Implementing free-space QKD systems between moving platforms: polarization vs. time-bin encoding

Thomas Jennewein,

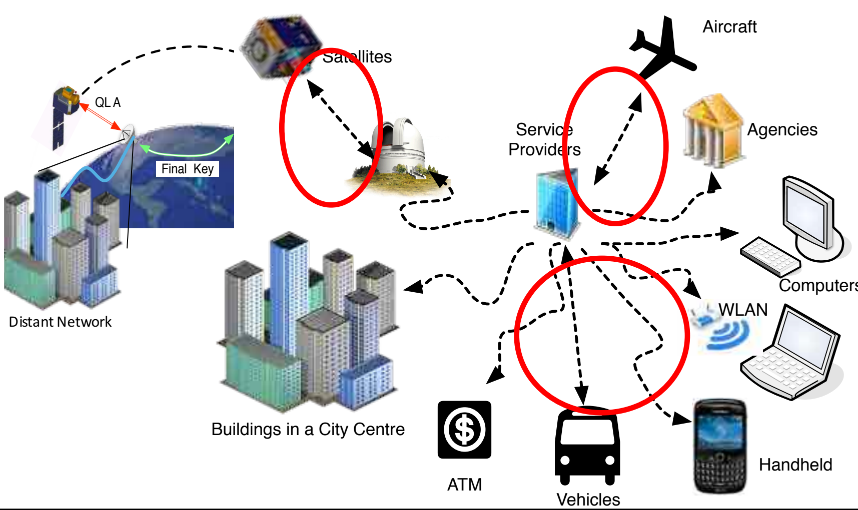
Institute for Quantum Computing & Department of Physics and Astronomy,

University of Waterloo

Thomas.Jennewein@uwaterloo.ca

Quantum Internet – the Long Term Vision

Qubit distribution with moving systems: satellites, aircraft, vehicles, ships, handheld



Polarisation vs. Time-bin Encoding for Free-Space QKD Links

Traditionally polarization encoding is preferred for free-space links implementations. Essentially implements the BB84 protocol.

$$|0\rangle \rightarrow |H\rangle$$
$$|1\rangle \rightarrow |V\rangle$$

Optical photons: Polarization is only affected by turbulence and atmospheric effects

Depolarization of a Laser Beam at 6328 A due to Atmospheric Transmission

D. H. Höhn

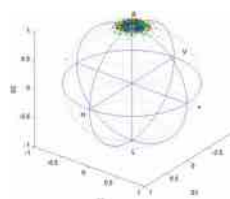
Pol. Error < 10^{-4} rad

February 1969 / Vol. 8, No. 2 / APPLIED OPTICS 367

Confirmed by many QKD tests:

- Horizontal QKD links (144km): QBER ca. 5%
- Laser links with satellites: Pol. Error 3.2 deg, QBER ca. 3%

Toyoshima et al., Vol. 17, No. 25 / OPTICS EXPRESS 22333 (2009)



Polarization Reference Frames between Moving Platforms

- Can move in many degrees of freedom for Alice, and Bob

Active control of polarization, via measurement and correction

Bourgoin, Higgins, Gigov, Holloway, Pugh, Kaiser, Cranmer, TJ, Optics Express, (2015) & arxiv 2015, 1505.00292

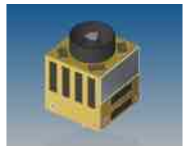
Reference Frame Independent Protocols, which essentially test the purity of received qubits

Use: L/R for Key, and P/M and H/V for link integrity test

Laing, Scarani, Rarity, O'Brien, PHYSICAL REVIEW A **82**, 012304 (2010)

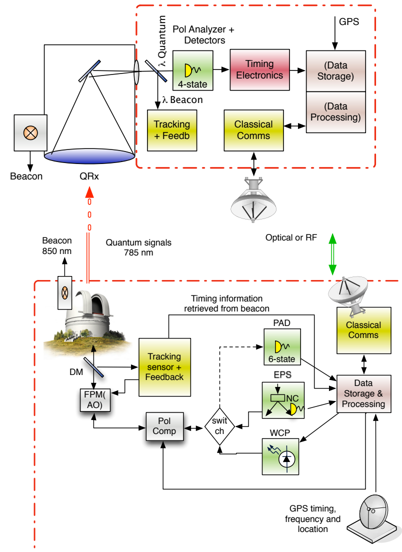
Canadian Quantum Satellite Studies

- **QEYSSat**
- Mission proposal for a micro-satellite quantum receiver
  - IQC scientific lead
  - Designed with Canadian Industry
  - LEO
  - Mass: 50kg,
  - Dimensions: 80×60×60 cm^3
- Status: Feasibility studies, mission and payload development (STDP), Form-fit-function prototype + rad tests, outdoor trials

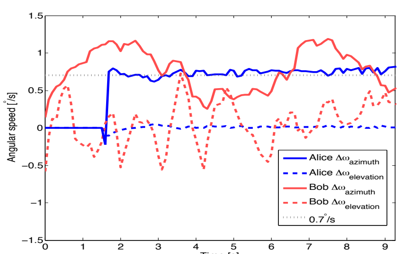


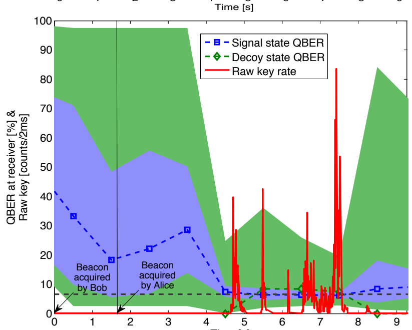
- **NanoQEY:**
- Concept for a Nano- Sat based Quantum Key Exchange satellite
  - Mass: 15 kg,
  - Dimensions: 40×26×20 cm^3

Link Analysis: J.P. Bourgoin, et al, NJP, 15:023006, (2013)
QYESSAT: T. Jennewein et al,, volume 8997 of Proceedings of SPIE, (2014).
NanoQEY: T. Jennewein et al, vol. 9254 of Proceedings of SPIE, (2014).



Outdoor Trials with Moving Truck





Bourgoin, Higgins, Gigov, Holloway, Pugh, Kaiser, Cranmer, TJ, Optics Express, (2015) & arxiv 2015, 1505.00292

- 1st generation system
- Quantum transmission range 650 m
- Quantum receiver truck driving 30 km/h
- Generated 160 bit secure key
- Realtime compensation of pointing, polarization and timing

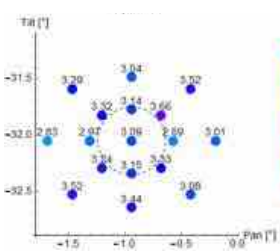
Physical Parameters

	IOA	Detectors	CDPU	Overall
Volume Budget	150 × 150 × 200 mm		150 × 150 × 200 mm	
Measured	48.2 × 56.8 × 120 mm	30 × 127 × 143 mm	25.4 × 106.6 × 118.4 mm	
Mass Budget	(3 kg)	(5 kg)	(4 kg)	12 kg
Measured	0.32 kg	0.516 kg	0.129 kg	< 2 kg
Power Budget		(2.5 W)	(2.5 W)*	6 W*
Measured		2.46 W	4 W*	6.46 W*

7

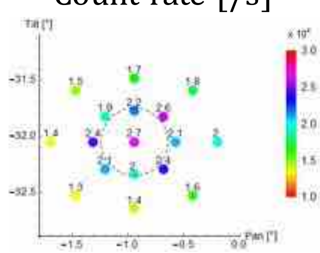
Optical Fine Pointing

QBER [%]

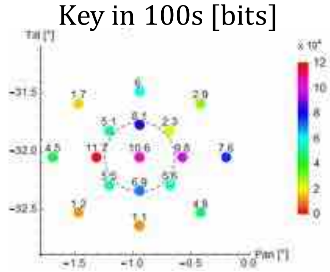


- Intrinsic source QBER ≈ 2%
- Near constant QBER over full FOV (0.7 deg)
- Count rate drops at the edges, reducing key length

Count rate [/s]

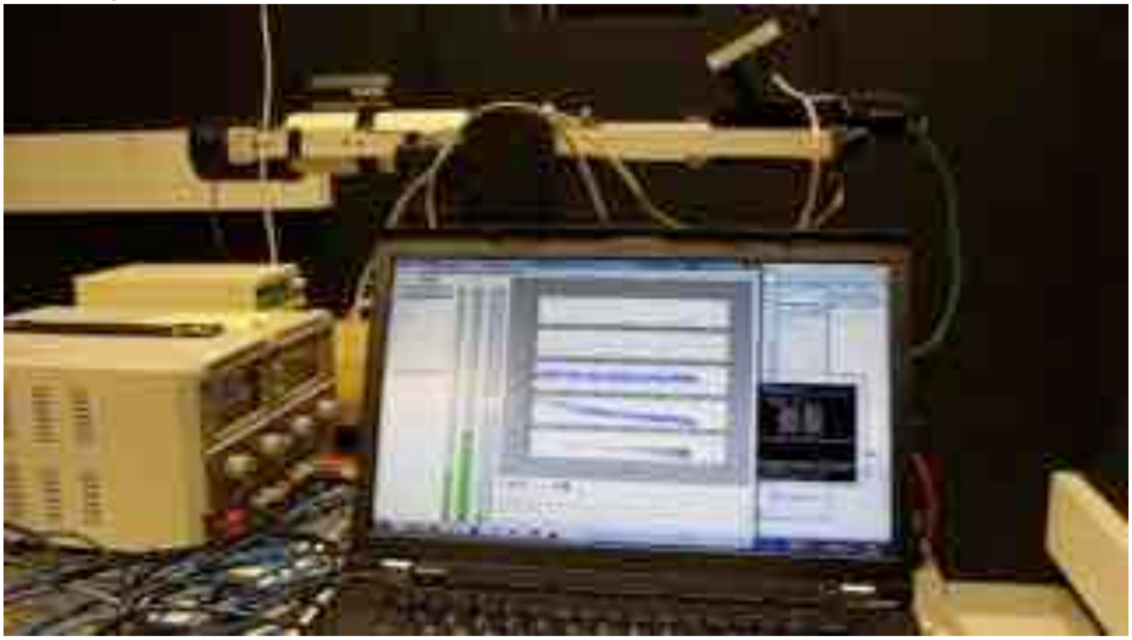


Key in 100s [bits]

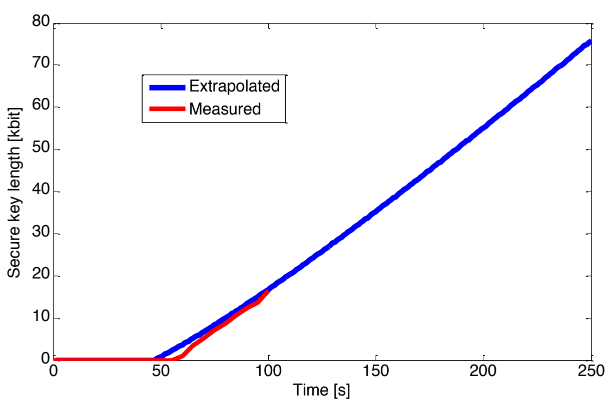


8

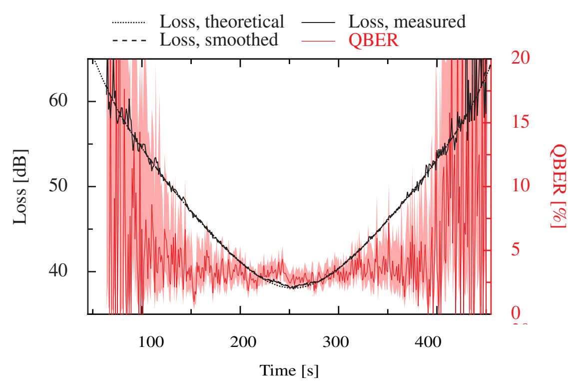
APT system in 'action'



Lab-demonstration of QKD with expected link losses



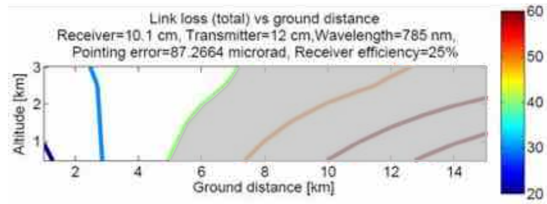
- **Because of finite size effects, secure key extracted only after 57s**
- 500MHz QKD at 38.7dB key vs. time
- Full BB-84 QKD protocol with decoy states (error correction, PA)
- The key length is predicted to reach 40kbit after 162s
- The key length is predicted to reach 75.8kbit after 250s



Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations. Bourgoin, Gigov, Higgins, Yan, Meyer-Scott, Khandani, Luetkenhaus, TJ, Phys. Rev. A 92, 052339 (2015)

Airborne QKD with quantum receiver

2nd generation system: Satellite prototype on aircraft
Goal: demonstrate quantum link with up to 1 deg/s angular speed
Analysis of air-speed, altitude, distance (graph on right)
Tests conducted week of Sept. 19th/2016



The Quantum Transmitter setup

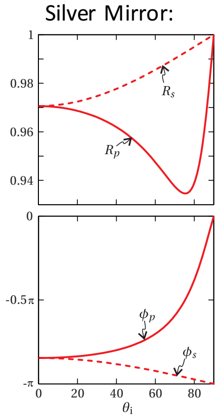
Integration & Test of Payload at aircraft

Quantum Receiver Payload

Polarization Issues within Optical Systems

Polarization effect of mirrors due to **Fresnel-coefficients**

Silver Mirror:



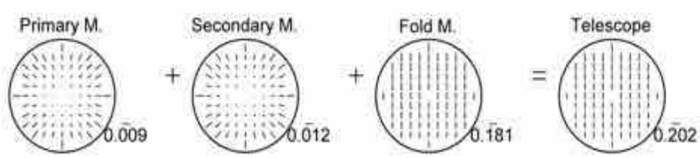
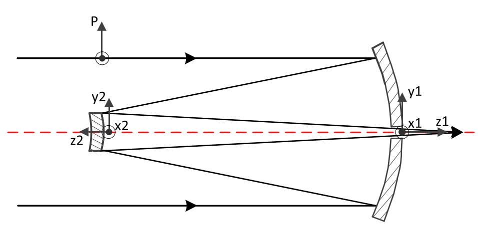


FIG. 6.—Retardance maps for each mirror element (*first three panels*) and the cumulative retardance for the entire telescope (*last panel*).

Breckinridge, Lam, Chipman, Publications of the Astronomical Society of the Pacific, Vol. 127, No. 951 (2015), pp. 445



2015 / Vol. 54, No. 3 / APPLIED OPTICS

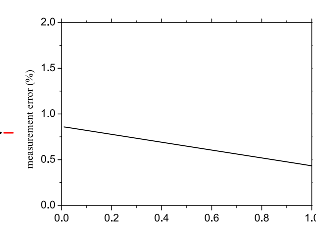
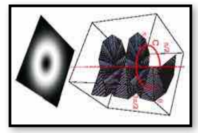
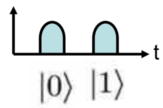


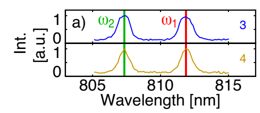
Fig. 4. Measurement error, induced by a Cassegrain telescope

Alternative Encoding for Quantum Information on Free-Space Photons?

- In principle degrees of freedom (D)F) of photons can be utilized to encode photonic qubits
  - Spatial Mode
    - paths
    - Orbital angular momentum, LG modes
  - Time bin
    - related: Differential Phase Shift, COW
  - Frequency bins, side bands
  - Quadrature of light (only continuous variables)

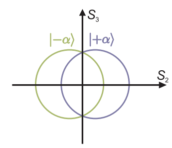






$$\hat{x}_k = \sqrt{\frac{\hbar}{2\omega_k}}(\hat{a}_k + \hat{a}_k^\dagger),$$

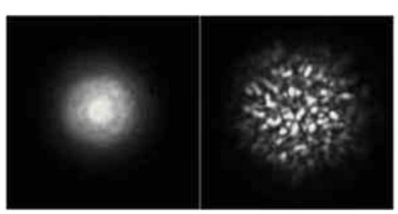
$$\hat{p}_k = -i\sqrt{\frac{\hbar\omega_k}{2}}(\hat{a}_k - \hat{a}_k^\dagger).$$



Are they suitable for a long distance free-space link?
Motion errors, atmospheric turbulence

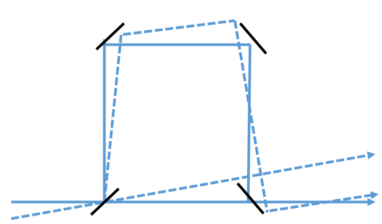
Time bin encoding for free-space

- Requires, that the unbalanced interferometers for encoding / decoding the qubits can work with multimodal beams



(left) Single mode ban (right) Test beam generated 2 m of MMF

Uncorrected Interferometer:



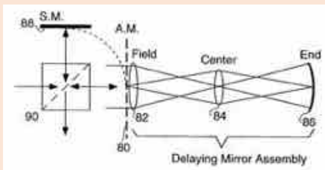
$$\mathcal{V}(\alpha) = \mathcal{V}_0 \, exp\left(-\left(\frac{\Delta l_0 \tan(\alpha)}{\sqrt{2}\sigma(1+\tan(\alpha))}\right)^2\right)$$

Prior Solutions:
Couple into single mode fiber (losses very high)
Adaptive optics (can be lossy, challenging)

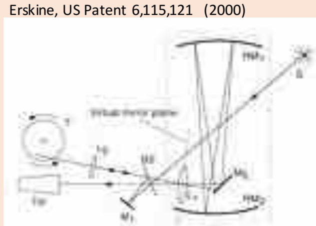
Multi-mode Michelson Interferometers

Used in applications for multi-mode images in Doppler-LIDAR Velocimetry with incoherent light sources, Astronomy, Narrowband Filters in LIDAR

Superimposing Interferometers



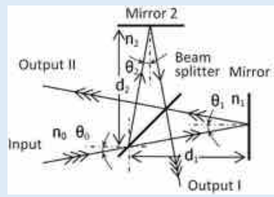
Erskine, US Patent 6,115,121 (2000)



Erskine, Holmes, Nature, Vol 377, p317 (1995)

Field-Widened Michelson Interferometers

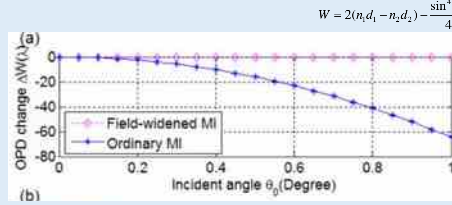
Appl. Opt. **11**(3), 507–516 (1972).
Appl. Opt. **24**(11), 1571–1584 (1985)



$$W = 2(n_1d_1 - n_2d_2) - \sin^2\theta_0\left(\frac{d_1}{n_1} - \frac{d_2}{n_2}\right) - \frac{\sin^4\theta_0}{4}\left(\frac{d_1}{n_1^3} - \frac{d_2}{n_2^3}\right) - \frac{\sin^6\theta_0}{8}\left(\frac{d_1}{n_1^5} - \frac{d_2}{n_2^5}\right)\ldots\ldots$$

$$\boxed{d_1/n_1 - d_2/n_2 = 0.}$$

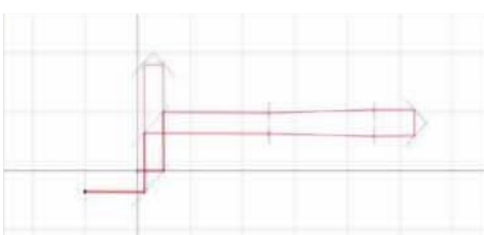
$$W = 2(n_1d_1 - n_2d_2) - \frac{\sin^4\theta_0}{4}\left(\frac{d_1}{n_1^3} - \frac{d_2}{n_2^3}\right) - \frac{\sin^6\theta_0}{8}\left(\frac{d_1}{n_1^5} - \frac{d_2}{n_2^5}\right)\ldots\ldots$$



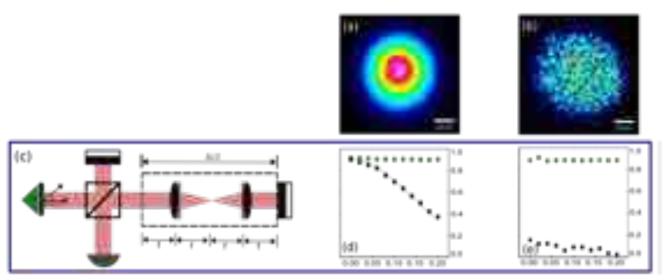
Liu et al, Vol. 20, No. 2 / OPTICS EXPRESS 1406 (2012)

Unbalanced Interferometer Suitable for Quantum Communications

- Compatibility with Photonic Qubits:
  - Dispersion, Polarization effects, stability ?



ZEMAX modelling of optical configuration



- [J. Jin, S. Agne, J.P. Bourgoin, Y. Zhang, N. Lutkenhaus, T. Jennewein, arXiv:1509.07490]

Demonstration using Entangled Photons

Type-I interferometer, relay lens
Time delay: 2 ns

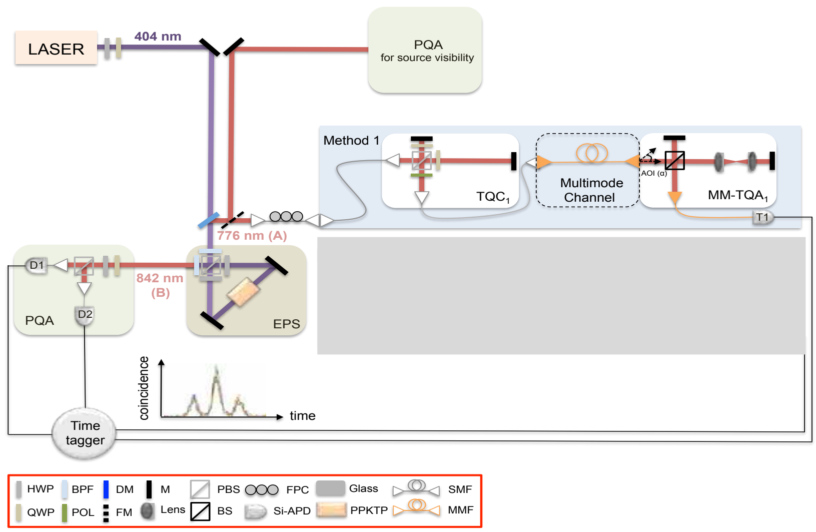
Hybrid entangled State:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\mathrm{V}\rangle_\mathrm{A}|\mathrm{H}\rangle_\mathrm{B} + |\mathrm{H}\rangle_\mathrm{A}|\mathrm{V}\rangle_\mathrm{B})$$

$$|\mathrm{V}\rangle \mapsto |\mathrm{E}\rangle \text{ and } |\mathrm{H}\rangle \mapsto |\mathrm{L}\rangle$$

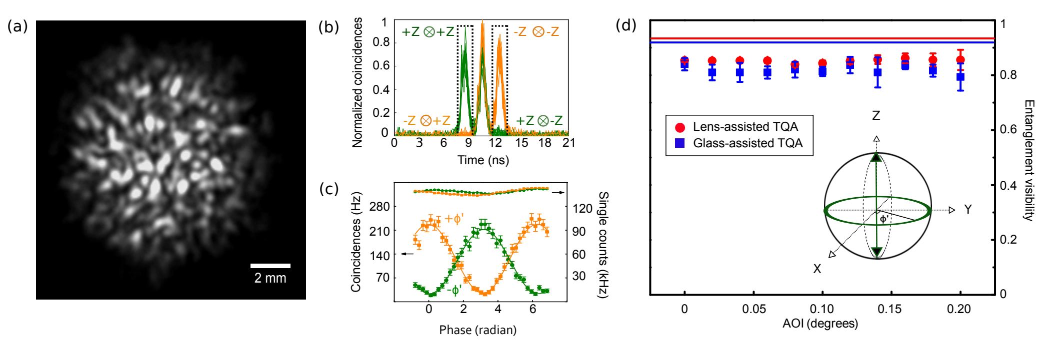
$$\boxed{|\psi\rangle = \frac{1}{\sqrt{2}}(|\mathrm{E}\rangle_\mathrm{A}|\mathrm{H}\rangle_\mathrm{B} + |\mathrm{L}\rangle_\mathrm{A}|\mathrm{V}\rangle_\mathrm{B}),}$$

Xiao-song Ma, et al, PHYSICAL REVIEW A, 79(4), (2009).



Experimental Test of Hybrid Entanglement

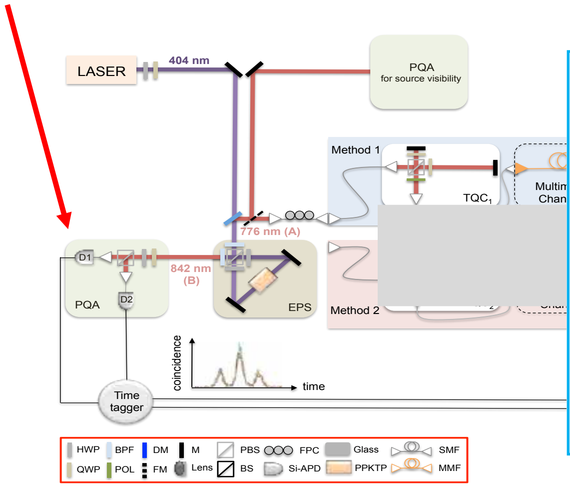
Highly multimodal beams, variation of angular input
Interferometer visibility > 90%, the system visibility reduced to ca.80% due to source, conversion, alignment

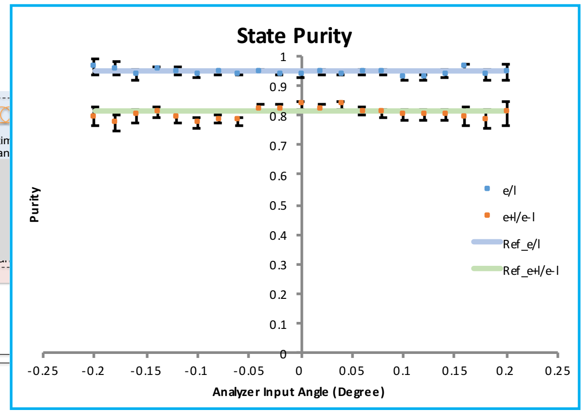


- [J. Jin, S. Agne, J.P. Bourgoin, Y. Zhang, N. Lutkenhaus, T. Jennewein, arXiv:1509.07490]

Quantum Tomography of Heralded Photon

Apply tomographic measurements on polarized photon: HV, RL and PM basis

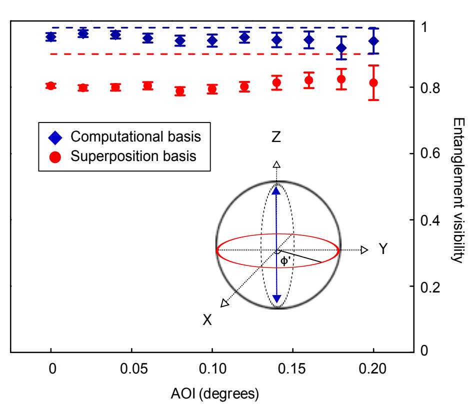




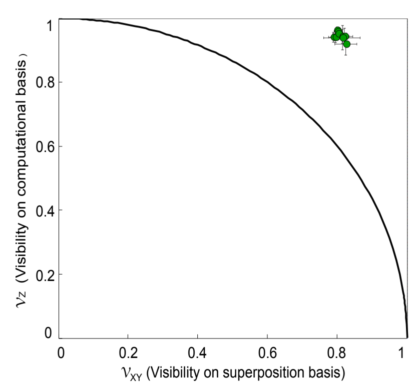
Entanglement and QKD verification

Two-basis measured: Early/Late basis high contrast, Superposition basis using interference

Experiment



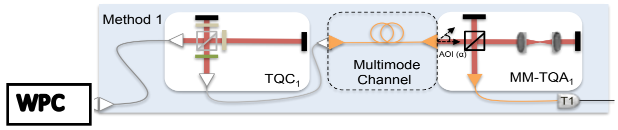
Combined with Theory (Group of Norbert Lutkenhaus)



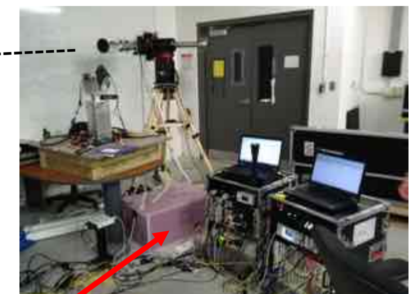
- [J. Jin, S. Agne, J.P. Bourgoin, Y. Zhang, N. Lutkenhaus, T. Jennewein, arXiv:1509.07490]

Outdoors? Time bin QKD over telescope link

- Preliminary link demonstrated
  - QBER: ca. 5%
  - Uses 2nd generation interferometers: >95% intrinsic visibility



Receiver interferometer

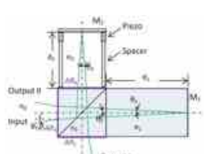


Transmitter interferometer

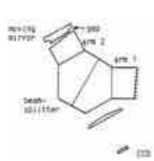
Time-bin interferometer using glass

- Tested a different approach: using refraction to compensate field
- Refractive index cancels walk-off

$$\boxed{d_1 / n_1 - d_2 / n_2 = 0.}$$



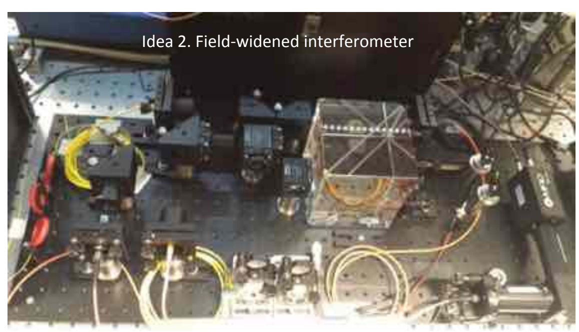
Dong Liu ,
2012 / Vol.20, No. 2 / OPTICS EXPRESS



DOPPLER IMAGING WITH FIELD-WIDENED
MICHELSON INTERFEROMETERS

G.G. Shepherd, W.A. Gault, R.H. Wiens, W. Ward
Centre for Research in Experimental Space Science
York University, Downsview, Ontario, M3J 1P3, Canada

Under the sponsorship of the Space Division of the National



Measured Interference Visibilities, 118 mm glass cube:
Time delay: 0.57 ns
Multimode Fiber input beam:
V= 0.95 (comp basis), V=0.90 (superposition basis)

Demonstration of Glass-based Interferometer

Type-II interferometer, refractiive index

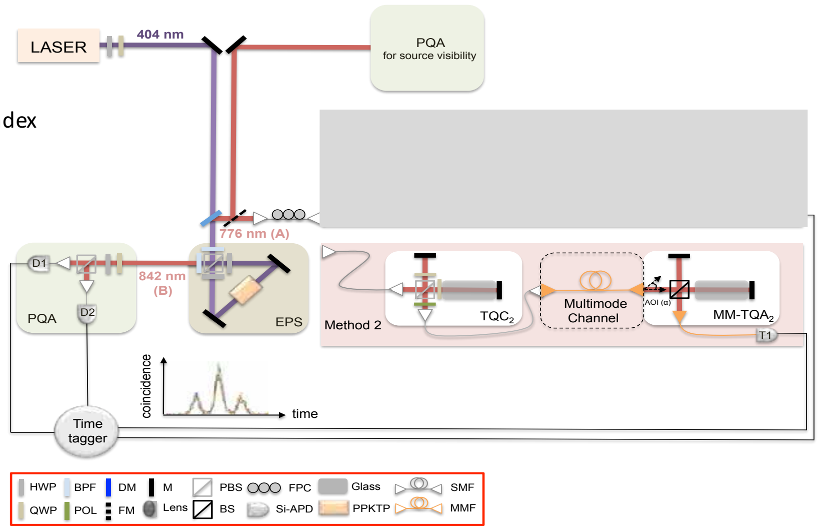
Hybrid entangled State:

$$|\psi\rangle = \tfrac{1}{\sqrt{2}}(|V\rangle_A|H\rangle_B + |H\rangle_A|V\rangle_B)$$

$$|V\rangle \mapsto |E\rangle \text{ and } |H\rangle \mapsto |L\rangle$$

$$\boxed{|\psi\rangle = \frac{1}{\sqrt{2}}(|E\rangle_A|H\rangle_B + |L\rangle_A|V\rangle_B),}$$

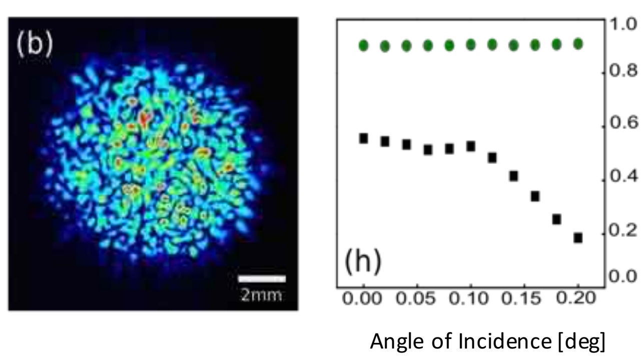
Xiao-song Ma, et al, PHYSICAL REVIEW A, 79(4), (2009).



Results for Type-II interferometer

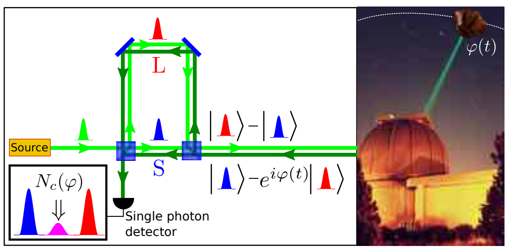
- Test with MMF, with (green) and without (black) glass
- Alignment turned out to be "very easy"
- **Challenge: dispersion of 5.48 waves/nm and 5.21 waves/ ◦C**

V= 0.95 (comp basis)
V=0.90 (superposition basis)



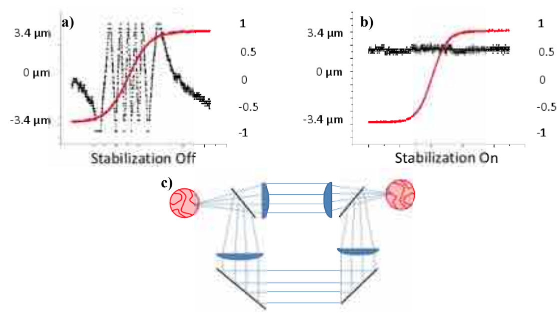
Quantum Interferometers for Multi-Mode beams Widely Studied

Villorsei, Padova group: Quantum interference along satellite-ground channels, PRL 2016, [arXiv:1509.07855 [quant-ph]]



P. Kwiat, U Illinois group:

Zeitler et al, SPIE Vol. 9739 973912-1 (2016)



Conclusion

- Time bin encoding viable for multi-mode channels!
- Purely passive optical correction of beams
- 80% coupling throughput of input signal into detectors
- Stable and consistent interference visibilities of up to 97% achieved

- Challenges:
  - stabilizing transmitter and receiver interferometers
  - Designing thermally stable and compact interferometers
  - Dispersion effects need to be cancelled

Outlook

- **Time-bin over free space channels, opens up several new directions**
- Polarizing effects of telescopes and optical path can be overcome
  - Broad variety of fine-steering systems technology
  - Compact, short telescopes
  - Optical fiber interfaced of photons with source and detectors
- Interfacing of fiber optical and free-soace links straight forward
- Direct compatibility between QKD and classical laser coms
- Implementation of differential-phase shift protocols over free-space DPS-QKD, COW-QKD
- Novel protocols for free-space
  - reference-frame independence
  - hyper dimensional encoding
- Novel media QKD, such as over multi-mode fiber (plastic fiber), depolarizing channels
- QIP: capture of multi-modal photons also suitable for experiments

Thank You

- *Polarization systems well advanced*
- *Time-bin can be an important alternative*
- *Could simplify optical systems design, pointing*
- *Enable novel protocols and schems*

Thank You

UNIVERSITY OF WATERLOO
IQC Institute for Quantum Computing
CSA ASC
UTIAS SFL
neptec
ONR
DEFENCE R&D DÉFENSE
INO
NSERC CRSNG
Industry Canada
Industrie Canada
Ontario
MINISTRY OF RESEARCH & INNOVATION
MINISTRY OF ECONOMIC DEVELOPMENT AND INNOVATION
CIFAR
CANADIAN INSTITUTE
ICIP CIPI
CANADA'S ECONOMIC ACTION PLAN
INNOVATION.CA
CANADA FOUNDATION FOR INNOVATION | FONDATION CANADIENNE POUR L'INNOVATION
COM DEV