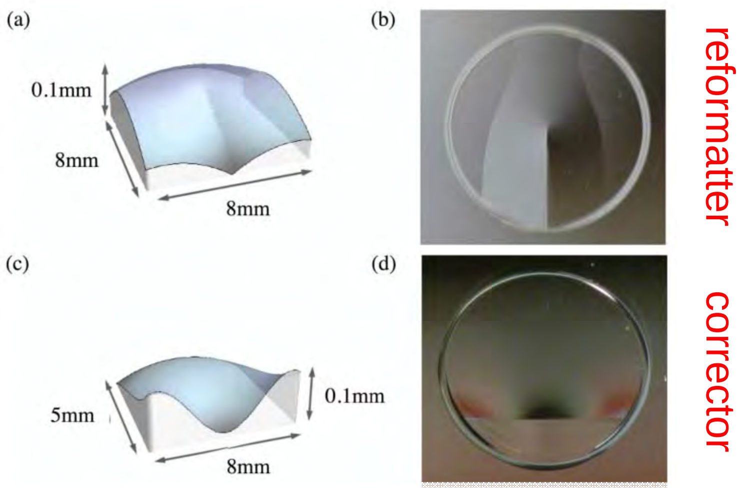
Some results







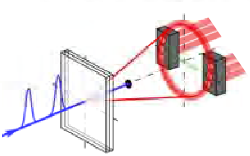
Measuring OAM, a multi-output beam splitter

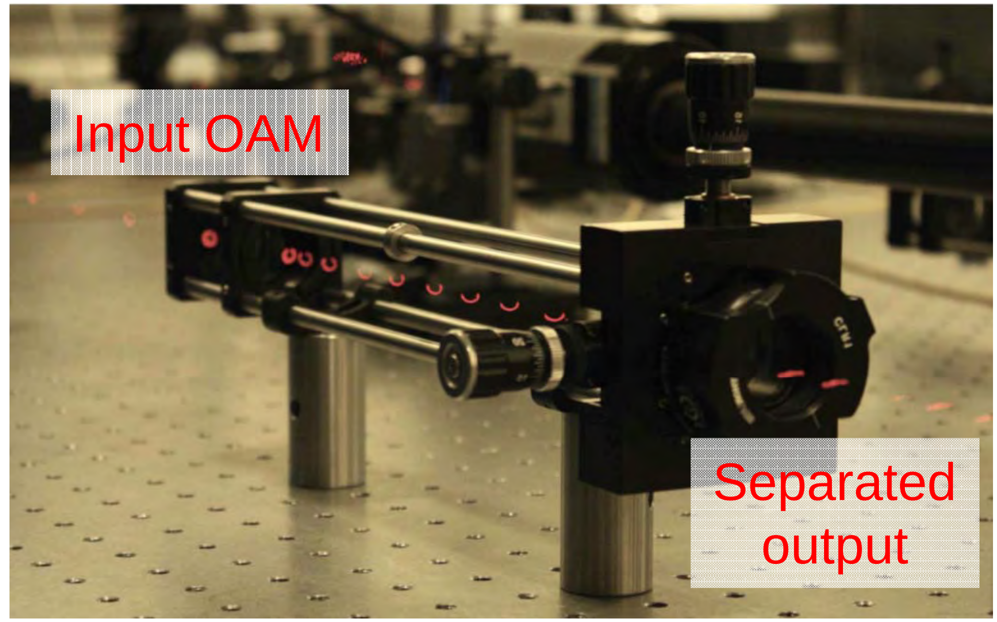


- Two bespoke optical components transform any OAM state to a single spot.
- The displacement of the spot is proportional to the OAM

Refractive elements for the measurement of the orbital angular momentum of a single photon

30 January 2012 / Vol. 20, No. 3 / OPTICS EXPRESS 2110





Mode-sorters enabled further inPho successes
- Boyd Group
- Willner Group

The first reported method for efficient sorting of OAM state, beating the 1/N limit of previous approaches

Direct Measurement of a Statevector in a Very Large Hilbert Space

We have measured the state vector of a state imbedded in a very large (27-dimensional) Hilbert space.

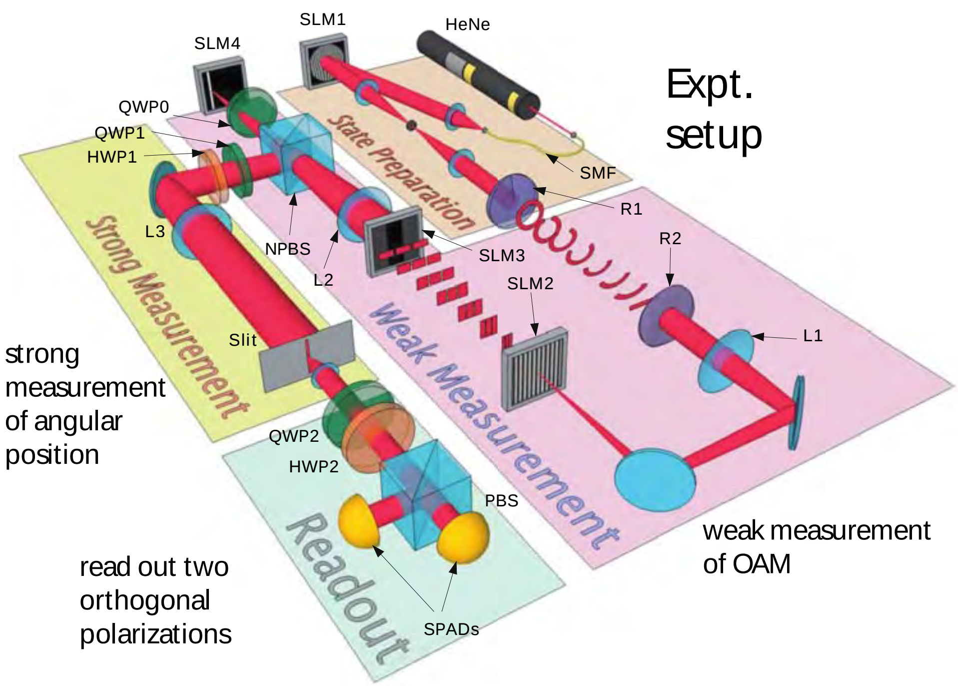
Procedure is based on Aharanov's "weak values" as developed by Lundeen et al. for state determination.

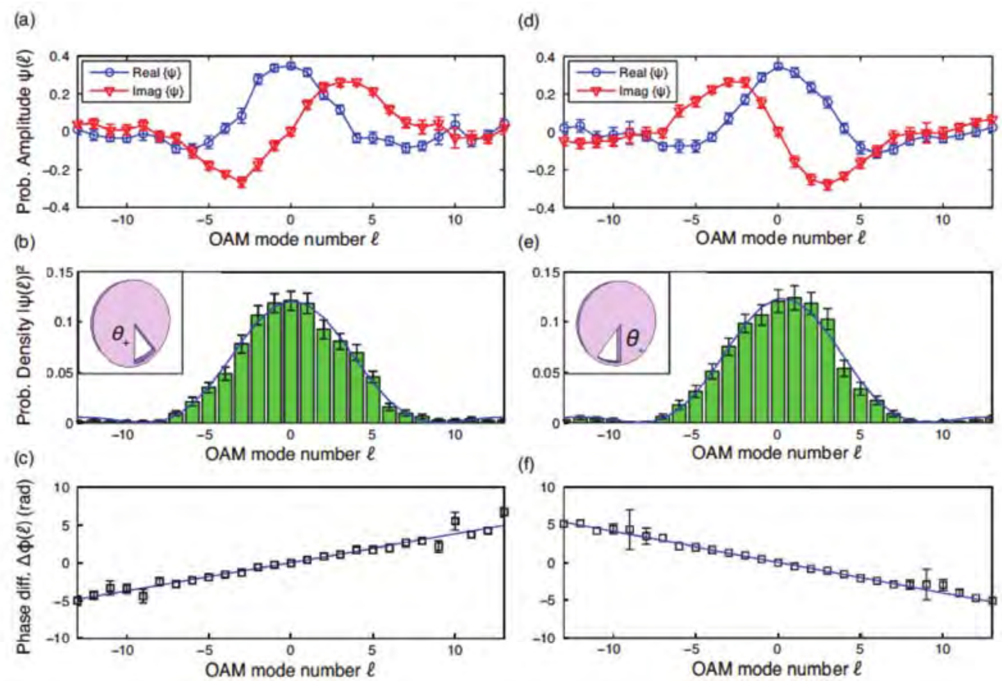
The concept of "direct measurement" based on "weak values" can successfully be applied even to quantum states embedded in a very high dimensional discrete state space.

OAM states $\ell = -13, \ldots, 13$

We measure the statevector of the light transmitted through a pie-shaped wedge

Note that the two cases have the same probability density but di erent phase structures



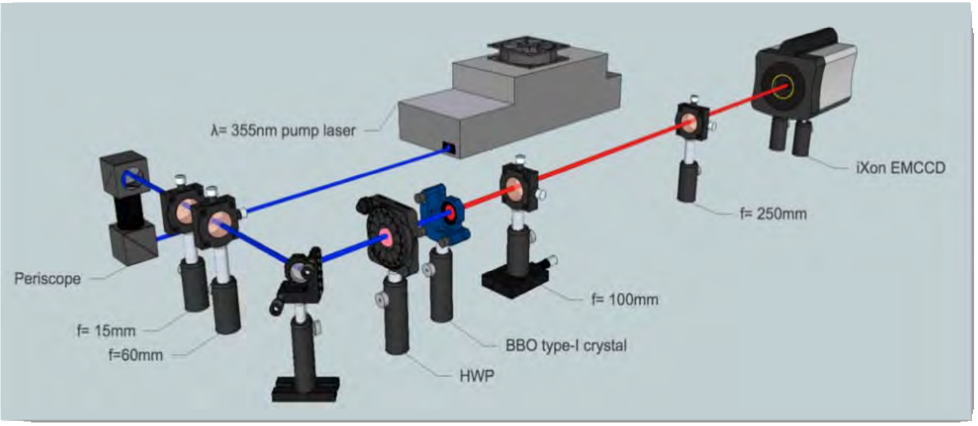


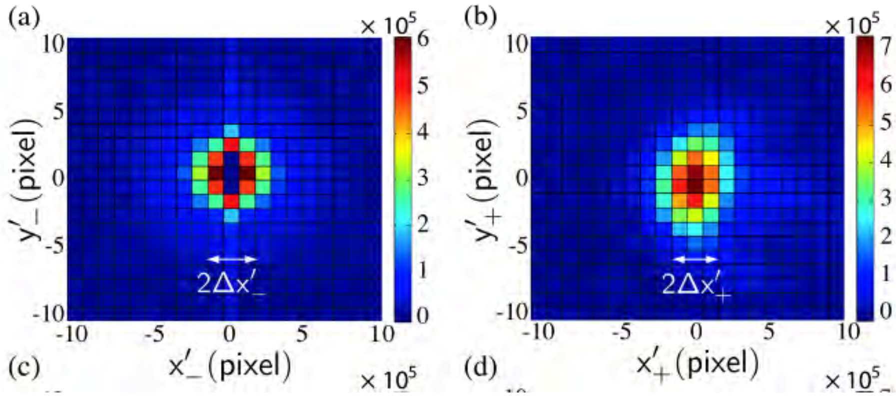
Malik, Mirhosseini, Lavery, Leach, Padgett, Boyd, Nature Communications, 5:3115 (2014)

EMCCD – images of entanglement

- EMCCD using to measure entanglement.
- Hilbert space >2000 modes
- Observation of position OR momentum correlation (i.e. EPR)

- EMCCD Cameras CAN be used high dimensional entanglement





nature COMMUNICATIONS OPEN

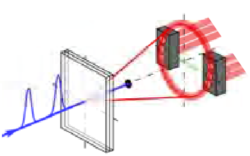
ARTICLE

Received 14 May 2012 | Accepted 4 Jul 2012 | Published 7 Aug 2012 DOI:10.1038/ncomms1988

Imaging high-dimensional spatial entanglement with a camera

EMCCD demonstration

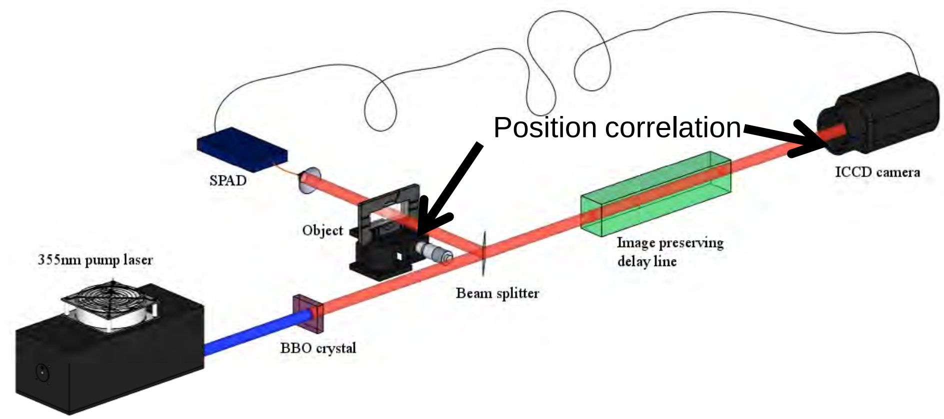
The first Camera-based demonstration of EPR (cameras are multi-dimension detectors, scanning detectors are not)

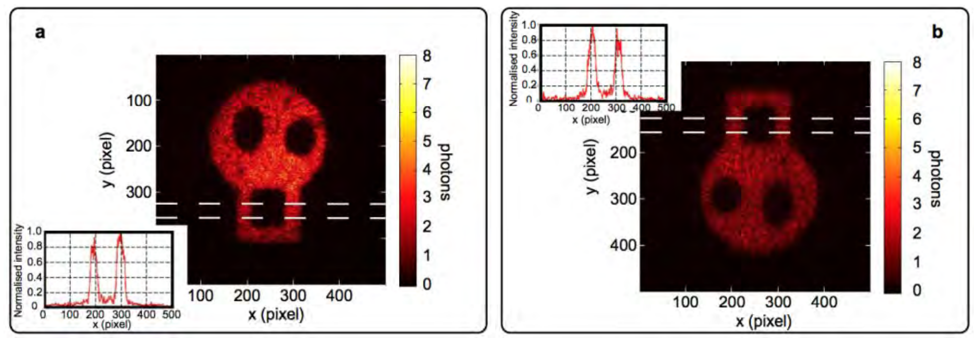


EPR enabled imaging

- Time-gated ICCD camera used for single photon imaging.
- ≈10 bits/photon
- Ghost image obtained from position OR momentum correlation (i.e. EPR)

- ICCD cameras CAN be used to measure high dimensional entanglement





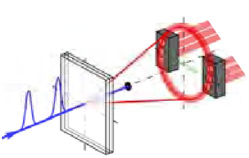
New Journal of Physics
The open access journal for physics

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

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

ICCD demonstration enabled further inPho successes
- Boyd Group

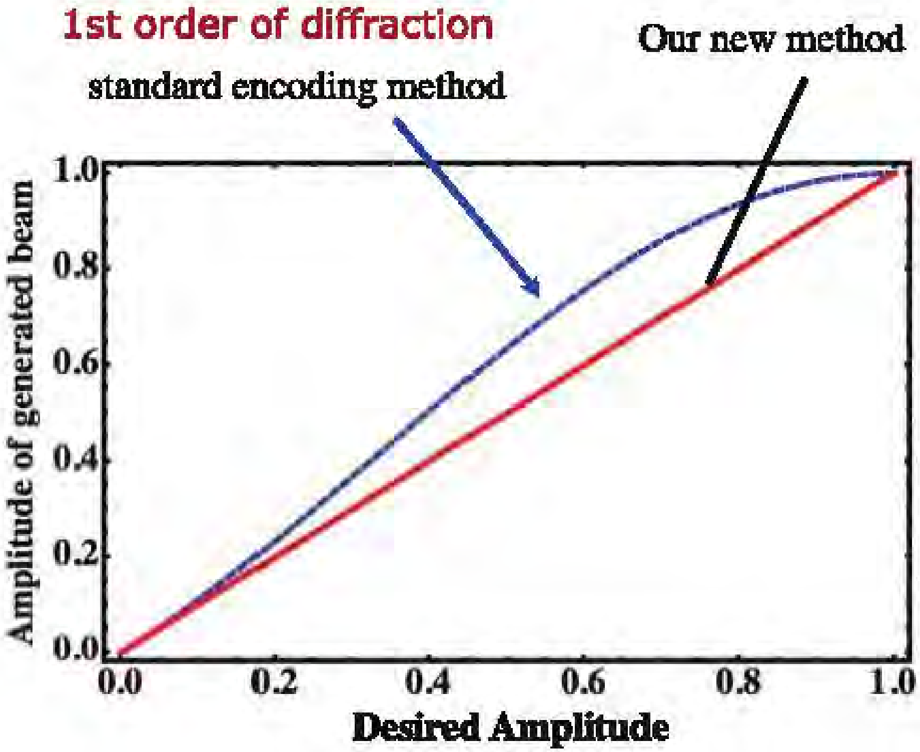
The first Camera-based quantum ghost imaging (cameras are multi-dimension detectors, scanning detectors are not)

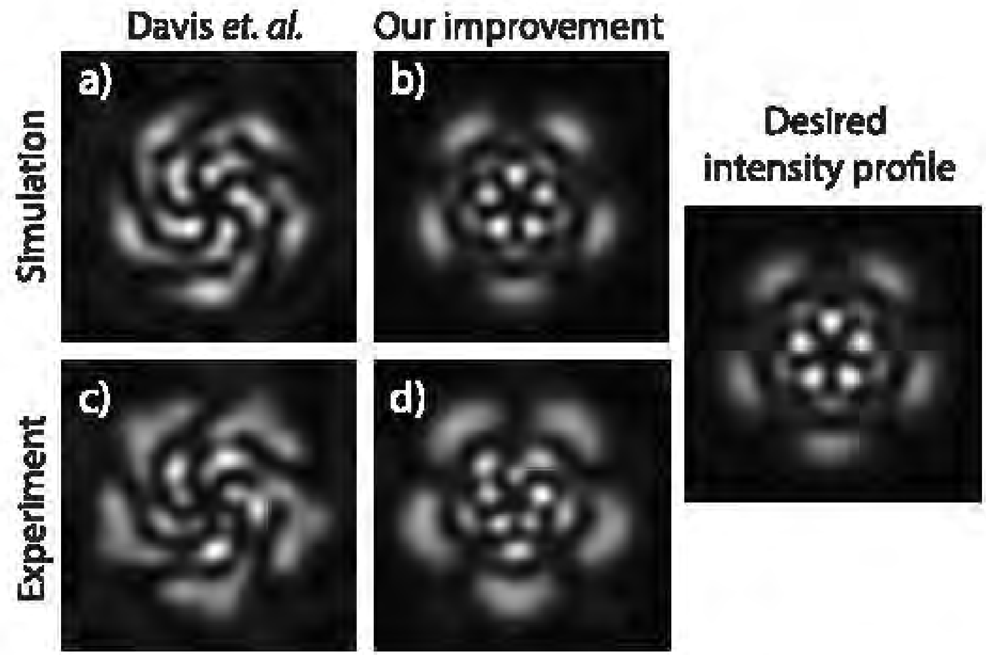


Improved Method for Encoding Computer-Generated Holograms onto an SLM

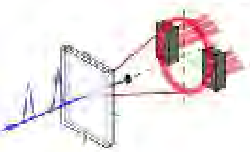
Previously workers used good but only approximate algorithms to encode holograms onto SLMs.

We have developed a protocol for encoding holograms onto an SLM that avoids the problems of earlier designs and that is in fact mathematically exact.



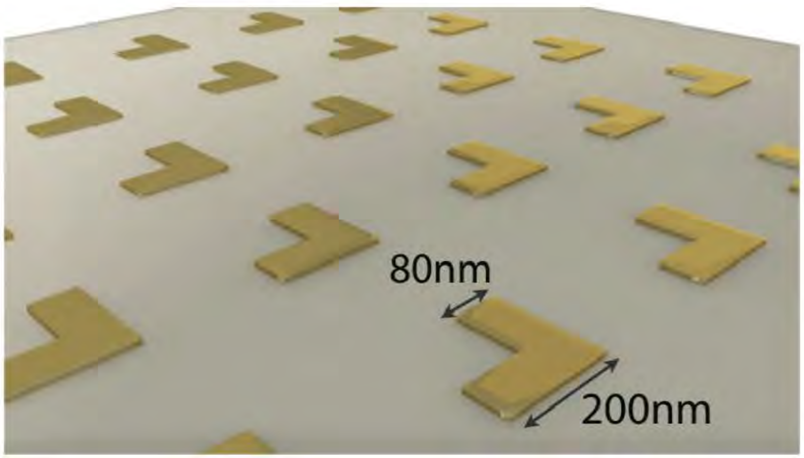


Bolduc et al., Optics Lett. 38, 3546 (2013)

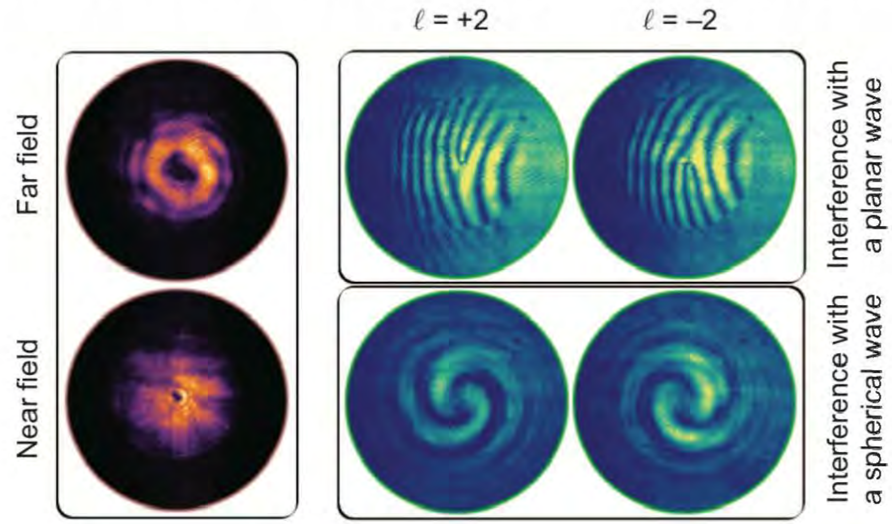


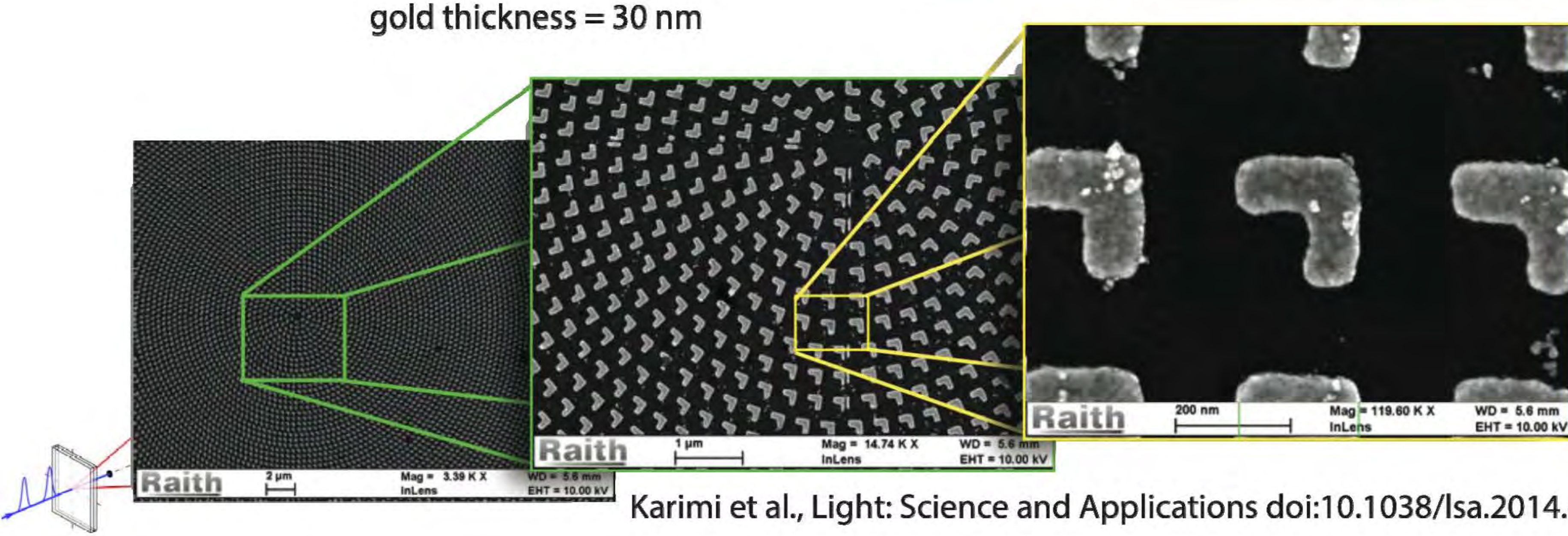
Development of a Nano-Structured Q-plate

- A q-plate is a device that converts spin angular momentum into orbital angular momentum.
- It functions as a quantum interface.
- Have shown ability to construct a spin-angular-momentum to orbital-angular-momentum converter in a structure only 30-nm-thick and thus suitable for use in integrated photonic circuits.



gold thickness = 30 nm

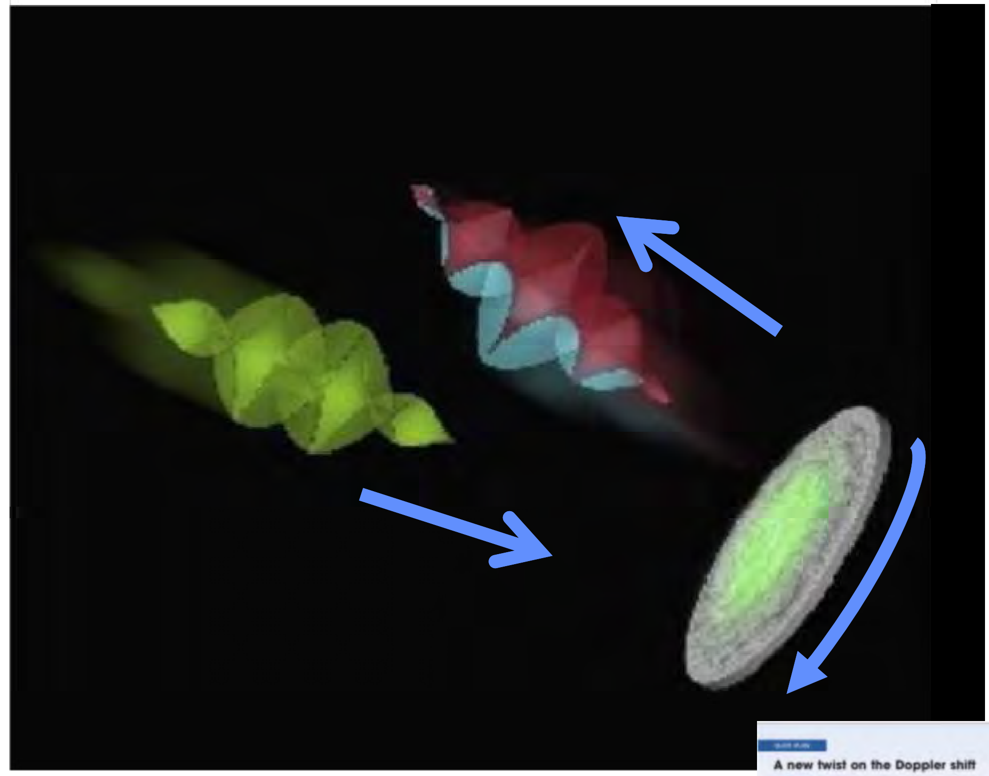




Karimi et al., Light: Science and Applications doi:10.1038/lsa.2014.48 (2014)

Remote detection of a spinning object

- Light scattered from a spinning object is shifted in frequency even when the linear Doppler shift is zero.
- The shift is proportional to the product of the OAM and the rotation speed

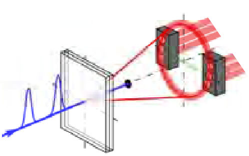



A new twist on the Doppler shift

Detection of a Spinning Object Using Light's Orbital Angular Momentum

SCIENCE VOL 341 2 AUGUST 2013

Featured in Physics Today

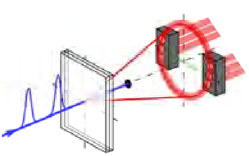


A new form of the Doppler effect, observable even when the traditional Doppler shift is zero

Designing arbitrary mode converters and linear optical components with no calculations

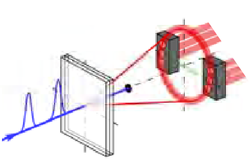
David Miller
Stanford University

Robert Boyd
University of Rochester



Mode converters and arbitrary optical design

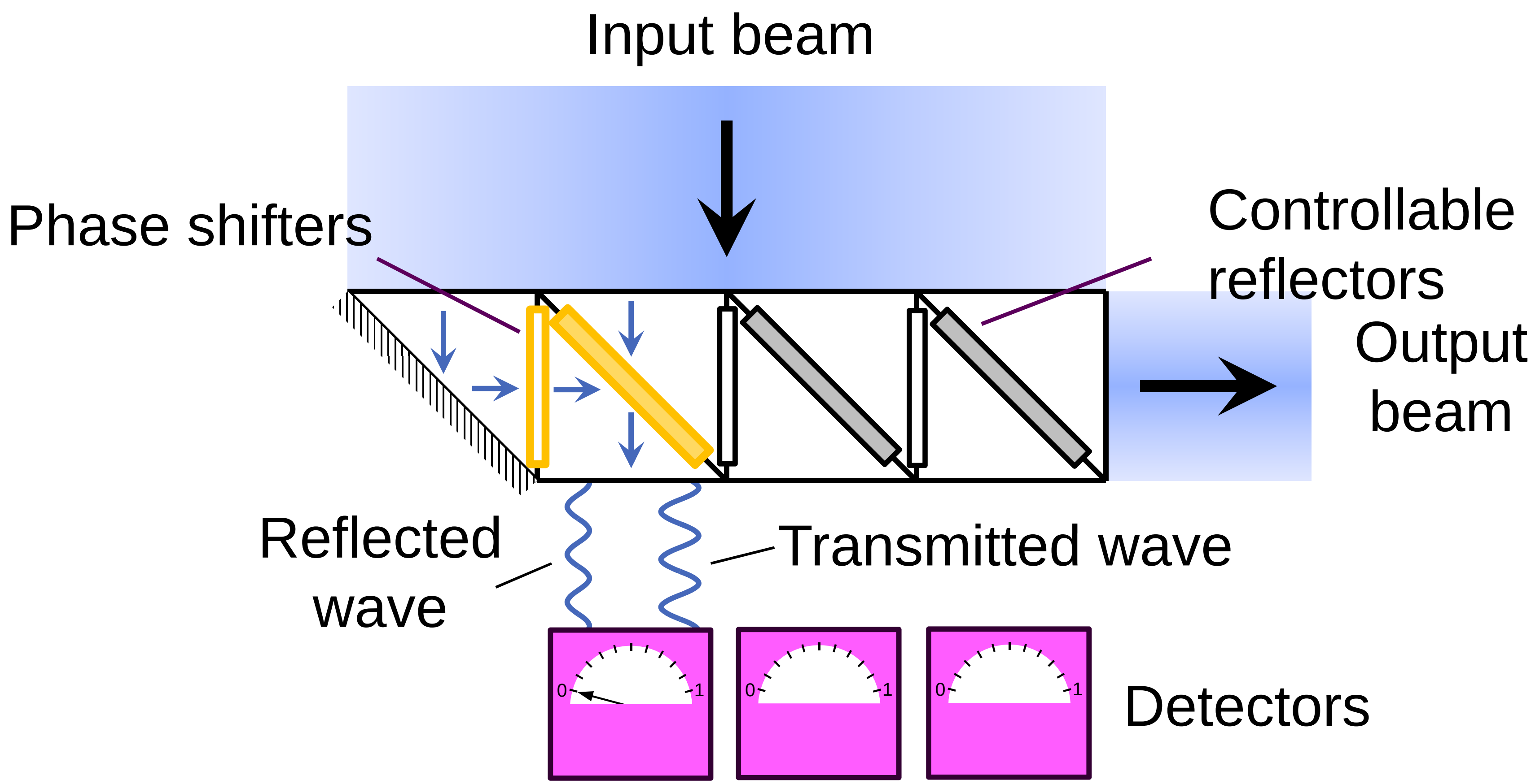
- Major previously-unsolved problem in optics
  - How can separate arbitrary orthogonal but overlapping beams
    - Without fundamental splitting loss?
- **Breakthrough - We have solved this problem**
  - **and** we can prove any linear optical component satisfying basic physical laws can be made in principle
    - with at least one progressive (i.e., non-iterative) way of designing it
- **Breakthrough** - We can also perform the design
  - in real-time in simple hardware, **with no calculations!**
- Additionally
  - We can reduce any linear optical component to a mode converter
  - We can calculate how complicated a component has to be
  - **Breakthrough** - We can automatically find optimum optical channels in linear optics
  - **Breakthrough** - We can design arbitrary spatial add-drop multiplexers



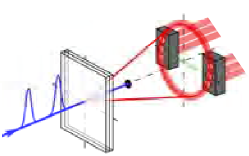
Work also funded in part by AFOSR MURIs
FA9550-10-1-0264 and FA9550-09-0704

David Miller, Stanford

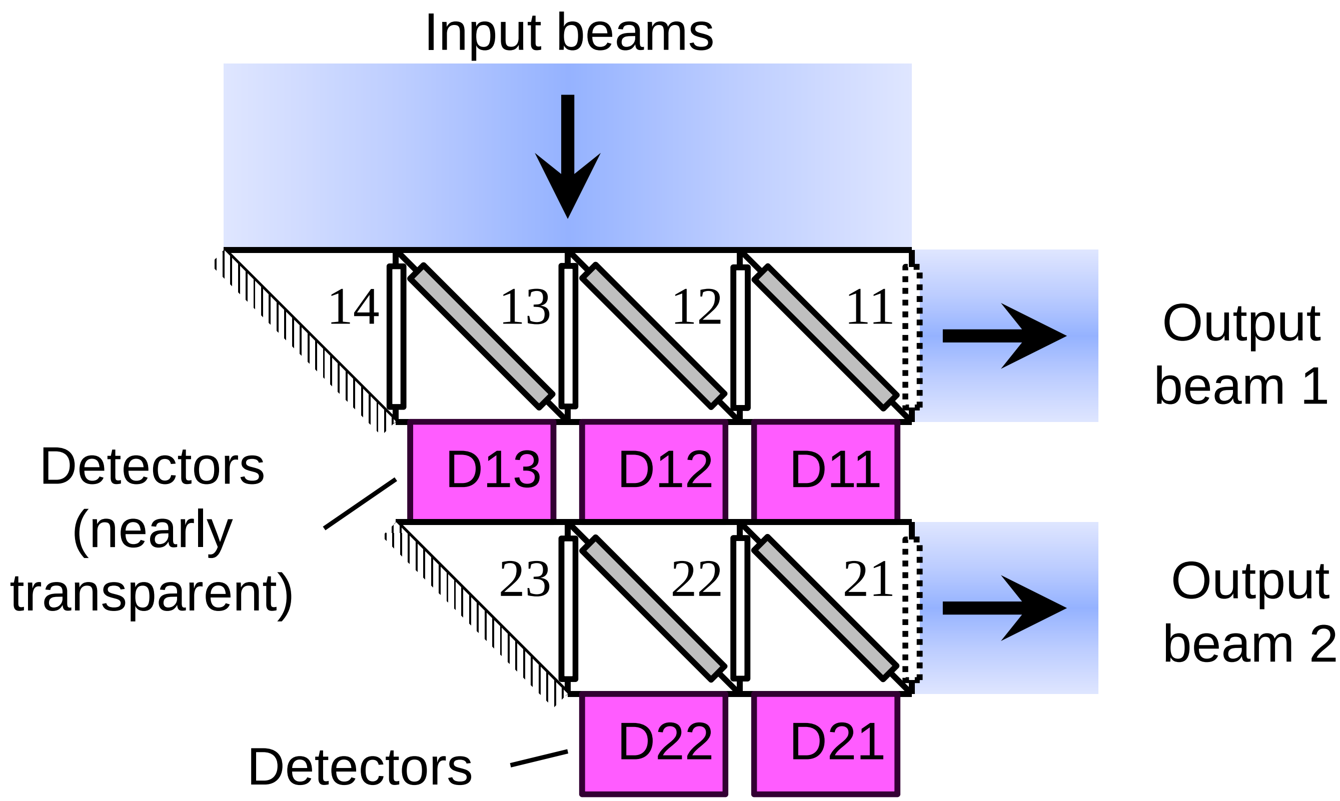
Self-aligning beam coupler



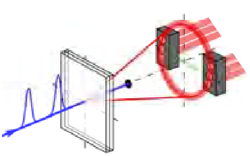
- Suppose a beam can be adequately represented by a finite number of segments
  - Adjust phase shifter in first block to minimize power in first detector
    - Then adjust reflectivity in first block to minimize power again in first detector
      - Repeat for each block
        - Leaves no power in detectors, all input power in output beam
          - Automatically aligns any beam



Self-aligning multiple orthogonal beams

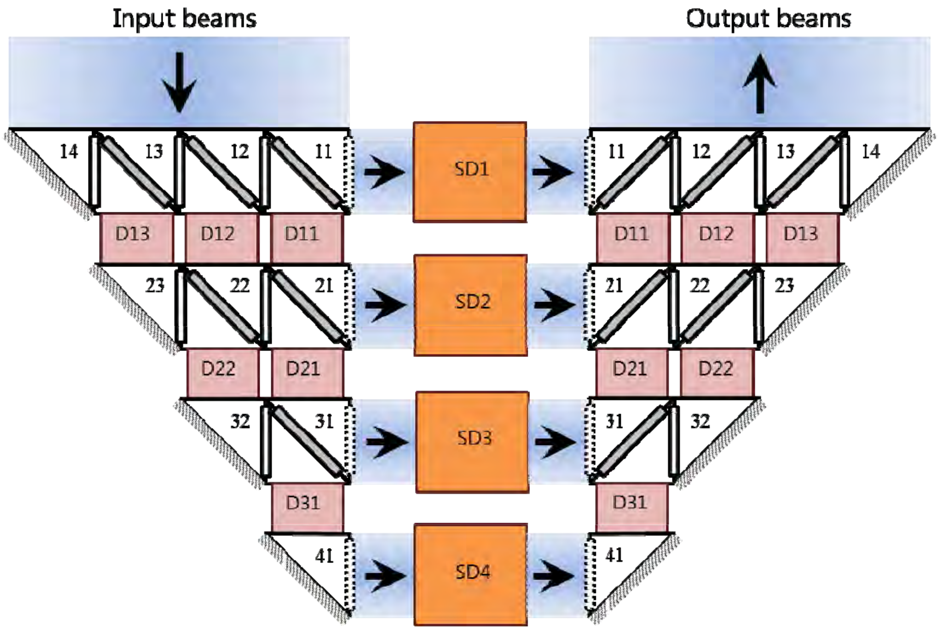


- Once we have aligned beam 1 using detectors D11 – D13
  - An orthogonal input beam 2 passes through the nearly transparent detectors to the second row
    - Where we can self-align it using detectors D21 – D22
- Separating two overlapping orthogonal beams to separate outputs
- Can continue, here up to four separated beams

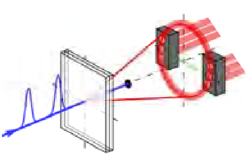


Corollaries and extensions

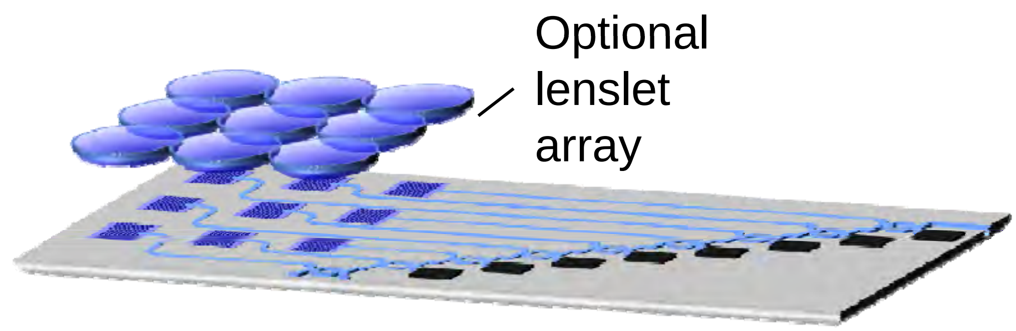
- Make arbitrary beam mode converter (including polarization conversion) by training an output section with desired output beams



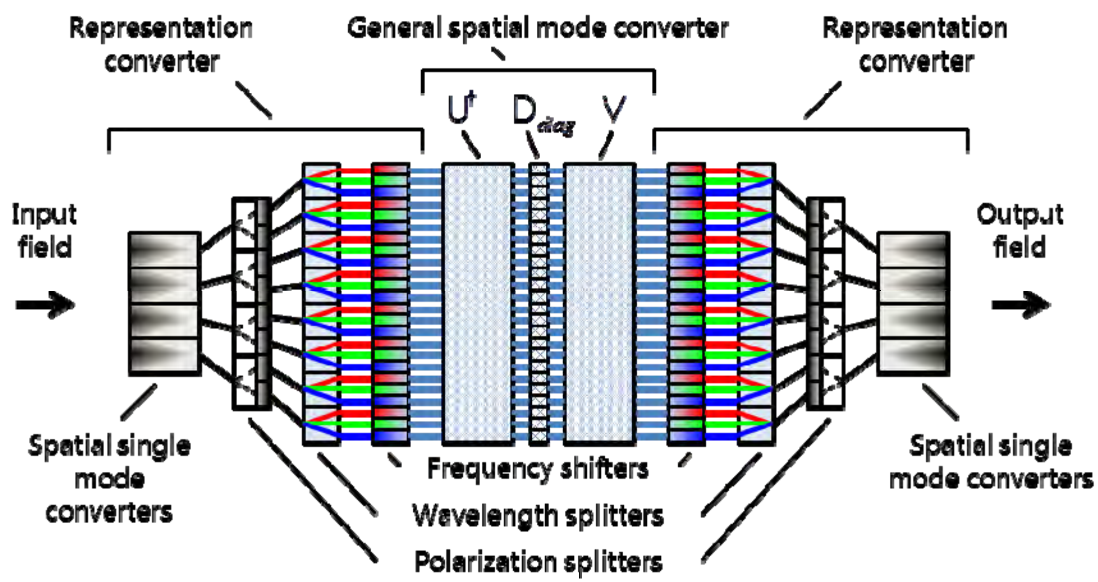
- Establish the optimum channels through arbitrary and changing scattering media
- Arbitrarily add and drop spatial modes losslessly



- Implement in silicon photonics with grating couplers and Mach-Zehnders



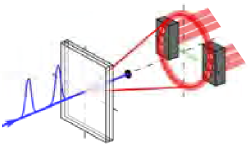
- Make any linear optical component in principle



Turbulence simulation and mitigation

Robert Boyd
University of Rochester

Glenn Tyler
the Optical Sciences Corporation

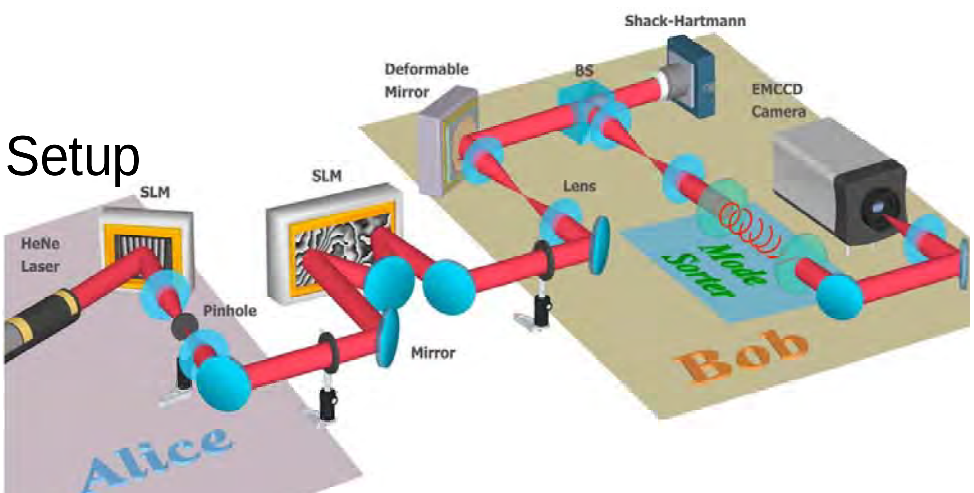


Accurate Simulation of Atmospheric Turbulence using Two Phase Screens

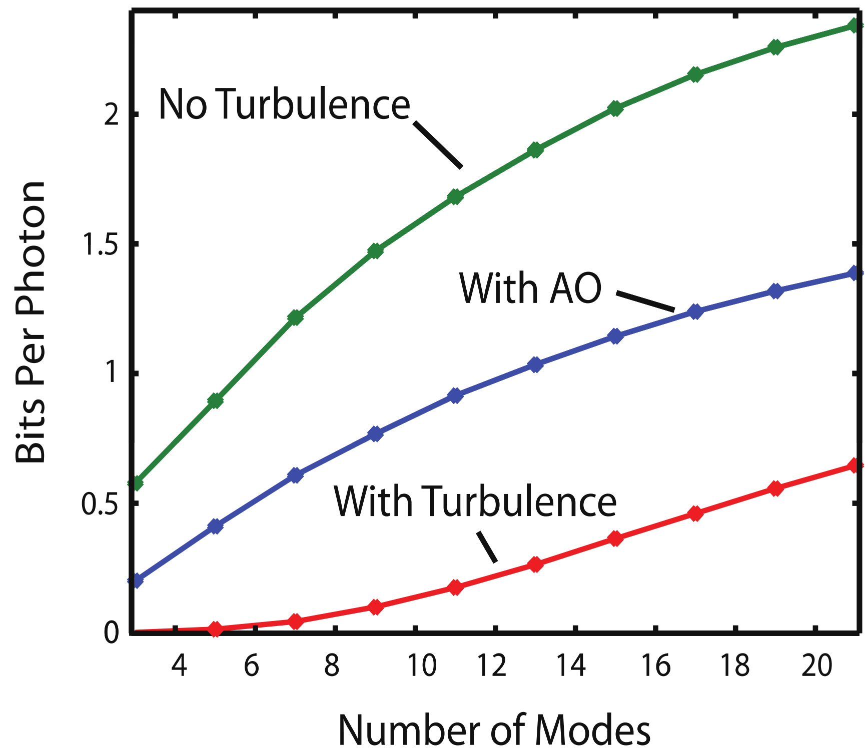
- A single Kolmogorov phase screen cannot model thick turbulence
- But only two phase screens are needed for realistic horizontal paths!
- Results given for 1 km path and $C_n^2 = 1.8 \times 10^{-14}\,\mathrm{m}^{-2/3}$
- By reversibility, only two deformable mirrors required to perform adaptive optics.

No turbulence | With turbulence | Turbulence and AO

Setup



Channel capacity

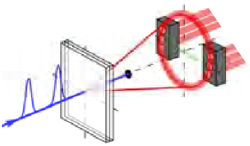


Rodenburg et al., New J. Physics 16, 033020 (2014).

Summary

We have developed a complete QKD system that operates at a

- record rate (on a table top)
- record efficiency
- encodes information in photon arrival time and polarization
- partial security obtained by checking polarization (assumes no QND attack possible that does not disturb polarization)
- a single channel operates at a “secure” rate over 10 Mbit/s
- multiplex many spatial and spectral channels to achieve 1 Gbit/s rate
- achieve > 4 bits/detected photon pair at high rate
- achieve > 8 bits/detected photon pair at low rate (maintain coherence in a very high dimension Hilbert space!)
- developed a wide range of new quantum technologies that will have an impact beyond this immediate project

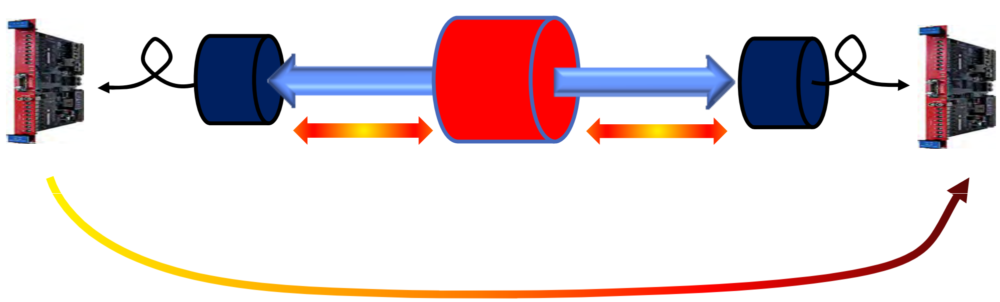


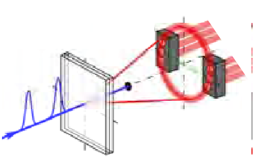
Quantum Key Distribution Using Hyperentanglement

Question: What are the fundamental limits of encoding/decoding information on a photon?

Goal: Develop a free-space, entanglement-based quantum key distribution (QKD) system that achieves >10 bits/photon received and >1 Gb/s

Steve Barnett, Strathclyde, **Robert Boyd**, Ottawa,
Daniel Gauthier, Duke, **Paul Kwiat**, UIUC, **David Miller**, Stanford,
Miles Padgett, Glasgow, **Glenn Tyler**, tOSC
Advisors/Partners:
Venkat Chadra, MIT Lincoln Labs, **Norbert Lütkenhaus**, U. Waterloo
Sae-Woo Nam, NIST





Primary Duke InPho Quantum Key Distribution System: Details for Site Visit

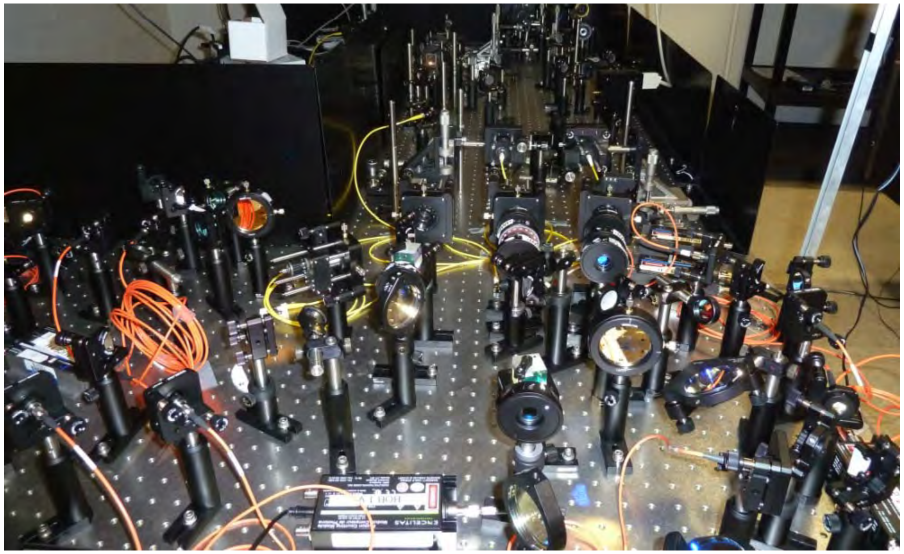
Paul Kwiat
University of Illinois, Urbana-Champaign

Daniel Gauthier
Duke University

Duke InPho: Free-Space Quantum Key Distribution
Quantum Communication

Accomplishment: **Set up 2-channel hyper-entanglement-based QKD system, with time-bin PPM secured using simultaneous polarization entanglement.**

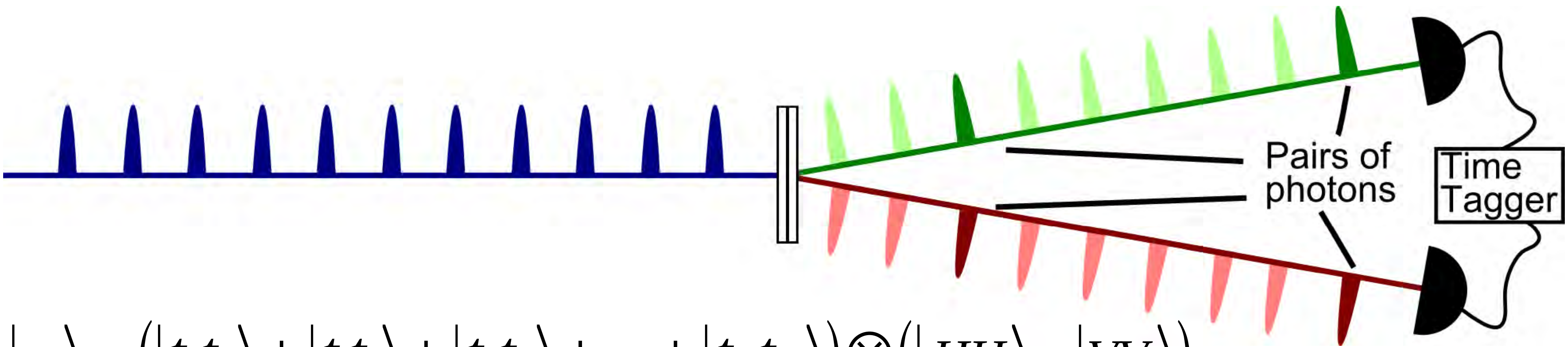
- Low jitter detectors (average 158-ps FWHM)
- x32 repetition-rate multipliers increase pulse frequency to 3.84 GHz
- Reduced detector deadtime (~25 ns) allows for high saturation
- Still photon-number limited
  - Use few-mode fibers (~x7 brightness)
  - Polarization decoherence issues with few-mode fiber
- Assumes intercept-resend attacks, and no polarization-independent QND measurements



June 2014	Low Power	High Power
Singles	50 kHz	10.1 MHz
Coincidences	8 kHz	2.9 MHz
Average BER	0.4 %	0.9 %
“Secure” bit/coincidence	8.3 bits	**2.2 bits**
“Secure” bit/second	67 kbits	**6.3x2 Mbits 12.6 Mbits**

Hyper-entanglement Secured QKD

Central Concept: Encode in time, verify in polarization



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

Alice and Bob use which time bin they detect a photon in to generate multiple bits per click, e.g., 1 pair in 1024 bins (2^{10}) → ~10 bits

Get extra 0.5 bpp from BB84 w. polarization.

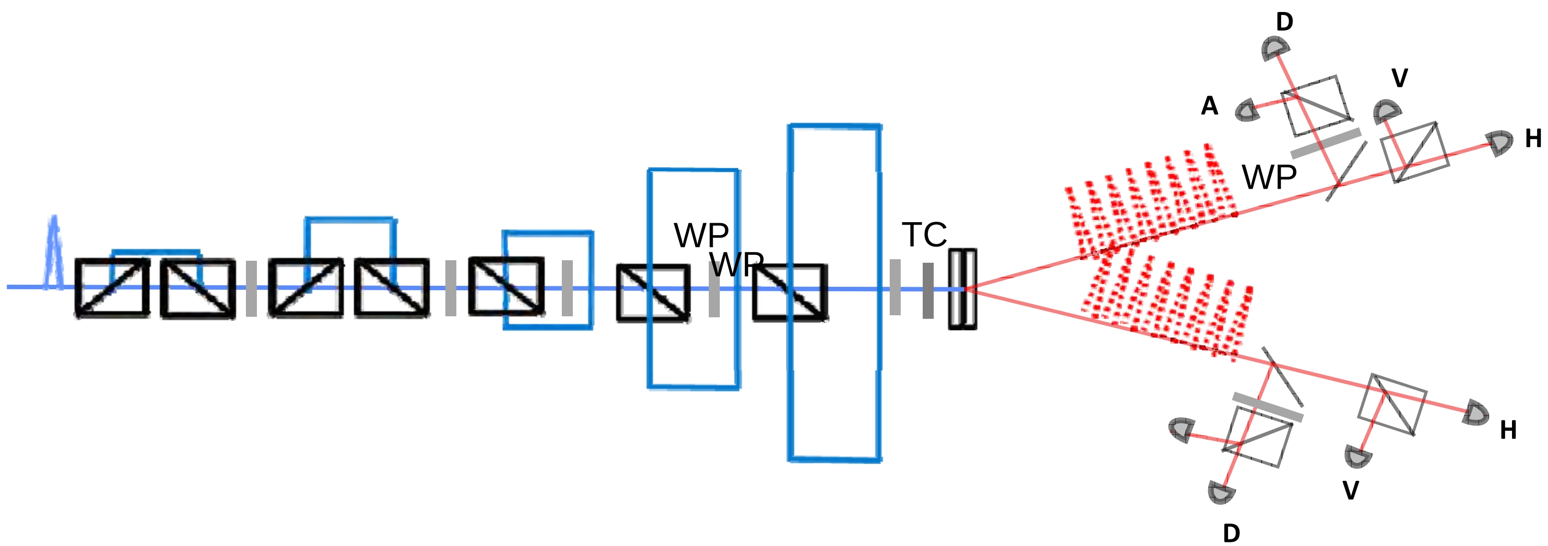
They can constantly check for an eavesdropper using the polarization DOF (assuming no QND capability for Eve).

Perform NON-standard error detection/correction and privacy amp.

First experiment to use one DOF to secure another.

Repetition Rate Multiplication System

Implemented rep-rate multiplication system (x32) to achieve detector-jitter limited system.



- Repetition-rate multipliers increase pulse frequency from 120 MHz → 3.84 GHz
- Time-bins (~260 ps) comparable to combined detector/time-tagger jitter
- Use spectrum-analyzer and high-speed detector to ~match path lengths (necessary for eventual mutually-unbiased basis checking)

World-Record Heralding Efficiency

Source Quality:

- $\eta = \eta_{spatial} * \eta_{spectral} * \eta_{optics}$
  $= 0.9 * 0.95 * 0.95 = 0.81$

- Used in detection-loophole-free Bell test

- Visibility in all bases >99.7% using temporal compensation,

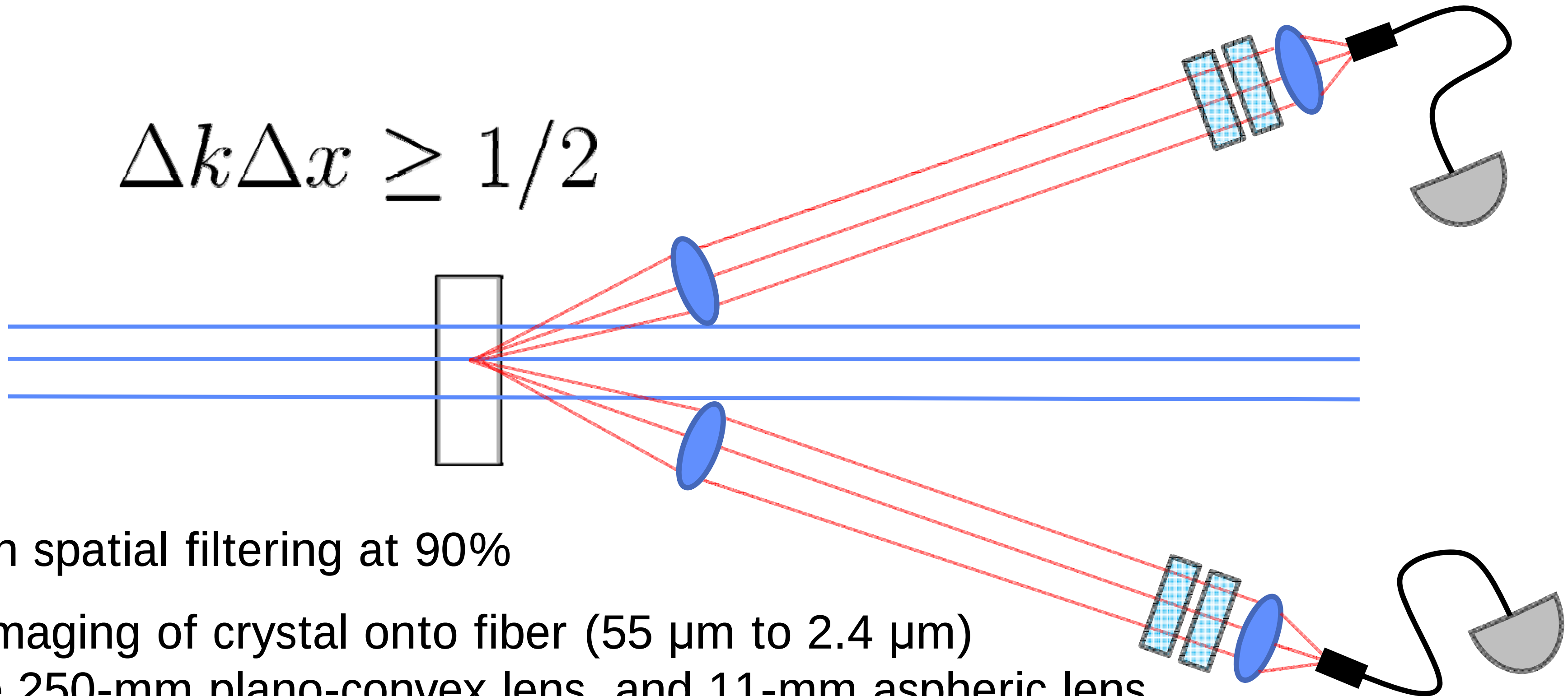
- World-record (?) pair production rate of 30 MHz into a single mode (over a >20 nm bandwidth at 710 nm)

- Other improvements possible (*e.g.*, achromatic coupling)

Developed one of the world's best entanglement sources.

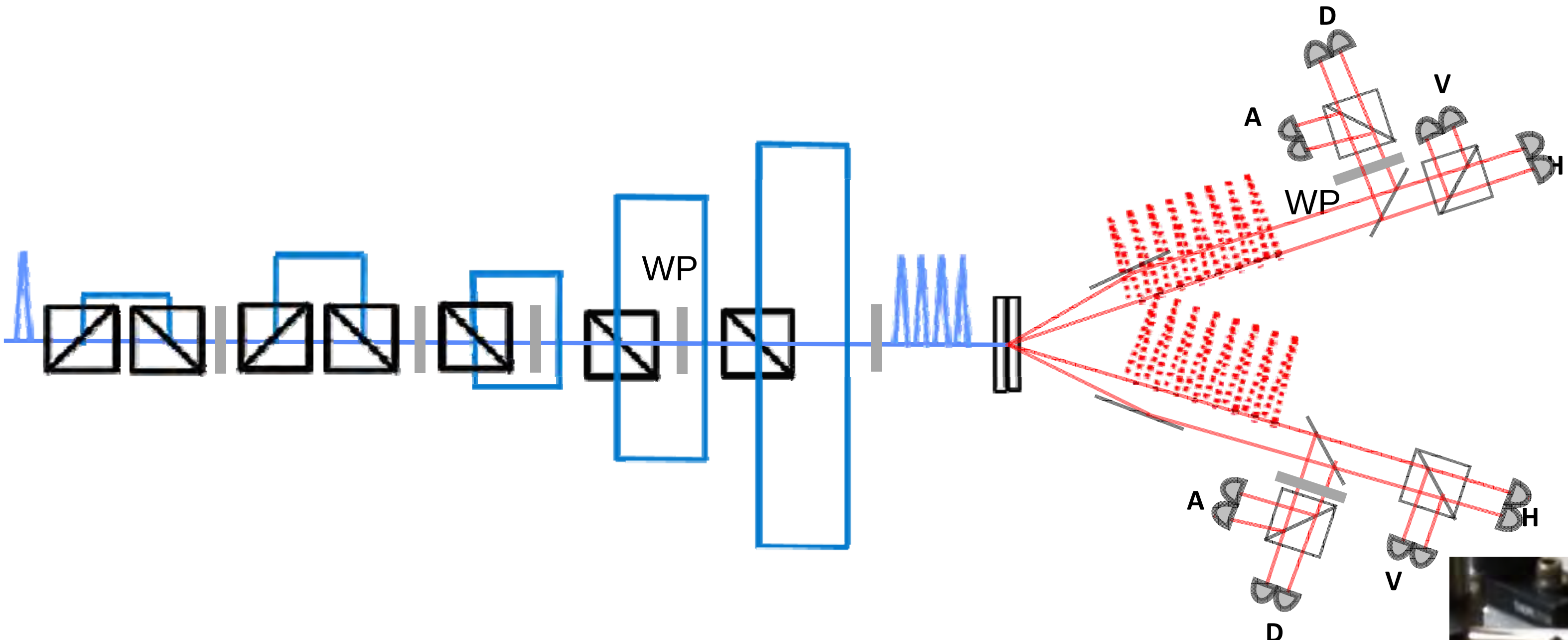
Spatial Collection Efficiency

$$\Delta k \Delta x \geq 1/2$$

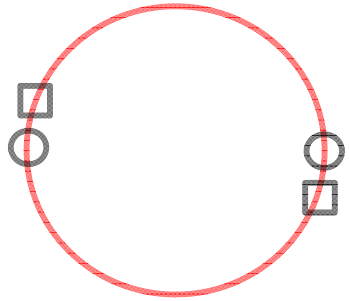


- Gaussian spatial filtering at 90%
- ~23:1 imaging of crystal onto fiber (55 μm to 2.4 μm)
  - Use 250-mm plano-convex lens, and 11-mm aspheric lens
- Pump radius of ~150 μm
  - Optimizes heralding efficiency over brightness
- 600-μm crystal
  - Reduced efficiency with two-crystal collection (90→78%) primarily from birefringent walk-off
  - Correctable using second birefringent 'stitching' crystal
- Chromatic aberration in collection lenses adds ~3% coupling loss
  - Optimized lenses should improve spatial collection efficiency 90 → 93%

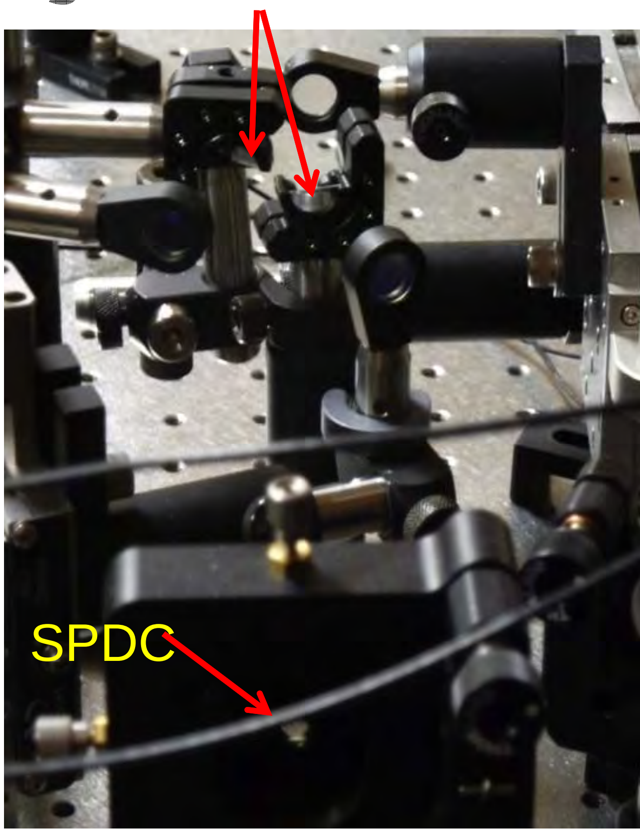
Add a second channel…



End view of SPDC cone



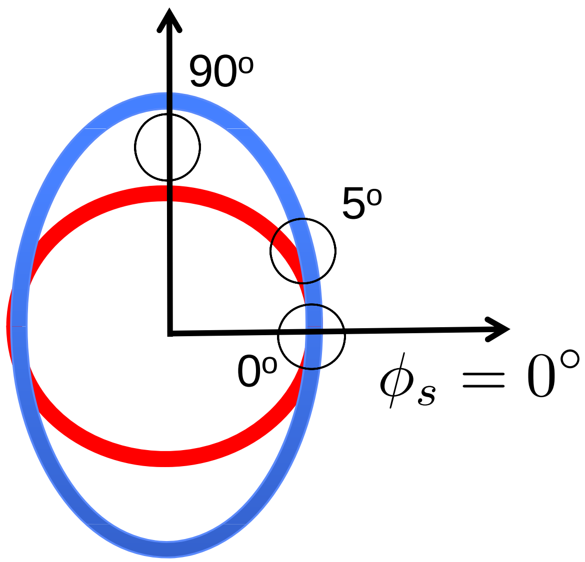
Pickoff mirrors



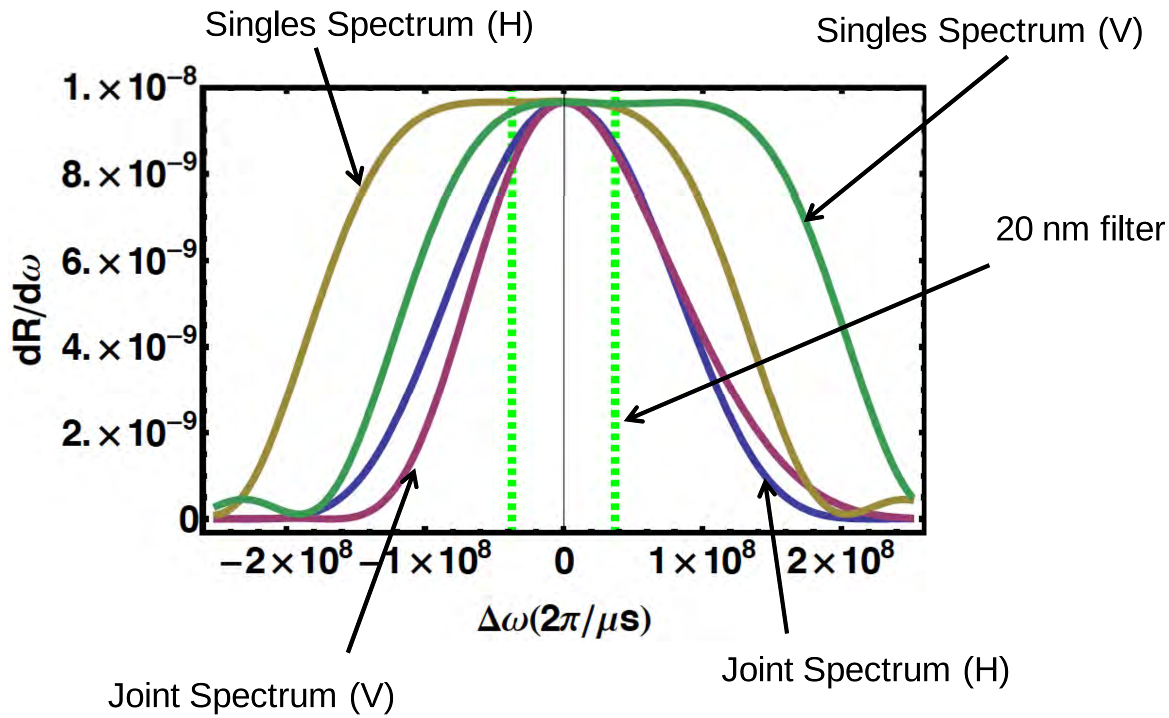
- 2nd-channel C/S ~47% (more constraints)
- Intrinsic pol BER still < 0.8%
- Currently 'time-sharing' time-taggers with Channel 1
- GOAL: 10 pairs around the cone (20 is feasible)

Heralding Efficiency for BiBO source

InPho Breakthrough – Develop complete model for coupling bi-photons into single mode fibers. Accounts for elliptical shape of down-conversion ring, spatial-spectral coupling



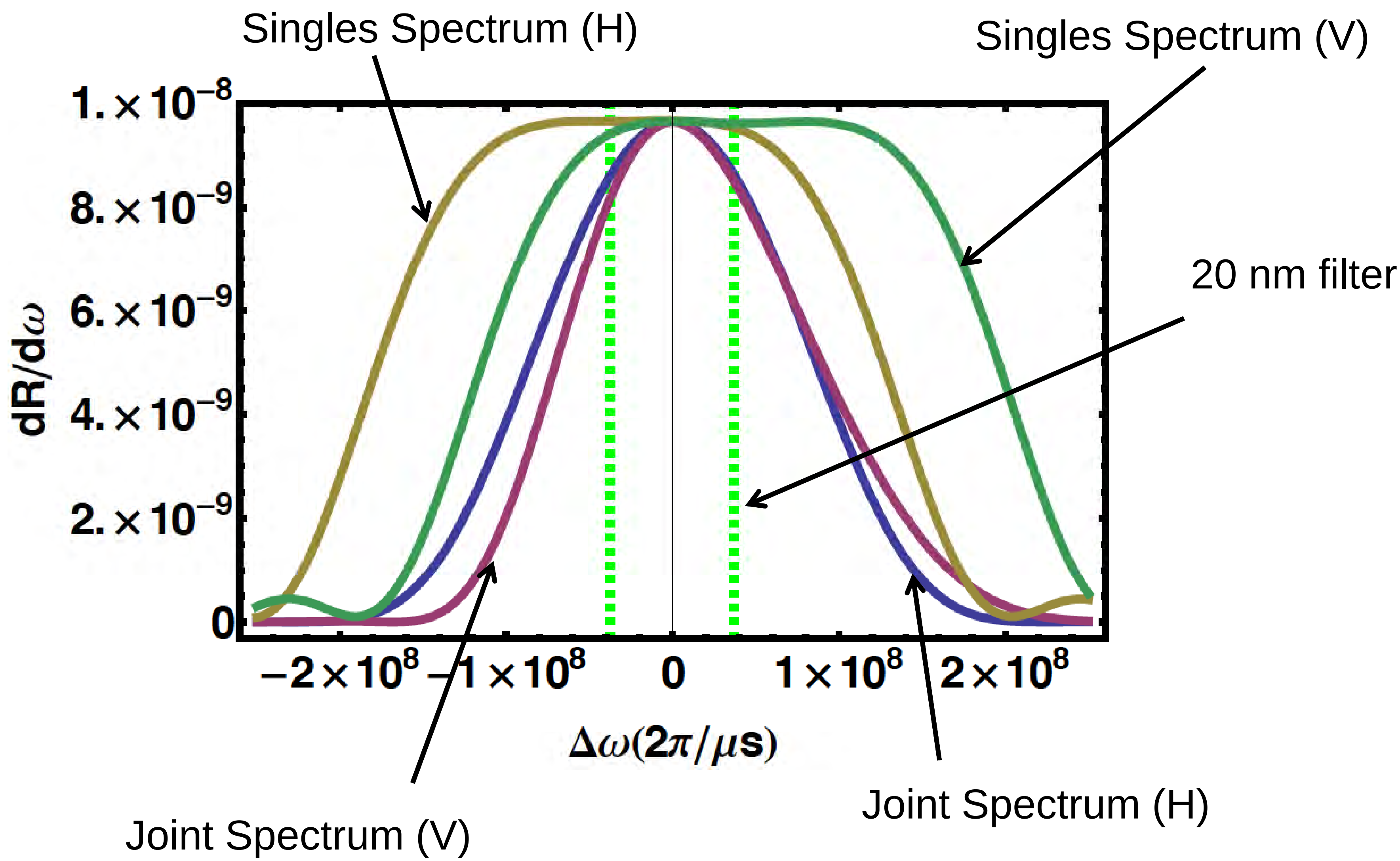
Note: Eccentricity exaggerated in drawing



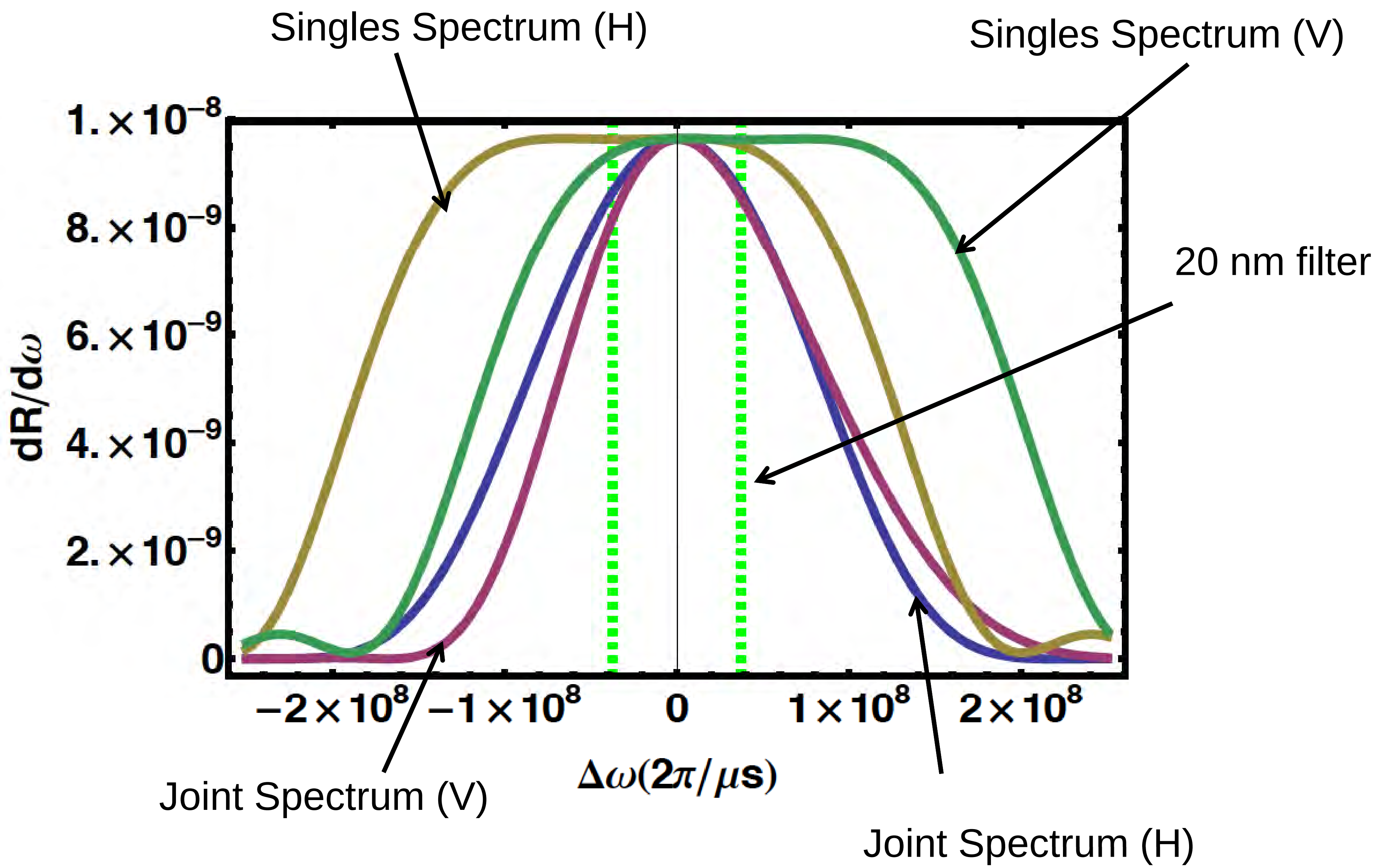
	Visibility	HE (H)	HE (V)
0o	99.986%	96.44%	95.71%
5o	99.982%	95.62%	96.23%
90o	99.971%	96.64%	95.84%

Predicted polarization visibility spatial/spectral heralding efficiency (20 nm bandwidth)

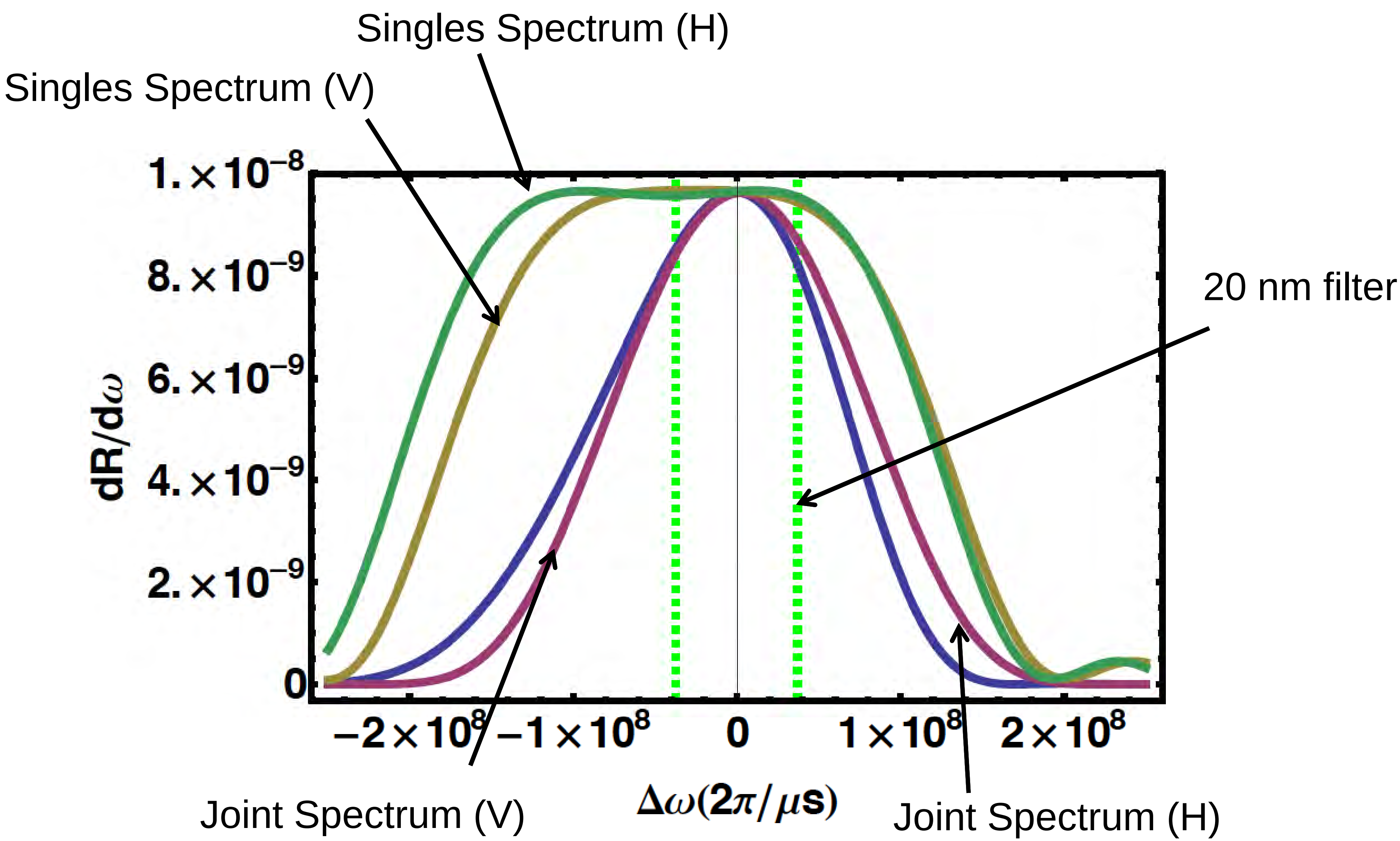
Spectra at 0º



Spectra at 5º

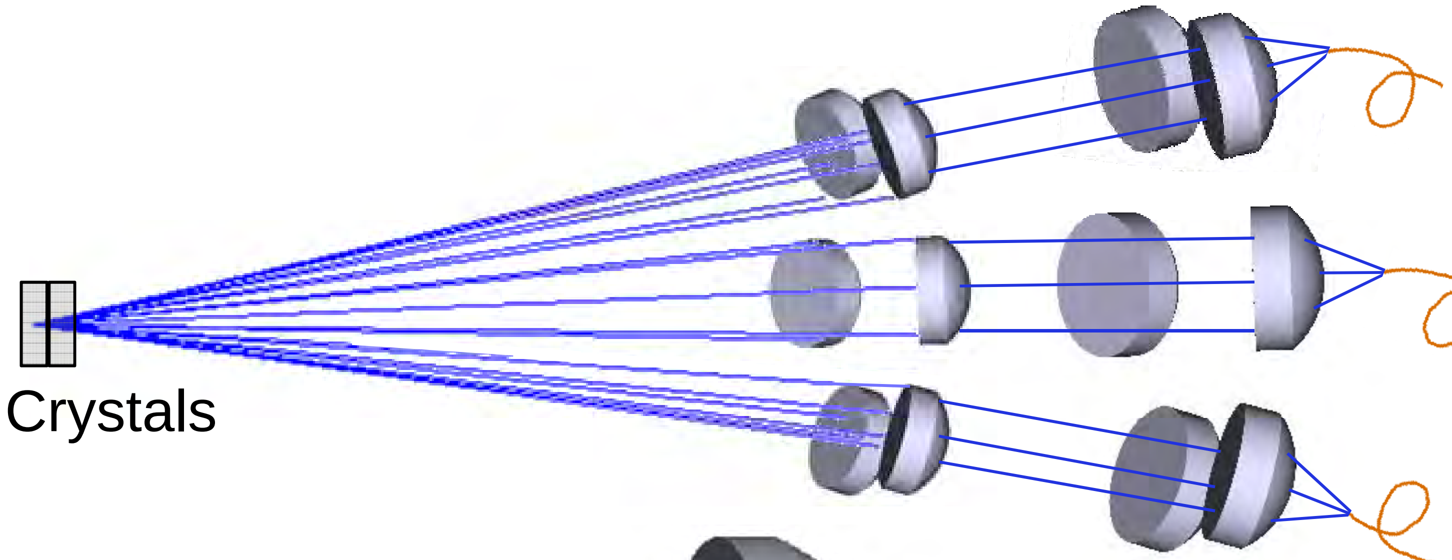


Spectra at 90º



Multi-channel collection optics

By collecting from multiple paired locations, count rates are directly increased.

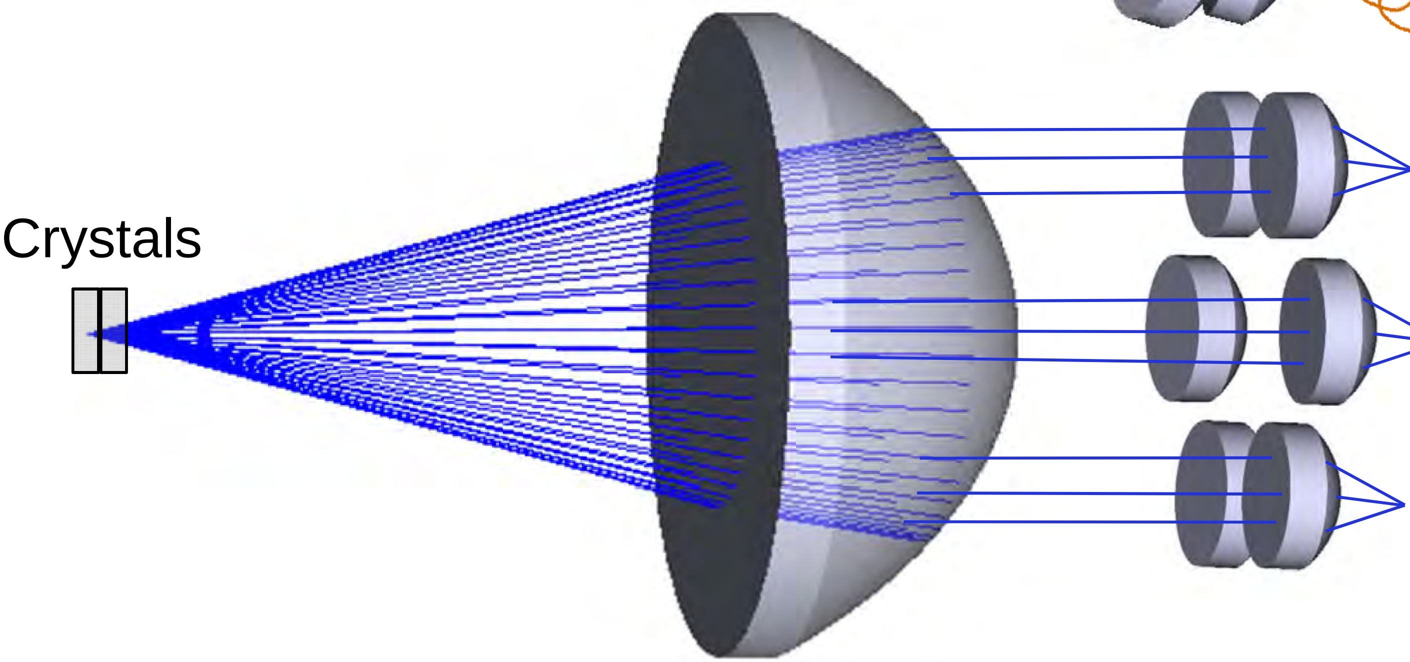


Single-mode fibers

Ideal case:
two lens arrays,
centered on a sphere

- hard to fabricate

- hard to align



Simpler setup:
lens and flat lens array

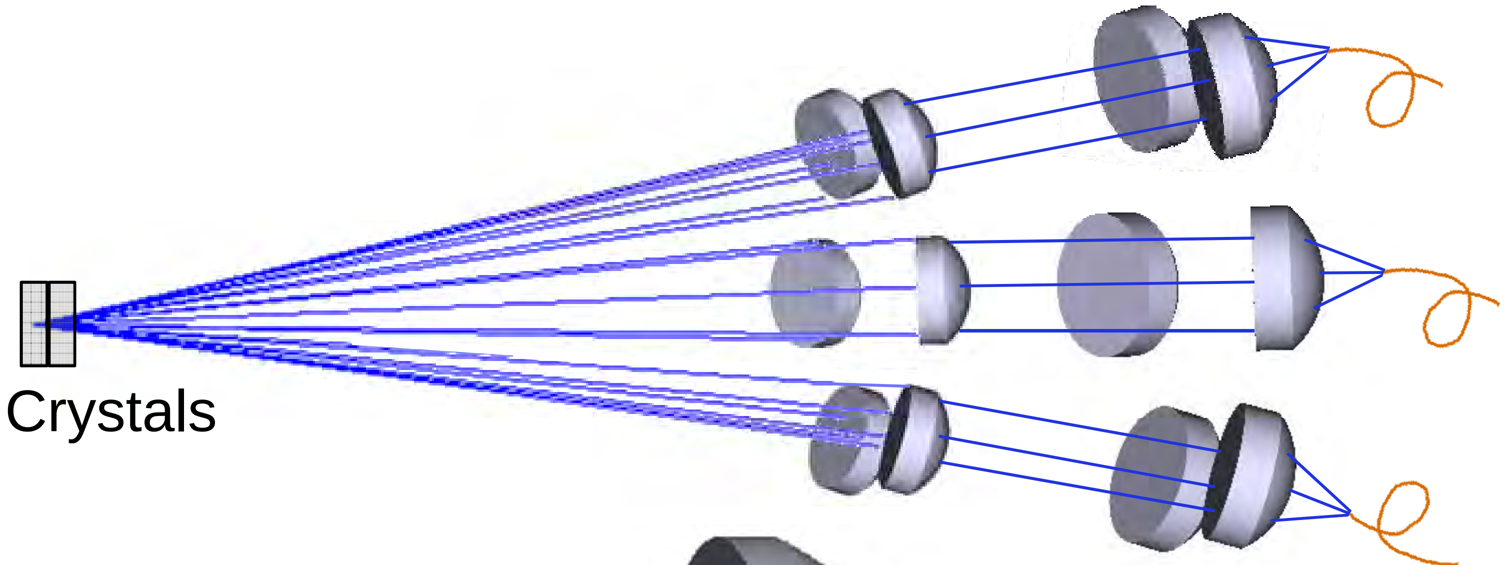
- 99.5% of theoretical maximum coupling

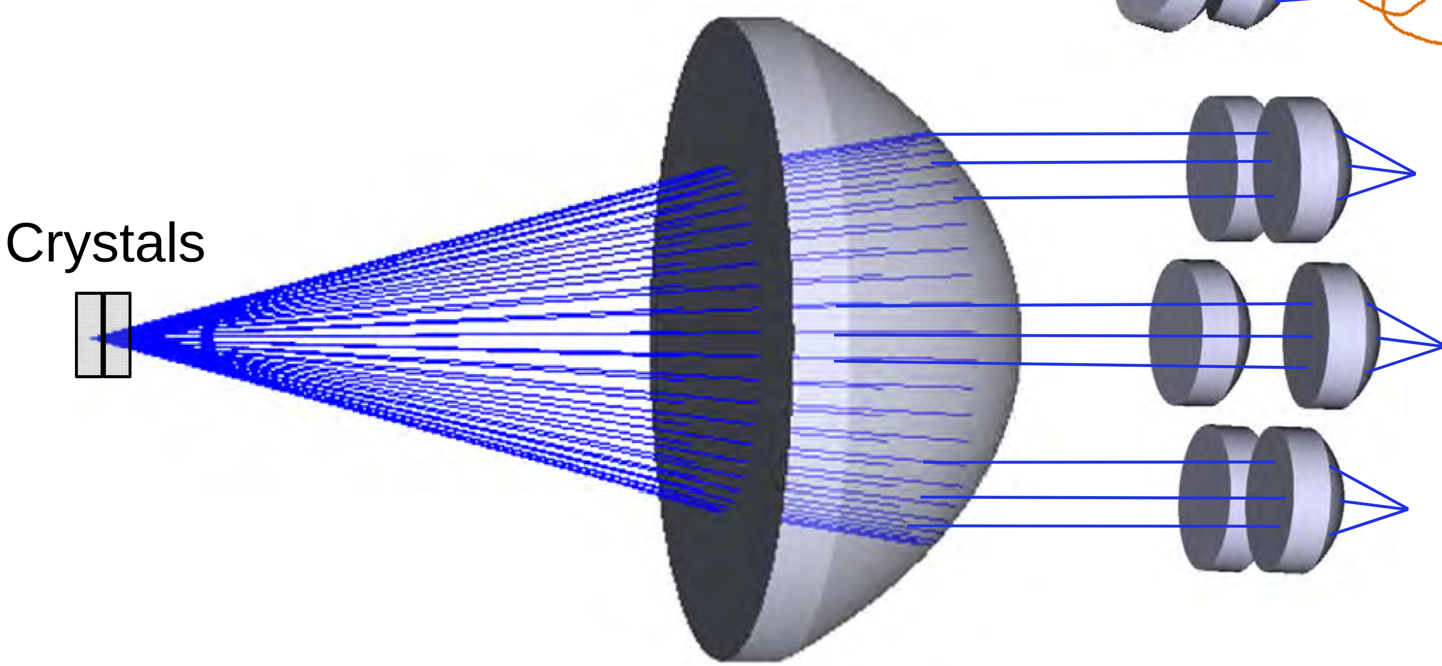
- robust to tolerancing

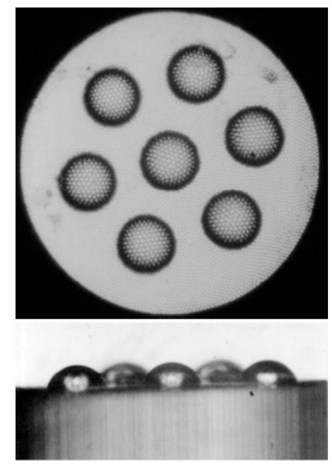
- commercially available

Multi-channel collection optics

By collecting from multiple paired locations, count rates are directly increased.

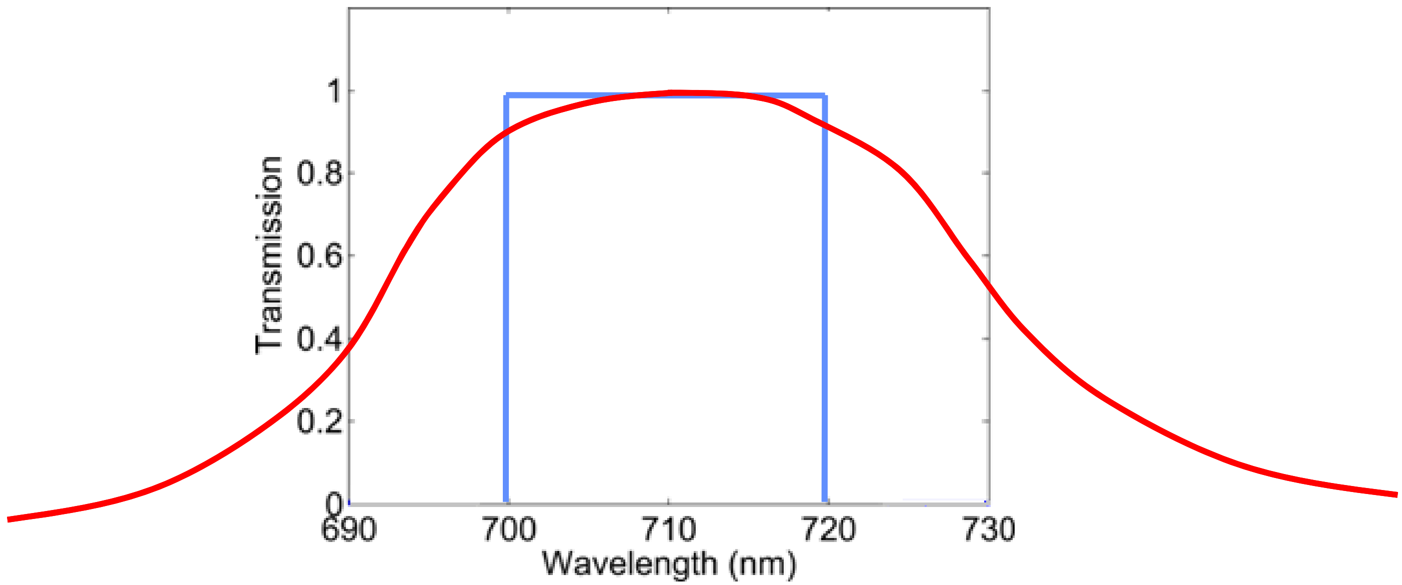






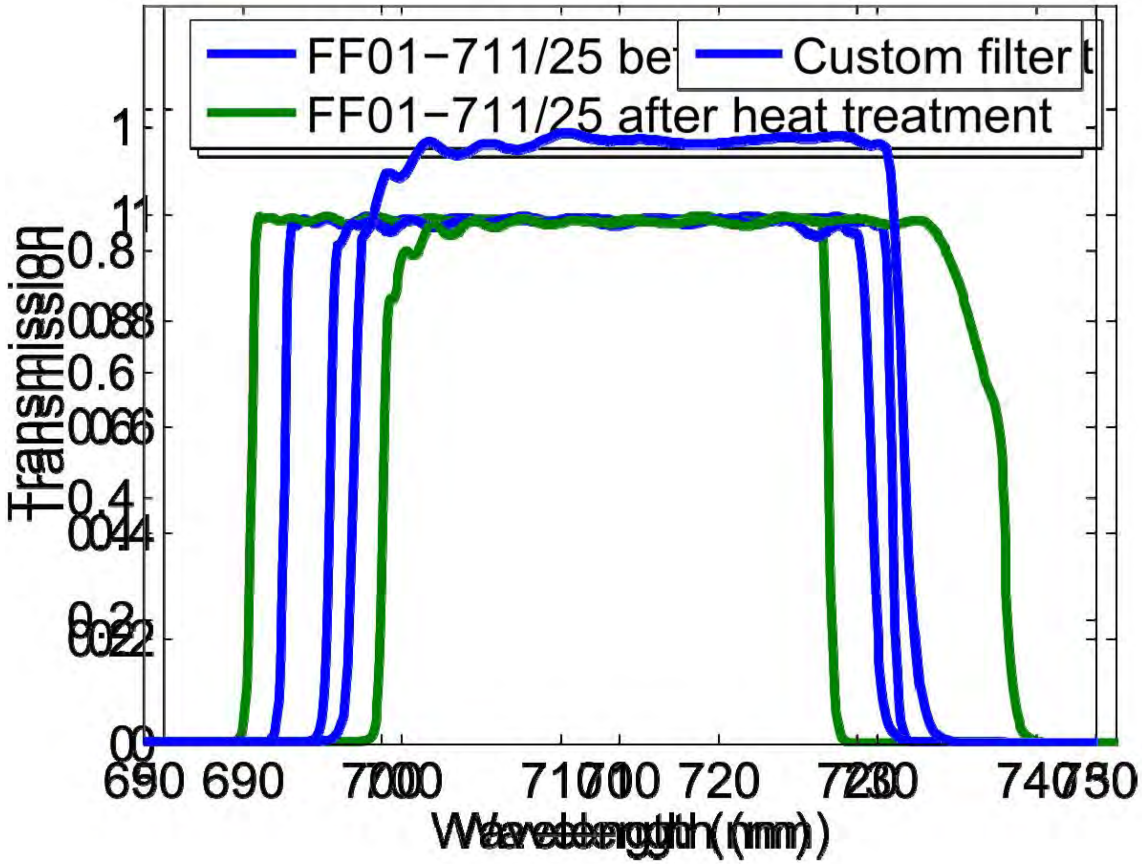
-commercially available, e.g., MicroFab Technologies Inc. (patterning ≈ $3,000)

Ideal Spectral Filter



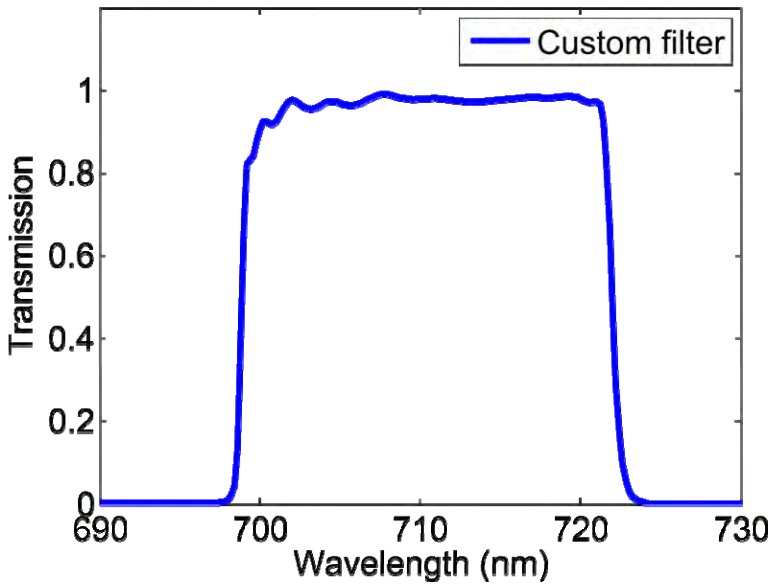
- For high heralding efficiency, want to pick off only part of the collected spectrum (the tail edges produce loss)
- Keep only the peak of the SMF-implied Gaussian filter (~70-nm FWHM)
- Want steep edges, symmetric about 710 nm

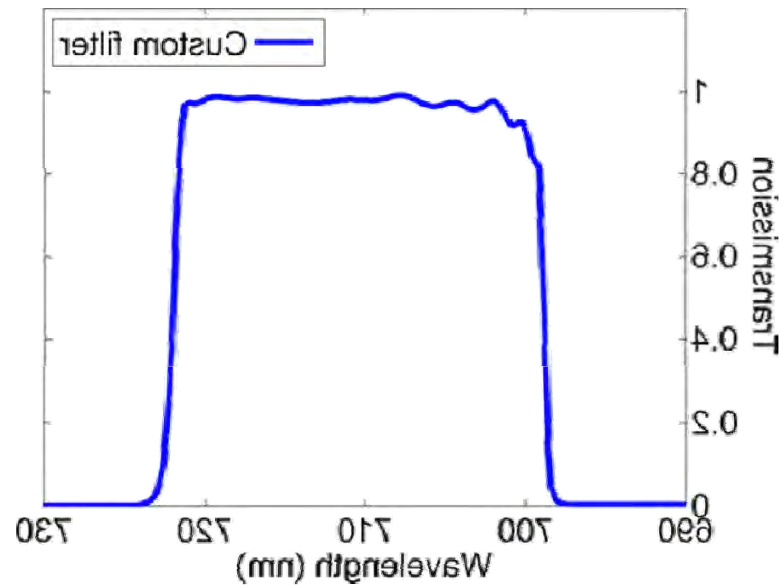
Spectral Heralding Efficiency



355 nm → 710 nm + 710 nm

Spectral Heralding Efficiency





- Spectral filter is decoupled from spatial filtering by picking out a top-hat spectrum

- We use two different filters to set the two edges of the top-hat filter
  - Lower wavelength edge is temperature tuned (permanent)
  - Upper edge is tilted, and used to match the temperature-tuned filter edge of the conjugate side

- Tilted filters are polarization dependant and cause polarization decoherence in the A/D basis→ need the filters *after* the polarization analysis

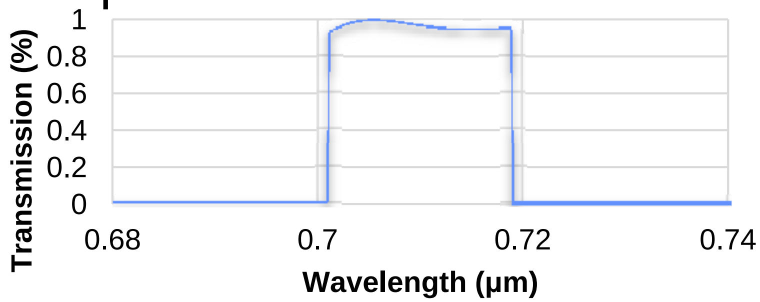
- Spectral heralding efficiency is 95%

Grating-based spectral filtering:

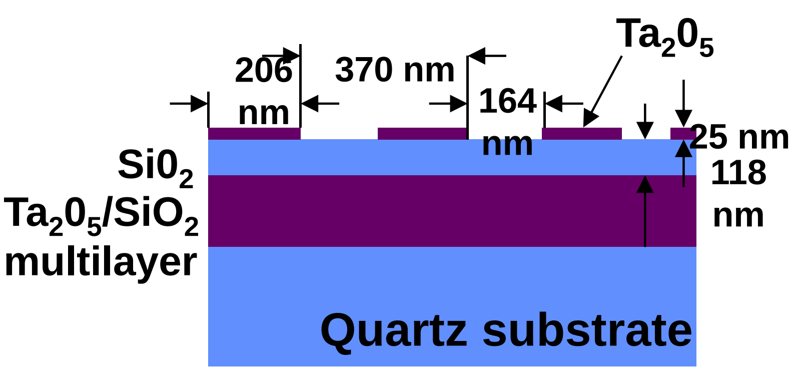
Wavelength-dependent transmission

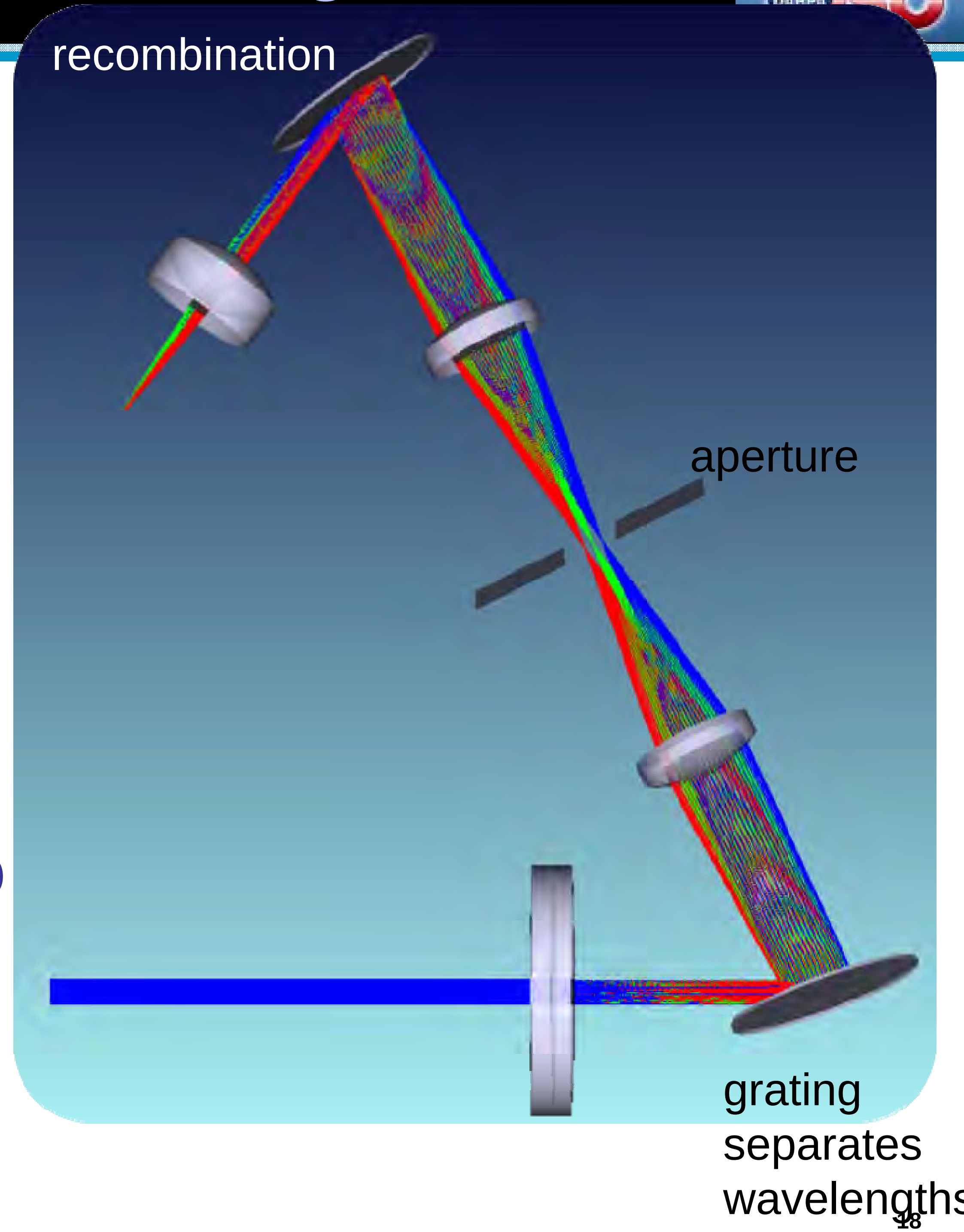
Goals:
-high total transmission
-sharp edges

Example:



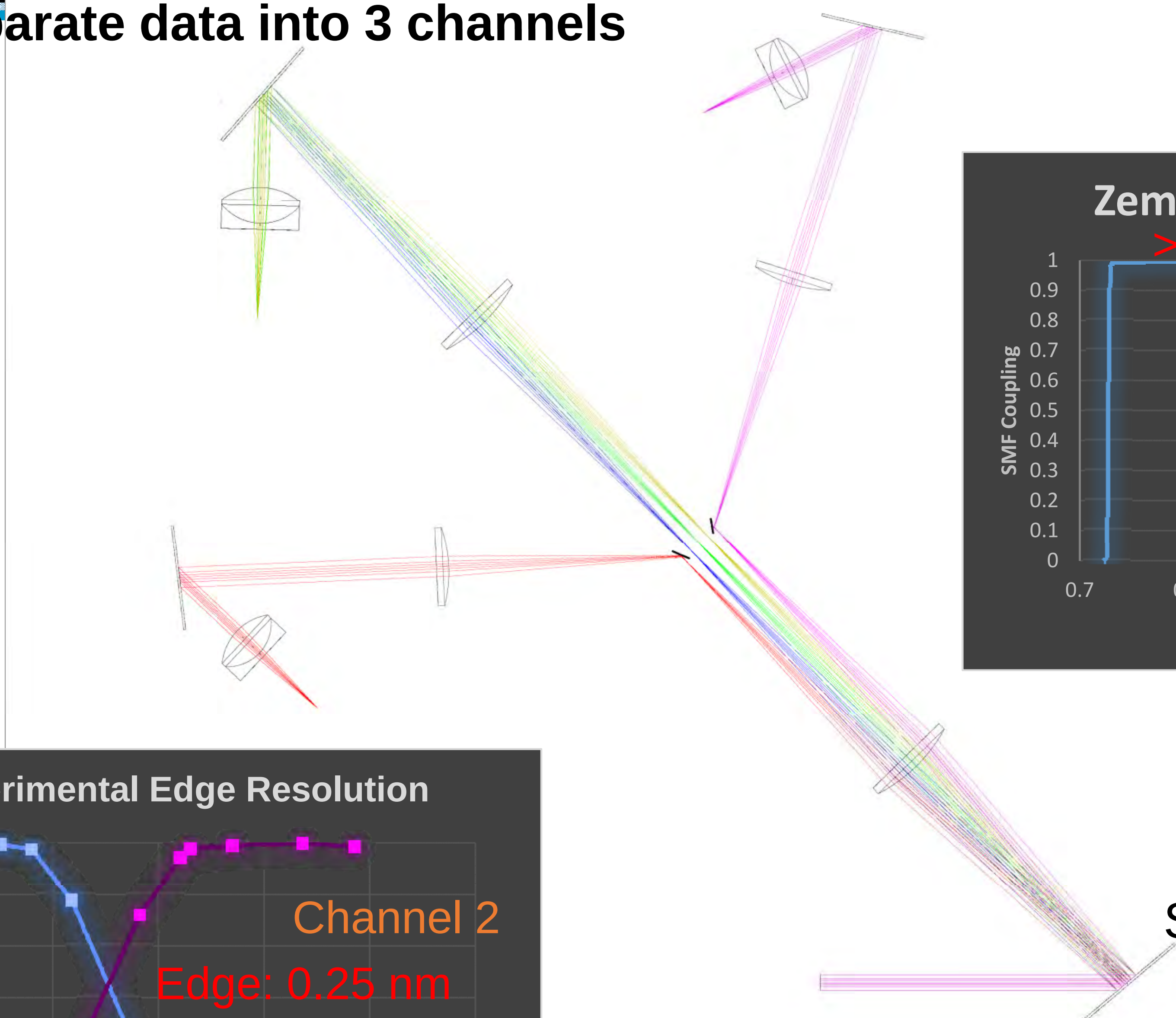
Plasmon-enhanced Grating
(Destouches et al., Opt. Exp. 13, 3230 (2005))



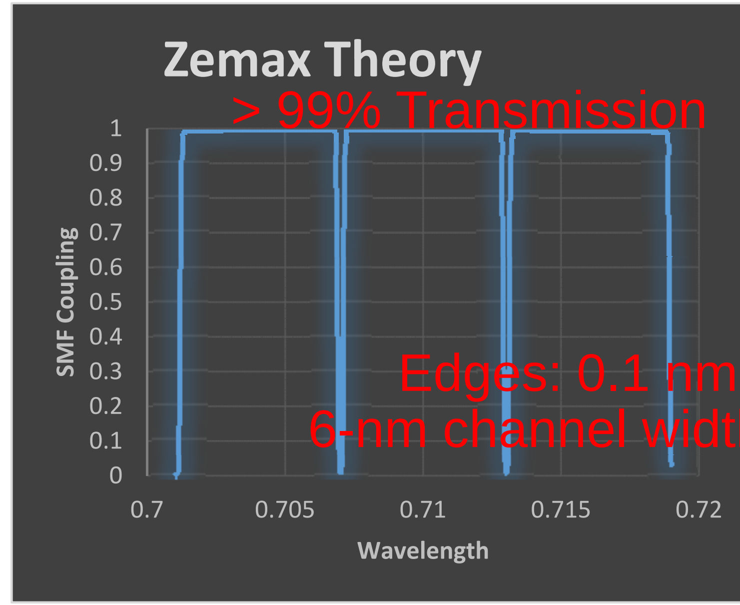


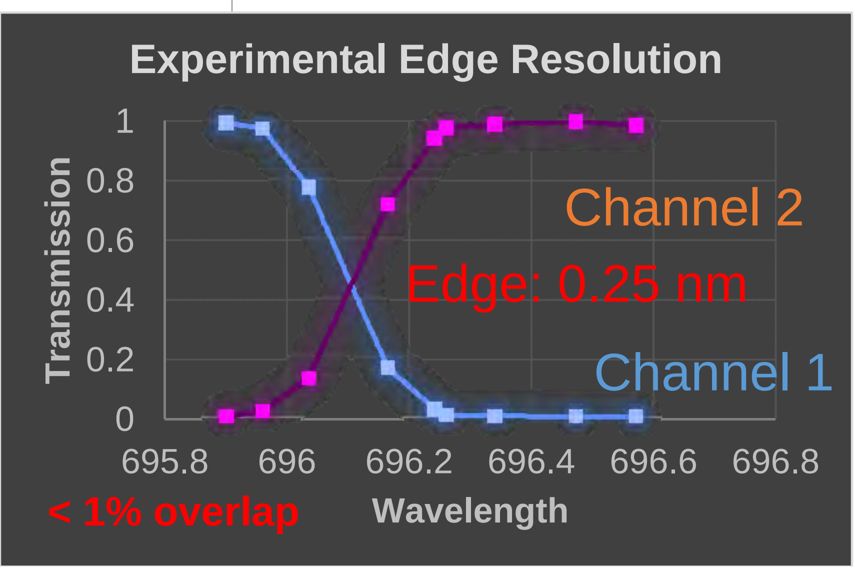
High-efficiency spectral multiplexing

-separate data into 3 channels



Setup

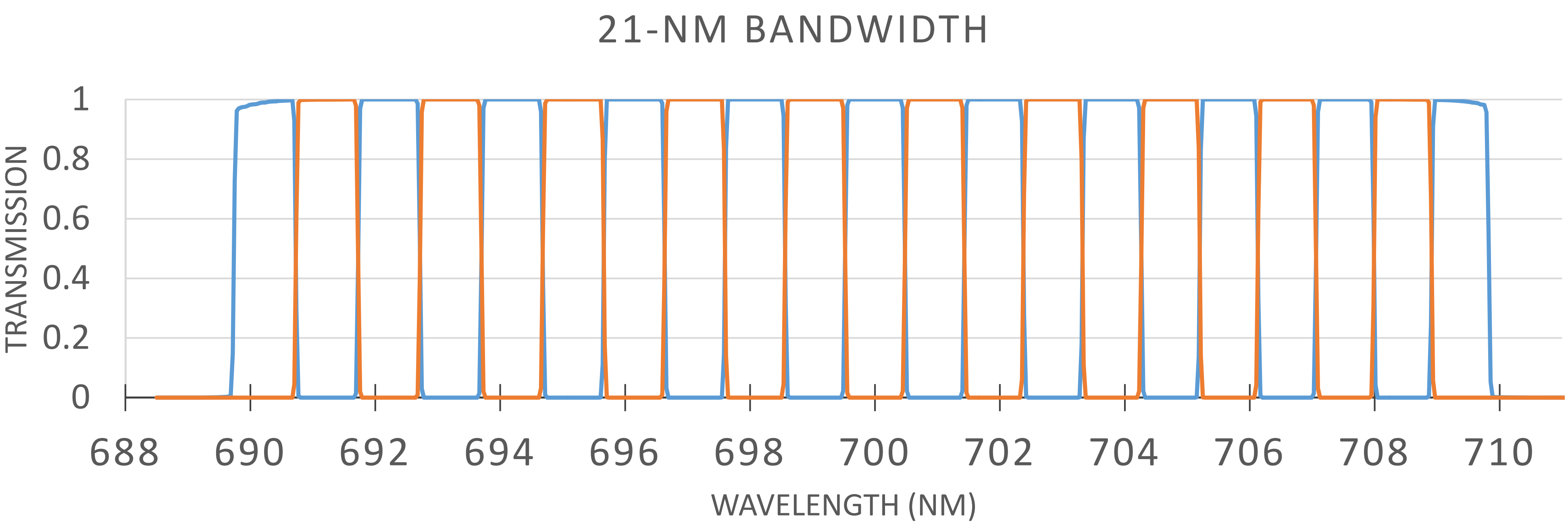




Ideal case: 3 “top hat” profiles

-minimal overlap between channels

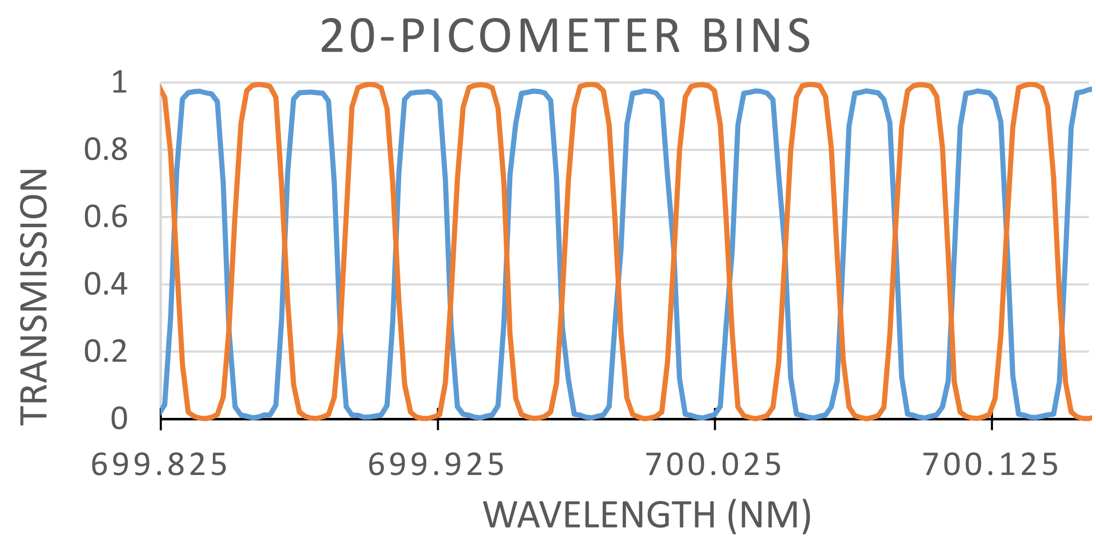
Many-bin multiplexing



21 1-nm wavelength channels
Could be saturated using:

- longer crystals
- higher power
- few-mode collection

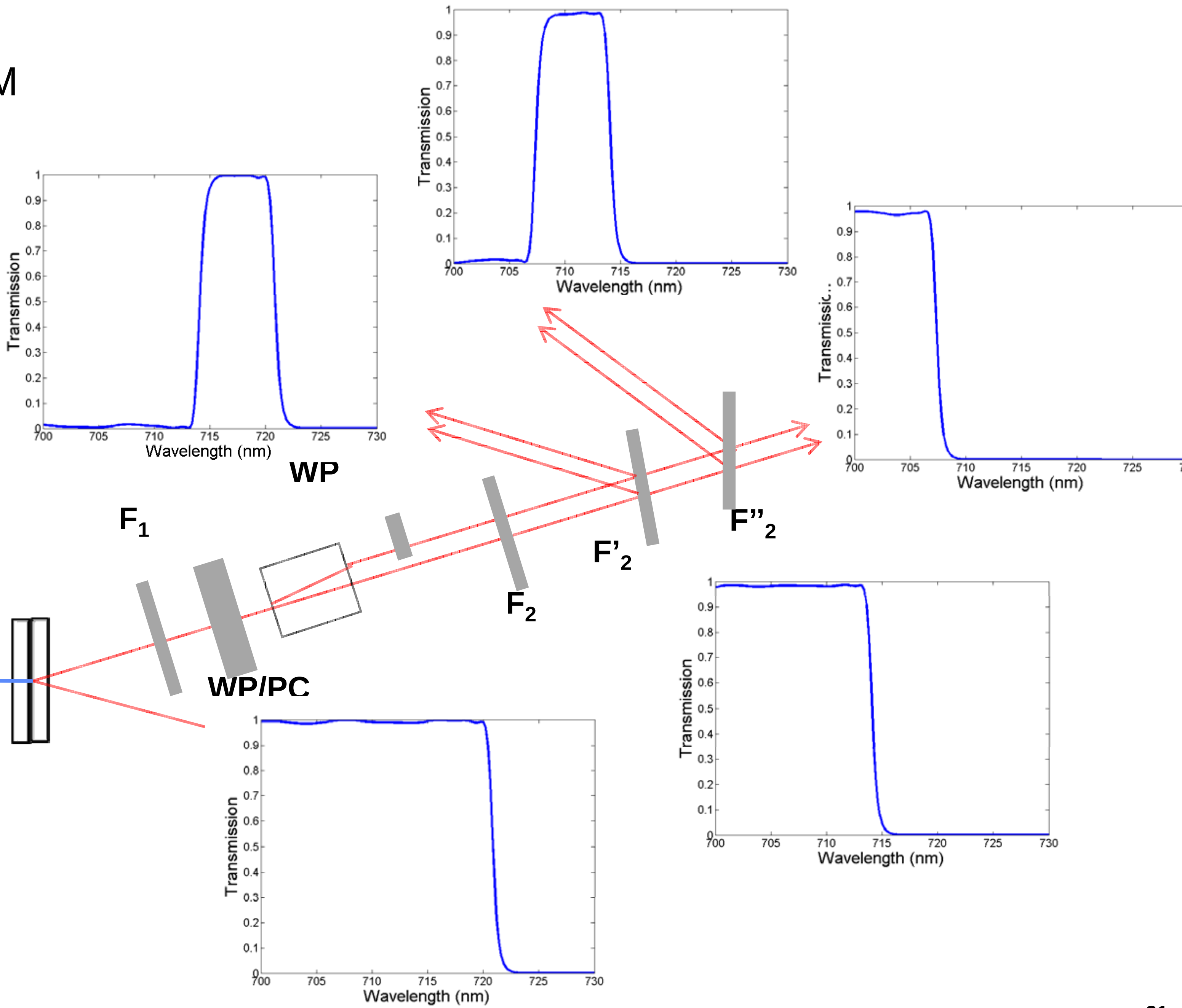
What’s the limit?



Note: No point in having spectral bin widths less than pump bandwidth (currently ~0.1 nm)

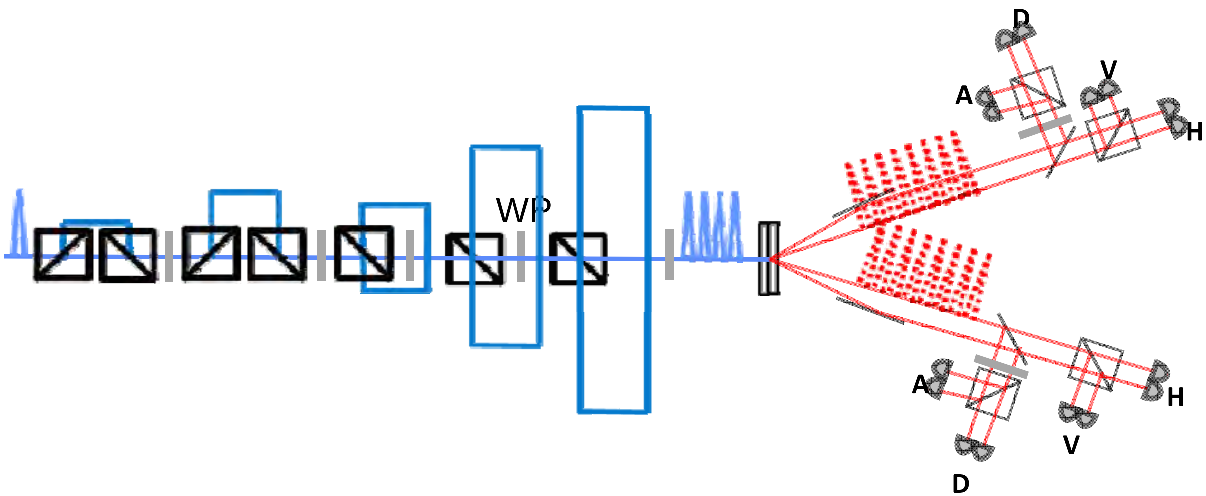
Multiple Spatial/Spectral Channels

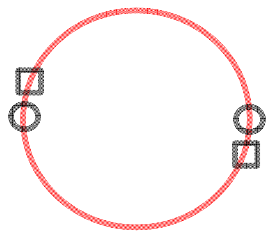
- Sequential tilted filters allow x3 WDM (~x20 possible)
- PC would allow for asymmetric basis checking
- Collection into few-mode fiber allows saturation of each channel
- Key rates above ~60MHz (with 2 spatial channels)



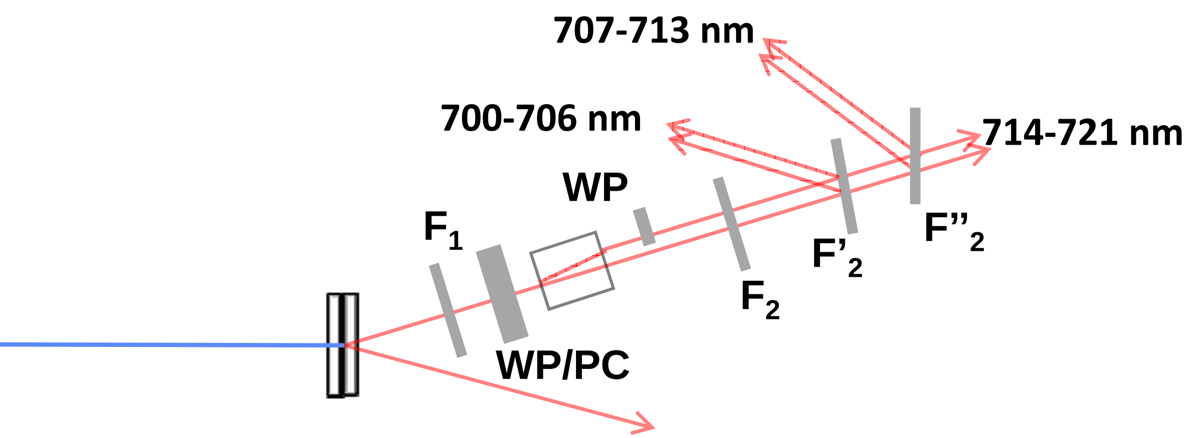
Summary: Multiple Spatial/Spectral Channels

Demonstrated/will demonstrate methods to achieve multiple independent spatial and spectral channels





End view of SPDC cone



- Up to 10 sets of spatial pairs possible/practical
- Sequential tilted filters allow x3 WDM (~x20 possible)
- Collection into few-mode fiber allows saturation of each channel
- Key rates above ~60 MHz (with 2 spatial channels)
- 10 channels + few-mode fiber → >1 GHz key rate!

Demonstrate all technologies to achieve milestones!

High-Efficiency, Low-Jitter, High-Saturation Rate Single-Photon-Counting Detectors

Develop custom electronics mated with Laser Components SAP-500 SPAD

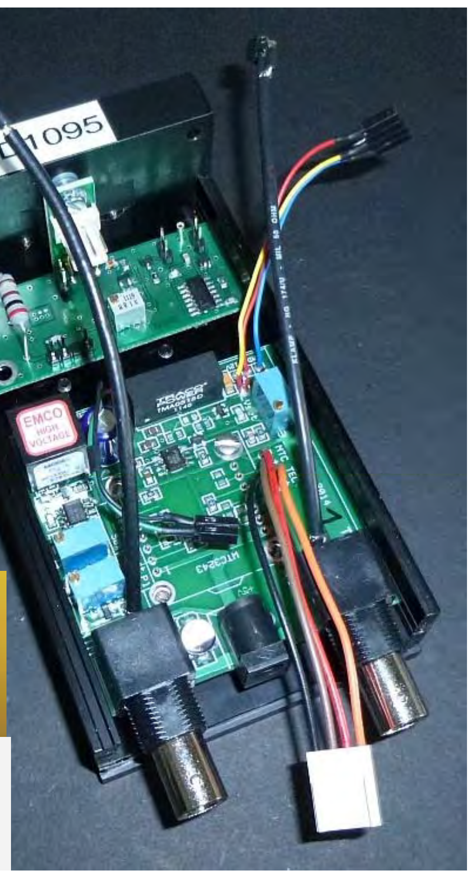
Quantum Efficiency @ 710 nm: ~70%

Deadtime: 24.5 ns (41 MHz saturation rate)

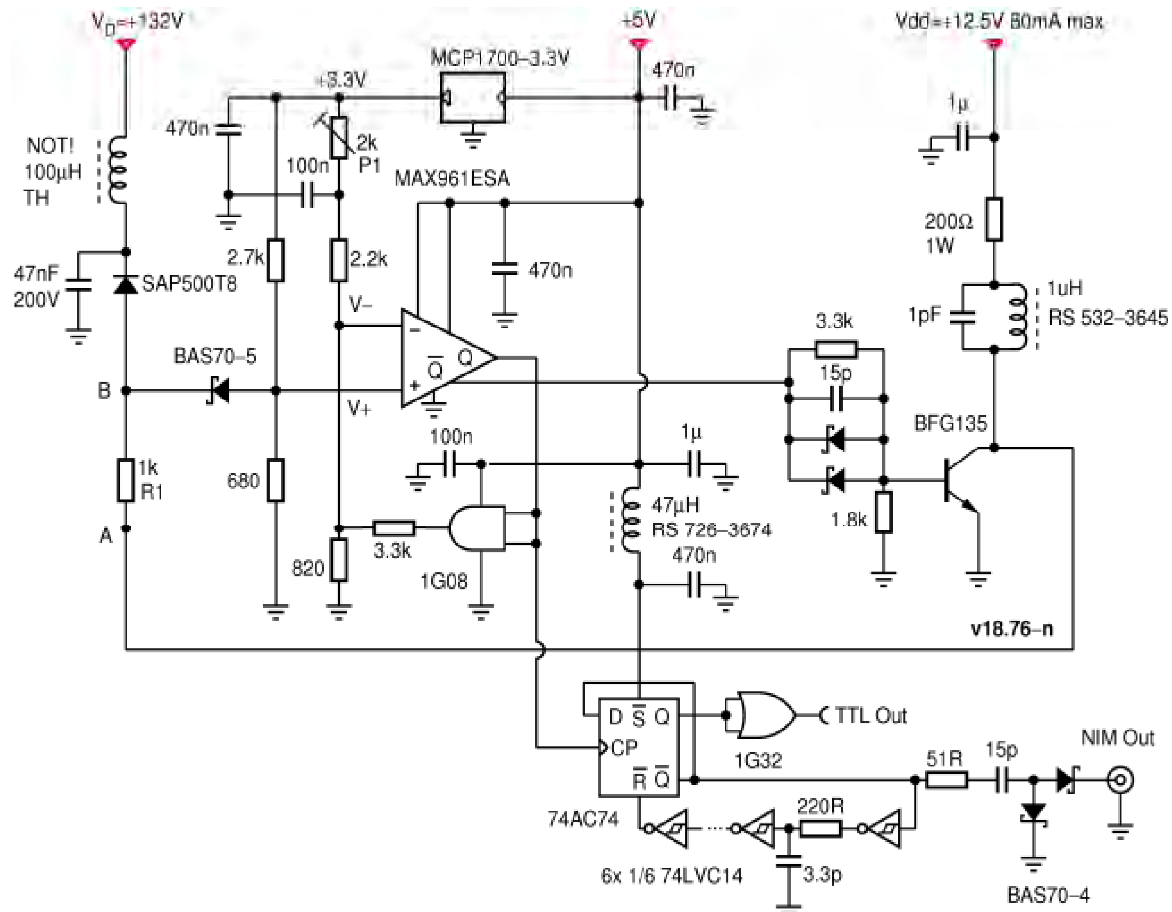
Afterpulsing probability: <0.1%

Jitter: 158 ps average for 15 detectors

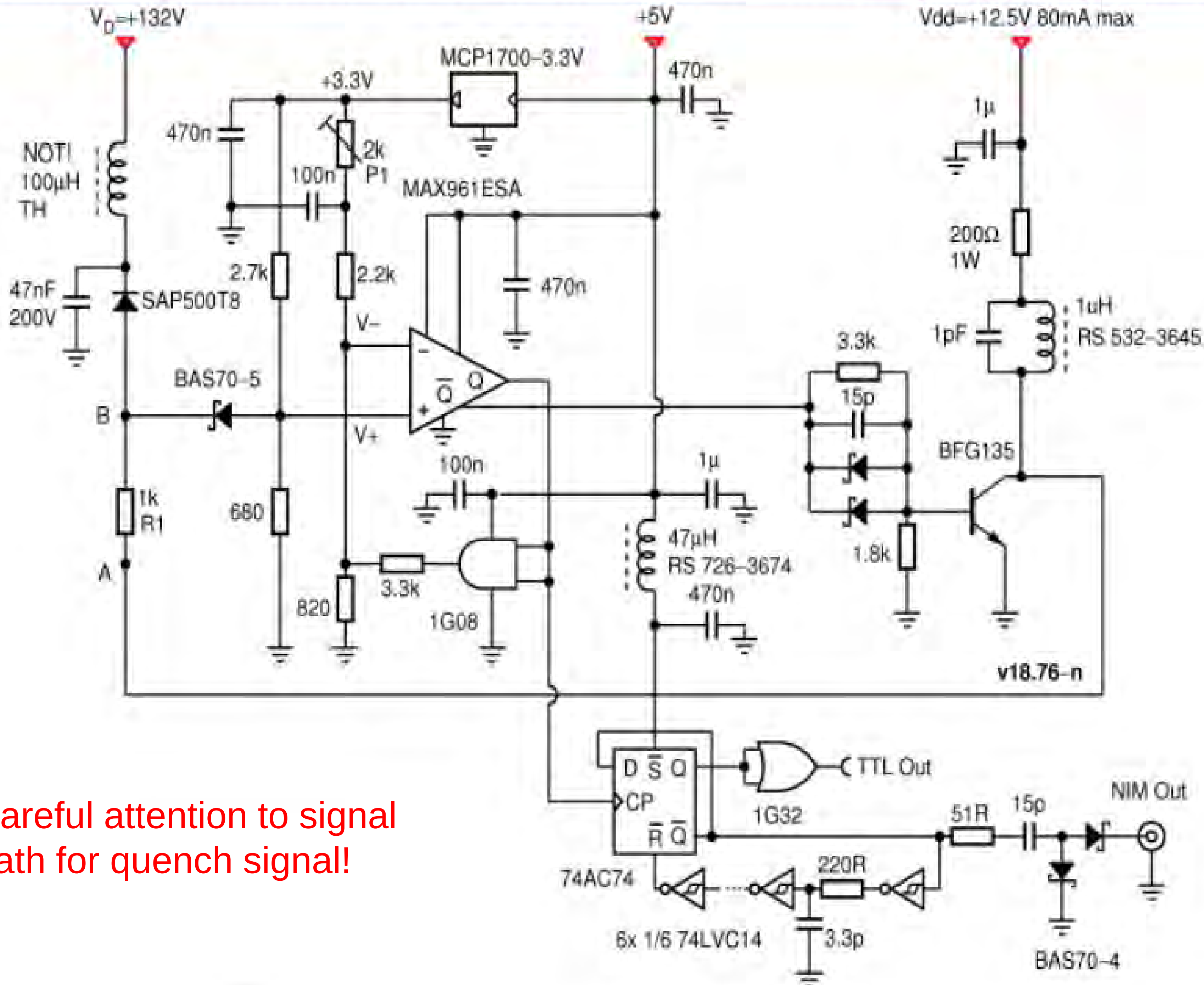
Dark Count Rate: ~3.5 kHz



LASER COMPONENTS



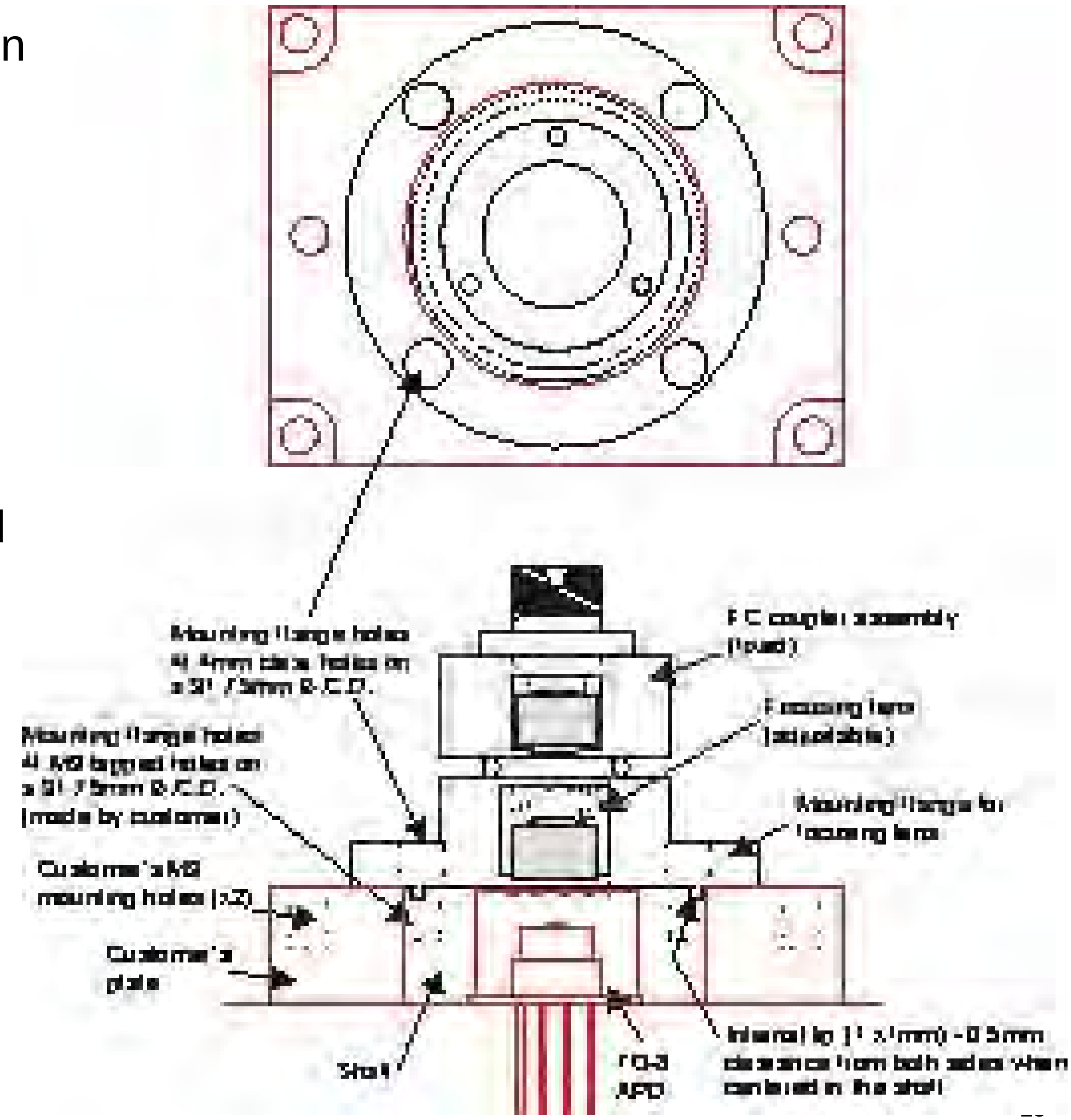
Active Quenching Circuit



Careful attention to signal path for quench signal!

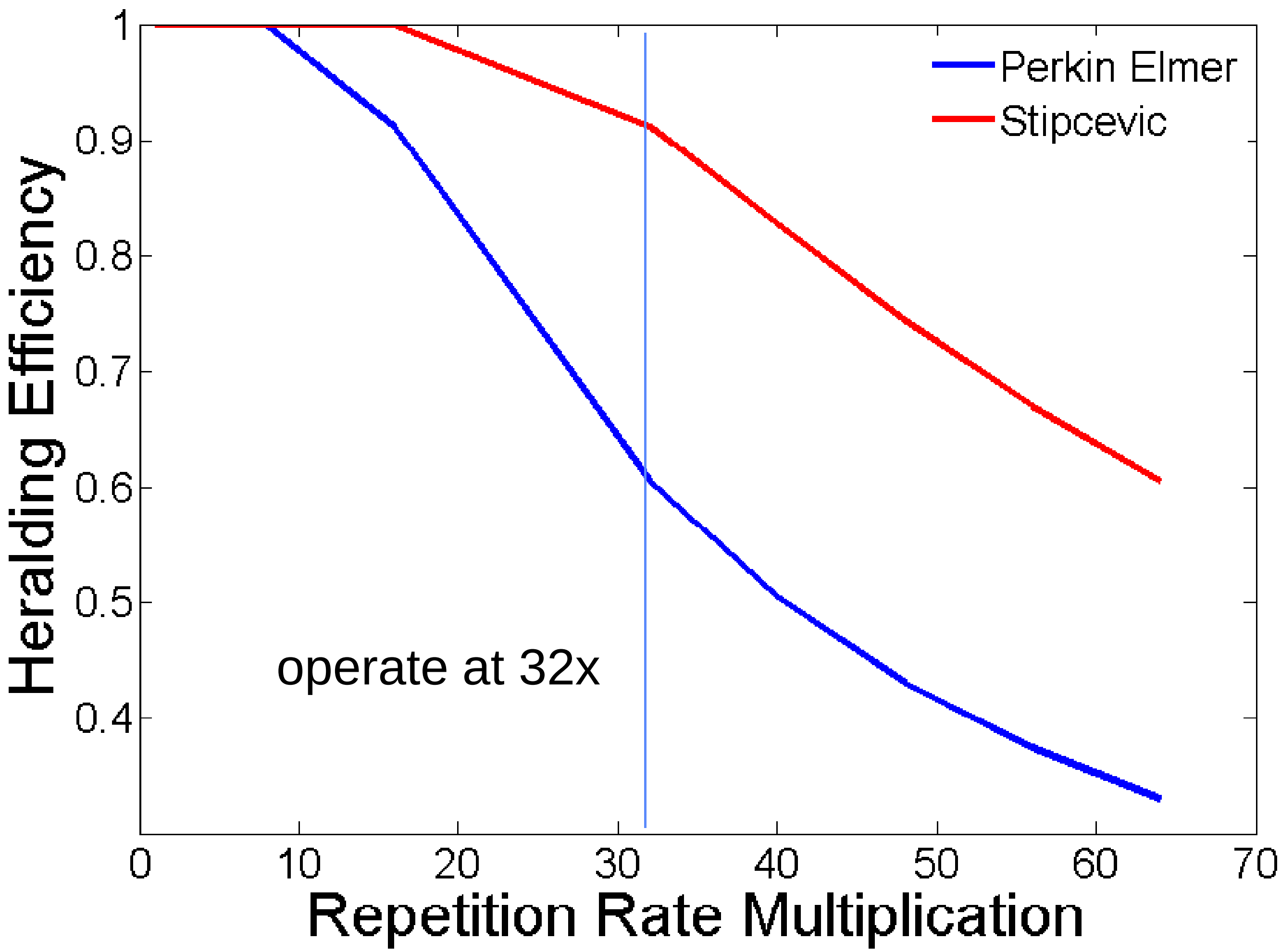
High fiber coupling efficiency for APDs

- Partner with OZ Optics to design fiber coupler with XYZ translation of the beam
- Adjust to achieve highest efficiency
- Lowest jitter requires finer adjustment
- 15 fiber-coupled detectors with custom quench circuit delivered to UIUC in April 2014



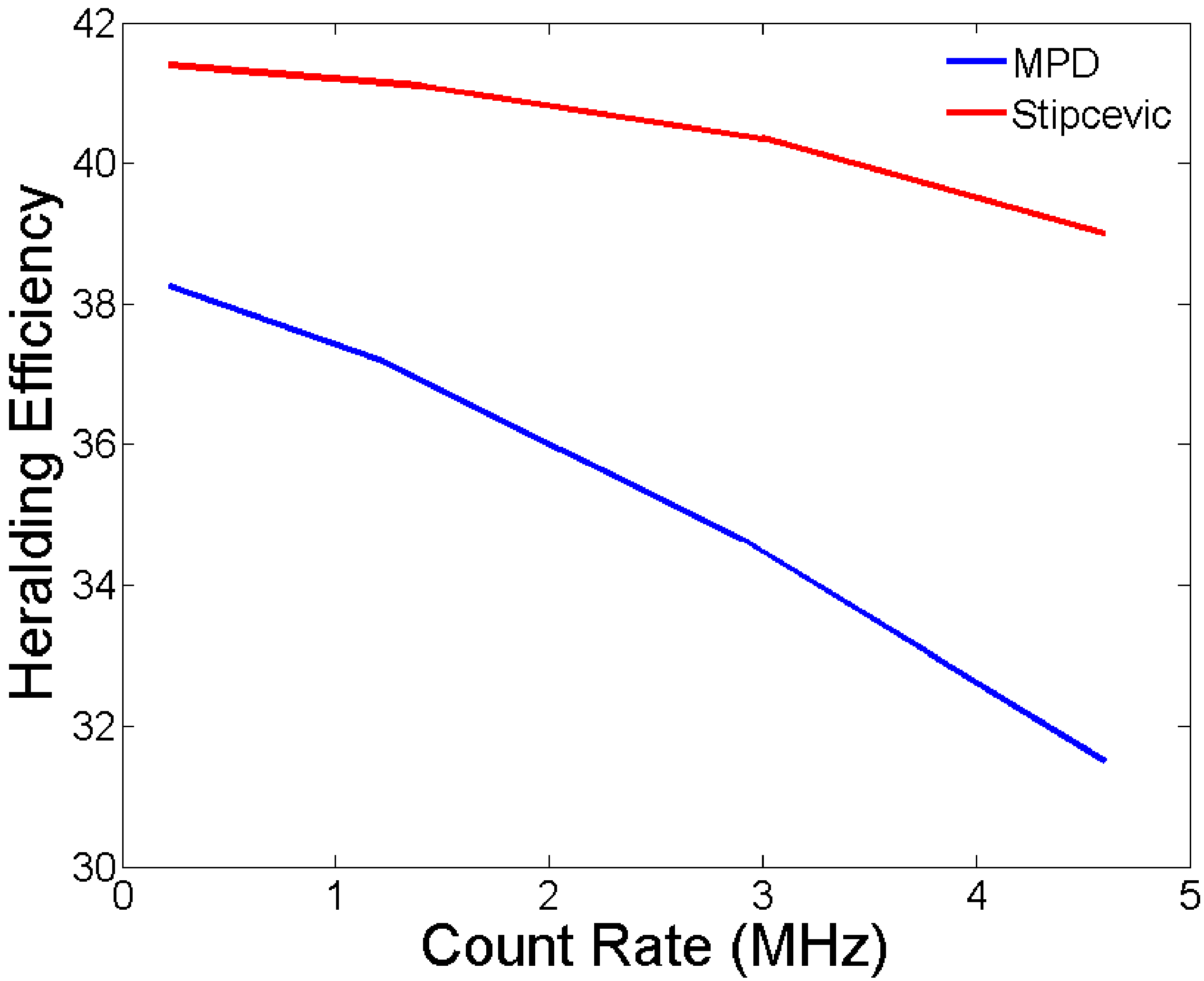
Pulse distinguishability: Perkin Elmer vs. Custom

Improved jitter in custom quench circuit allows for greater repetition-rate multiplication and higher photon efficiency

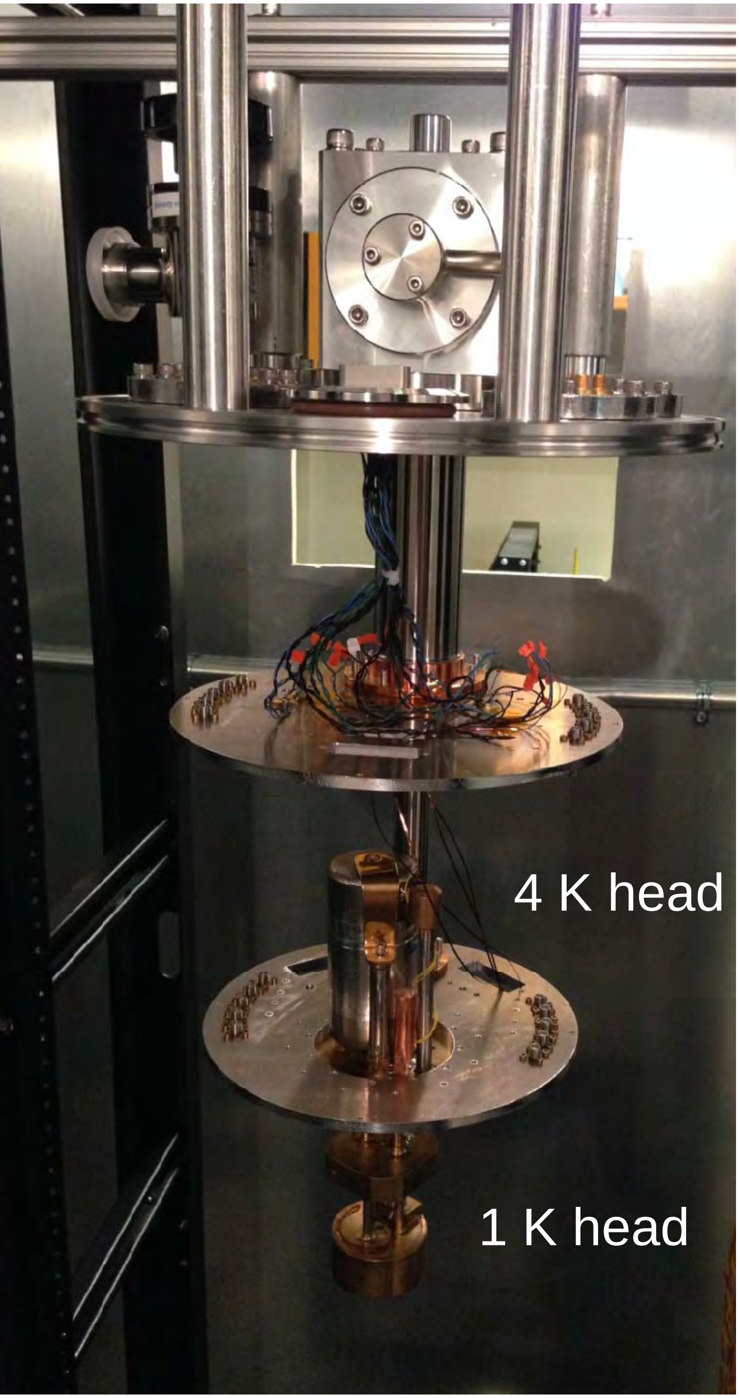


Saturation characteristics: MPD vs. custom quench circuits

Higher saturation rate with similar jitter with custom circuit vs. MPD circuit allows for higher key rate and photon efficiency



Superconducting nanowire detectors



Develop 8 channel SiW superconducting nanowire detectors optimized for 710 nm in collaboration with NIST

Status report (6/4/14): Cryostat constructed, chill-down tests, detectors fabricated, undergoing testing

Anticipated performance:

Quantum Efficiency: >90%
Jitter: 100 ps
Deadtime: <20 ns

High-Resolution, High-Throughput Timetaggers for Time-Bin QKD

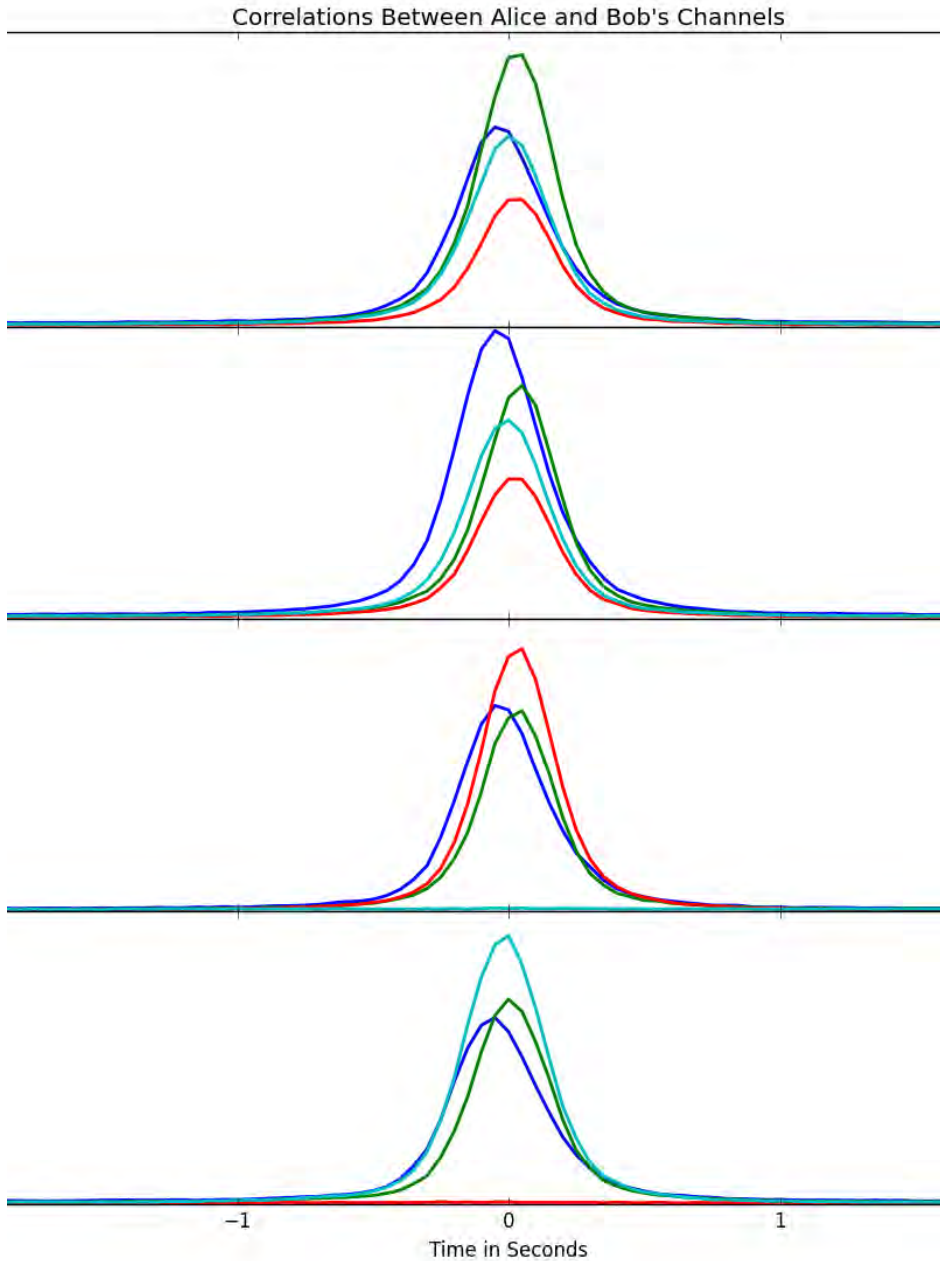
Assess and qualify time-taggers for time-bin QKD. Developed high-throughput custom time-tagger.

	Agilent	IQC	UIUC/NIST
Max count rate:	80 MHz (20 MHz continuous)	12 MHz	200 MHz (400 MHz possible)
Resolution (jitter):	50 ps (60 ps)	156 ps (180 ps)	50-100 ps (10 ps)
Channels:	6	12	4

- The Agilent timetagger can run up to 80 MHz in "burst mode" where only a few milliseconds of data are taken at a time.
- Custom UIUC/NIST timetagger count rate limited by hard-drive write-speed. At high rates, less bits per count (currently 32 bits) can be used allowing up to 400 MHz continuous. Resolution limited by the FPGA clock, the current board has a 100-ps resolution. A better board could allow for a 50-ps time-bin size.

Mysterious rate-dependent jitter in one time tagger

Alice-Bob cross correlation



time in ns

Mutual Information of the quantum key distribution system including error correction, privacy amplification, and security analysis

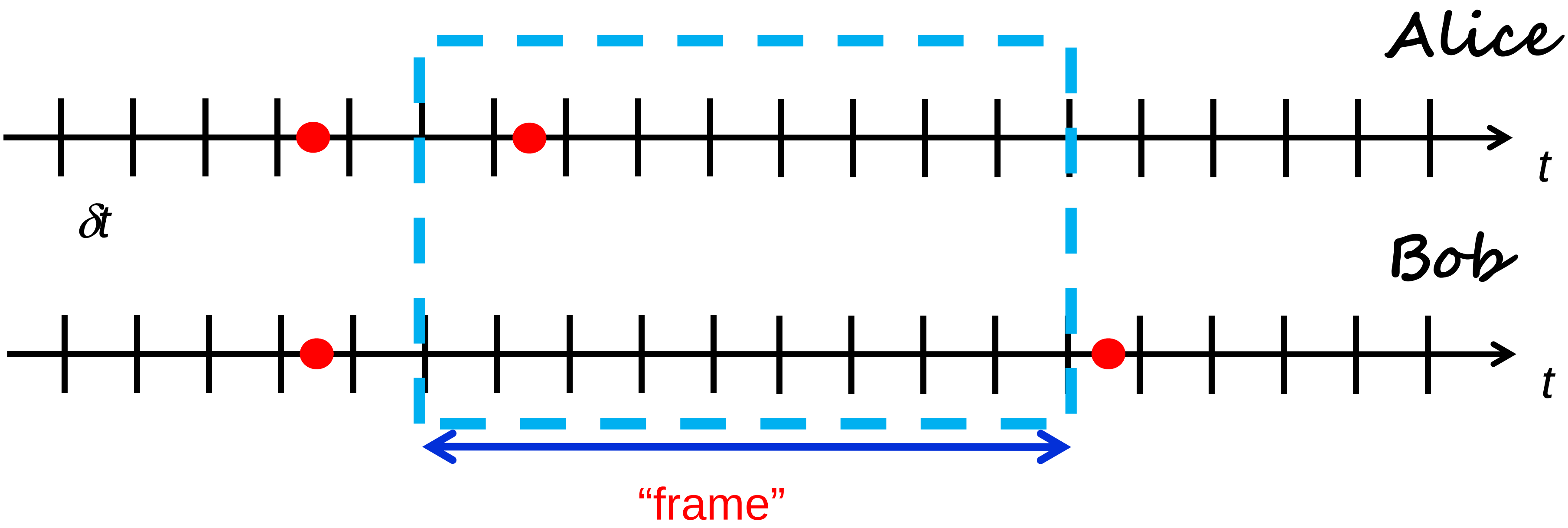
Steve Barnett
University of Strathclyde/Glasgow University

Paul Kwiat
University of Illinois, Urbana-Champaign

Daniel Gauthier
Duke University

The information per photon pair

• Number bits / photon depend on errors. Typical errors are ***finite efficiency***, ***channel losses***, ***dark counts, after-pulsing, jitter, etc***.



• *Even* with errors, we can get **>*10 bits per detected photon pair**** *.

• ***InPho Breakthrough***: Developed new model, takes account of ***frame-encoding, losses, dark counts, jitter, multiple photons in each frame and dead-time***.

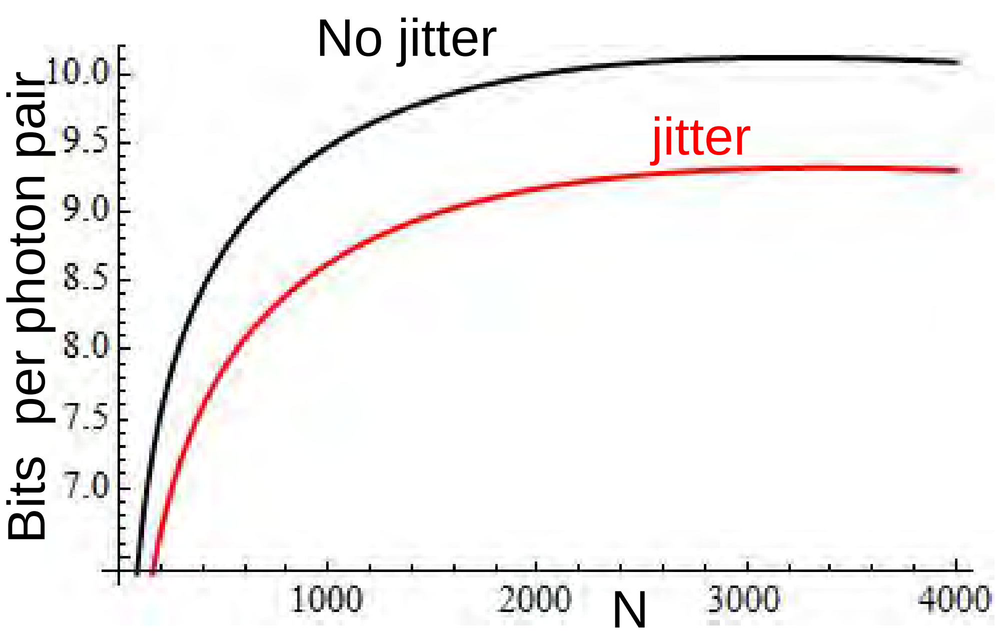
• Very general, applies to other high-D QKD setups.

* Brougham & Barnett, PRA **85**, 032322 (2012).

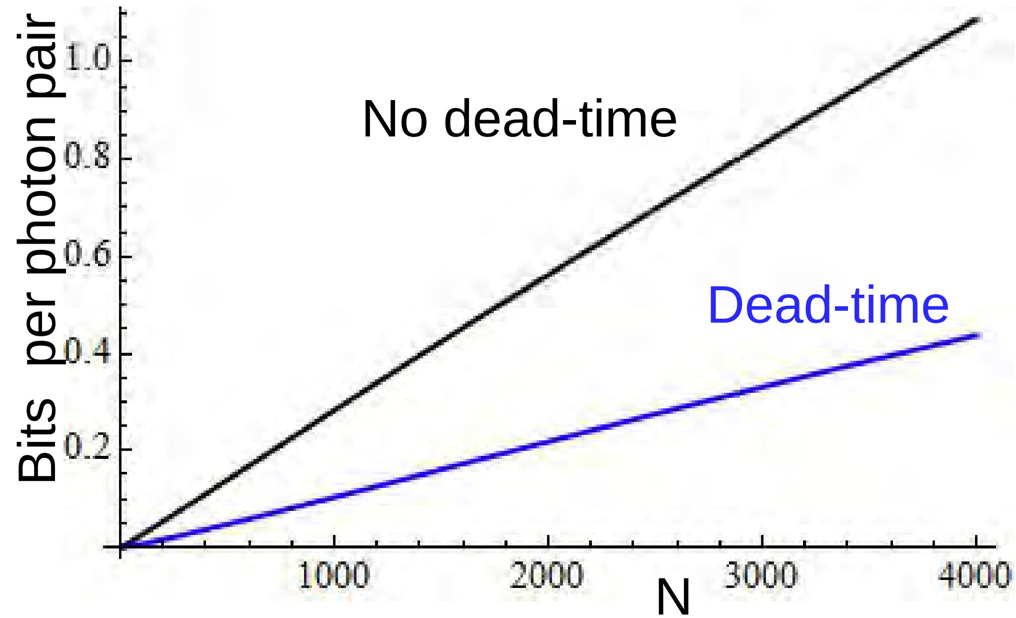
Information in frame-encoded photons

Can optimize frame size, N, in presence of realistic errors

Information in 1,1-frames



Information in 2,2-frames



η = 0.3, λ = 6.0x10^{-5} , pulse interval = 1 ns,
jitter probability = 0.1, dead-time = 1 time-bin
dark count rate = 300/s, after-pulsing rate = 1000/s

T. Brougham, C. F. Wildfeuer, S. M. Barnett and D. J. Gauthier, manuscript in preparation.

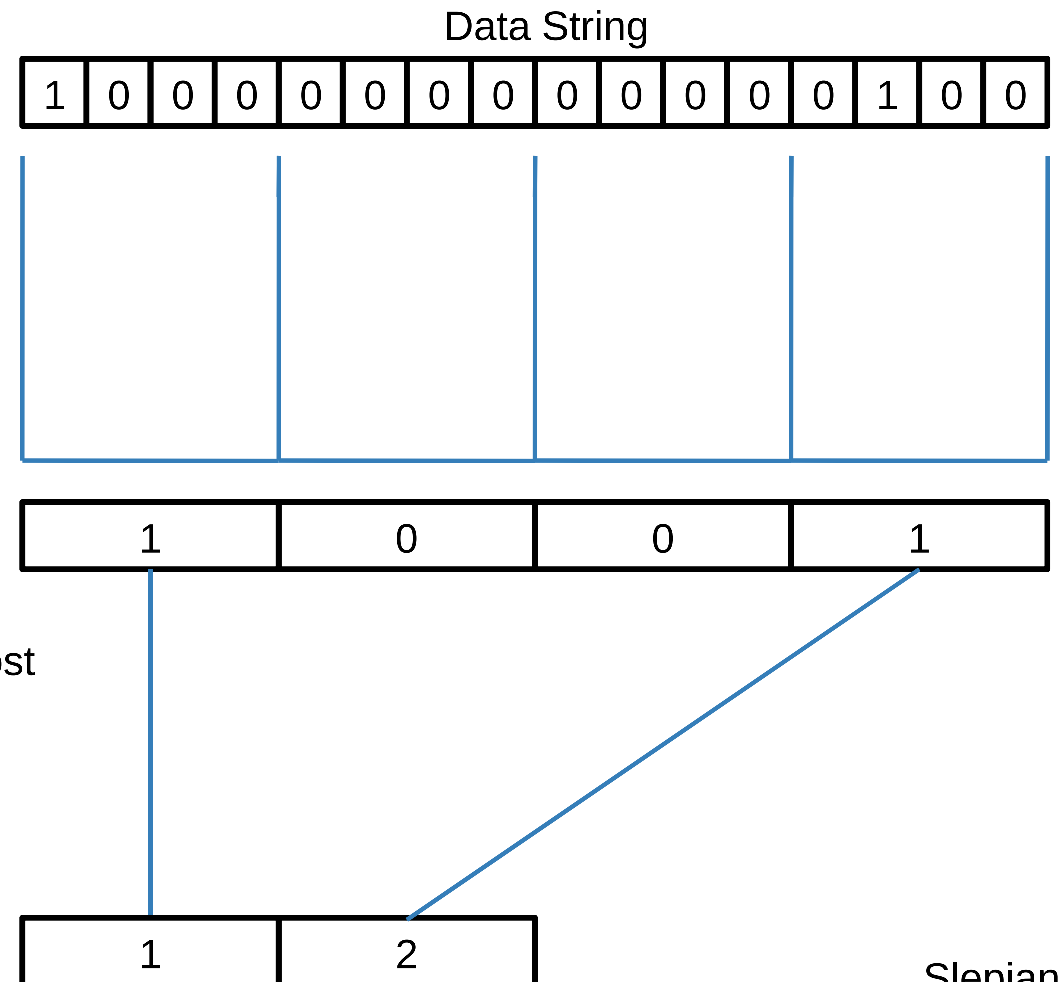
Error Correction

Implemented novel Slepian-Wolf-based error correction to cope with sparse data sets

A data string is generated with the QKD source

The data string is broken into two data strings: an occupancy string and a letter string.

10% of the entropy is primarily lost due to jitter, frame edge effects, and location entropy from multi-events per frame



Numbers below assume 16-bin frame size, high-power data

occupancy

occupancy 50% of the Shannon-limit entropy

location

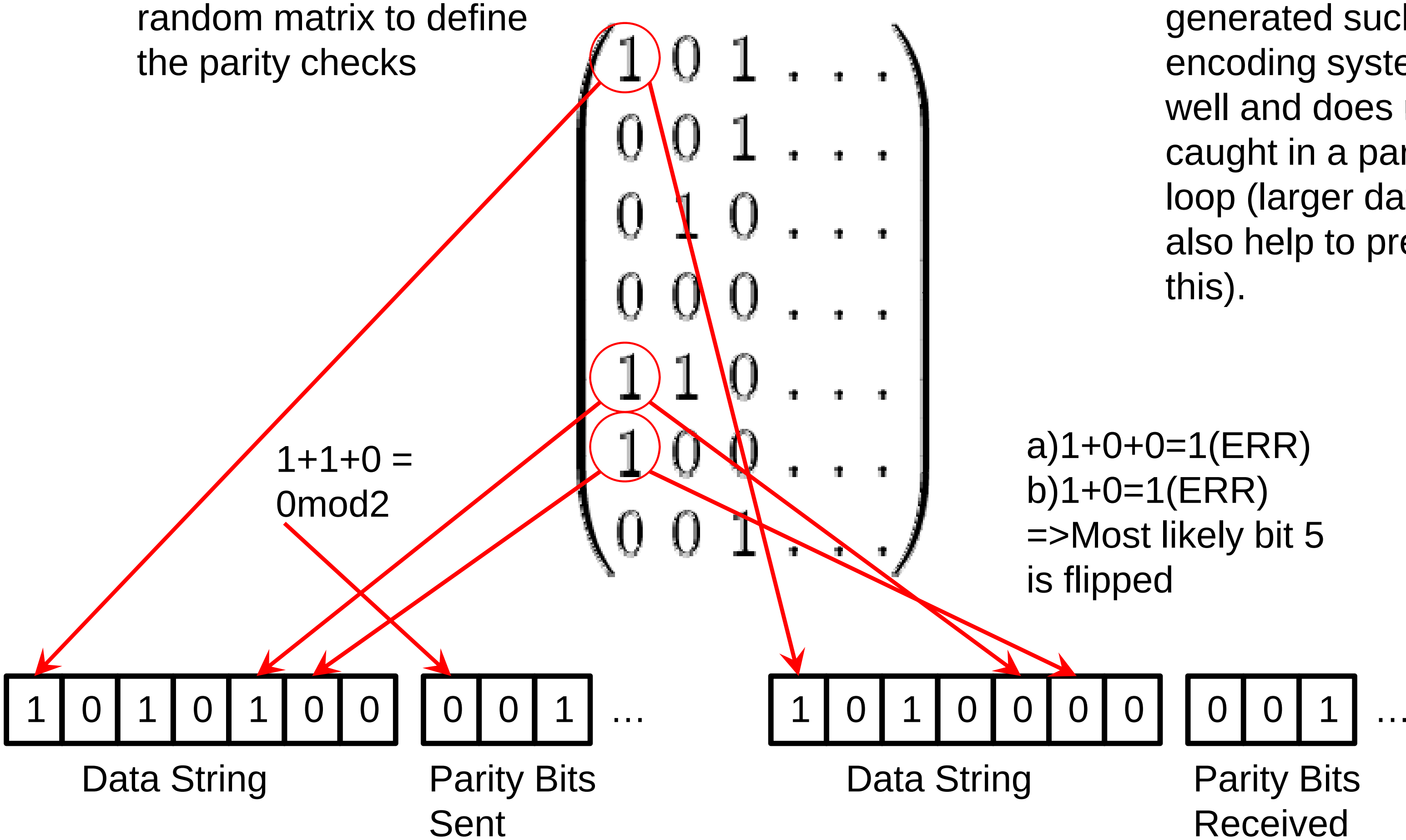
location (1:1 frames): 40% of the Shannon-limit entropy

Both occupancy and location data go into separate non-binary Slepian-Wolf codes → Slepian-Wolf codes retain ~65% of the Shannon-limit entropy for both occupancy and location

Error Correction

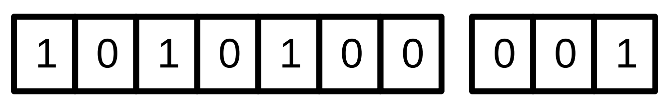
Shared sparse pseudo-random matrix to define the parity checks

Matrices have to be generated such that the encoding system works well and does not get caught in a parity check loop (larger data sets also help to prevent this).



ALICE

After looping over all parity checks, all the errors are corrected if enough bits are sent

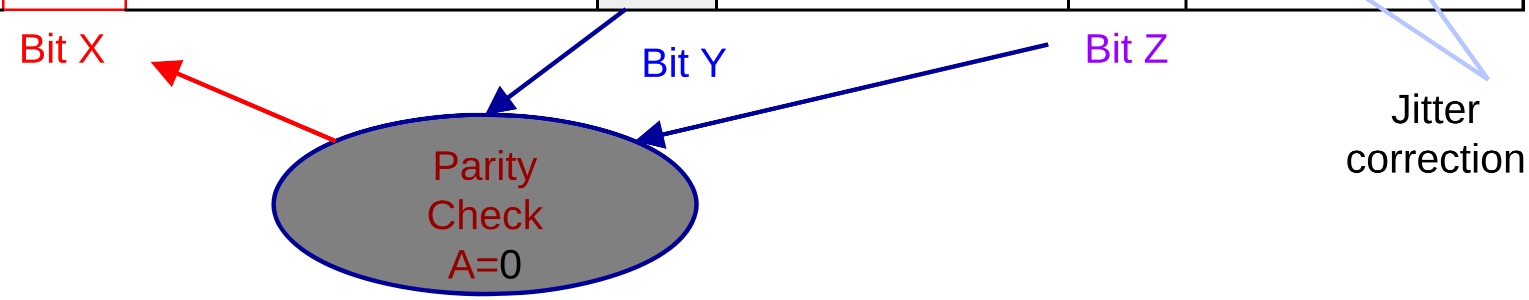


BOB

Binary SW code is same, except mod(N) instead of mod(2) for the parity checks

Probabilities and jitter corrections are based upon data statistics

Alphabet of 4	...	0	...	2	...	1	...
p0	...	.40	...	.16	...	.22	...
p1	...	.28	...	.22	...	.40	...
p2	...	.16	...	.40	...	.22	..
p3	...	.16	...	.22	...	.16	...



Example of Parity Check A's correction to bit X's probability of being 1

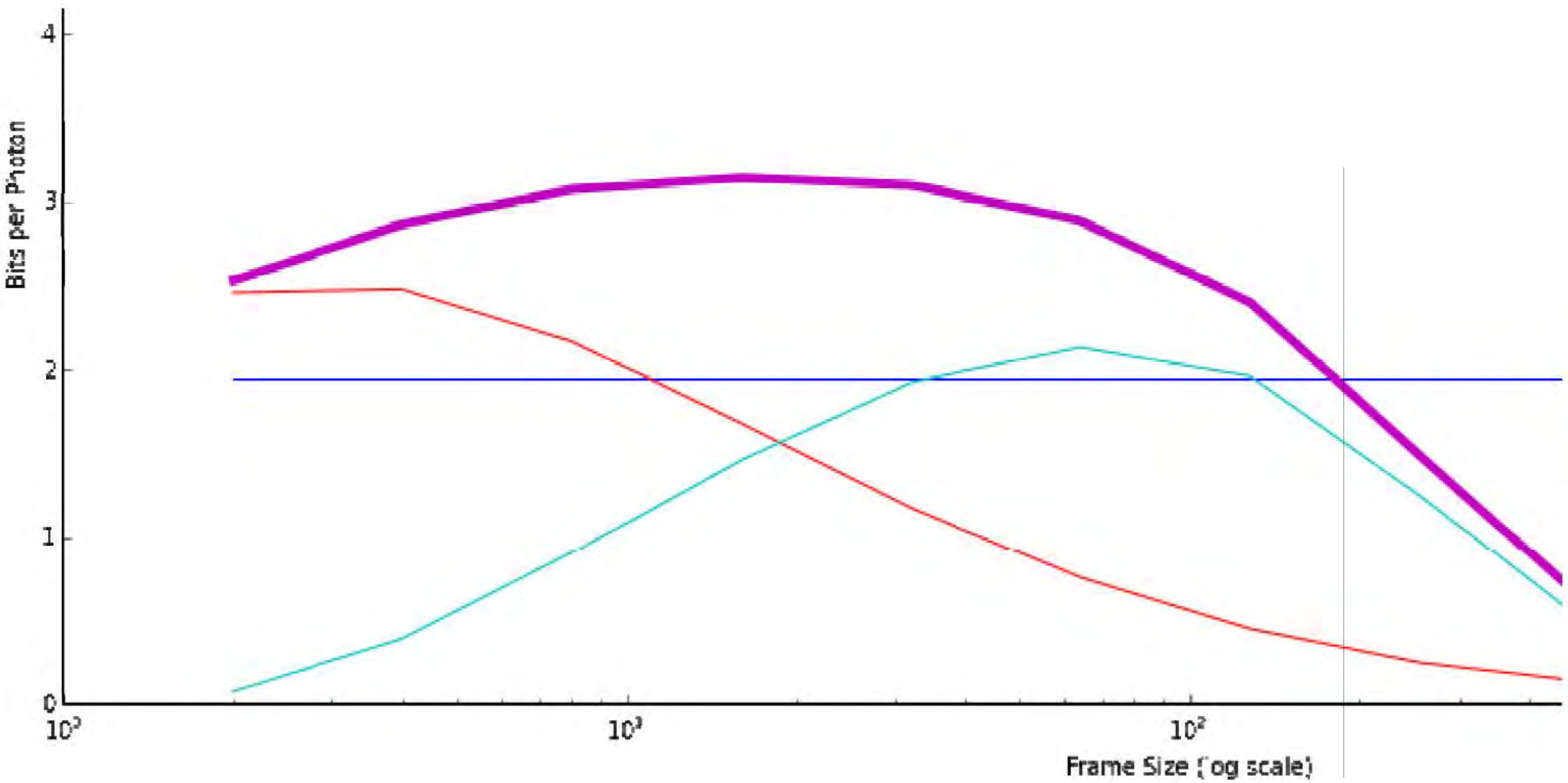
P(Bit X is 1 given A) = P(Bits Y and Z mod 4 add up to 4-1=3)

0	+	3	mod 4 =	3
1		2		3
2		1		3
3		0		3

so **P(X=1|A) = sum**

Y	×	Z
p0		p3
p1		p2
p2		p1
p3		p0

Example “extractable” entropy



Detecting Eve and leaked information I

- ***InPho breakthrough***: Bound information leaked to Eve for reasonable attacks (not QND). Standard results don't work for our setup.

- **Direct attack**: Eve measures time by making as general a POVM, with constrain that she ***absorbs and possibly re-emits photons***.

- Photons in state $$|\psi\rangle \propto \left(|HH\rangle + |VV\rangle\right) \otimes \left[|11\rangle + |22\rangle + \ldots + |dd\rangle\right]$$

Polarization is *entangled.*

- Eve's attack must disturb polarization (as it is not a QND measurement).

- Detect Eve by checking *polarization correlation* within two mutually unbiased bases.

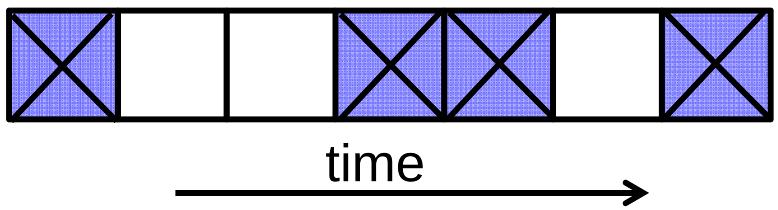
- Example: η=0.3, λ=5.33x10^{-5} , D.C =300/s and a bit error rate of P_E= 0.02

I_{AB} = 10.3 bits / photon pair & I_{Eve} = 0.82 bits / photon pair

Detecting Eve and leaked information II

•**Blocking attack**: Eve randomly blocks several, *non-contiguous,* time-bins.

• Eve knows photons not found in certain time-bins. ***This reduces her uncertainty and thus she gains information.***



• Eve can also ***partially block*** time-bins, reduces probability that photons found within those time-bins.

• ***InPho breakthrough*:** Developed new methods to detect ***sophisticated blocking attacks***

• Detect attacks using ***'decoy' pulses***.
• From detection statistics for pulses, we estimate blocked and partial blocking time-bins.

• Example: η=0.3, λ=5.33x10^{-5} ,D.C =300/s and *fully* blocking ½ of all time-bins

$$I_{AB} = 10.3 \text{ bits / photon pair} \quad \& \quad I_{Eve} = 0.74 \text{ bits / photon pair}$$

• Setup still vulnerable to QND attacks

Security against QND attacks: Franson interferometers

- Franson interferometer secure in the limit of 3-4 bits per photon (8 to16 time-bins), PRL**112**, 120506 (2014).

- ***InPho breakthrough*:-** Showed ***single*** interferometers insecure in **high-dimensions** ~10 bits per photon*. Would need visibility >99.8%.

- ***InPho breakthrough*:-** Developed bounds for Eve's information gain for ***multiple*** interferometers.
- Bounds valid for collective attacks#.

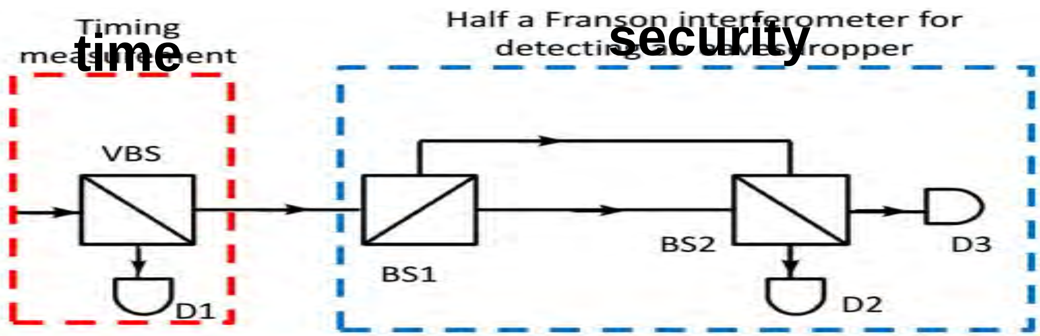
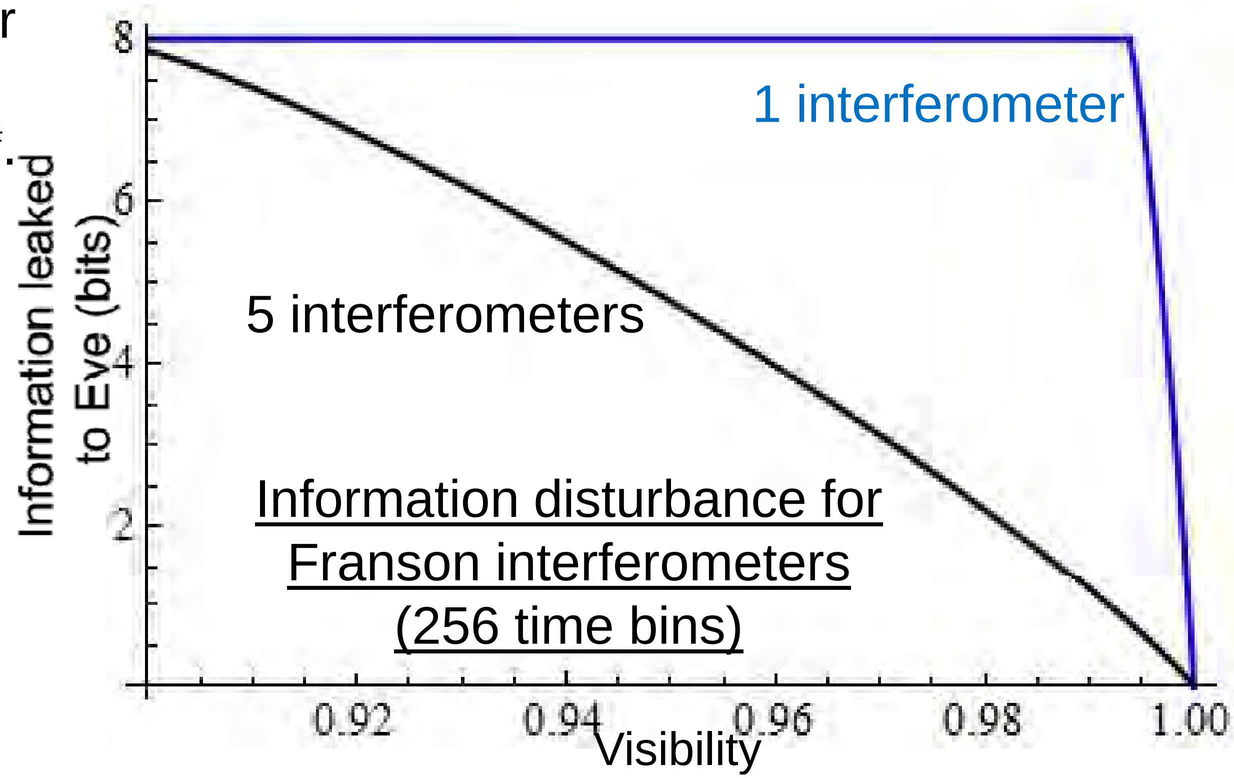


Figure 1. One half of the optical setup that Alice and Bob would each have. VBS is a variable beam splitter, while BS1 and BS2



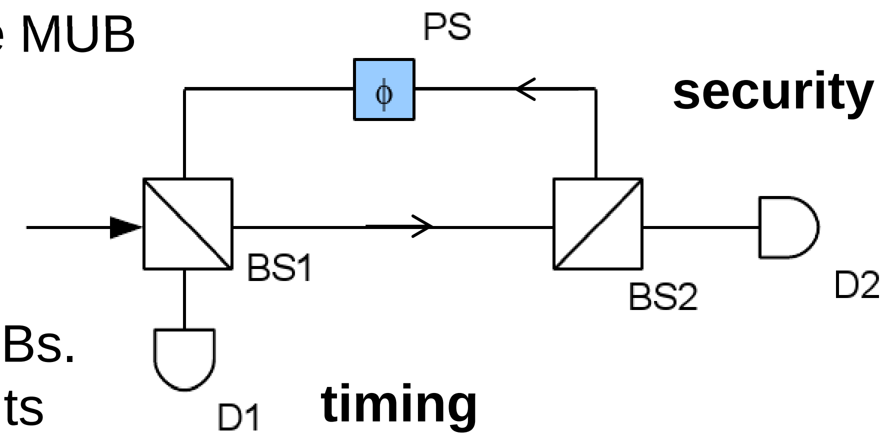
* J. Phys. B **46**, 104010 (2013).

Manuscript in preparation.

Security against QND attacks: implementing MUBs using a cavity

- ***InPho breakthrough*:-** Scheme that uses cavity to project onto ***very high-dimensional*** MUB states.

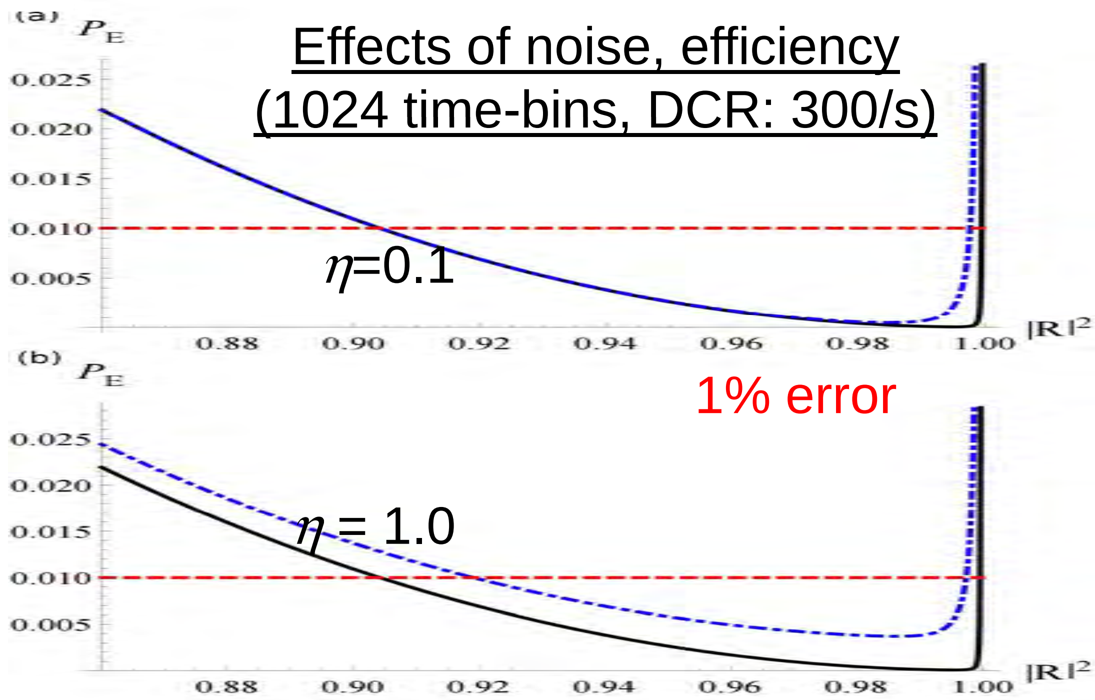
Alice and Bob's setup



- Detection at D2 is projects onto the approximate MUB state

$$\sum_{m=0}^{N-1} |R_1|^m |R_2|^m e^{im(\phi+\pi)} |N-m\rangle \quad \text{where } R_1 \approx R_2 \approx 1$$

- Different values for ϕ correspond to different MUBs.
- Setup robust to errors for 1024 time-bins (~10 bits per photon pair).



Brougham & Barnett, EPL **104**, 30003 (2013).

Brougham & Barnett, to appear in J. Phys. B

Summary

We have developed a complete QKD system that operates at a

- record rate (on a table top)
- record efficiency
- encodes information in photon arrival time and polarization
- partial security obtained by checking polarization (assumes no QND attack possible that does not disturb polarization)
- a single channel operates at a “secure” rate over 10 Mbit/s
- multiplex many spatial and spectral channels to achieve 1 Gbit/s rate
- achieve > 4 bits/detected photon pair at high rate
- achieve > 8 bits/detected photon pair at low rate (maintain coherence in a very high dimension Hilbert space!)
- developed a wide range of new quantum technologies that will have an impact beyond this immediate project