Novel techniques for ground to space quantum channels

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

Thomas Jennewein

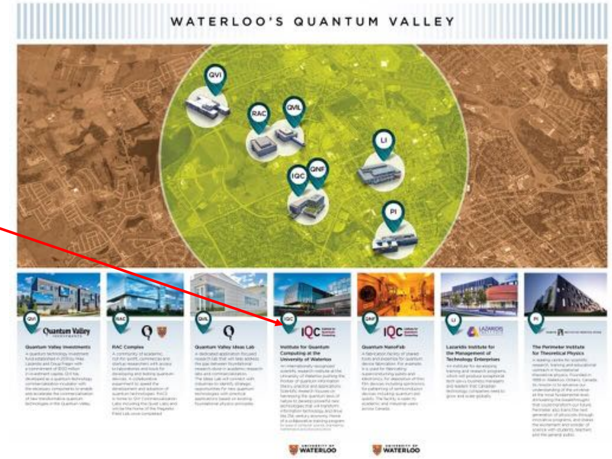
Institute for Quantum Computing & Department of Physics and Astronomy,
University of Waterloo

Thomas.Jennewein@uwaterloo.ca

2020.07

1

IQC @ 2019:
31 faculty
157 Grad students
57 Postdoc
1800+ publications
$600M+ funding
13 spin-offs



2

Quantum Internet


REVIEW SUMMARY

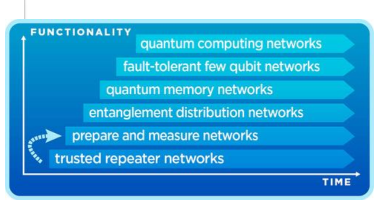
QUANTUM INFORMATION

Quantum internet: A vision for the road ahead

Stephanie Wehner*, David Elkouss, Ronald Hanson

Science 362, 303 (2018)

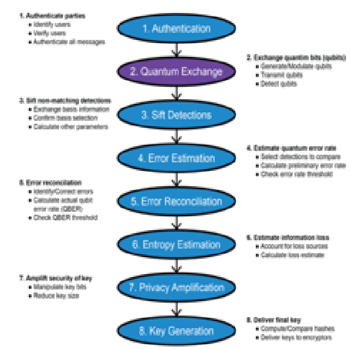
Quantum computing in the cloud:



10

Quantum Key Distribution

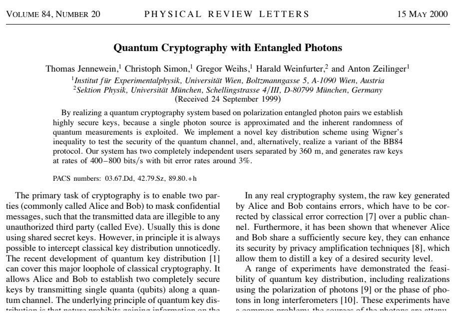
Fixes the loophole of key distribution, where classical keys could be copied or compromised during transport.
Only transmit single quanta of light per bit.



L. O. Mailloux et. al. Journal of Cyber Security and Information Systems, 4, 2 – Basic Complexity

11

Historical note on QKD



VOLUME 84, NUMBER 20 PHYSICAL REVIEW LETTERS 15 MAY 2000

Quantum Cryptography with Entangled Photons

Thomas Jennewein,[1] Christoph Simon,[1] Gregor Weihs,[1] Harald Weinfurter,[2] and Anton Zeilinger[1]
[1]*Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090 Wien, Austria*
[2]*Sektion Physik, Universität München, Schellingstrasse 4/III, D-80799 München, Germany*
(Received 24 September 1999)

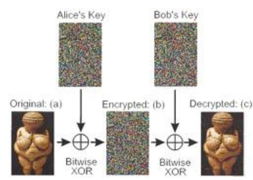
By realizing a quantum cryptography system based on polarization entangled photon pairs we establish highly secure keys, because a single photon source is approximated and the inherent randomness of quantum measurements is exploited. We implement a novel key distribution scheme using Wigner's inequality to test the security of the quantum channel, and, alternatively, realize a variant of the BB84 protocol. Our system has two completely independent users separated by 360 m, and generates raw keys at rates of 400–800 bits/s with bit error rates around 3%.

PACS numbers: 03.67.Dd, 42.79.Sz, 89.80.+h

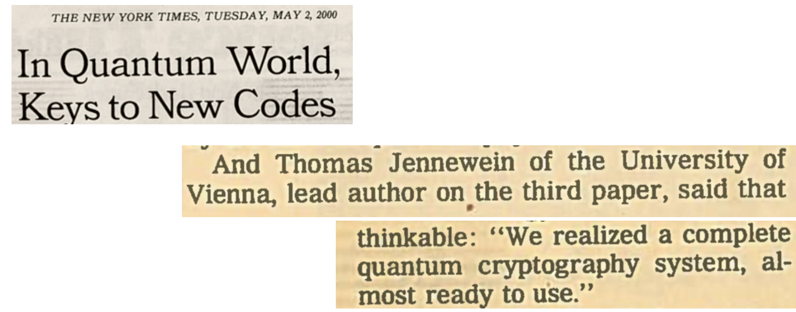
The primary task of cryptography is to enable two parties (commonly called Alice and Bob) to mask confidential messages, such that the transmitted data are illegible to any unauthorized third party (called Eve). Usually this is done using shared secret keys. However, in principle it is always possible to intercept classical key distribution unnoticedly. The recent development of quantum key distribution [1] can cover this major loophole of classical cryptography. It allows Alice and Bob to establish two completely secure keys by transmitting single quanta (qubits) along a quantum channel. The underlying principle of quantum key dis-

In any real cryptography system, the raw key generated by Alice and Bob contains errors, which have to be corrected by classical error correction [7] over a public channel. Furthermore, it has been shown that whenever Alice and Bob share a sufficiently secure key, they can enhance its security by privacy amplification techniques [8], which allow them to distill a key of a desired security level.

A range of experiments have demonstrated the feasibility of quantum key distribution, including realizations using the polarization of photons [9] or the phase of photons in long interferometers [10]. These experiments have



12



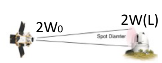
13

Why Satellites for Long Distance Q-Com?

- Ground-based
  - Practical systems typically 100 km
  - Demonstrations up to to 400 km
  - Optic fibre loss 0.15 dB/km at best
  - Free-space limited due to line-of-sight
  - Commercial Devices available:
  - **Note: Optical amplifiers not possible!**
- Longer distances:
  - Trusted Repeaters (> 2000km network China)
  - Long lifetime Quantum Memories
  - Quantum Repeaters
  - **Satellites**

Takesue et al, Nature Photonics 1, 343 - 348 (2007)
Ma, Fung, Lo, Phys. Rev. A 76, 012307 (2007)

$$T_{geo} \approx \frac{D_R^2 D_T^2}{\lambda^2 L^2}$$



14

Quantum Communication in Space

Dedicated quantum hardware in Space:

- China (J.W. Pan)
  - **Entanglement Distribution over 1200 km !** (Science, 2017)
  - QKD, Teleportation (Nature 549, 43–47 and 70-73 (2017)
  - **QKD between Bejing and Graz (PRL), QKD using Bell-pairs (CLEO 2019, Nature2020)**
- Japan (NICT)
  - 50 kg satellite: Nature Photonics 11, 502–508 (2017)
- Singapore (A. Ling)
  - Correlated Photon Source onboard CubeSat (Phys. Rev. Applied 5, 054022, 2016)
  - SpooQey-1: July 2019: Entanglement in space
- Several more missions in preparation

Beijing and Vienna have a quantum conversation
September 2017, www.physicsworld.com
http://english.cas.cn/newsroom/news/201709/t20170928_183577.shtml

19

And was noticed by the world!


TIME | TIME 100

JIAN-WEI PAN

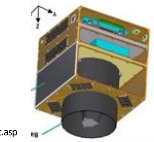
by Anton Zeilinger

I can't imagine the emergence of quantum technology without Jian-Wei Pan. The world came to appreciate his work last summer, when he achieved quantum communication using quantum states of photons between Earth and China's Micius satellite orbiting more than 300 miles overhead—and establishing the country as a leader in the field.

In the section **Pioneers**.
Announced April, 2018.

20

Canadian Quantum Satellite



http://www.asc-csa.gc.ca/eng/sciences/qeyssat.asp


Government of Canada | Gouvernement du Canada

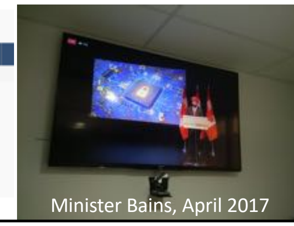
Home → Innovation, Science and Economic Development Canada

Ministers Bains and Garneau celebrate $80.9 million for the Canadian Space Agency

News Release

From Innovation, Science and Economic Development Canada

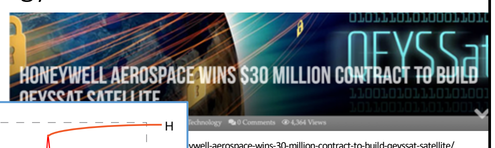
Funding will support new projects that will use Canadian innovations in space

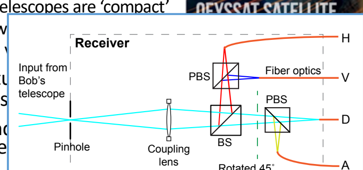


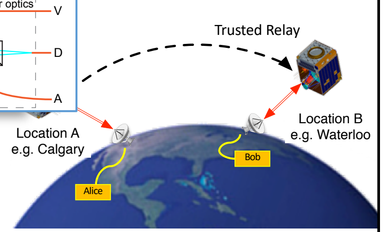
21

QEYSSat will be a Technology Demonstration Platform

- Optimized Quantum Receiver
- Multiple partners across Canada
  - Transmitter telescopes are 'compact'
  - Networking w…
  - Test link with …
- Study of quantu… entanglement s…
- Multiple groun… and around the…
- Research on ground station capabilities such as AO or different quantum emitters, etc.



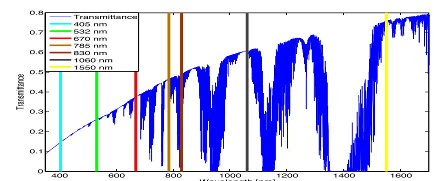




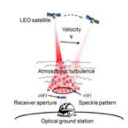
23

Modeling the performance of satellite to ground quantum link

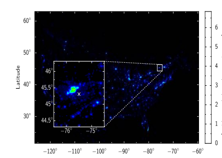
- Analysis of wavelengths with windows of 'good' atmospheric transmission
- Link modelled using turbulence; diffraction to account for beam obstruction; background signals



North America – the cutout is centred around Ottawa



M. Toyoshima, op.Ex. 2011



Wavelength (nm)	Secure key length obtained for the upper quartile satellite pass (kbit): Downlink, WCP source	Uplink, WCP source	Downlink, entangled photon source	Uplink, entangled photon source
405	68.5	3.5	6.2	0
532	264.5	33.1	119.3	12.1
670	465.6	87.7	324.7	67.4
785	458.3	111.3	272.9	75.7
830	317.3	82.1	136.1	39.7
1060	175.4	67.6	21.8	8.1
1550	123.9	94.8	12.8	14.4

J.P. Bourgoin, et al, NJP, 15:023006, 2013

Related analysis:
J. Rarity et al, NJP, 2002
P. Villoresi group, NJP, 2009
R. Ursin group, NJP, 2013

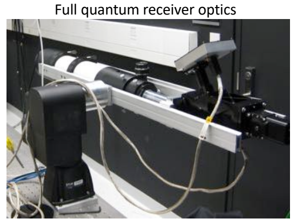
29

QEYSSat Payload Prototype

UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing

- Fully functional form-representative quantum-payload
- Components have 'path to flight'
- Projected mass: ~ 23 kg, Power <30W, envelope ~ 60cm^3
- Tests: Radiation, TVAC, aircraft link

Full quantum receiver optics



Payload detectors and electronics

C. Pugh et al., Quantum Science and Technology, 2017; 2 (2): 024009

Press release: https://uwaterloo.ca/institute-for-quantum-computing/news/iqc-advances-quantum-satellite-mission

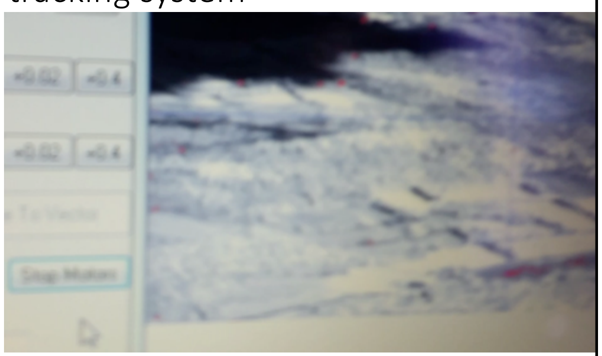
34

Ground to Aircraft Demonstration

36

Airborne QKD tracking system

- Airborne Trials 2016- Sep. 20 / 21
- Night #1: 7 passes, of which 2 acquired signal. Night #2: 8 passes, of which 5 acquired signal.
  - **3 km line pass:** secure key (finite size included) of 46805 bit, 35 seconds.
  - **10 km arc pass:** secure key (finite size included) 41899 bit, 250 seconds.



C. Pugh et al, Quantum Science and Technology, 2, 2, 024009 (2017)

37

Novel Protocols for Free-Space Quantum Communications

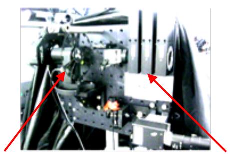
Lessons learnt from previous tests

- Reference Frame Independent QKD
- Alternative Encoding of Photonic Qubits
- HOM Interference with Structured Pulses

38

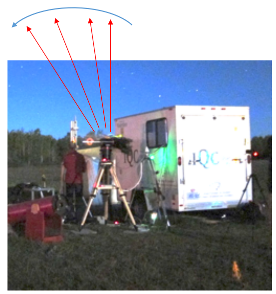
I. Reference-Frame Alignment

- Challenge for QKD implementations
  - How to align the reference frames (e.g. polarization states at Alice have to match Bob's)?
  - Particular problem in our case is the motion of the telescope
  - Realtime Compensation:



arxiv.org 1810.04112

Tomography   Compensation



Airborne Transmitter, Smith Falls, 2016

39

Our satellite receiver has limited resource of 4 states

- New variant of the protocol: 6 – 4 state protocol

A. Laing et. al, Phys. Rev. A, 82(1):012304, Jul 2010.

R. Tannous,. MsC thesis, 2018. Arxiv 1905.09197

Channel Verification:

$$C = \sqrt{\langle X_A X_B \rangle^2 + \langle Y_A X_B \rangle^2},$$

$$\langle \sigma_Z \otimes \sigma_Z \rangle = (1-2Q)$$
$$\langle \sigma_X \otimes \sigma_X \rangle = (1-2Q) \cdot \cos\theta$$
$$\langle \sigma_Y \otimes \sigma_X \rangle = -(1-2Q) \cdot \sin\theta$$

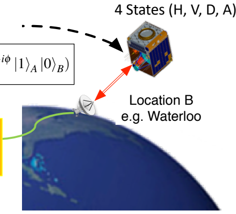
$$\langle \sigma_V \otimes \sigma_X \rangle = (1-2Q)$$
$$\sigma_V = (\cos\theta)\sigma_X - (\sin\theta)\sigma_Y$$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B + e^{-i\phi}|1\rangle_A |0\rangle_B)$$

4 States (H, V, D, A)

Location B e.g. Waterloo

Bob 6 stats – H, V, D, A, L, R

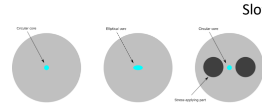


C will be constant even under varying phase theta, and if C drops <1, would reveal Eve!

41

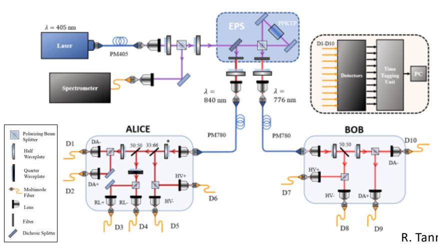
Experimental Setup

- Transmission over polarization maintaining fiber



Slow axis = V

Fast axis = H



Birefringent walkoff

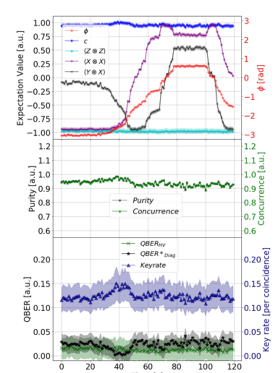
$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B + e^{-i\phi}|1\rangle_A |0\rangle_B)$$

R. Tannous, APPLIED PHYSICS LETTERS, 115(21), 2019.

42

R. Tannous, APPLIED PHYSICS LETTERS, 115(21), 2019.

Results



The phase is varied by tuning a birefringent element.

Coincidence Counts

Tomography to determine purity of state

$$\mathrm{QBER}_{HV} = \frac{1-\langle Z\otimes Z\rangle}{2} = \frac{N_{\text{bad}}}{N_{\text{total}}},$$
$$\mathrm{QBER}^*_{Diag} = \frac{1-C}{2}.$$

$$R \geq Q_\lambda(1 - f H_2(\mathrm{QBER}_{HV}) - H_2(\mathrm{QBER}^*_{Diag}))$$

43

II: Myth: You can only use polarization encoding in free-space quantum communications

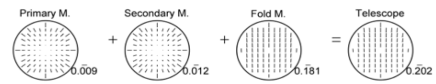
Depolarization of a Laser Beam at 6328 A due to Atmospheric Transmission

D. H. Höhn

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

Dpolarization measured ca. 10^{-7} to 10^{-5} rad.
Limited by apparatus and background light.

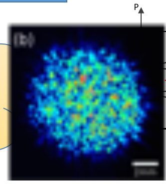
Polarization effect of mirrors due to **Fresnel-coefficients**

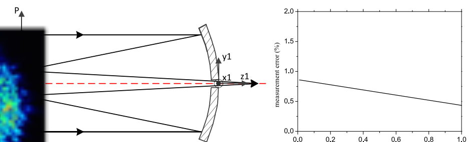


Retardance maps for each mirror element (*first three panels*) and the cumulative retardance for the entire telescope (*last panel*).

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

What about Time-bin encoding in Free-Space?



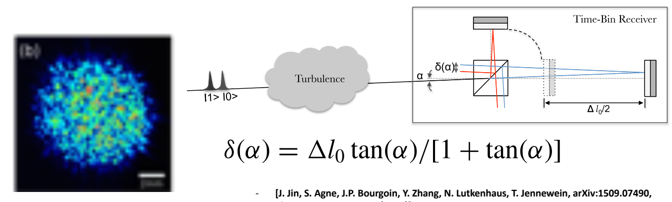


2015 / Vol. 54, No. 3 / APPLIED OPTICS

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

The issue with asymmetric MZI and distorted modes

- Different incident angles and modal distortions experience different Phase
- Tim—bin analyzer interferometer with 'flat' optics not suitable



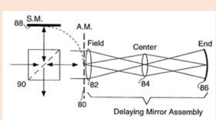
$$\delta(\alpha) = \Delta l_0 \tan(\alpha)/[1+\tan(\alpha)]$$

- [J. Jin, S. Agne, J.P. Bourgoin, Y. Zhang, N. Lutkenhaus, T. Jennewein, arXiv:1509.07490,
- Phys. Rev. A 97, 043847 (2018)]

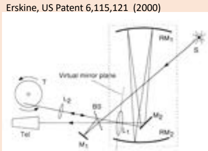
Multi-mode Michelson Interferometers

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

Superimposing Interferometers



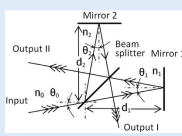
Erskine, US Patent 6,115,121 (2000)



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

Field-Widened Michelson Interferometers

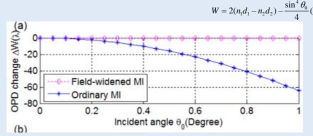
Appl. Opt. **11**(3), 507–516 (1972).
Appl. Opt. **24**(11), 1571–1584 (1985)



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

$$d_1/n_1 - d_2/n_2 = 0.$$

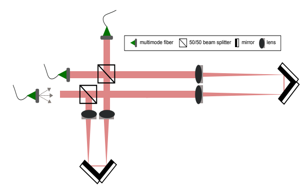
$$W = 2(n_1 d_1 - n_2 d_2) - \frac{\sin^4\theta_0}{4}\left(\frac{d_1}{n_1^3} - \frac{d_2}{n_2^3}\right) - \frac{\sin^6\theta_0}{8}\left(\frac{d_1}{n_1^5} - \frac{d_2}{n_2^5}\right)\cdots\cdots$$



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

New Configuration with Symmetric Imaging Paths

- Observed interference visibilities of >97 % in both outputs,
- Average visibility of 98.5 % for the 4 QKD states.
- Photon collection into a multimode fiber of 80 %, from input to output!



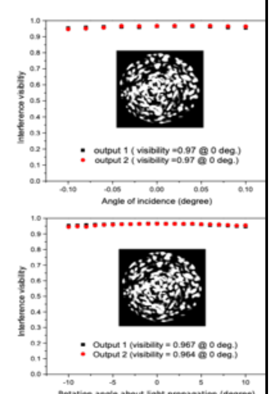
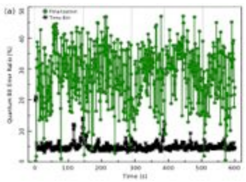


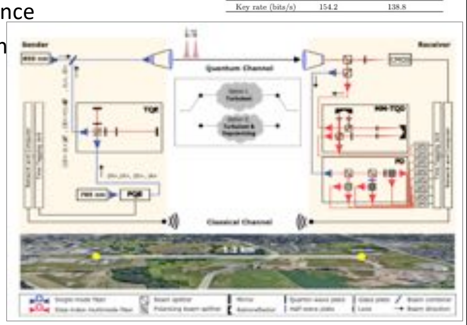
Figure 2. Measured interference visibilities with multimode beam (inset) while varying incidence (a) and rotation (b) angles.

Outdoor Time-Bin QKD Channel

- 1.2 km outdoor link
- Introduced additional turbulence
- also introduced depolarization
- Full BB84 protocol

	Turbulent	Turbulent & Depolarzing
Signal photons/ pulse	0.488	0.520
Decoy photons/ pulse	0.082	0.094
Background/ pulse	3.65×10^{-7}	3.45×10^{-7}
Channel loss (dB)	38.4	38.8
$QBER_{time}^{mean}$ (%)	5.32	5.08
Key rate (bits/s)	154.2	138.8



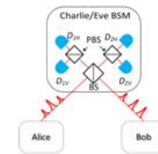


J. Jin et al., OPTICS EXPRESS, 27(26):37214–37223, 2019.

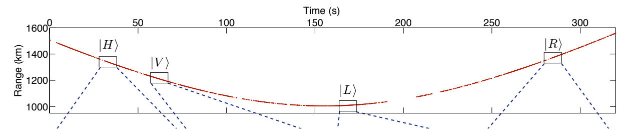
49

Towards free-space MDI-QKD

- No trust on the central Bell-state measurement
- Ideally, the BSM would be located on the moving Systems, such as airplanes or satellites.
  - Challenge: The time-of-flight for each channel will be variable



Hoi-Kwong Lo group, Physical Review Letters 112(19), 2013

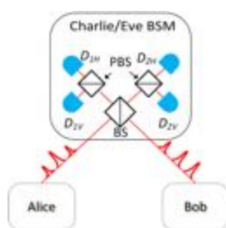


Vallone et al. PRL, 2014

54

Challenge

- How to synchronize the wave packets emitted by Alice, Bob, such that they interfere on Charlie's beam splitter?
- With a moving systems, a real-time compensation is challenging.
  - Alice-Charlie, and Bob-Charlie, must independently measure the exact round trip time for their channels, and actively compensate for any changes.
  - This measurement requires two-way propagation of synchronization information (a-la Einstein)



Hoi-Kwong Lo group, Physical Review Letters 112(19), 2013

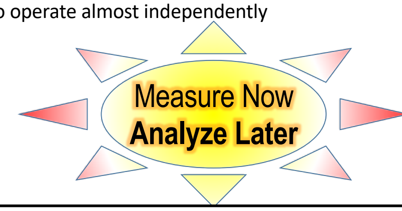
55

Goal: Extract the synchronization of Alice and Bob only **after** the measurements

- Combination of DV and CV MDI-QKD, bring out the best of both worlds:
  - **Photon Detection** from Discrete Variable Schemes allows for channels with long distances / high transmission losses
  - **Long coherence wave packets**, inspired by Continuous Variables Schemes, offer ability for Alice, Bob, Charlie to operate almost independently

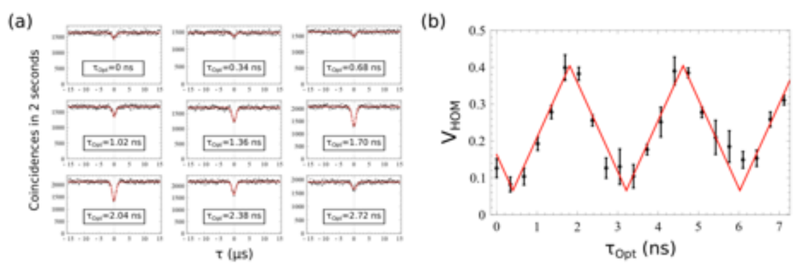
S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, U. L. Andersen, High-rate measurement-device-independent quantum cryptography, *Nat. Photon.* 9, p. 397-402, 2015.

Ulrik L. Andersen, Tobias Gehring, Christian S. Jacobsen and Stefano Pirandola, Effective measurement-device-independent quantum cryptography, SPIE Newsroom. DOI: 10.1117/2.1201509.006119



56

Triangular HOM Interference

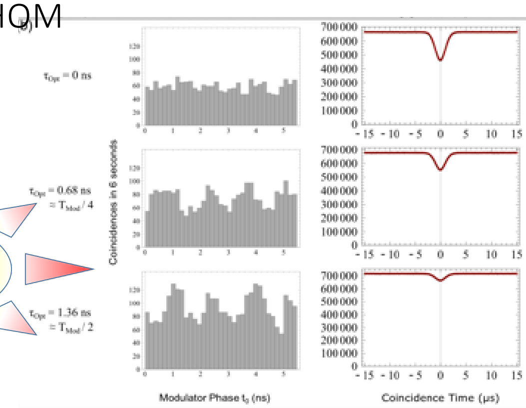


S. Agne PhD thesis, Aug. 2018.
S. Agne et al, arXiv:2004.11259 [quant-ph], accepted in Optics Express, 2020.

59

Time-resolved HOM

HOM coincidences sorted based on modulation timing.



S. Agne PhD thesis, Aug. 2018.
S. Agne et al, Optics Express, 2020.

60

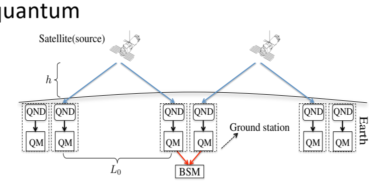
Research on Quantum Networks

- Efficient and robust q-channels
- Dimensions – power – mass
  - chip scale systems ?
- Interfaces / transducers
  - connect channels with stationary qubits
- Long term q-memories
- Routing technologies
- Cost

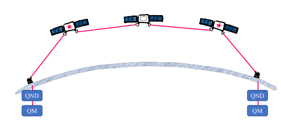
61

Global Quantum Networks?

- A hybrid between satellite links and quantum repeaters may achieve overall best performance
- Satellites and Q-Repeaters
  - Distances up to 20,000 km



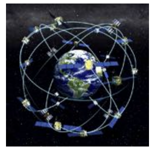
K. Boone, Bourgoin, Meyer-Scott, Heshami, TJ, Simon. PRA 91, 052325 (2015)



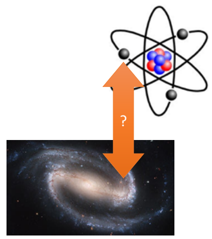
Daniel Oi, Strathclyde Group: Study on Quantum Memories on Satellites,
Mustafa Gündogan, et al, arXiv:2006.10636v1 62

62

Long-term vision for fundamental science



- Global Quantum Networks with satellites
  - We need to understand all (fundamental) effects that are going on in order to get desired behavior
- Question of unification of quantum theory and relativity
  - We need to explore regimes with large (relativistic) velocities and speeds, and gravitational influences.
  - Test the interplay of quantum mechanics and gravity

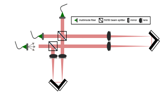


Review of possible science test for quantum entanglement in space:
Fundamental quantum optics experiments conceivable with satellites-reaching relativistic distances and velocities
D. Rideout, T.J, et al. Class. Quant. Grav., 29(22):224011 , 2012.

63

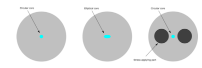
Summary

- Quantum Communication in Space
- QEYSSat mission
- Exploring new directions for robust Free-Space Quantum Communications:
  - Time-bin
  - RFI-QKD
  - towards MDI-QKD



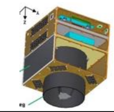
- J. Jin et al., OPTICS EXPRESS, 27(26):37214–37223, (2019).
- J. Jin, et al. Phys. Rev. A 97, 043847 (2018)

- C. Pugh et al, Quantum Science and Technology, 2, 2, 024009 (2017)

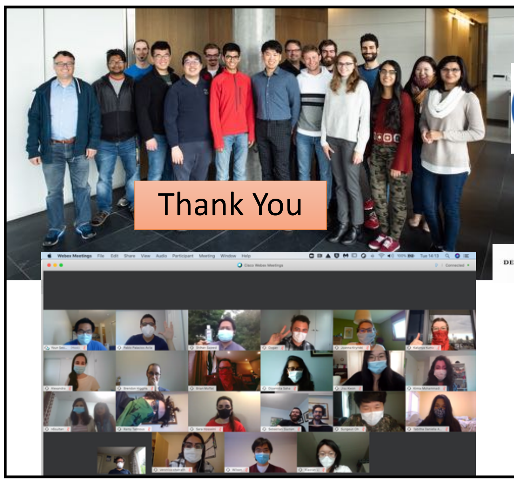


- R. Tannous, APPLIED PHYSICS LETTERS, 115(21), (2019).

- S. Agne et al, Optics Express, (2020).
- K. Boone, et al. PRA 91, 052325 (2015)
- J.P. Bourgoin, et al, NJP, 15:023006, (2013).



65



UNIVERSITY OF WATERLOO | IQC Institute for Quantum Computing
CSA ASC | UTIAS SFL | Honeywell | neptec | Xiphos Technologies | INO
QEYnet | EXCELITAS TECHNOLOGIES | UQDevices
DEFENCE RD DÉFENSE | NSERC CRSNG
Industry Canada | Industrie Canada
TQT Transformative Quantum Technologies | CIFAR CANADIAN INSTITUTE for ADVANCED RESEARCH
Ontario MINISTRY OF RESEARCH & INNOVATION | MINISTRY OF ECONOMIC DEVELOPMENT AND INNOVATION
INNOVATION.CA CANADA FOUNDATION FOR INNOVATION | FONDATION CANADIENNE POUR L'INNOVATION

66