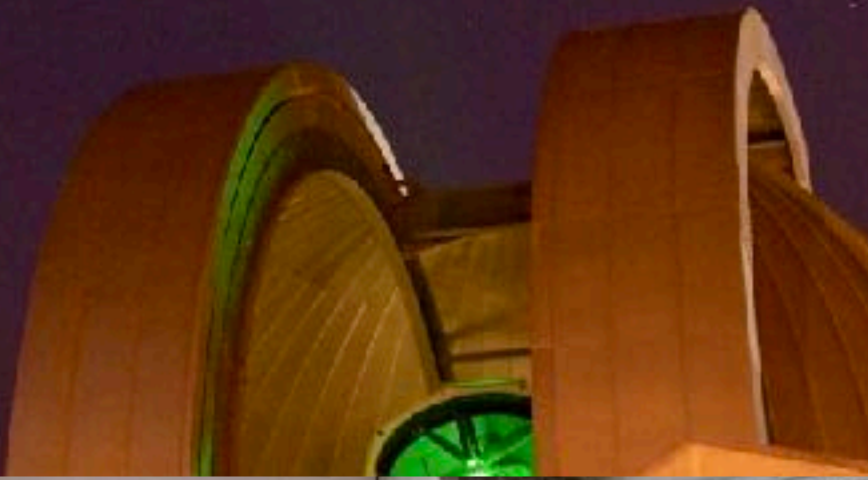
There's Plenty of Room.. out in Space for QKD!

Paolo Villoresi
QuantumFuture Research Group

University of Padua, Italy
Padua Quantum Technologies Research Center
Department of Information Engineering

Tutorial talk at QCrypt 2021



Università degli Studi di Padova

There's Plenty of Room.. out in Space for QKD!

Paolo Villoresi
QuantumFuture Research Group

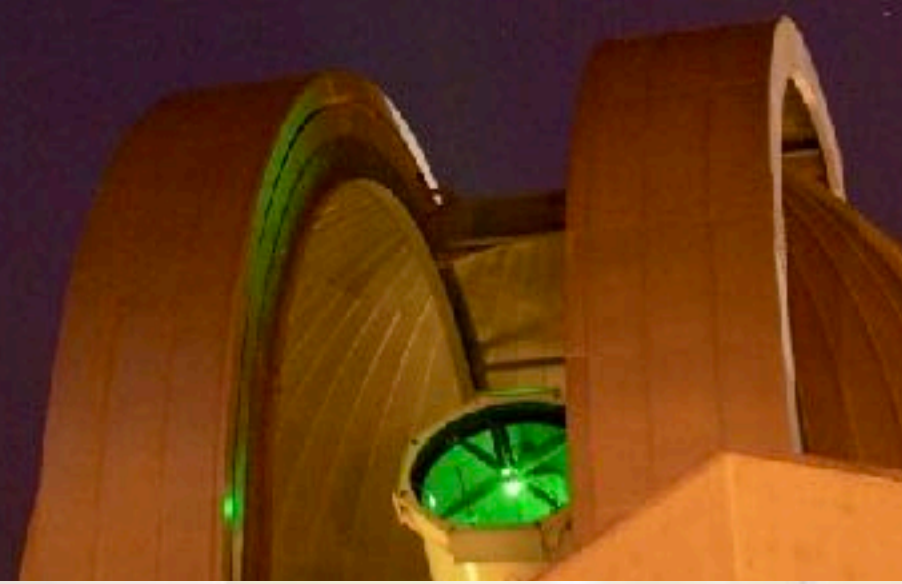
University of Padua, Italy
Padua Quantum Technologies Research Center
Department of Information Engineering

Tutorial talk at QCrypt 2021

1222 · 2022
800 ANNI

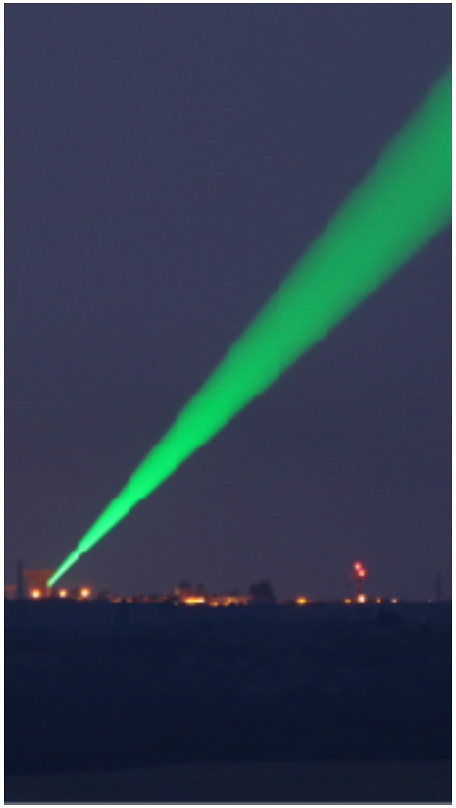
UNIVERSITÀ DEGLI STUDI DI PADOVA

PADUA Q TECH



overview

- rationale for Space QKD
- how to design it
- how we got to demonstrate it
- next moves



QKD for the largest scale

- the QKD in the Space is developing from a scientific research subject in experimental Quantum Communications, in a phase for demonstrators of different realisations to a technology for supporting cybersecurity at the planetary scale and beyond
- at present, space-QKD is point-to-point, eg. one terminal in orbit an one on the ground, or inter-satellite-links ISL, or two terminals on the ground fed by one orbiter simultaneously

image from: www.esa.int/ESA_Multimedia/Directorates/Observing_the_Earth

QKD for the largest scale

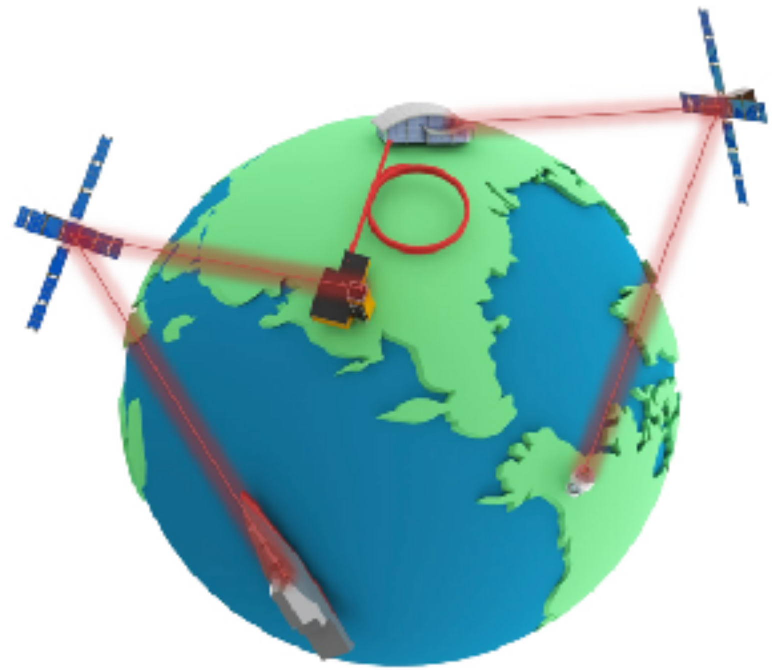
- the QKD in the Space is developing from a scientific research subject in experimental Quantum Communications, in a phase for demonstrators of different realisations to a technology for supporting cybersecurity at the planetary scale and beyond
- at present, space-QKD is point-to-point, eg. one terminal in orbit an one on the ground, or inter-satellite-links ISL, or two terminals on the ground fed by one orbiter simultaneously
- one satellite in orbit may connect terminals all over the planet and a constellation of satellites may speed up the mutual connection of two random spots on the ground in the need of a shared secret key
- the satellite design shall envisage a networking use, with versatility of the interlocutors

image from: www.esa.int/ESA_Multimedia/Directorates/Observing_the_Earth

why going in the Space?

optical communications in space

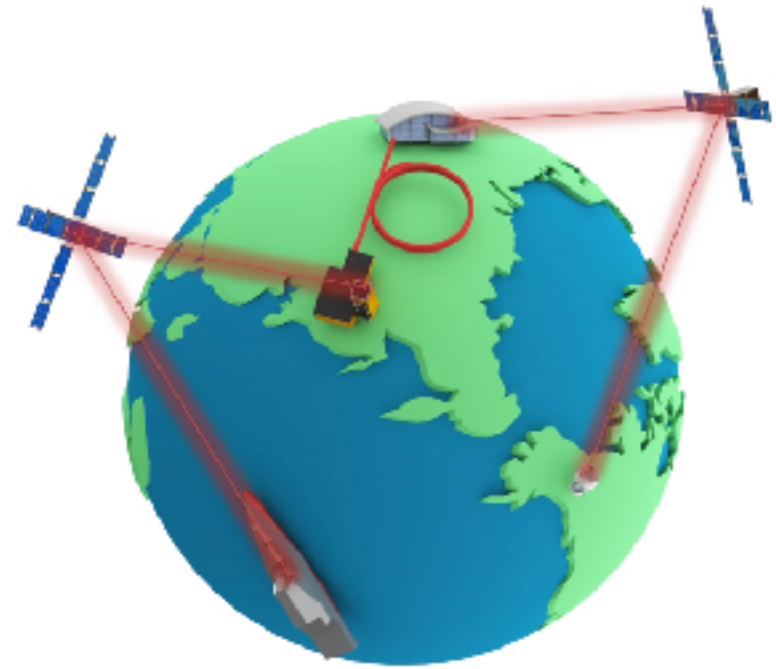
- ⭐ larger bandwidth of optical w.r.t. RF
- ⭐ lighter, smaller and less power-hungry
- ⭐ smaller footprint
- ⭐ spectrum less regulated, multiplexing
- ○ atmospheric absorption along the line-of-sight (cloud, rain, turbulence)
- ○ background noise (daylight)



H. Hemmati Near-Earth Laser Communications (2nd ed.). CRC Press (2020)

why going in the Space, with QKD?

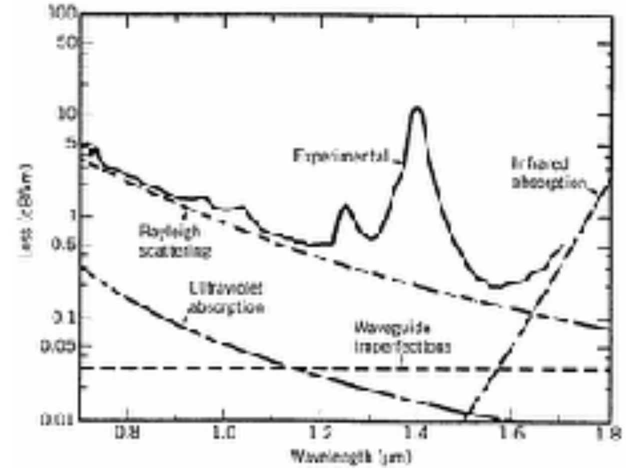
- cybersecurity is a global issue
- even a single Country needs to communicate globally, for reaching embassies or commercial branches
- QKD for inter-governmental communications, eg within EU27 Countries, require the connection of capitals in a range >4000 km and including islands
- mobile terminals require free-space links and ships are not typically at sight from land

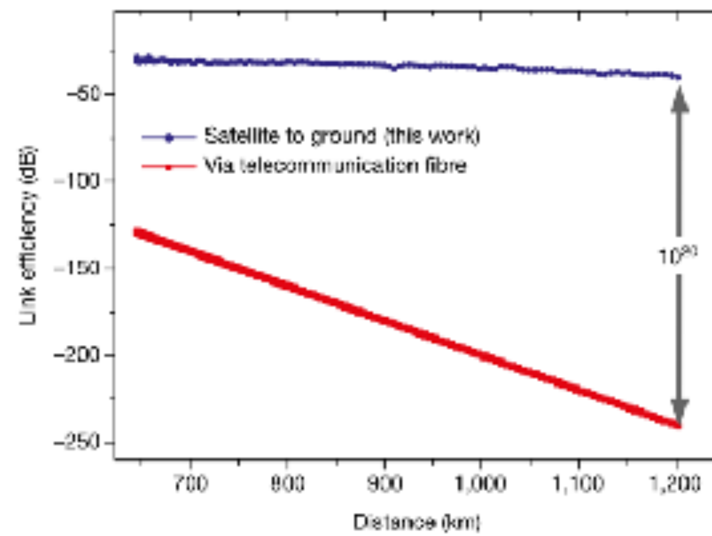


J.S. Sidhu et al. Advances in space quantum communications. IET Quantum Commun. qtc2.12015 (2021)

beyond fiber-based QKD

- propagation along fiber is affected by an exponential attenuation, strongly depended on photon wavelength
- lowest values about 0.15 dB/km are obtained around 1550 nm
- free-space propagation losses, in the far field, scales with the inverse square of the distance
- there is a **crucial advantage in the loss law** when considering planetary scale and when amplifier are not used
- from *Liao et al*. "over a distance of 1,200 km, even with a perfect 10-GHz single-photon source and ideal single-photon detectors with no dark count, transmission through optical fibres would result in only a 1-bit sifted key over six million years"

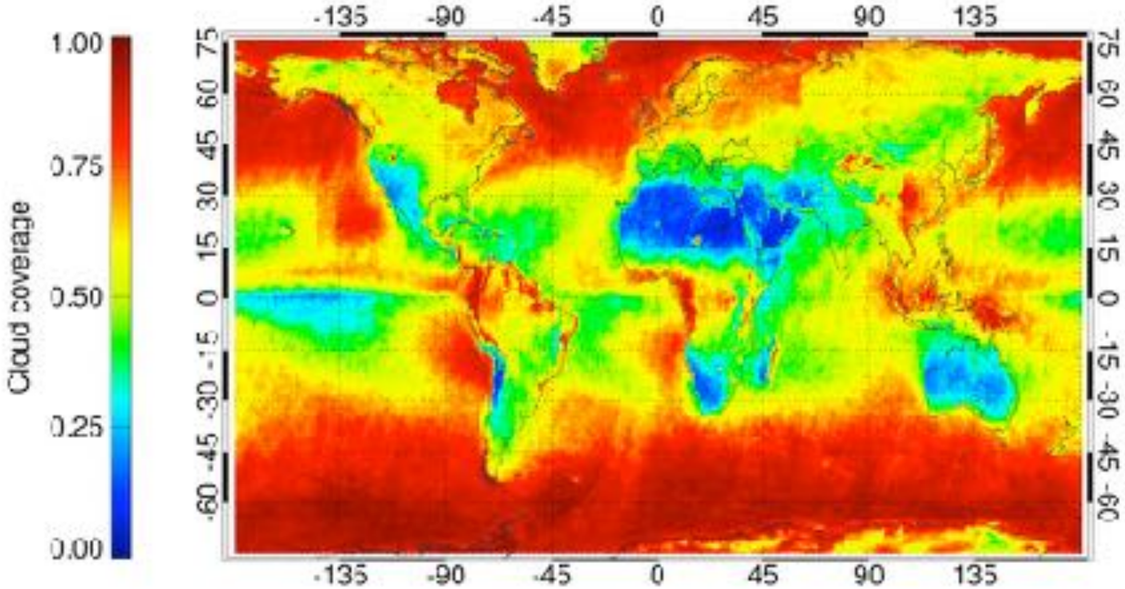




Liao, S.-K. et al. Satellite-to-ground quantum key distribution. Nature 549, 43–47 (2017)

Space QKD requires clear skies

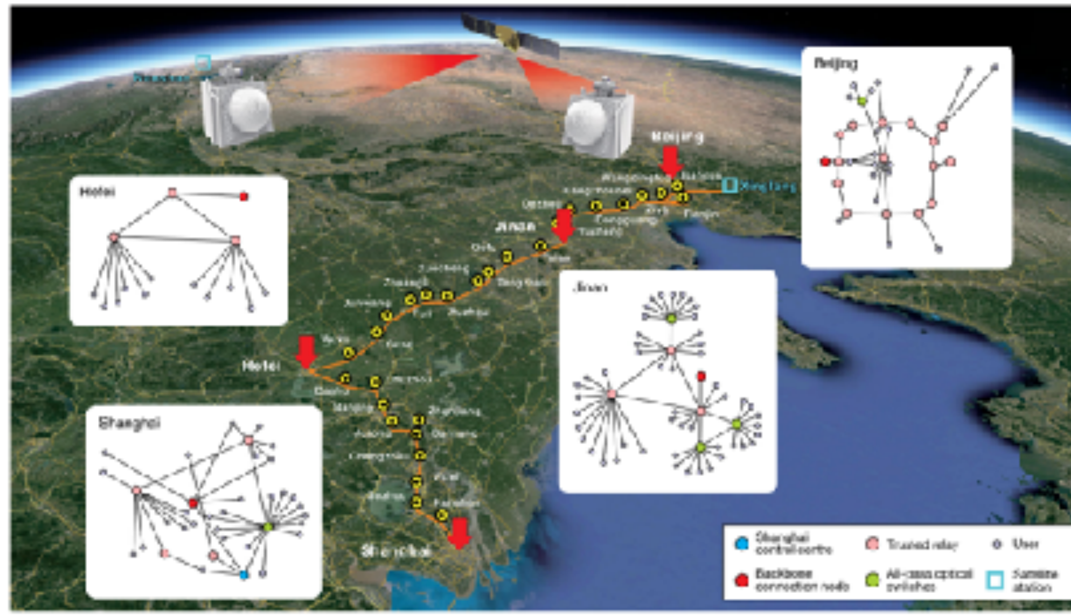
- turbulence and scattering from clouds impair optical links
- turbulence may be mitigated using adaptive optics
- cloud coverage impose diversity in the ground terminals



ESA - MERIS and AATSR instruments on Envisat
https://www.esa.int/Applications/Observing_the_Earth/Space_for_our_climate/Highlights/Cloud_cover

ground and space links for QKD

- fiber links on ground are very pervasive (up to the fiber-to-the-home service)
- they are naturally organized in hierarchy, as dorsal, national, regional, metropolitan and local networks
- satellite terminals are to be integrated on network nodes as well as connecting isolated users



Y.-A. Chen et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature 589, 214–219 (2021).

QKD networking with satellites

The Sat may be a flying

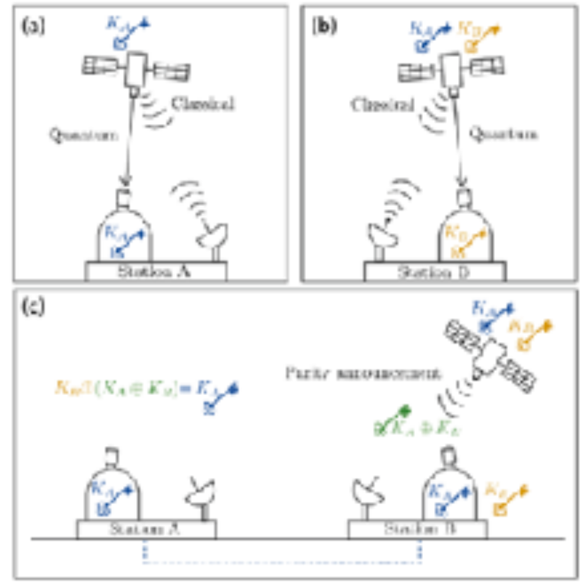
trusted-node or an untrusted one

QKD operations with distinct ground stations to establish independent secret keys with each of them: **sat holds all keys, while the stations only have access to their own keys**.

To enable any pair of stations to share a common key, the satellite combines their respective keys KA and KB and broadcasts their bit-wise parity KA ⊕ KB.

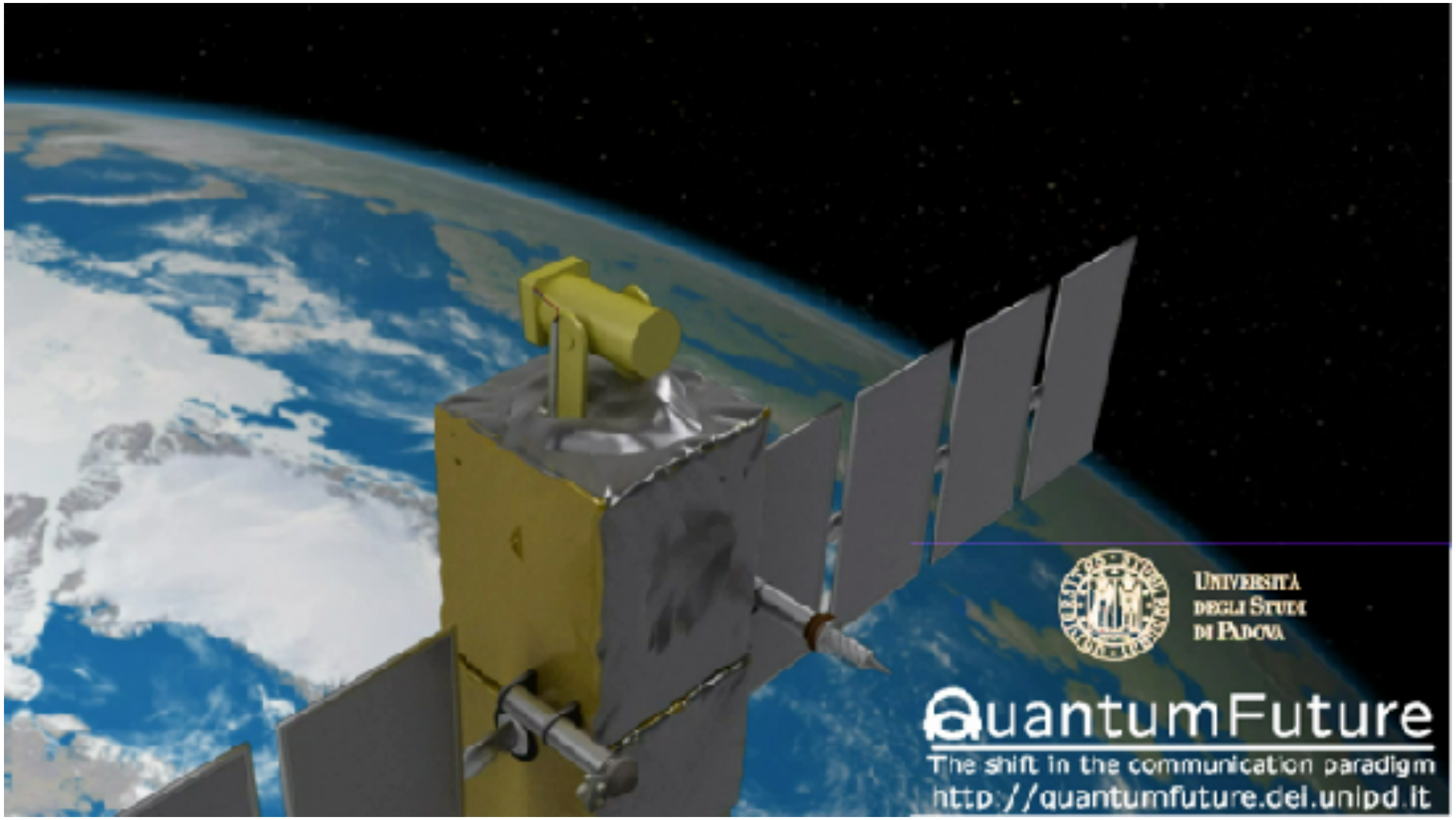
stations can retrieve each other's keys because KA ⊕ (KA ⊕ KB)= KB and KB ⊕ (KA ⊕ KB)= KA.

Original keys are independent secret strings, their bit-wise parity is just a uniformly random string, (no useful information to potential eavesdroppers revealed)



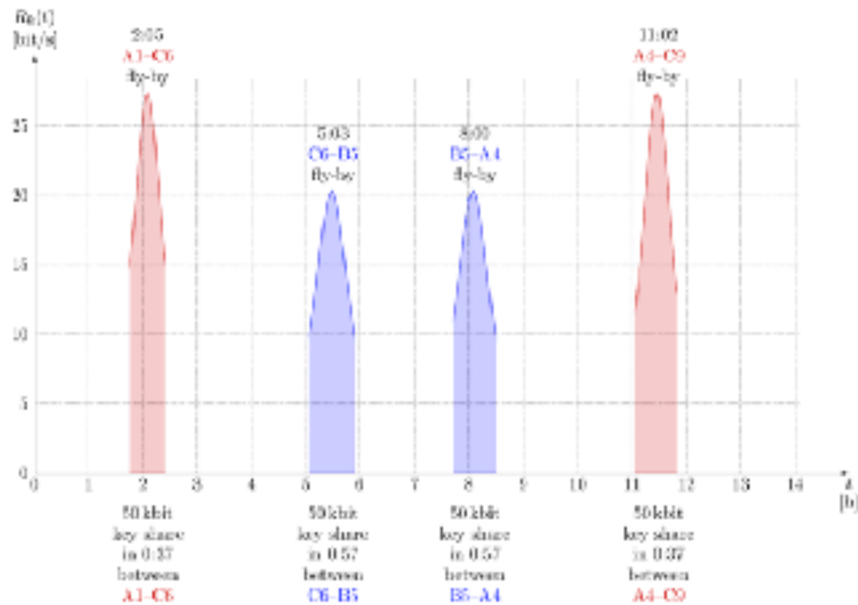
H-K Lo et al. Secure quantum key distribution Nat. Phot. 8 595 (2014)

the intersat QKD concept

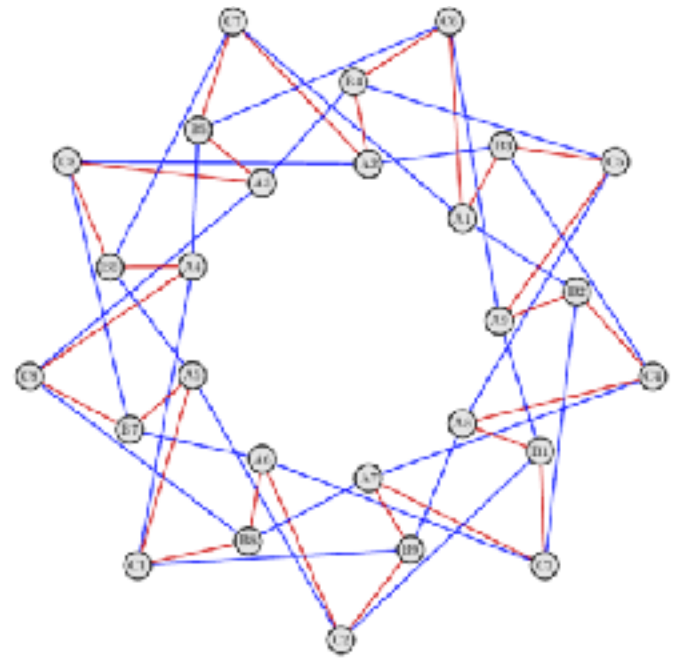


Project ESA Q-GNSS 2011-2015
F. Gerlin et al. Proc. 2013 Int. Conf. Localization and GNSS

the intersat QKD concept



Sequence of four hops to share secret key material between satellite A1 and C9, through C6, B5, A4.



Project ESA Q-GNSS 2011-2015
F. Gerlin et al. Proc. 2013 Int. Conf. Localization and GNSS

and so.. multiple schemes are at hand!

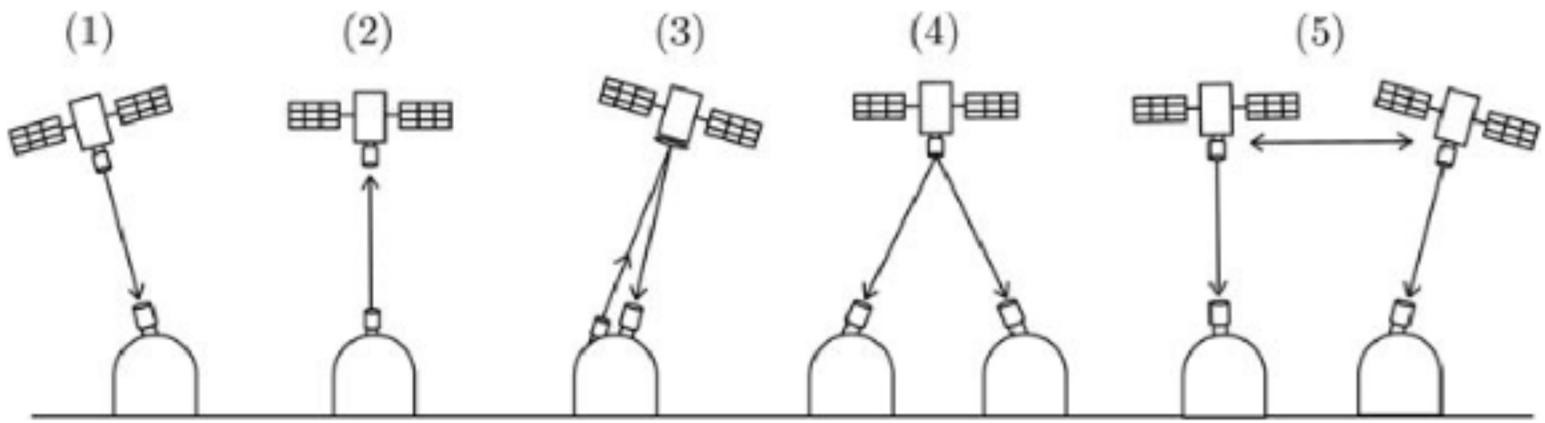


Illustration of different platforms for performing satellite QKD. Scenarios (1) and (2) depict a downlink and an uplink, respectively, while in scenario (3) a downlink is simulated by using a retro-reflector on board the satellite. In (4) pairs of entangled photons are being transmitted to Earth so that two ground stations can share entangled states. Finally, scenario (5) illustrates how inter-satellite links can allow more complex satellite QKD networks

R. Bedington et al. Progress in satellite quantum key distribution," *npj Quantum Inf.* **3** 30 2017

G. Vallone et al, Experimental Satellite Quantum Communications Physical Review Letters, 115 040502, 2015

more space QKD motivations

- resilience to emergencies/disaster and redundancy in ground QKD networks is needed
- classical large memories onboard for keys are fragile
- combining different secure communications techniques (classical crypto, PQK, ..) is a good sense approach
- growing share of satellites with optical terminals for different purposes makes the QKD payload integration easier

how to design Sat QKD network?

technical

- **type of protocol**
  - type of protocol and SKR
  - optimal clock rate
- **losses**
  - orbit type and altitude
  - size of telescopes
  - pointing and beam spot size
  - turbulence mitigation
- **noise level**
  - background level
  - intrinsic noise

functional

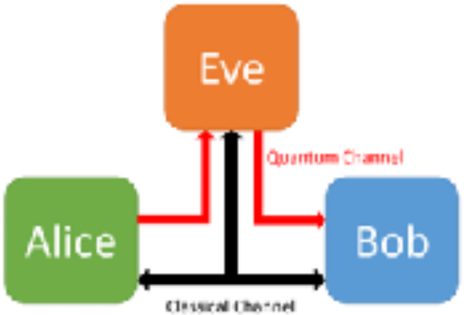
- effective key rate
- local passage duration
- secure bits with telescope A

network

- coverage on ground network
- secure bits with A, B, C ..
- secure networking

on protocols for space links

- with QKD protocols we realise the bit strings that are random and known to the two legitimate parties only, that is that they are clear from shared info with third parties
- prepare-and-measure (P&M) and entanglement-based (EB) protocols may be considered for Space QKD
- in P&M, we need first to send and measure a series of quantum states chosen at random in nonorthogonal bases
- the result is a pair of bit strings that are made of the same length by discarding the events that were not detected or measured in the wrong basis - sifted key
- we then perform a post-processing for the error correction (EC), for spotting errors in the two sequences and cleaning them, and the privacy amplification (PA), that allows them to reduce Eve's stolen information to a negligible amount.



S. Pirandola et al. Advances in quantum cryptography. Adv. Opt. Photonics 12, 1012 (2020)

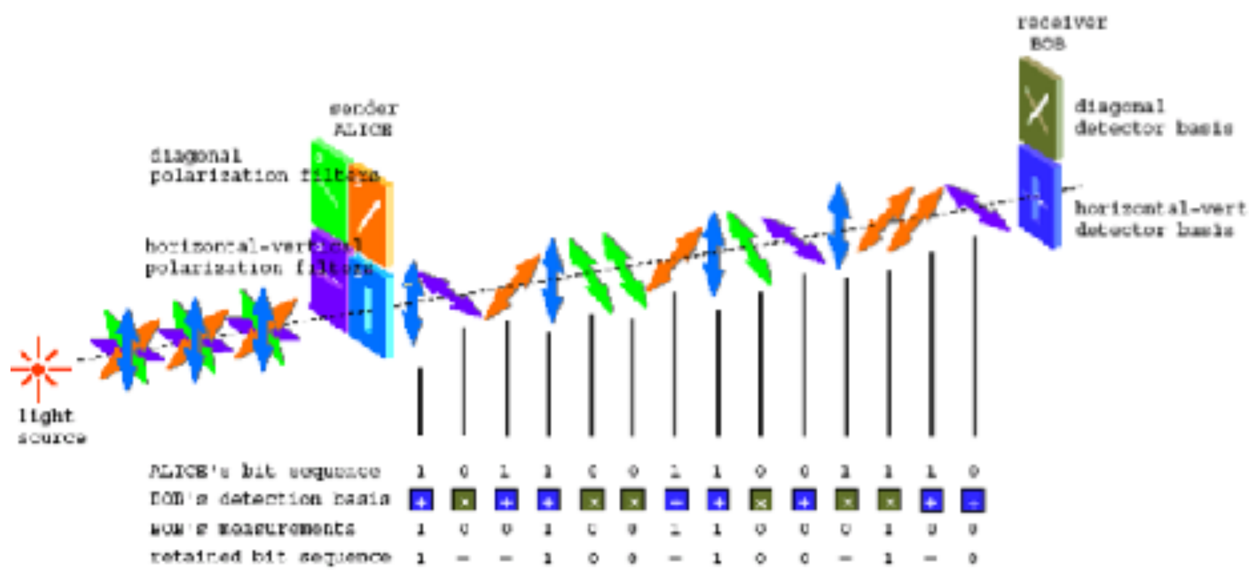
on the dimensions for quantum states

- the polarization encoding spans a dimension-two space
- temporal modes and phase coding may allow to increase this value
- the need of checking for the eavesdropper, doing measures in the conjugate basis, imposes a stringent requirement on visibility of both mutually unbiased bases (MUB), depending also on fluctuation of transmission, accurate synchronisation, ..
- them, going beyond the dim. two proved difficult so far
- an alternative to dimension larger than two is to multiplex in wavelength while using the same channel

S. Pirandola et al. Advances in quantum cryptography. Adv. Opt. Photonics 12, 1012 (2020)

BB84 polarization protocol

- BB84 protocol serves as the baseline for the prepare-and-measure protocol
- Alice generate a train of state picked at random out of four states in two MUBs.
- These are usually chosen as |0>, |1> (Z basis), and |+>, |−> (X basis).
- Bob measures them in one of the two bases Z or X, which picks at random



S. Pirandola et al. Advances in quantum cryptography. Adv. Opt. Photonics 12, 1012 (2020)

efficient, three-states and decoy BB84

- the state of the art in P&M protocols encodes three quantum states and use one-decoy state method
- this latter is needed as weak coherent pulses are used instead of true single photons, to prevent photon number splitting attacks
- the splitting ratio in Bob's choices of the measurement basis is suitably unbalanced toward the key base Z
- this is motivated by the use of the X basis that is only to check for Eve's presence

Boaron, A. et al. Simple 2.5 GHz time-bin quantum key distribution. Appl. Phys. Lett. 112, 2–5 (2018)

finite-key analysis

- most QKD systems may be operated for a finite time
- satellite passages are clearly setting a finite duration of links
- Eve might try to conceal her action in statistical fluctuations from passage to passage, leading Alice and Bob to overestimate the length of their secret key
- neglecting these fluctuations is the so-called infinite-key assumption
- a more careful analysis need to include this limitation, by choosing a confidence level that quantifies the maximum accepted failure probability of the QKD procedure, that eventually reduces the length of the secret key that Alice and Bob can extract using PA

S. Pirandola et al. Advances in quantum cryptography. Adv. Opt. Photonics 12, 1012 (2020)

secret key rate (SKR) for efficient BB84

$$R = \{ Q_1[1 - H_2(e_1)] - Q_\mu f(E_\mu) H_2(E_\mu) \} /2$$

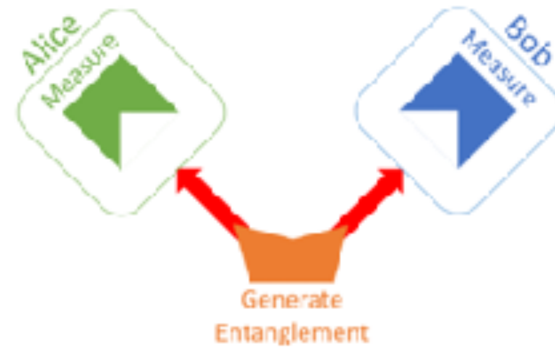
- Q_1 is Alice's single-photon pulses probability for being detected by Bob, and e_1 the QBER associated with their detection.
- Q_μ is the gain of the protocol, that is the success probability that Bob's detector clicks when triggered by Alice's pulse, and the QBER E_μ, which is the overall error affecting this detection.
- $H_2(p) := -p \log_2 p - (1 - p) \log_2(1 - p)$ is the binary Shannon entropy
- $f(x) \geq 1$ is the EC efficiency

S. Pirandola et al. Advances in quantum cryptography. Adv. Opt. Photonics 12, 1012 (2020)

entanglement-based EB protocols

- The security of EB as Arthur Ekert's E91 protocol is guaranteed by a Bell-like test to rule out Eve.

- *In the following I describe a quantum channel which distributes the key without any "element of reality" associated with the key and which is protected by the completeness of quantum mechanics.*



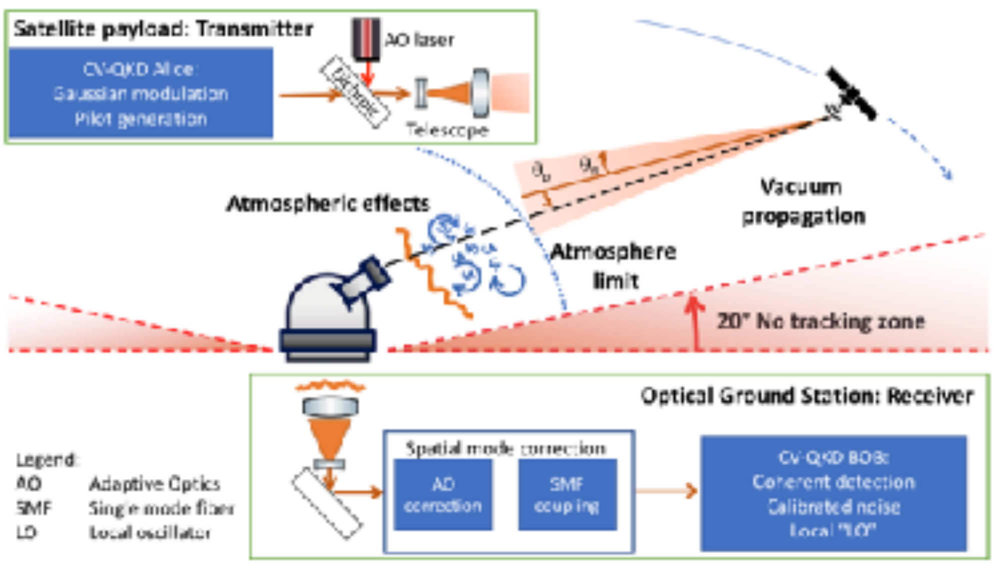
- The BBM92 works more efficiently by having both the legitimate parties each measure in only two differing MUBs instead of the three bases of E91, which may be the same as BB84.

- the general SKR is $1 - \eta_{EC} - \eta_{PA}$ where the EC and PA efficiencies are derived from the secrecy analysis

A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. 67, 661 (1991)
C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. 68, 557 (1992)
S. Pirandola et al. Advances in quantum cryptography. Adv. Opt. Photonics 12, 1012 (2020)

CV-QKD for space links

- CV QKD scheme with a coherent detector with a free running LO and reference symbols (pilots) transmitted for phase recovery.
- using an orbit subdivision in time slots and a parallel intense probe beam to mitigate the effects of transmission fluctuations, a positive SKR is envisaged for a sat in LEO



D. Dequal et al. Feasibility of satellite-to-ground continuous-variable quantum key distribution npj Quantum Inf. 7, (2021)

Quantum-limited measurements of optical signals from a geostationary satellite

Kevin Günthner, Imran Khan, Dominique Elser, Birgit Stiller, Ömer Bayraktar, Christian R. Müller, Karen Saucke, Daniel Tröndle, Frank Heine, Stefan Seel, Peter Greulich, Herwig Zech, Björn Gütlich, Sabine Philipp-May, Christoph Marquardt, and Gerd Leuchs

quantum limited states arrive at the ground station despite the long propagation path including Earth's atmospheric layers. We have bound the overall excess noise that can degrade the quantum states in the satellite-ground link and the atmospheric layers. This work can be seen as the first step in developing quantum communication from GEO

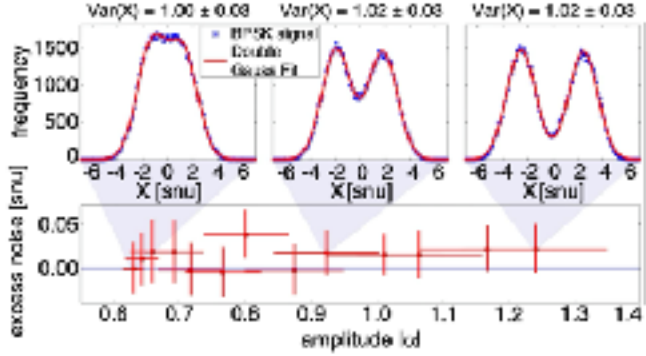
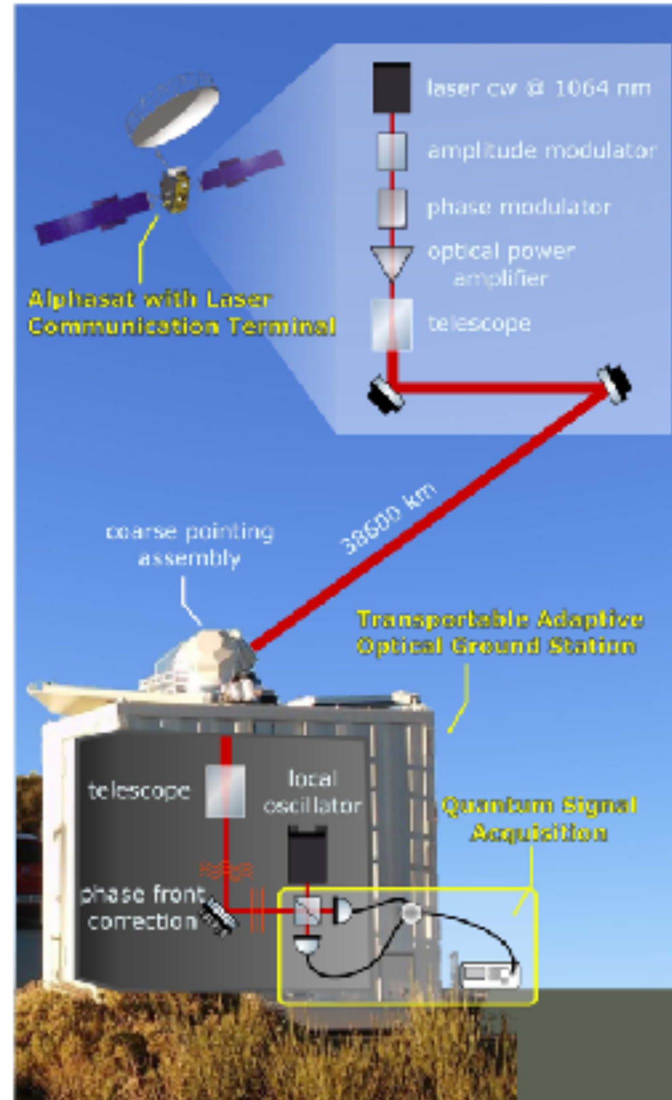


Fig. 3. Experimental results for excess noise variance in units of quantum uncertainty of the vacuum state (shot noise unit snu). Data is shown for different detected signal amplitudes, $|\alpha|$ (the mean amplitude is 0.86). In the upper row, three exemplary histograms ($|\alpha| = 0.63, 0.92, 1.24$) illustrate the observed quadrature distribution along the X quadrature. Each of the histograms contains about 70,000 data points.

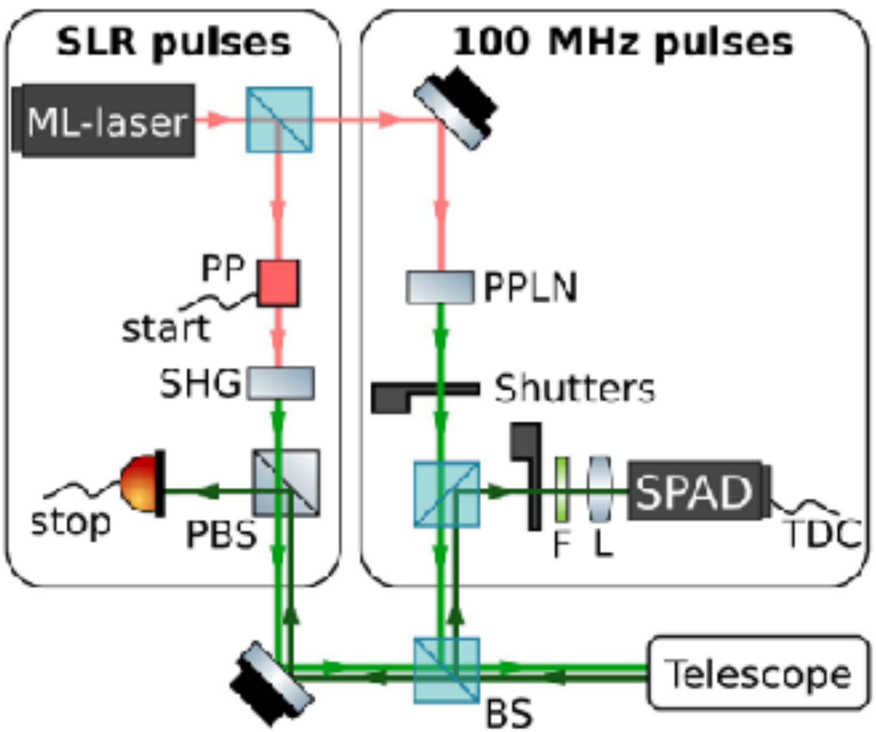


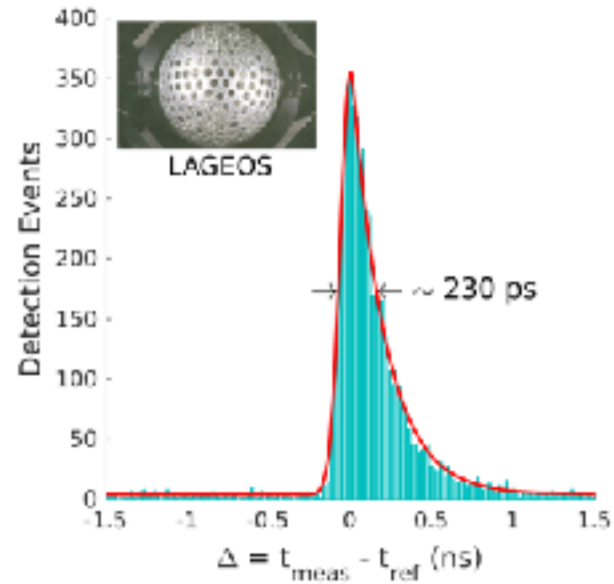
Günthner, K. et al. Quantum-limited measurements of optical signals from a geostationary satellite. Optica 4, 611 (2017)

on the clock rate

- SKR scales with the number of uses of the channel
- higher rates are both wished and feared
- indeed, it improves the key rate
- however the discrimination of Alice's state at the receiver requires corresponding temporal resolution and orbit determination
- moreover, cranking up the generation rate also increase the demand of power for the state generator, the computing and storage capacity of both terminals and the data exchange in the post-processing
- suitable values are in the 100 MHz range

temporal resolution in the single photon detection:
230 ps over 7000km





The 100-MHz pulse train is detected after a 50:50 BS to separate the outgoing and incoming beams and 3 nm spectral filter a silicon single photon avalanche detector SPAD (Micro-Photon-Devices Srl) with ≈ 50% quantum efficiency, ≈ 400 Hz dark count rate and 40 ps of jitter.

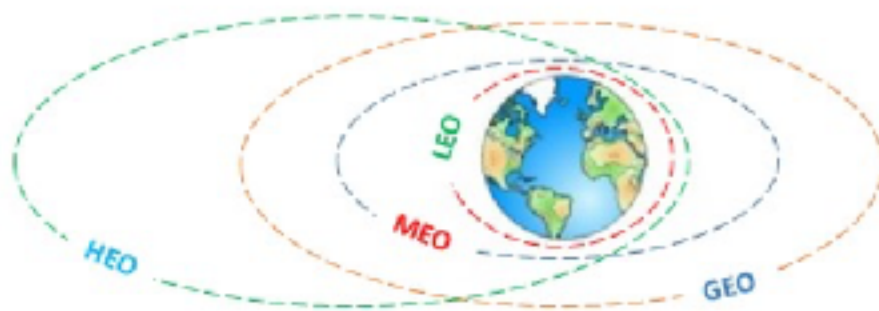
The time of arrival is tagged with 1 ps resolution (quTAG TDC from qutools GmbH)

C. Agnesi et al., *Sub-ns timing accuracy for satellite quantum communications*, **JOSA B** 36 B59 (2019)

sending states from the Space.. where from?

low-Earth-orbits LEO orbits (<2000 km)
rapid passages – large coverage – small payloads (potentially numerous)
secure communications (QKD – encryption of data)
fundamental test of Quantum Physics (Bell's test)
Micius and SOTA are here

Medium-Earth-orbits MEO orbits, including GNSS
dual use of the QKD setup (to Space, to ground)
securing positioning and navigation service
securing timing applications
GALILEO sats are here



GEOstationary orbits (36000 km)
large optical aperture
securing data relay - EDRS

Intersat links and deep space missions
exploring the limits of quantum correlations
interconnession of atomic clocks

on satellites number and visual impact

- wide-field surveys of the sky are impacted by satellite swarms sunlight diffusion, visible at night
- low scattering profiles and absorbing materials are needed

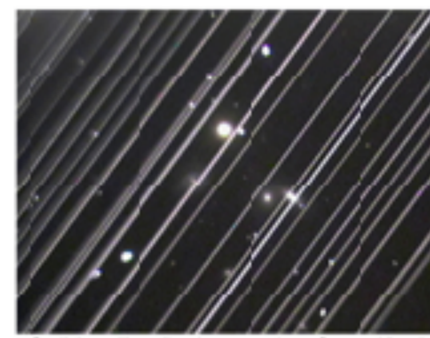
Astronomers have recently raised concerns about the impact of satellite mega-constellations on scientific research. To better understand the effect these constellations could have on astronomical observations, ESO commissioned a scientific study of their impact, focusing on observations with ESO telescopes in the visible and infrared but also considering other observatories. The study, which considers a total of 18 representative satellite constellations under development by SpaceX, Amazon, OneWeb and others, together amounting to over 25 thousand satellites [1], has now been accepted for publication in Astronomy & Astrophysics.

5 DECEMBER 2019

AAS Works to Mitigate Impact of Satellite Constellations on Ground-Based Observing

Kelsie Krafton
American Astronomical Society (AAS)

The first launch of SpaceX's Starlink satellite constellation was on 23 May 2019. The response from our community was loud enough that SpaceX reached out to the AAS looking to establish a line of communication. Since optical/infrared interference doesn't have a statutory or regulatory framework like radio interference, they hadn't had any interactions with that part of our community.



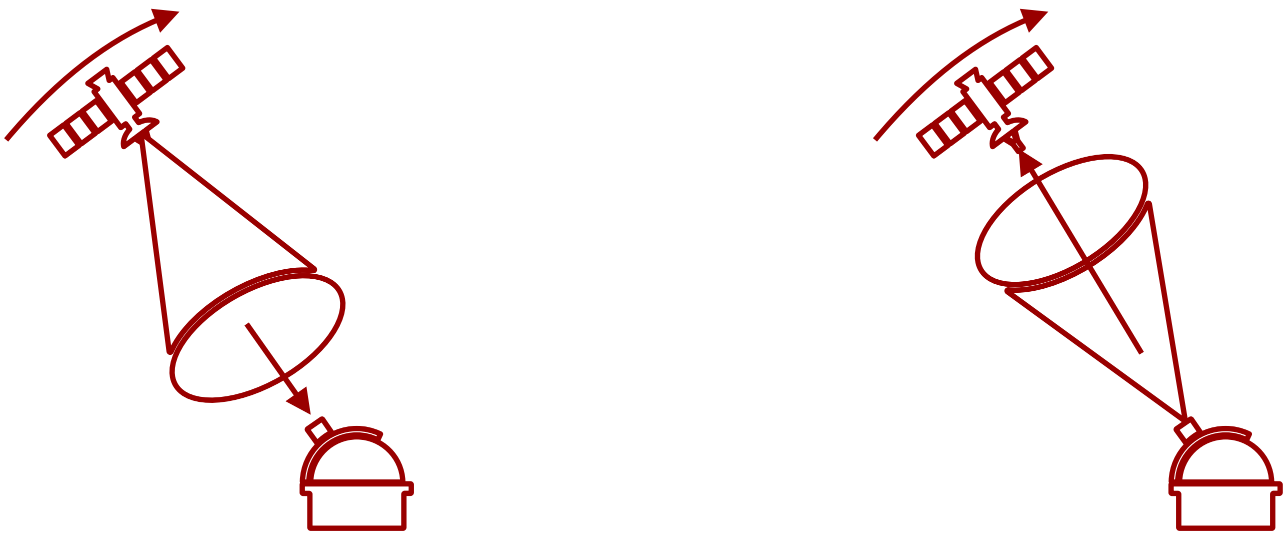
Starlink satellite trails ruin an astrophoto. Courtesy Victoria Girgis/Lowell Observatory.

The AAS Public Policy staff worked with the AAS Committee on Light Pollution, Radio Interference, and Space Debris to assemble a working group that would be the main channel of communication between the astronomical scientific community and SpaceX.

https://aas.org/posts/advocacy/2019/12/aas-works-mitigate-impact-satellite-constellations-ground-based-observing
https://www.eso.org/public/news/eso2004/?lang&fbclid=IwAR067phOG_f1cmiRQ0k9JALdMzNuVDmn3VUGEHQEujlk2beI82QFU2WBOOU

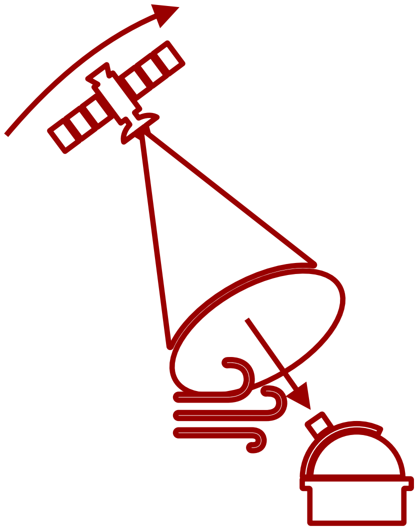
sharing states with the Space..

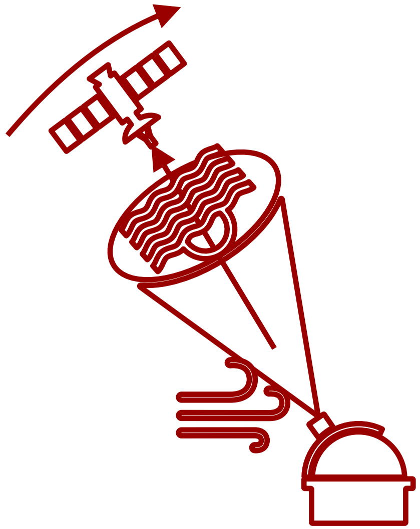
- first question: better downlink or uplink?



sharing states with the Space..

- wavefront degradation occurs near the ground, then in general the downlink has lower losses, unless for specific motivations



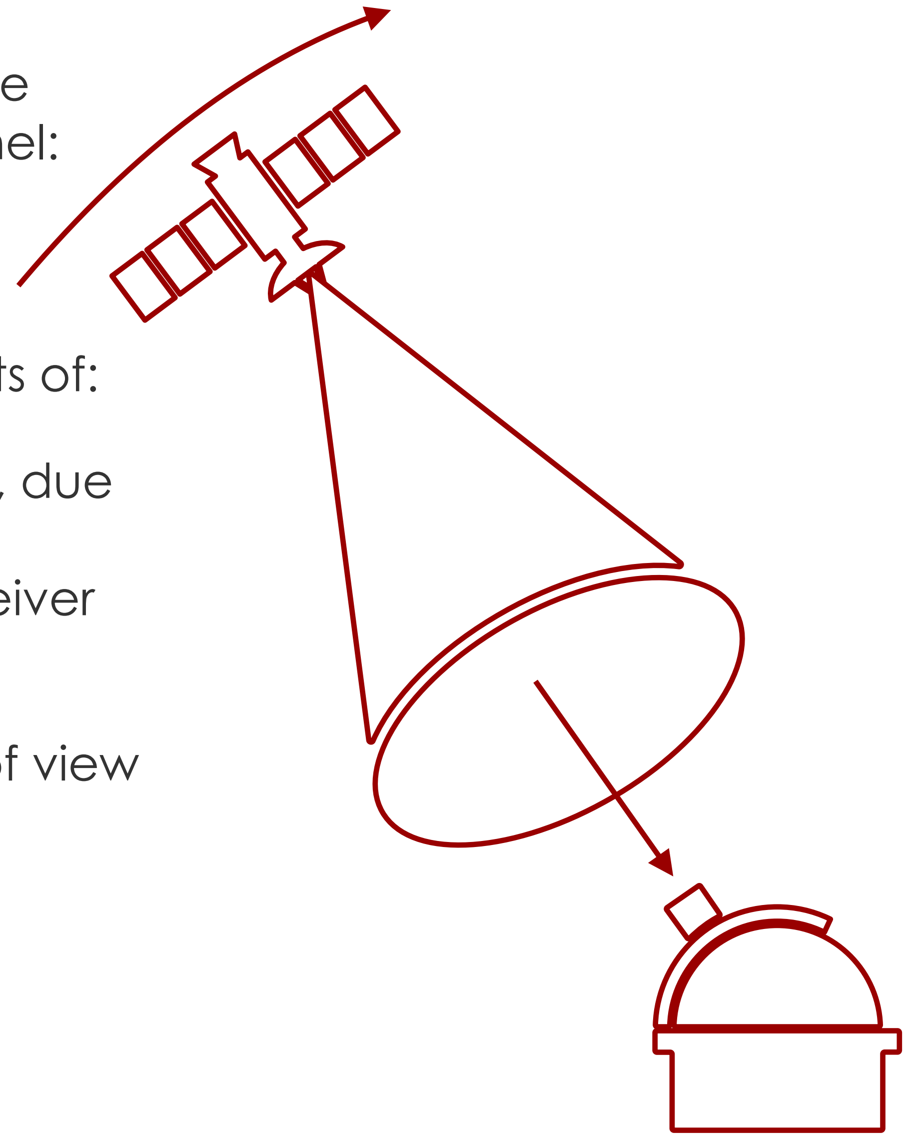


sending states from the Space..

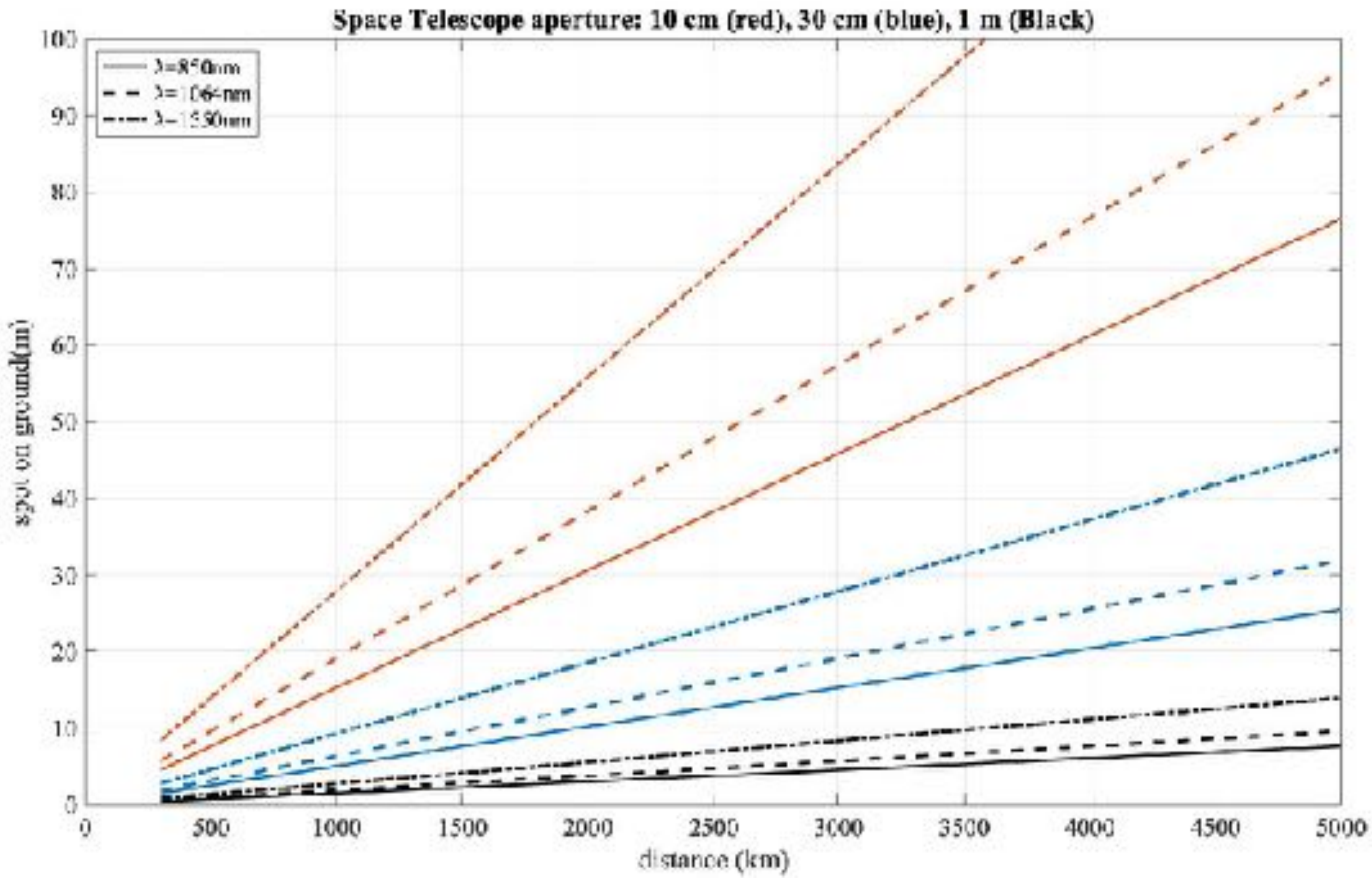
- scaling of the link losses, in term of the transmission coefficient of the channel:

$$\eta_{CH} = \eta_{Clip} \cdot \eta_{FOV} \cdot \eta_{Atm}$$

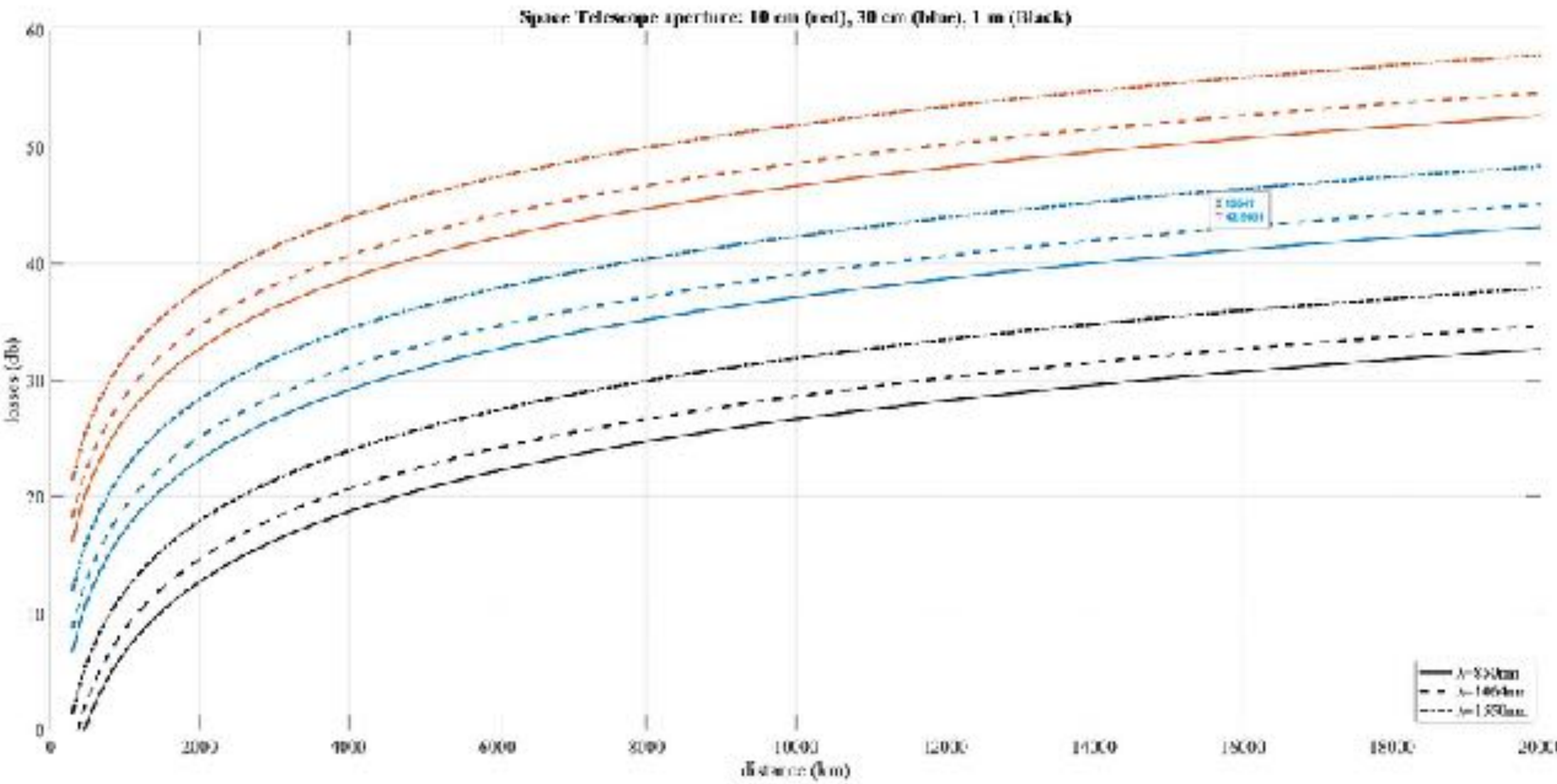
- where the factors are the coefficients of:
  - geometric clipping at the receiver, due to the beam divergence - also turbulence induced - and the receiver area
  - losses caused by the limited field of view of the receiver system
  - atmospheric transmittance



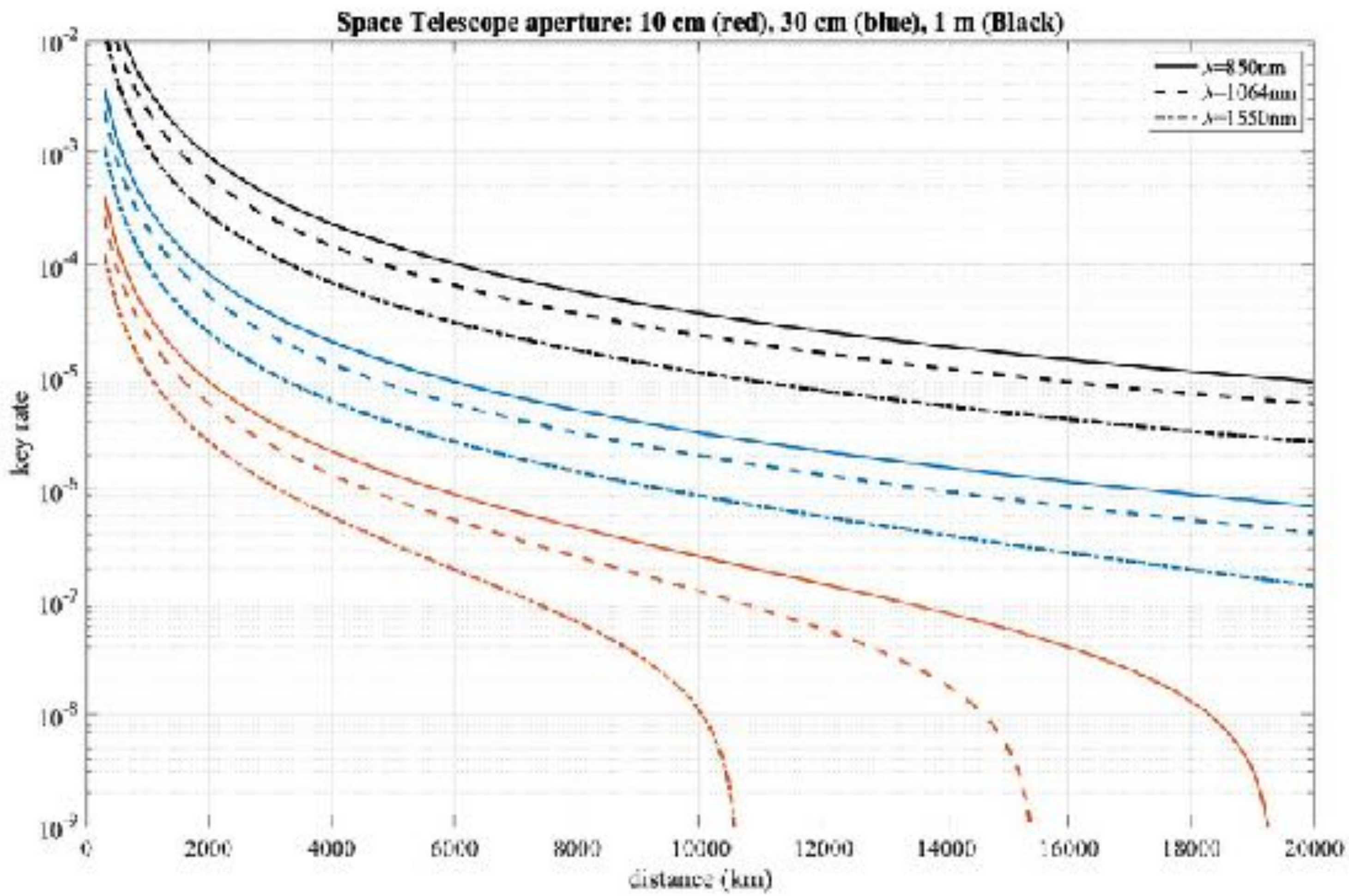
let’s model the spot on the ground



optical losses with a 50 cm ground telescope as receiver

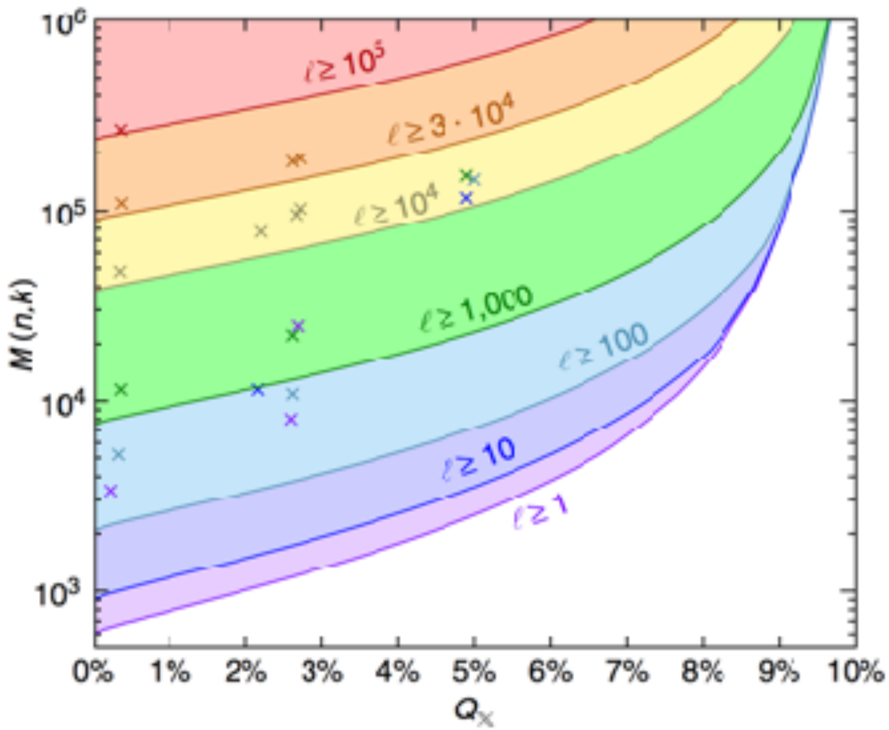


QKD rate
50 cm ground telescope as receiver



Map to assess the qubit needed for a given key at a QBER value

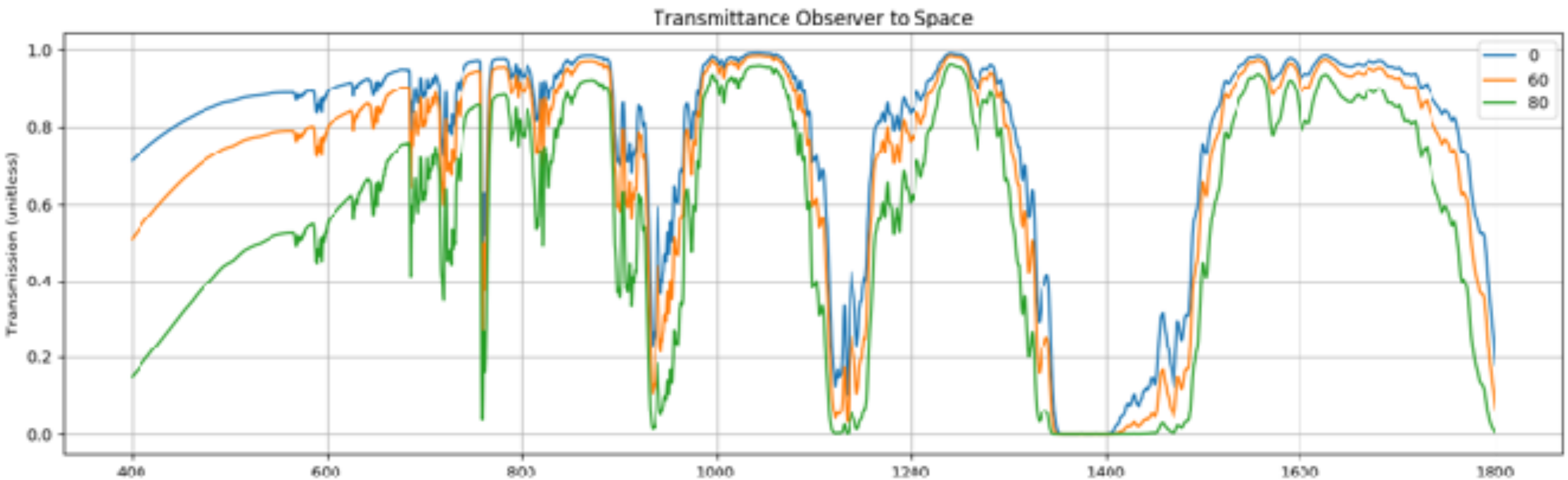
For ***finite length with noise***, the key rate shall be designed according to satellite type of orbit and losses.



The **minimum number of received bits M(n,k) needed to obtain a key of a given length ℓ** (as labelled on each curve) versus the QBER - Q_X.

Bacco et al. ***Experimental quantum key distribution with finite-key security analysis for noisy channels*** Nature Communications **4** 2363(2013).

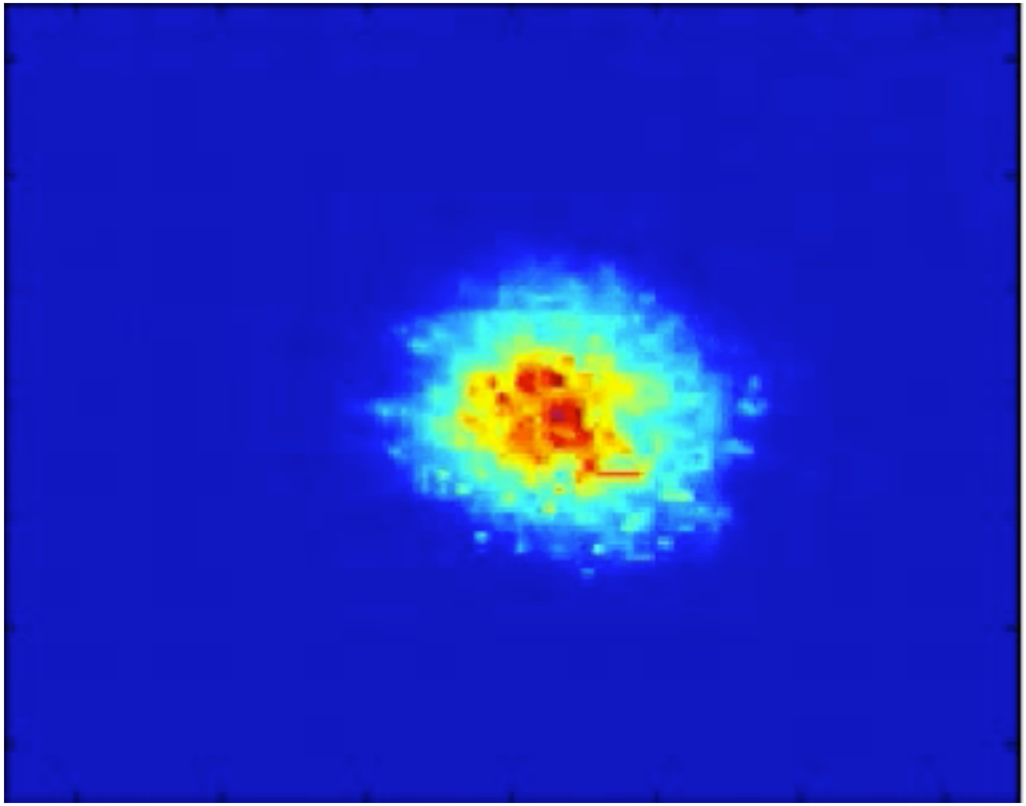
Optical absorption in vertical beam propagation



- modeling using the lowtran suite under python

turbulence effects and mitigation

- star (Vega) spot as seen with a 1.5 m telescope (ASI-MLRO, Matera)

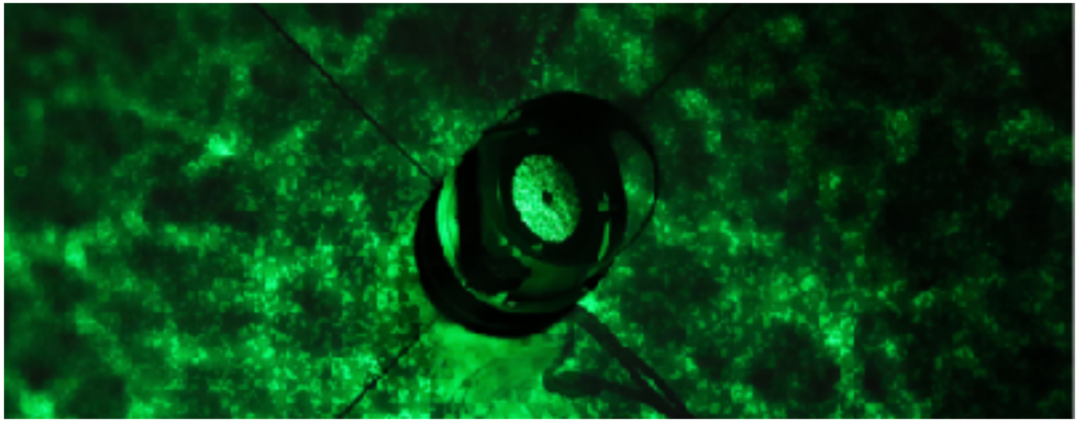


focalplane area 600x800 μm

Bonato, C., Tomaello, A., Da Deppo, V., Naletto, G. & Villoresi, P. Feasibility of satellite quantum key distribution. New J. Phys. 11, 45017 (2009)

adaptive optics solutions

- the optical comm from space has advantages w.r.t. astronomical imaging as:
  - you only need to look at the sat signal and not at an image
  - you may use the beacon laser for the instantaneous wavefront measurement



M. Wright et al. Adaptive optics correction into single mode fiber for a low Earth orbiting space to ground optical communication link using the OPALS downlink, Opt. Express, 23, 252822 (2015)

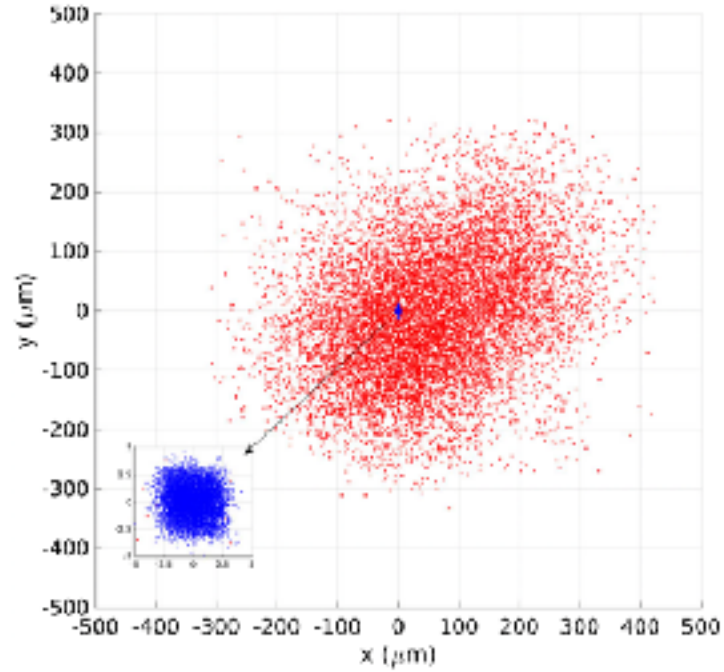
C. Petit et al., Investigation on adaptive optics performance from propagation channel characterization with the small optical transponder, Opt. Eng. 55, 111611-1–111611-17 (2016)

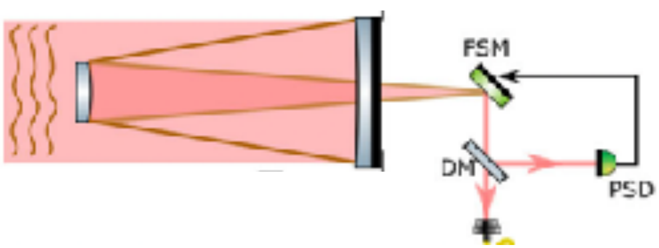
L. Roberts et al. Performance Predictions for the Adaptive Optics System at LCRD's Ground Station 1, Imaging and Applied Optics 2015 OSA paper JW4F.4

E. Fischer et al., Use of adaptive optics in ground stations for high data rate satellite-to-ground links, Proc. SPIE 10562, 105623L (2017)

turbulence effects and mitigation

- for small telescopes, the tip/tilt (blue dots) correction is enough w.r.t. uncorrected (red dots)
- $D/r_0 \sim 3$ and $D \sim 120$ mm
- SMF-coupling losses 12 dB





M. Avesani et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. npj Quantum Inf. 7, 93 (2021)

how we got to demonstrate Space QKD

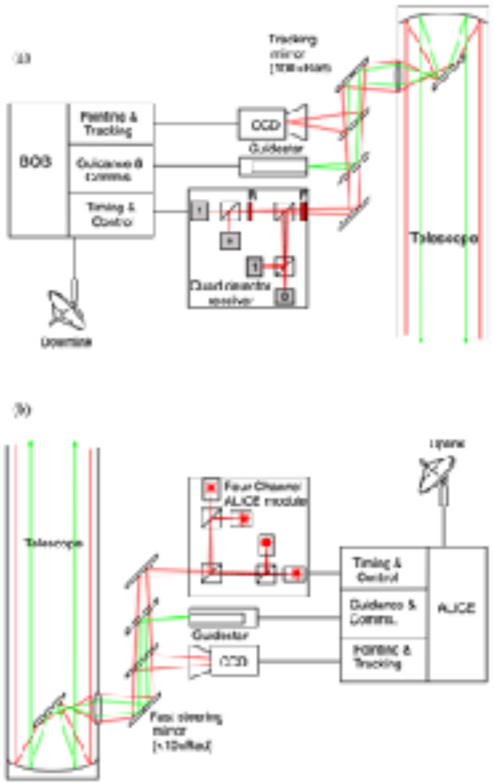
- early 2000: proposals and modeling
- 2008-2017: feasibility demonstrations
- 2017 on: investments on space QKD deployment

proposals and modeling

Ground to satellite secure key exchange using quantum cryptography

J G Rarity[1], P R Tapster[1], P M Gorman[1] and P Knight[2]
[1] Optronics Department, QinetiQ, Malvern WR14 3PS, UK
[2] Space Department, QinetiQ, Farnborough GU14 0LX, UK
E-mail: rarity@qinetiq.com

New Journal of Physics 4 (2002) 82.1–82.21 (http://www.njp.org/)
Received 26 June 2002, in final form 7 October 2002
Published 29 October 2002



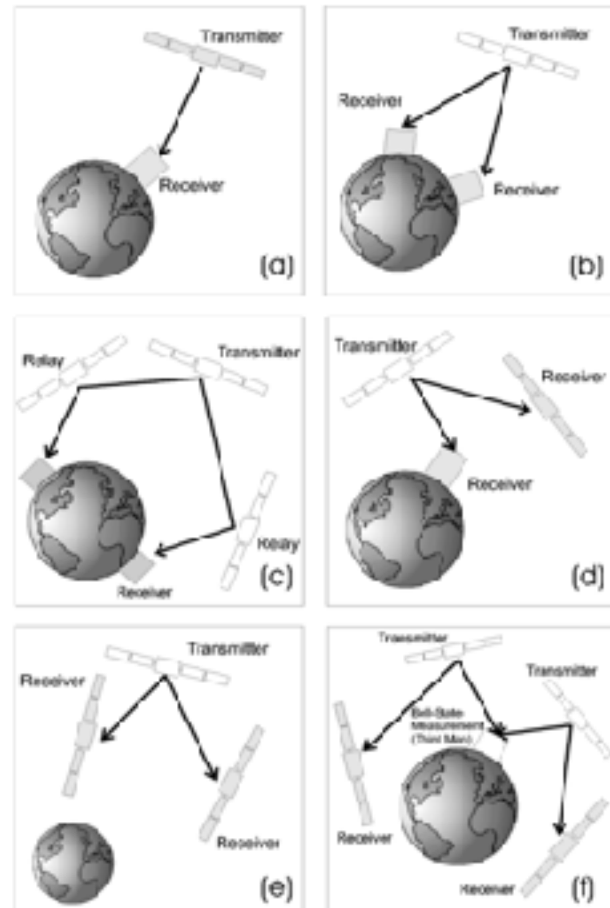
At this stage we favour option (B), using a down-looking transmitter. Here the expected key rates are up to 7 kbits s−1 when operating at 100 MHz repetition rates, <1000 km range and using a 1 m diameter telescope.

IEEE JOURNAL OF SELECTED TOPICS IN QUANTUM ELECTRONICS, VOL. 9, NO. 6, NOVEMBER/DECEMBER 2003 1541

Long-Distance Quantum Communication With Entangled Photons Using Satellites

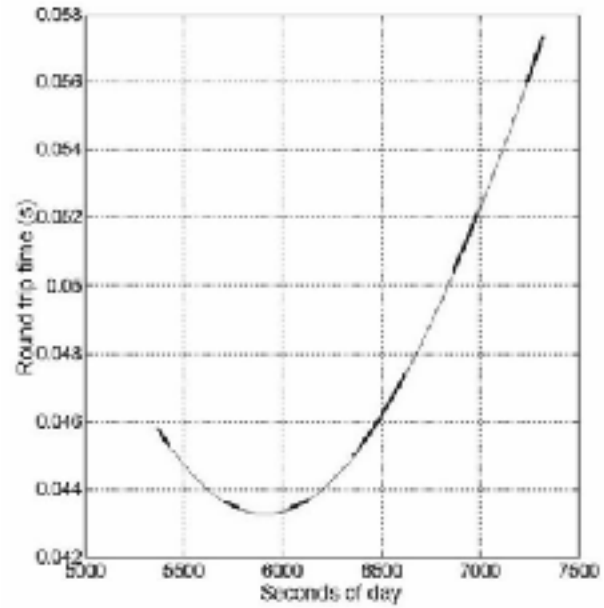
Markus Aspelmeyer, Thomas Jennewein, Martin Pfennigbauer, *Student Member, IEEE*, Walter R. Leeb, and Anton Zeilinger

Based on present-day technology and assuming reasonable link parameters, it seems feasible to achieve enough entangled photons per receiver pair to demonstrate a quantum communication protocol.

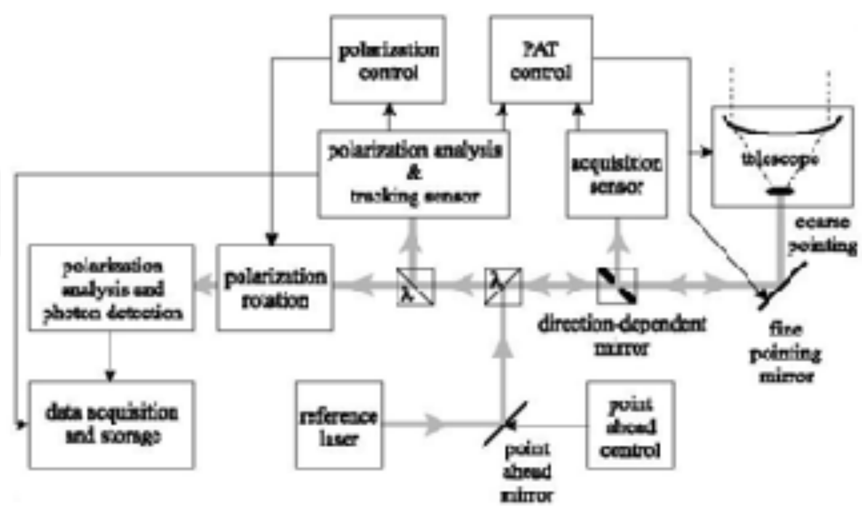


19 October 2004

Space-to-ground quantum communication using an optical ground station: a feasibility study



Our experiments already indicate the suitability of the MLRO telescope to act as a receiving station in a quantum communication experiment.
This underlines our view that with existing technology the realization of a satellite-to- ground quantum communication link is actually feasible.
Our work is intended to serve as the basis for future developments of dedicated systems for quantum communication between space and ground.



P. Villoresi et al. Space-to-ground quantum communication using an optical ground station: a feasibility study. in Proceedings of SPIE (eds. Meyers, R. E. & Shih, Y.) 5551, 113 (2004)

PRL 94, 150501 (2005) PHYSICAL REVIEW LETTERS week ending 22 APRIL 2005

Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km: Towards Satellite-Based Global Quantum Communication

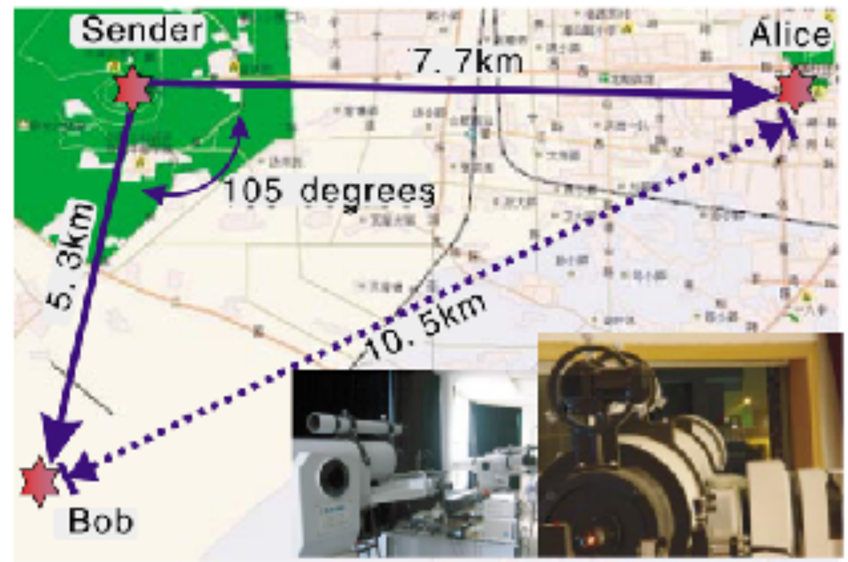
Cheng-Zhi Peng,[1,2] Tao Yang,[1] Xiao-Hui Bao,[1] Jun Zhang,[1] Xian-Min Jin,[1] Fa-Yong Feng,[1] Bin Yang,[1] Jian Yang,[1] Juan Yin,[1] Qiang Zhang,[1] Nan Li,[1] Bao-Li Tian,[1] and Jian-Wei Pan[1,2]

[1]*Department of Modern Physics and Hefei National Laboratory for Physical Sciences at Microscale, University of Science and Technology of China, Hefei, Anhui 230026, China*

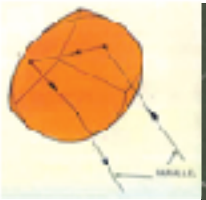
[2]*Physikalisches Institut der Universitaet Heidelberg, Philosophenweg 12, Heidelberg 69120, Germany*

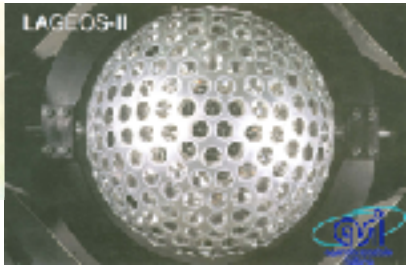
our experiment demonstrated for the first time that entanglement can still survive after penetrating the effective thickness of the aerosphere by showing a violation of the Bell inequality with spacelike separated observers

the link efficiency of entangled photon pairs achieved in our experiment is about a few percent, which is well beyond the threshold required for satellite-based free-space quantum communication



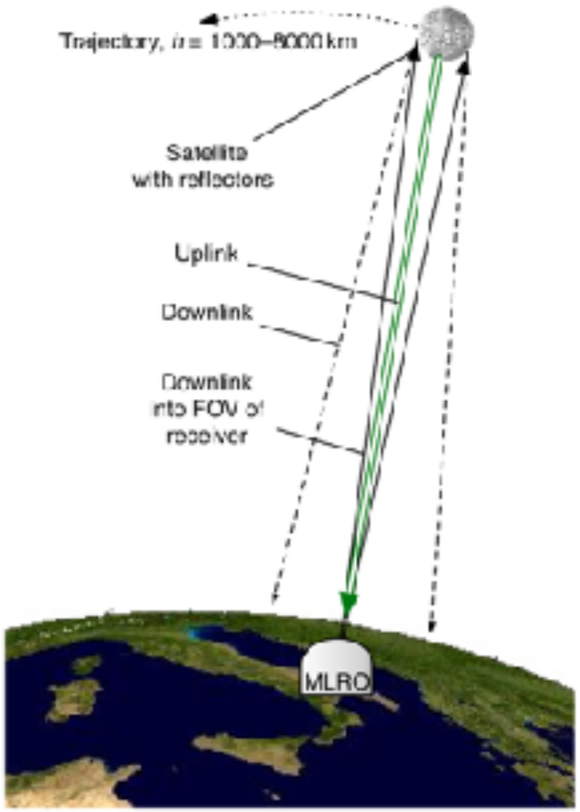
C.Z. Peng et al. Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication. Phys. Rev. Lett. 94, 1–4 (2005)





demonstrating the downlink

- exploiting retroreflectors on satellite (often available)
- Return peak of 5 cps was observed at D=0 above the background.
- In the downlink channel, μ = 0.4, attesting the single-photon regime
- Total losses are of -157 dB.



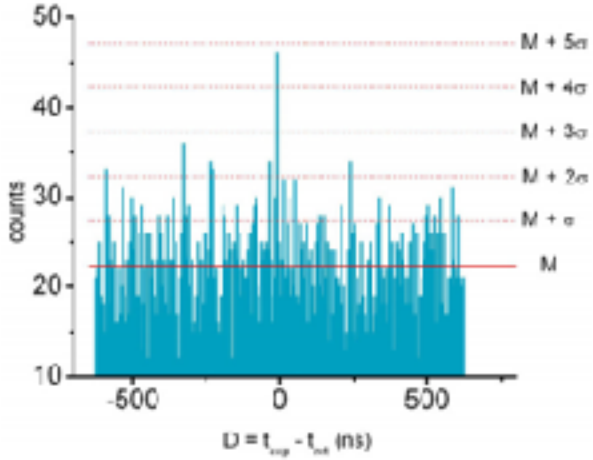
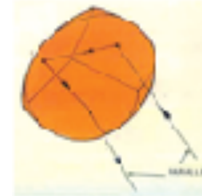


Figure 3. Histogram of the differences D between expected and observed detections for Ajisai satellite. The peak of the histogram is centered at $D = t_{exp} - t_{ret} = 0$ ns, as expected, and is larger than the mean value of the background counts by 4.5 standard deviations. The bin size is $\Delta t = 5$ ns.

P. Villoresi et al. Experimental verification of the feasibility of a quantum channel between space and Earth. New J. Phys. 10, 033038 (2008)

demonstrating the downlink



- e
  a
- R
  th
- Ir
  si
- To

Figure 3. Histogram of the differences D between expected and observed detections for Ajisai satellite. The peak of the histogram is centered at $D = t_{exp} - t_{ret} = 0$ ns, as expected, and is larger than the mean value of the background counts by 4.5 standard deviations. The bin size is $\Delta t = 5$ ns.

P. Villoresi et al. Experimental verification of the feasibility of a quantum channel between space and Earth. New J. Phys. 10, 033038 (2008)

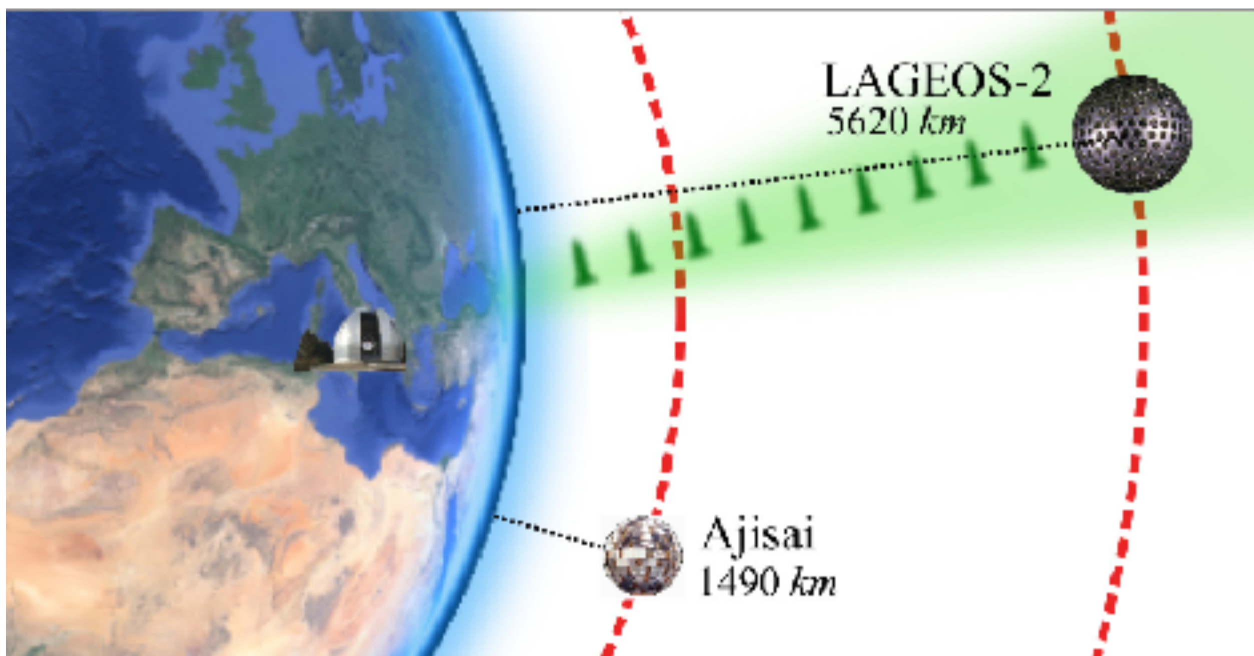
RAPID COMMUNI

PHYSICAL REVIEW A 93, 010301(R) (2016)

Experimental single-photon exchange along a space link of 7000 km

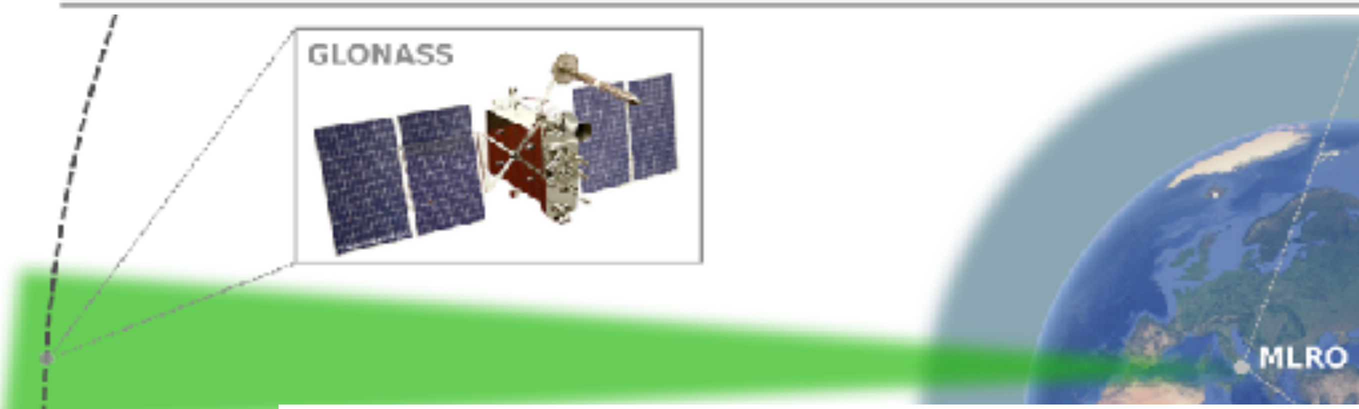
Daniele Dequal,[1] Giuseppe Vallone,[1,2] Davide Bacco,[1] Simone Gaiarin,[1] Vincenza Luceri,[3]
Giuseppe Bianco,[4] and Paolo Villoresi[1,2,*]

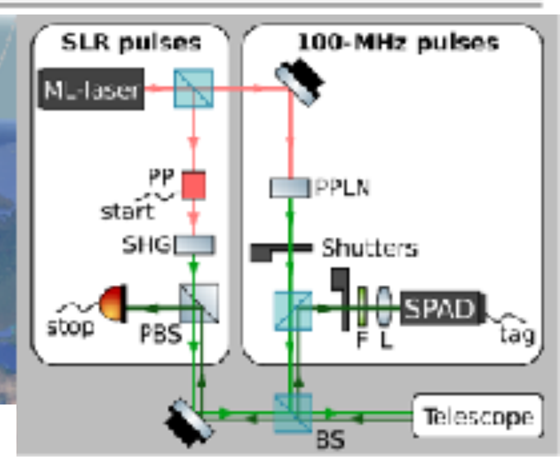
Demonstration of the detection of photon from the satellite which, according to the radar equation, is emitting a single photon per pulse from a **Medium-Earth-Orbit MEO** satellite.



Single photon exchange exploiting GLONASS CCRs at 20000 km

Satellite passage	Slant distance (km)	Detector	$\overline{R}_{\mathrm{det}}$ (Hz)	SNR	$\overline{\mu}_{\mathrm{sat}}$	l_{down} (dB)	l_{rec} (dB)
Glonass-134	19,500	SPAD	58	0.53	15	62.1	11.8
	20,200	SPAD	59	0.41	16	62.5	11.8
Glonass-131	20,250	SPAD	27	0.43	15	62.6	14.8
		PMT	6	0.21	16	62.6	21.8





Quantum Sci. Technol. 4(2019) 015012 https://doi.org/10.1088/2058-9565/aaefd4

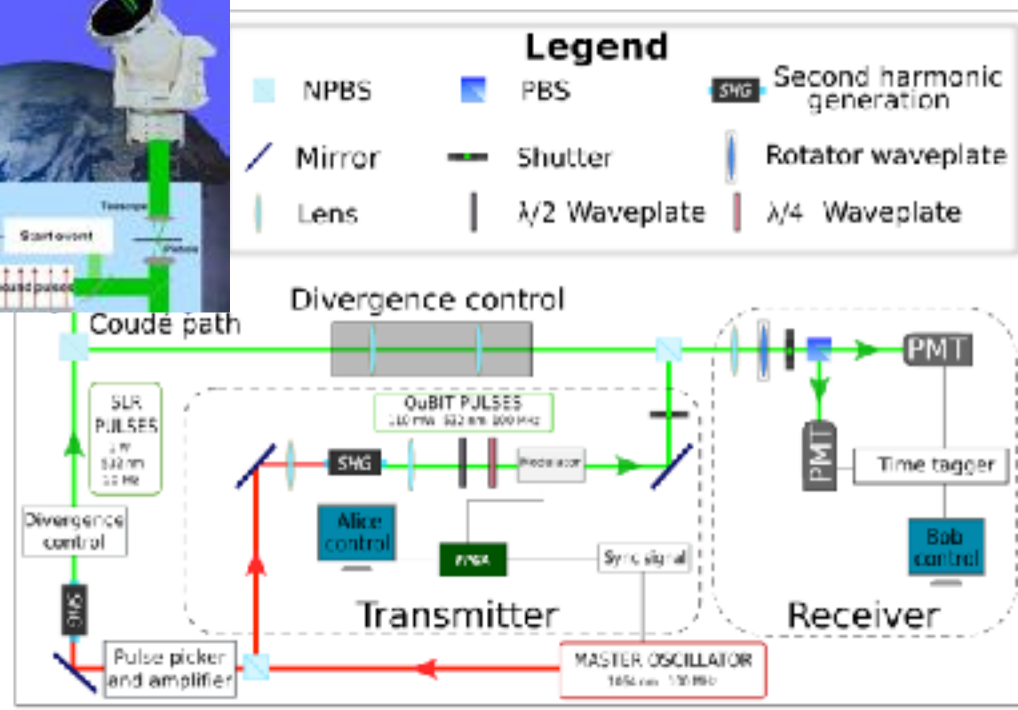
Quantum Science and Technology

Towards quantum communication from global navigation satellite system

Luca Calderaro[1,2], Costantino Agnesi[1,2], Daniele Dequal[3], Francesco Vedovato[1,2], Matteo Schiavon[1,2], Alberto Santamato[1], Vincenza Luceri[4], Giuseppe Bianco[3], Giuseppe Vallone[1,2] and Paolo Villoresi[1,2]

polarisation encoding and space QBER

- BB84 states in downlink, exploiting CCR with metallic coating (LARETS, Jason-2, Starlette, Stella)
- instantaneous distance and orbit reconstruction using interleaved ranging pulses
- radar equation for assessment of the μ< 1 condition at the satellite

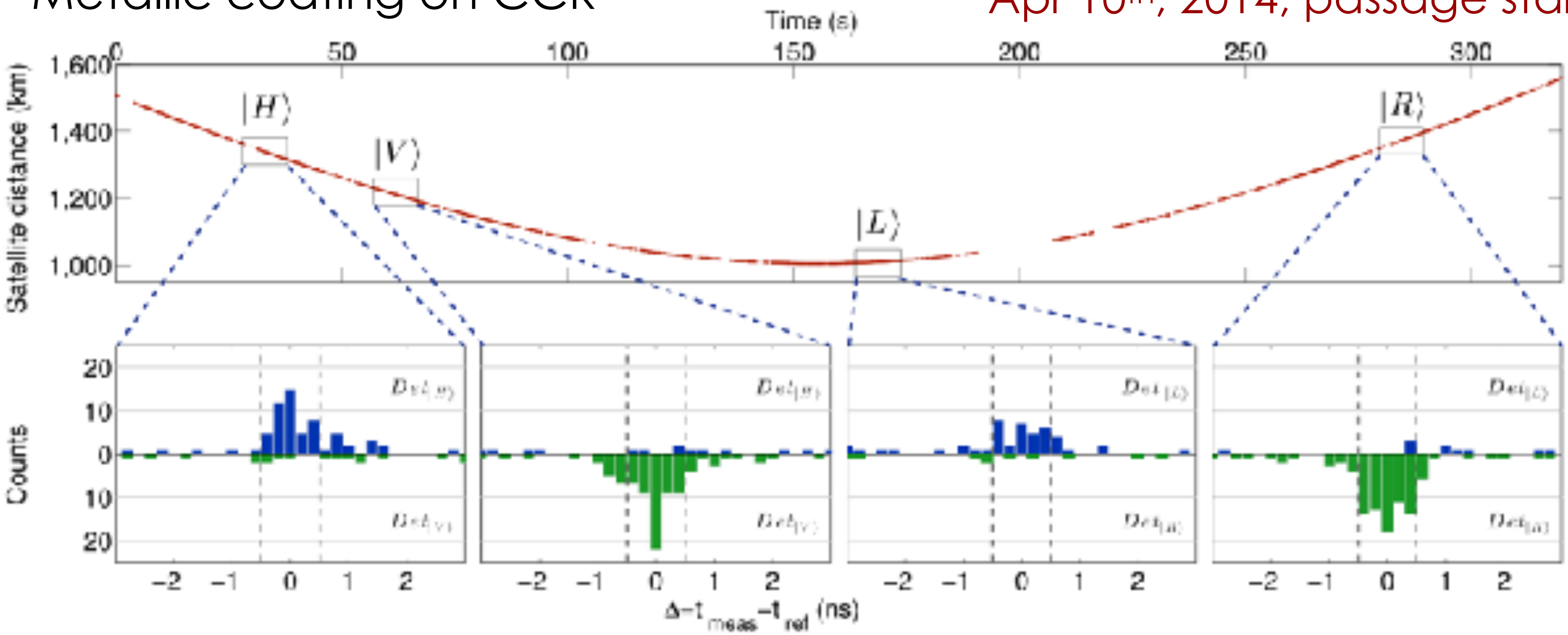


G. Vallone et al, ***Experimental Satellite Quantum Communications***, Phys. Rev. Lett. **115** 040502, 2015

first results: LARETS

Orbit height 690 km - spherical brass body
24 cm in diameter, 23 kg mass,
60 cube corner retroreflectors (CCR)
Metallic coating on CCR

Apr 10th, 2014, passage start 4:40 am



Return rate 147 cps
10^4 bits/passage

G. Vallone et al, ***Experimental Satellite Quantum Communications***, Phys. Rev. Lett. **115** 040502, 2015

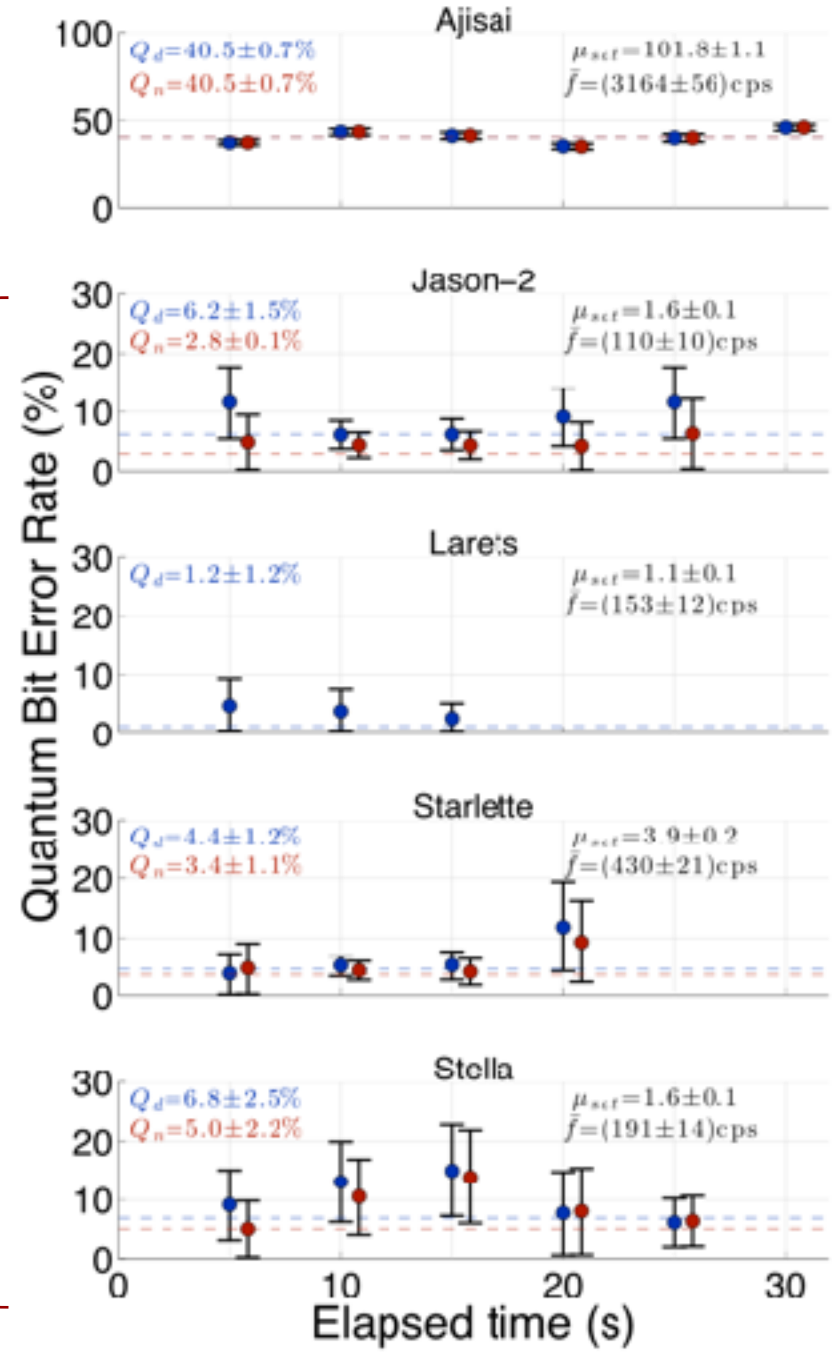
QBER

Non polarization maintaining CCR
Polarization QComm not possible

Polarization maintaining CCR

Polarization QComm with QBER compatible with applications

Demonstration of stable QBER over extended link duration



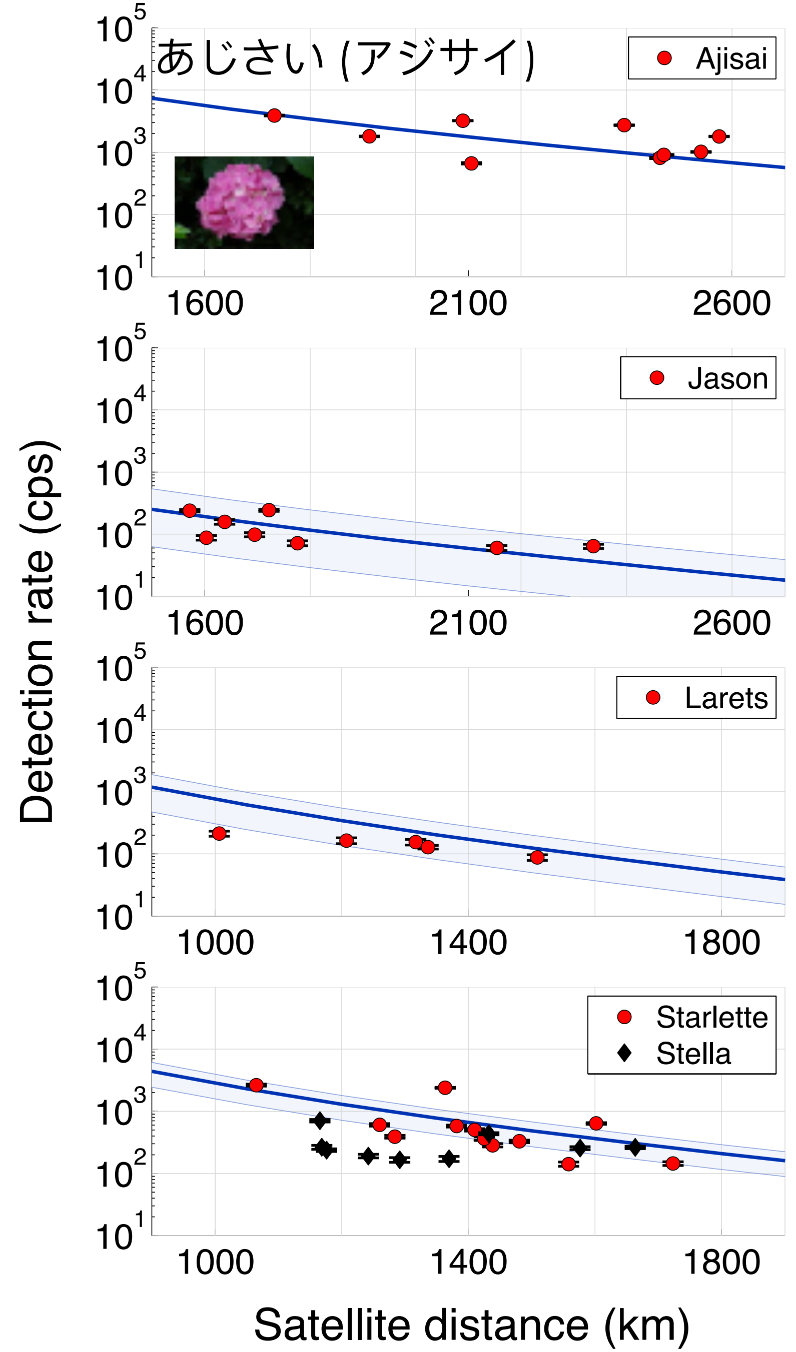
G. Vallone et al, ***Experimental Satellite Quantum Communications***, Phys. Rev. Lett. **115** 040502, 2015

Link Budget and photon return rate

Radar equation for the prediction of detected number of photons per pulse

$$\mu_{rx} = \mu_{tx}\,\eta_{tx}\,G_t\,\Sigma\left(\frac{1}{4\pi R^2}\right)^2 T_a^2\,A_t\,\eta_{rx}\,\eta_{det}$$

The results show that **radar equation model provides a precise fit** for the measured counts and the μvalue for the different satellites.



G. Vallone et al, ***Experimental Satellite Quantum Communications***, Phys. Rev. Lett. **115** 040502, 2015

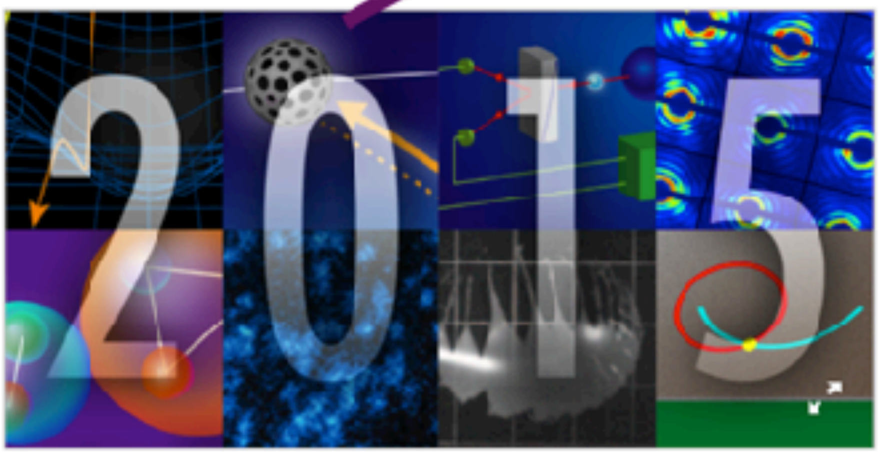
Highlights of the Year

December 18, 2015 • *Physics* 8, 126

***Physics* picks its favorite stories from 2015.**

Qubits in Space

Photons have been used to securely transmit quantum encryption keys over more than 300 kilometers of optical fiber. Ultimately, light attenuation limits how far a fiber can transmit a signal without degrading its quantum properties. But satellite-to-Earth links might soon open new frontiers for quantum communication. Researchers from the University of Padua and the Matera Laser Ranging Observatory, both in Italy, demonstrated that qubits encoded in photons can preserve their fragile quantum properties even after a round trip to satellites located more than one thousand kilometers away from Earth (see Viewpoint: Sending Quantum Messages Through Space). The authors encoded qubits in the photons' polarization and sent them to five satellites that bounced the light back to Earth. After the long journey, different qubit states could be distinguished reliably enough for viable quantum protocols.



As 2015 draws to a close, we look back on the research covered in *Physics* that really made waves in and beyond the physics community

Wishing everyone an excellent 2016.

–The Editors

the dedicated QKD missions, so far..

- mayor missions with dedicated satellite in Asia

- feasibility studies and progress to in-orbit-validation elsewhere

NICT Japan: Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite

- compact satellite-to-ground lasercom systems and microsatellite QKD systems
- adaptive optics correction (Grasse F)
- the polarized quantum states were received by the quantum receiver and discriminated in an unambiguous way with a quantum bit error rate (QBER) of <5%.

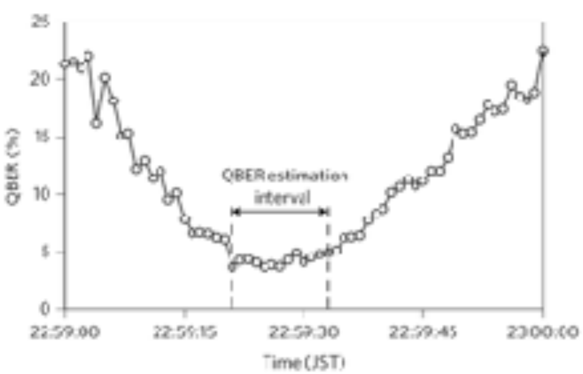
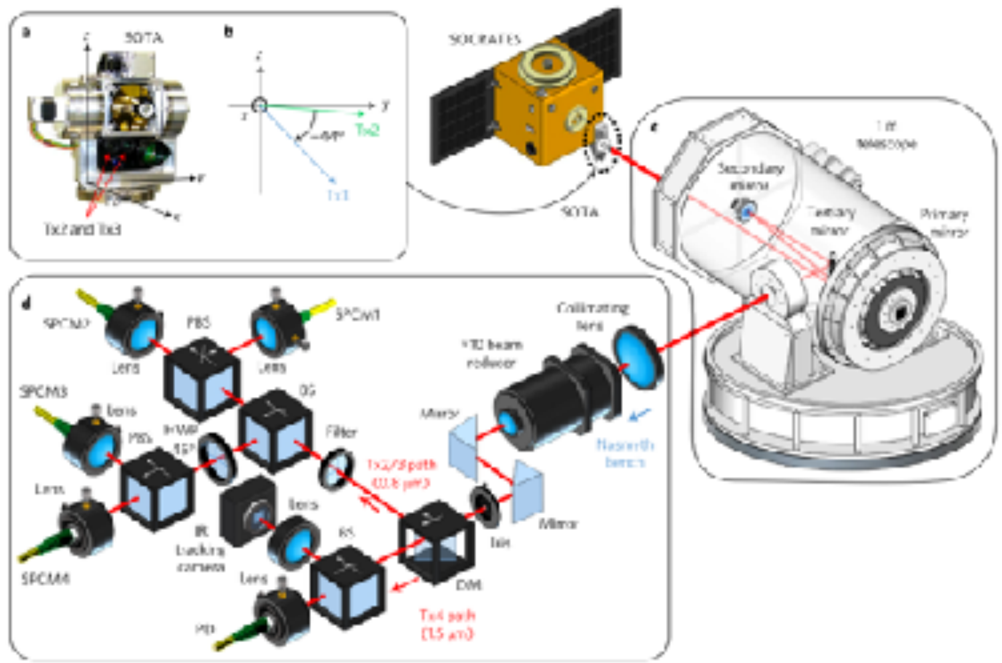


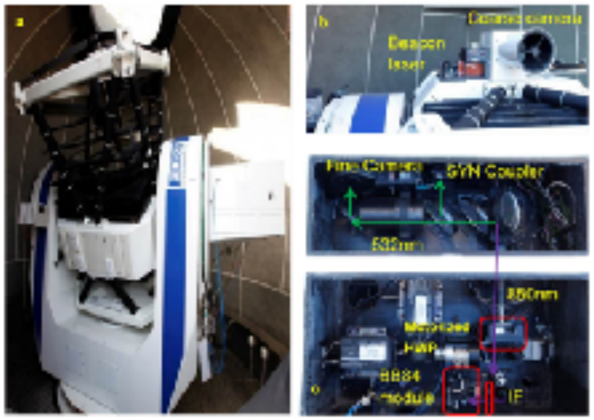
Figure 5 | **Variation of the QBER in the emulated B92 protocol for a 1 min duration of ~22:59:00–23:00:00 on 5 August 2016**

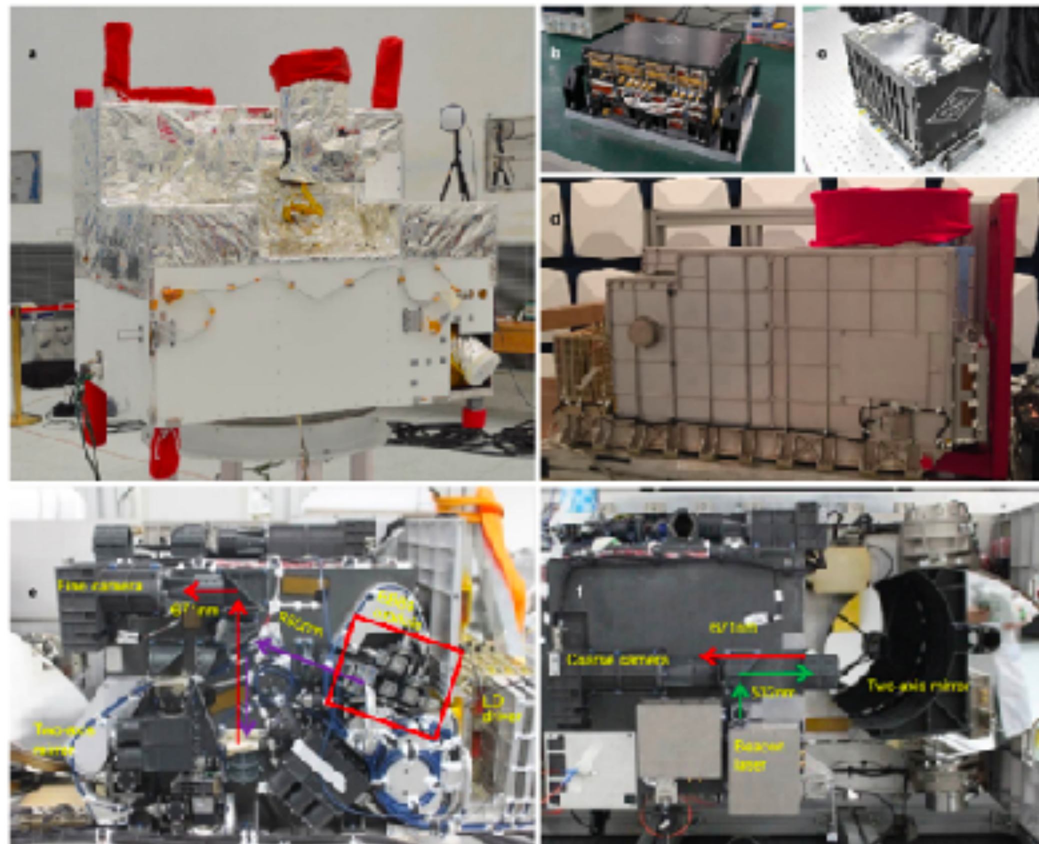


H. Takenaka et al Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. Nat. Photonics 11, 502–508 (2017)

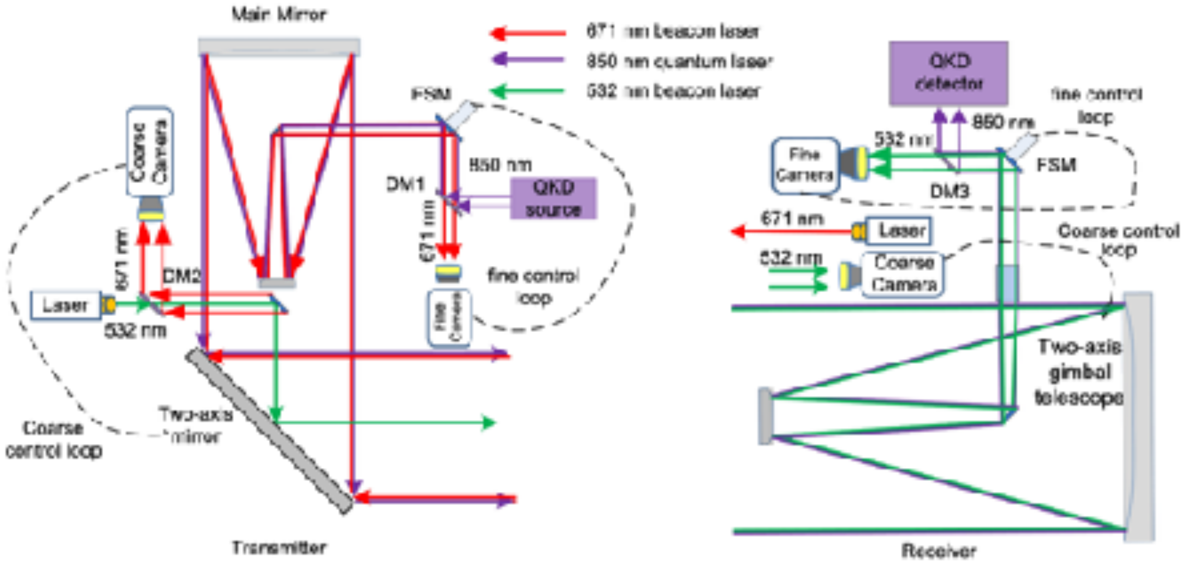
the multipurpose CAS-Micius mission

- launched on 16 August 2016 by a Long March 2D rocket from the Jiuquan Satellite Launch Centre, China





Extended Data Figure 2 | The Micius satellite and the payloads. a, A full view of the Micius satellite before being assembled into the rocket. b, The experimental control box. c, The APT control box. d, The optical transmitter. e, Left side view of the optical transmitter optics head. f, Top side view of the optical transmitter optics head.



Beacon laser	Wavelength	531.9 nm	671 nm
	Divergence	1.25 mrad	0.9 mrad
	Tracking error (1δ)	0.6~1.5 μrad	1~2 μrad

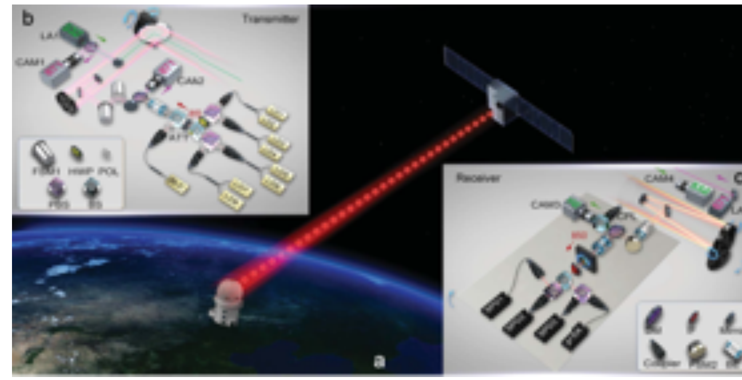
S-K Liao et al, Satellite-to-ground quantum key distribution Nature 549, 43 (2017)

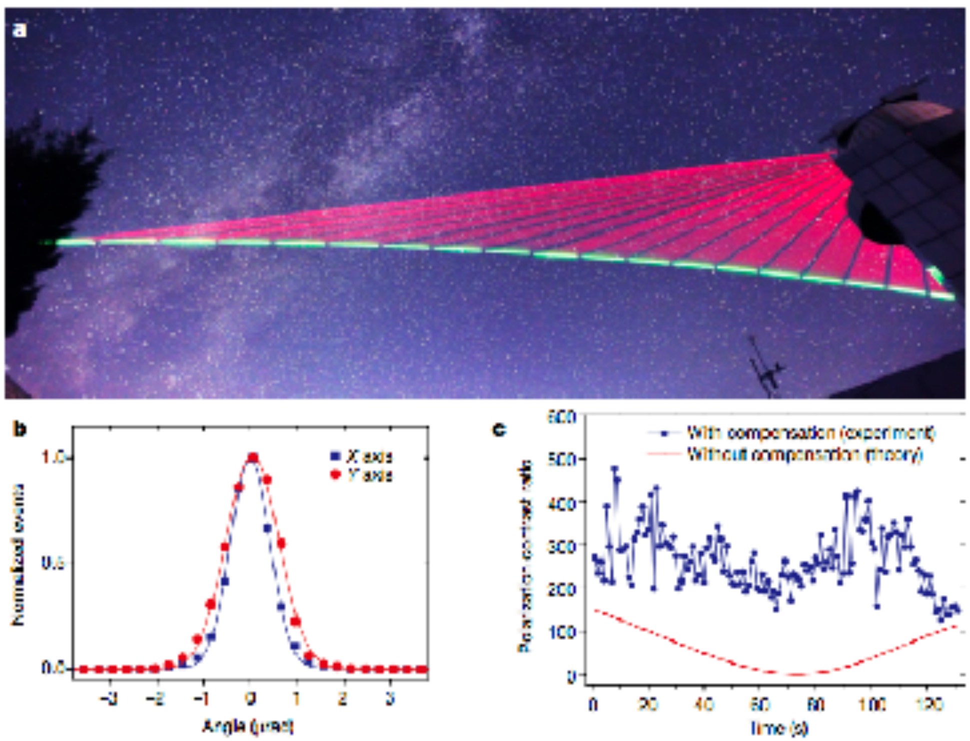
Satellite-to-ground quantum key distribution

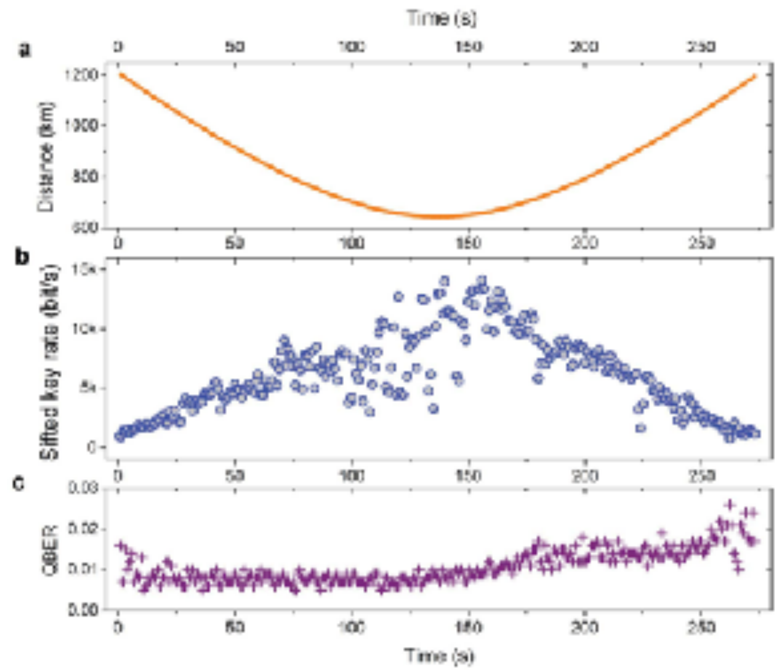
Sheng-Kai Liao[1,2], Wen-Qi Cai[1,2], Wei-Yue Liu[1,2], Liang Zhang[2,3], Yang Li[1,2], Ji-Gang Ren[1,2], Juan Yin[1,2], Qi Shen[1,2], Yuan Cao[1,2], Zheng-Ping Li[1,2], Feng-Zhi Li[1,2], Xia-Wei Chen[1,2], Li-Hua Sun[1,2], Jian-Jun Jia[3], Jin-Cai Wu[3], Xiao-Jun Jiang[4], Jian-Feng Wang[4], Yong-Mei Huang[5], Qiang Wang[5], Yi-Lin Zhou[6], Lei Deng[6], Tao Xi[7], Lu Ma[8], Tai Hu[9], Qiang Zhang[1,2], Yu-Ao Chen[1,2], Nai-Le Liu[1,2], Xiang-Bin Wang[2], Zhen-Cai Zhu[6], Chao-Yang Lu[1,2], Rong Shu[2,3], Cheng-Zhi Peng[1,2], Jian-Yu Wang[2,3] & Jian-Wei Pan[1,2]

decoy–state QKD with a kilo-hertz key rate over a distance of 1200 km.

This key rate is around 20 orders of magnitudes greater than that expected using an optical fibre of the same length







S-K Liao et al, Satellite-to-ground quantum key distribution Nature 549, 43 (2017)

Satellite-Relayed Intercontinental Quantum Network

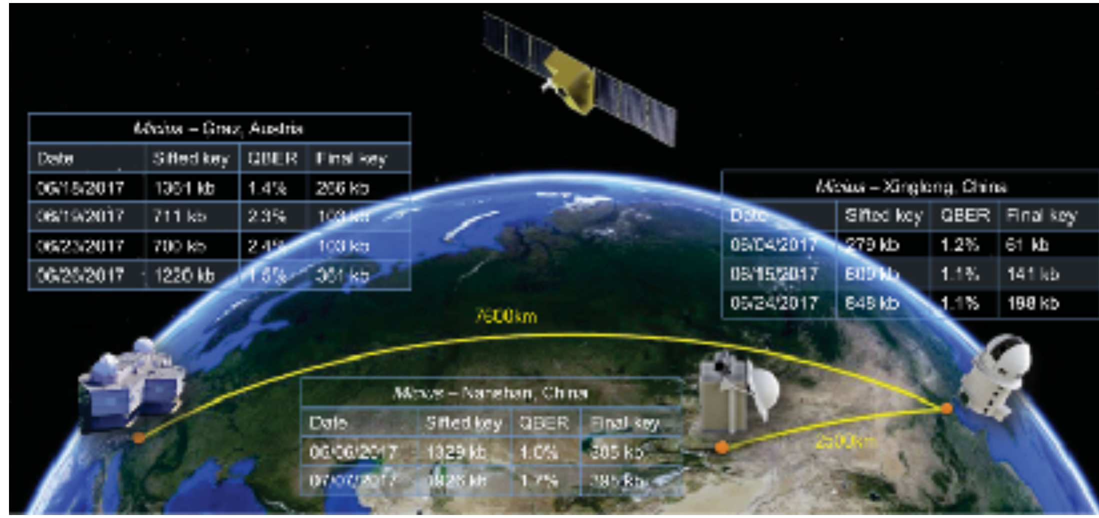
Micius satellite as a trusted relay to distribute secure keys between multiple distant locations in China and Europe

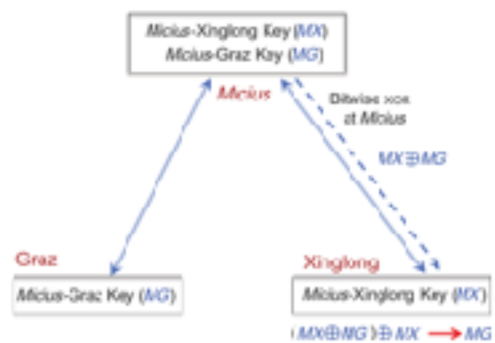
QKD is performed in a downlink scenario—from the satellite to the ground.

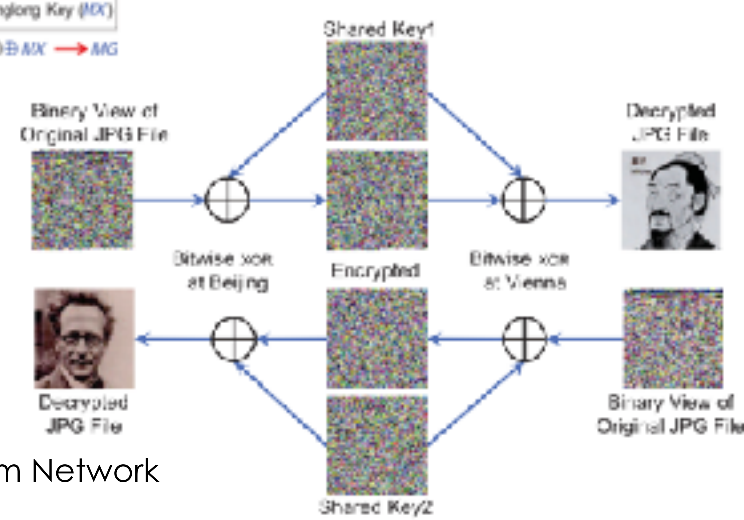
sifted key rate of a ~3 kb/s at ~1000 km physical separation distance and ~9 kb/s at ~600 km distance (at the maximal elevation angle),

In this work, we establish a 100 kB secure key between Xinglong and Graz.

Video conference with AES-128 protocol that refreshed the 128-bit seed keys every second.







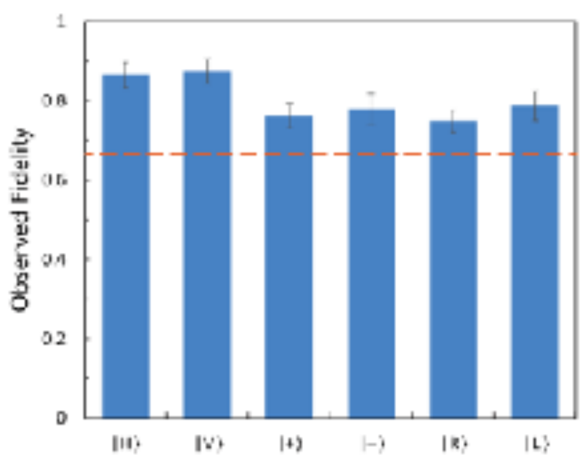
S-K Liao et al, Satellite-Relayed Intercontinental Quantum Network
Phys. Rev. Lett. 120, 030501 (2018)

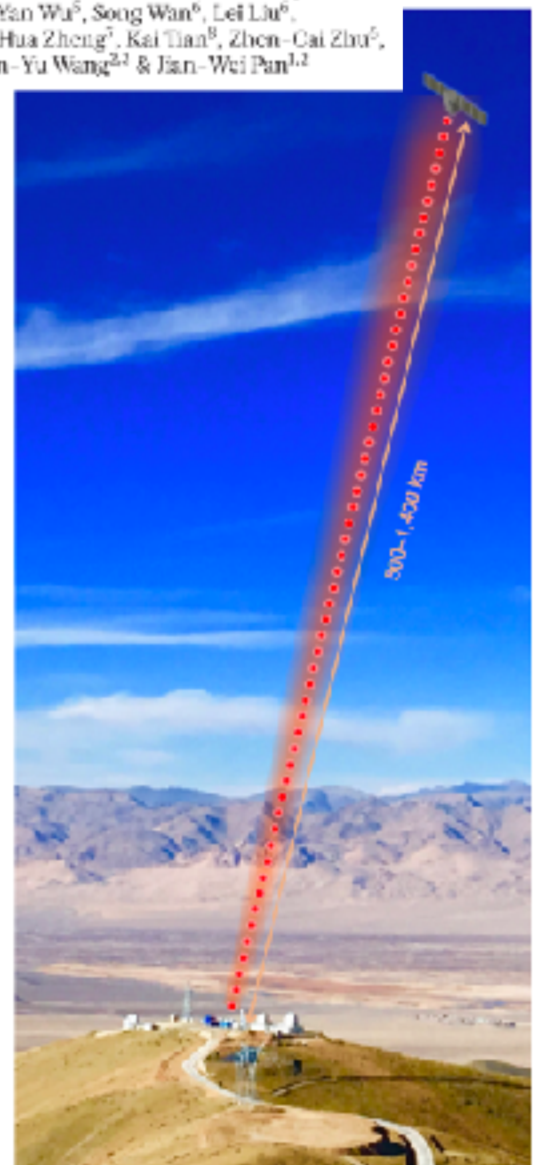
Ground-to-satellite quantum teleportation

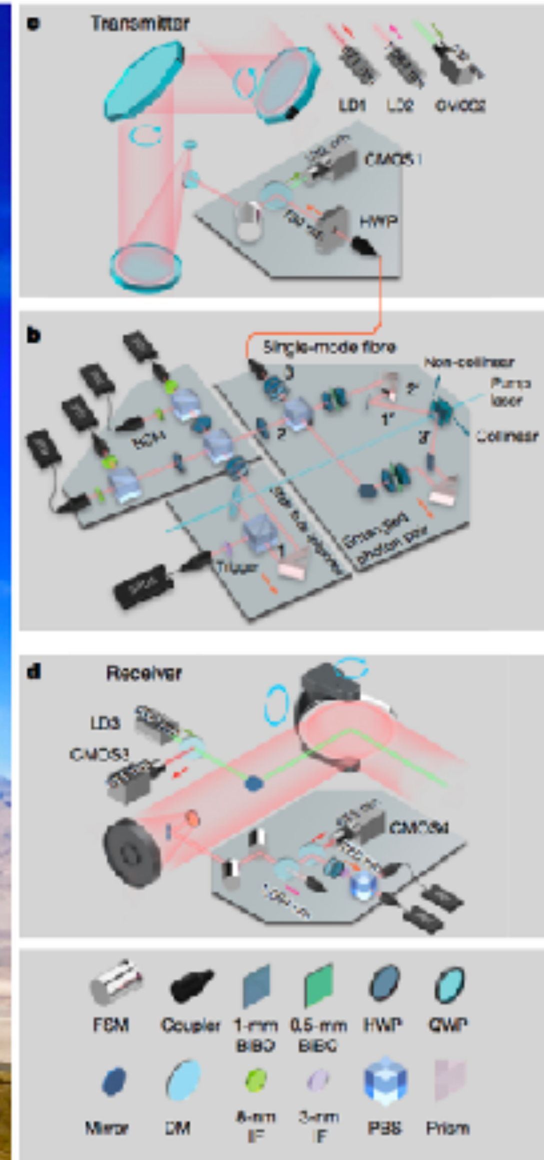
Ji-Gang Ren[1,2], Ping Xu[1,2], Hai-Lin Yong[1,2], Liang Zhang[2,3], Sheng-Kai Liao[1,2], Juan Yin[1,2], Wei-Yue Liu[1,2], Wen-Qi Cai[1,2], Meng Yang[1,2], Li Li[1,2], Kui-Xing Yang[1,2], Xuan Han[1,2], Yong-Qiang Yao[4], Ji Li[5], Hai-Yan Wu[5], Song Wan[6], Lei Liu[6], Ding-Quan Liu[3], Yao-Wu Kuang[3], Zhi-Ping He[3], Peng Shang[1,2], Cheng Guo[1,2], Ru-Hua Zheng[7], Kai Tian[8], Zhen-Cai Zhu[5], Nai-Le Liu[1,2], Chao-Yang Lu[1,2], Rong Shu[2,3], Yu-Ao Chen[1,2], Cheng-Zhi Peng[1,2], Jian-Yu Wang[2,3] & Jian-Wei Pan[1,2]

quantum teleportation has been demonstrated through an uplink channel for ground-to-satellite quantum teleportation over distances of up to 1400 km.

This demonstration successfully teleported six input states in mutually unbiased bases with an average fidelity of 0.80 ± 0.01, which is above the optimal state- estimation fidelity on a single copy of a qubit







J.-G. Ren et al, Ground-to-satellite quantum teleportation. Nature 549, 70–73 (2017)

Satellite-based entanglement distribution over 1200 kilometers

Juan Yin,[1,2] Yuan Cao,[1,2] Yu-Huai Li,[1,2] Sheng-Kai Liao,[1,2] Liang Zhang,[2,3] Ji-Gang Ren,[1,2] Wen-Qi Cai,[1,2] Wei-Yue Liu,[1,2] Bo Li,[1,2] Hui Dai,[1,2] Guang-Bing Li,[1,2] Qi-Ming Lu,[1,2] Yun-Hong Gong,[1,2] Yu Xu,[1,2] Shuang-Lin Li,[1,2] Feng-Zhi Li,[1,2] Ya-Yun Yin,[1,2] Zi-Qing Jiang,[3] Ming Li,[3] Jian-Jun Jia,[3] Ge Ren,[4] Dong He,[4] Yi-Lin Zhou,[5] Xiao-Xiang Zhang,[6] Na Wang,[7] Xiang Chang,[8] Zhen-Cai Zhu,[3] Nai-Le Liu,[1,2] Yu-Ao Chen,[1,2] Chao-Yang Lu,[1,2] Rong Shu,[2,3] Cheng-Zhi Peng,[1,2*] Jian-Yu Wang,[2,3*] Jian-Wei Pan[1,2*]

Long-distance entanglement distribution is essential for both foundational tests of quantum physics and scalable quantum networks. Owing to channel loss, however, the previously achieved distance was limited to ~100 kilometers. Here we demonstrate satellite-based distribution of entangled photon pairs to two locations separated by 1203 kilometers on Earth, through two satellite-to-ground downlinks with a summed length varying from 1600 to 2400 kilometers. We observed a survival of two-photon entanglement and a violation of Bell inequality by 2.37 ± 0.09 under strict Einstein locality conditions. The obtained effective link efficiency is orders of magnitude higher than that of the direct bidirectional transmission of the two photons through telecommunication fibers.

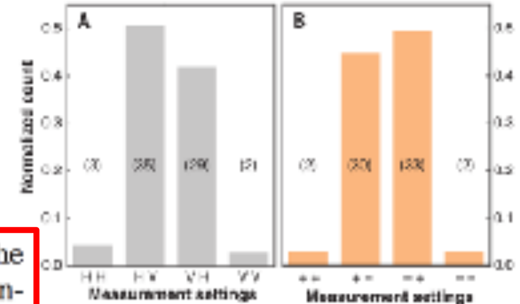


Fig. 4. Measurement of the received entangled photons after transmission by the two-downlink channel. (A) Normalized two-photon coincidence counts in the measurement setting of the |H⟩/|V⟩ basis. (B) Normalized counts in the diagonal |±⟩ basis. Numbers in parentheses

we found $S = 2.37 \pm 0.09$, with a violation of the CHSH-type Bell inequality $S \leq 2$ by four standard deviations. The result again confirms the nonlocal feature of entanglement and excludes the models of reality that rest on the notions of locality and realism—on a previously unattained scale of thousands of kilometers.

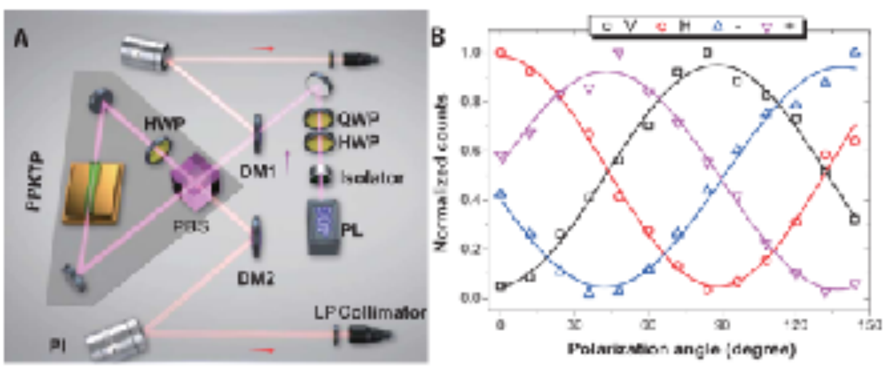


Fig. 1. Schematic of the spaceborne entangled-photon source and its in-orbit performance. (A) The thickness of the $KTiOPO_4$ (PPKTP) crystal is 15 mm. A pair of off-axis concave mirrors focus the pump laser (PL) in the center of the PPKTP crystal. At the output of the Sagnac interferometer, two dichromatic mirrors (DMs) and long-pass filters are used to separate the signal photons from the pump laser. Two additional electrically driven piezo steering mirrors (PIs), remotely controllable on the ground, are used for fine adjustment of the beam-pointing for an optimal collection efficiency into the single-mode fibers. QWP, quarter-wave plate; HWP, half-wave plate; PBS, polarizing beam splitter. (B) The two-photon correlation curves measured on-satellite by sampling 1% of each path of the entangled photons. The count rate measured from the overall 0.01% sampling is about 590 Hz, from which we can estimate the source brightness of 5.9 MHz.

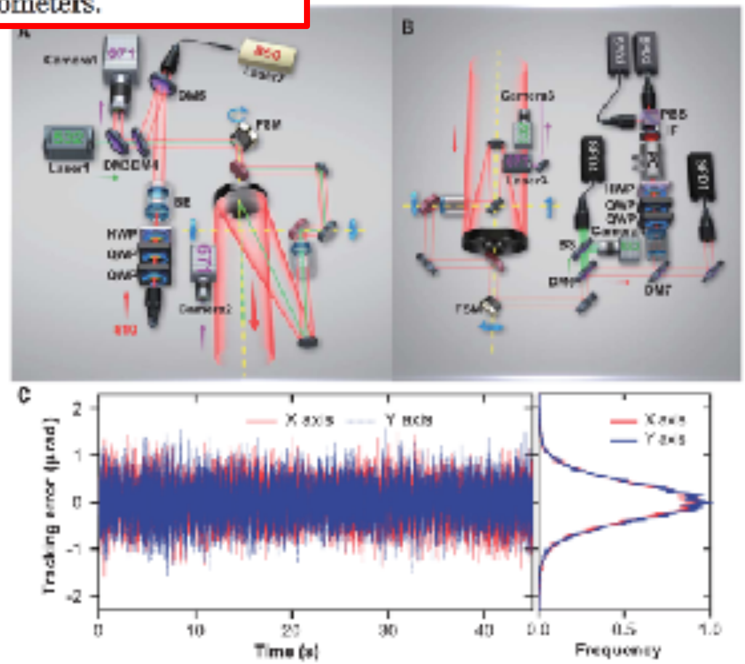


Fig. 2. The transmitters, receivers, and APT performance. (A) The entangled photon beam (810 nm) is combined and co-aligned with a pulsed infrared laser (850 nm) for synchronization and a green laser (532 nm) for tracking by three DMs and sent out from an 8× telescope. For polarization compensation, two motorized QWPs and a HWP are remotely controlled. A fast steering mirror (FSM) and a two-axis turntable are used for closed-loop fine and coarse tracking, based on the 671-nm beacon laser images captured by cameras 1 and 2. BE, beam expander. (B) Schematic of the receiver at Delingha. The cooperating APT and polarization compensation systems are the same as those on the satellite. The tracking and synchronization lasers are separate from the signal photon and detected by single-photon detectors (SPDs). For polarization analysis along bases that are randomly switching quickly, two QWPs, a HWP, a Pockels cell (PC), and a PBS are used. BS, beam splitter. IF, interference filter. (C) The APT system starts tracking after the satellite reaches a 5° elevation angle.

J. Yin et al. Satellite-based entanglement distribution over 1200 kilometers. Science 80 1140 (2017)

Entanglement-based secure quantum cryptography over 1,120 kilometres

https://doi.org/10.1038/s41586-020-2401-y

Received: 15 July 2019

Accepted: 13 May 2020

Published online: 15 June 2020

Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Yuan Cao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Shuang-Lin Li, Rong Shu, Yong-Mei Huang, Lei Deng, Li Li, Qiang Zhang, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Xiang-Bin Wang, Feihu Xu, Jian-Yu Wang, Cheng-Zhi Peng, Artur K. Ekert & Jian-Wei Pan

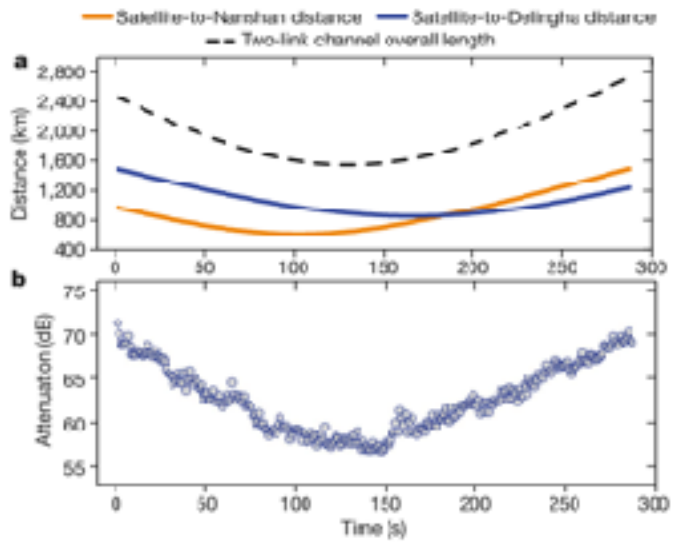
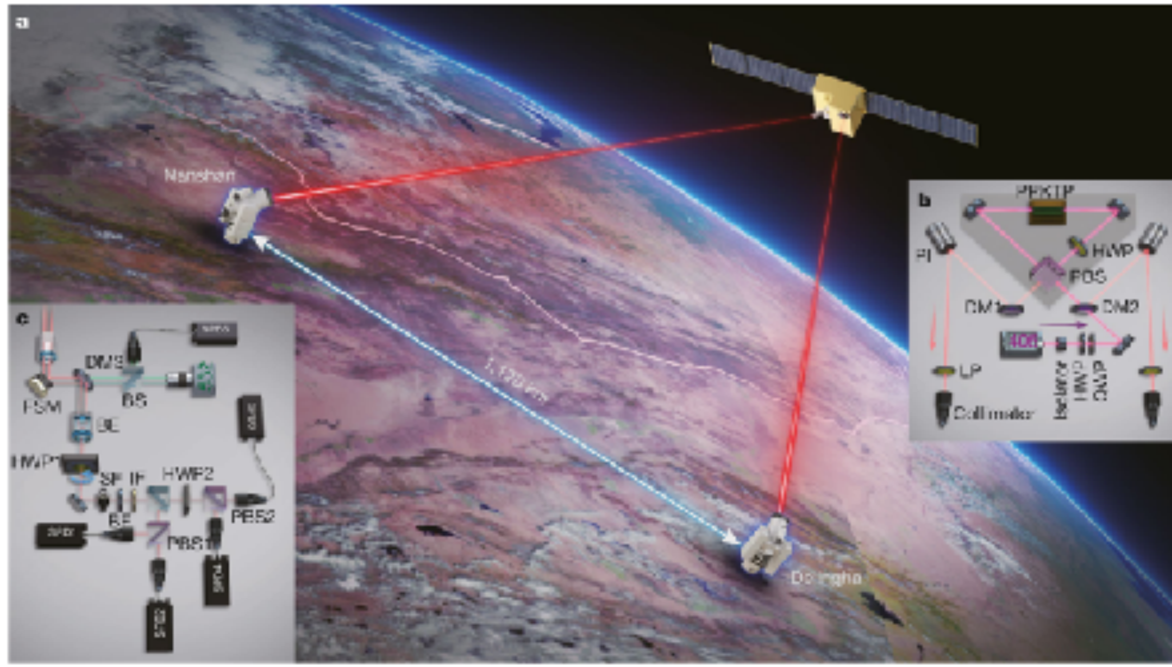


Fig. 2 | Distances and attenuations from satellite to Nanshan (Delingha). **a**, A typical two-downlink trial from satellite to Nanshan, and to Delingha, lasts about 285 s (>13° elevation angle for both ground stations) in a single pass of the satellite. The distance from satellite to Nanshan (Delingha) is from 618 km (853 km) to about 1,500 km, and the total length of the two downlinks varies from 1,545 km to 2,730 km. **b**, The measured satellite-to-ground two-downlink channel attenuation.



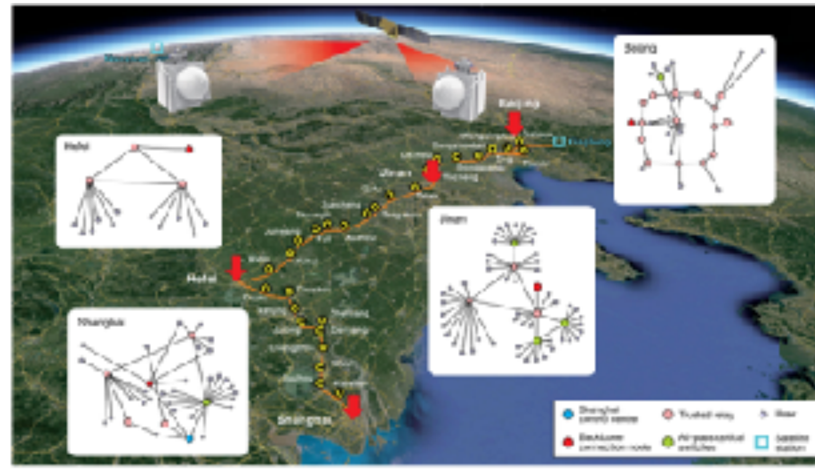
we have demonstrated entanglement-based QKD between two ground stations separated by 1,120 km. We increase the link efficiency of the two-photon distribution by a factor of about 4 compared to the previous work and obtain a finite-key secret key rate of 0.12 bits per second.
The brightness of our spaceborne entangled photon source can be increased by about two orders of magnitude in our latest research, which could readily increase the average final key to tens of bits per second or tens of kilobits per orbit

J. Yin et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature 582, 501 (2020)

An integrated space-to-ground quantum communication network over 4,600 kilometres

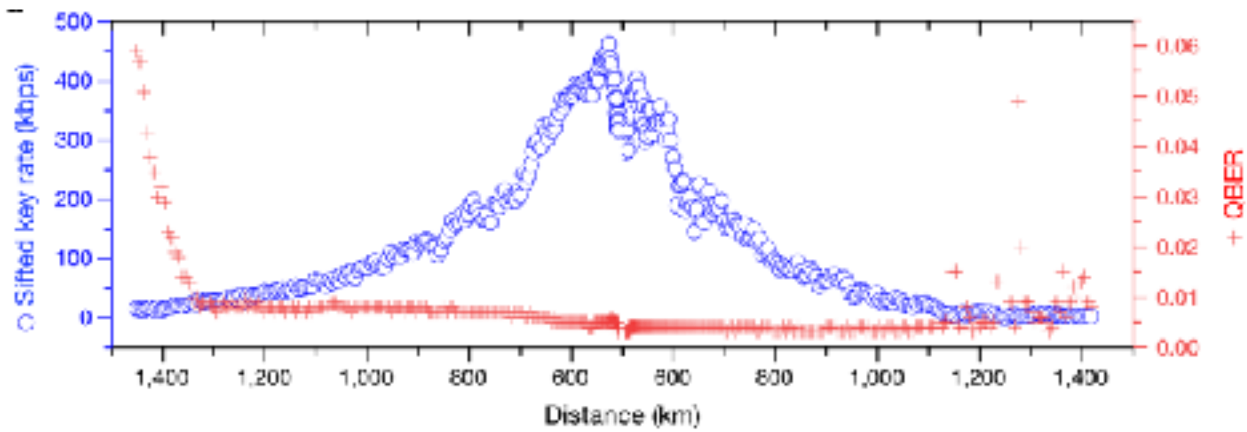
https://doi.org/10.1038/s41586-020-03093-8
Received: 1 March 2019
Accepted: 2 November 2020
Published online: 6 January 2021

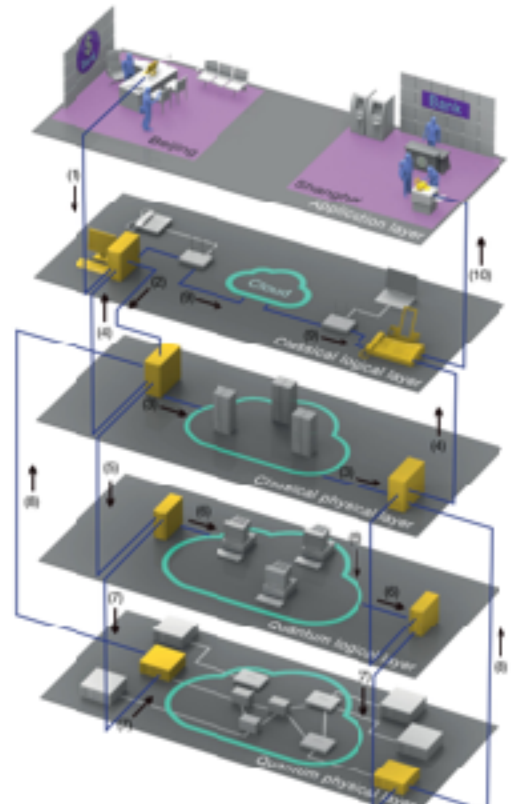
Yu-Ao Chen[1,2,3], Qiang Zhang[1,2], Teng-Yun Chen[1,2], Wen-Qi Cai[1,2], Sheng-Kai Liao[1,2], Jun Zhang[1,2], Kai Chen[1,2], Juan Yin[1,2], Ji-Gang Ren[1,2], Zhu Chen[1,2], Sheng-Long Han[1,2], Qing Yu[3], Ken Liang[3], Fei Zhou[4], Xiao Yuan[1,2], Mei-Sheng Zhao[1,2], Tian-Yin Wang[1,2], Xiao Jiang[1,2], Liang Zhang[2,5], Wei-Yue Liu[1,2], Yang Li[1,2], Qi Shen[1,2], Yuan Cao[1,2], Chao-Yang Lu[1,2], Rong Shu[2,5], Jian-Yu Wang[2,5], Li Li[1,2], Nai-Le Liu[1,2], Feihu Xu[1,2], Xiang-Bin Wang[4], Cheng-Zhi Peng[1,2,3] & Jian-Wei Pan[1,2,3]



large–scale, hybrid quantum communication network has been realised by integrating the Micius space links to a 2000 km long Beijing–Shanghai trusted node link

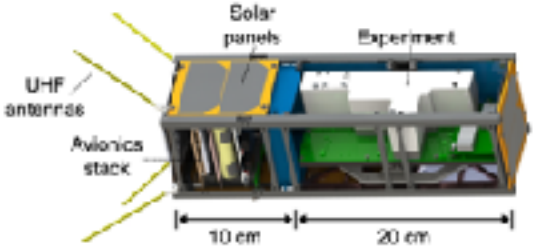
this result in a total quantum communication distance of 4600 km, showing the first example of an inter-continental scale QKD network with around 150 users.

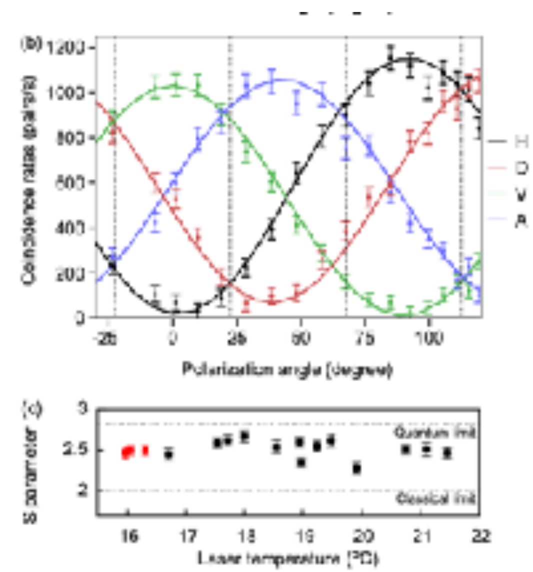




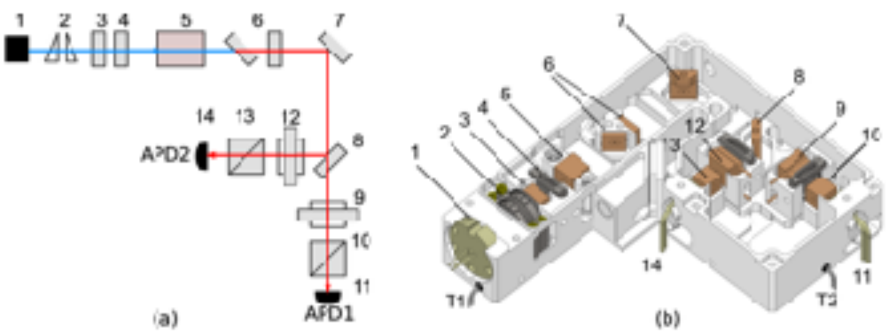
Singapore quantum cubesats

- polarization entangled photon-pair source on board of SpooQy-1 a CubeSat in LEO
- entanglement technology can be deployed with minimal resources in novel operating environments,
- this demonstration follows another cubesat experiment devoted to demonstrate pair generation and polarization correlation



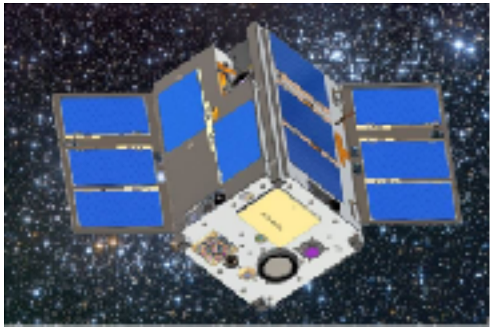


Correlation curves and Bell test measured in orbit on 16th July 2019

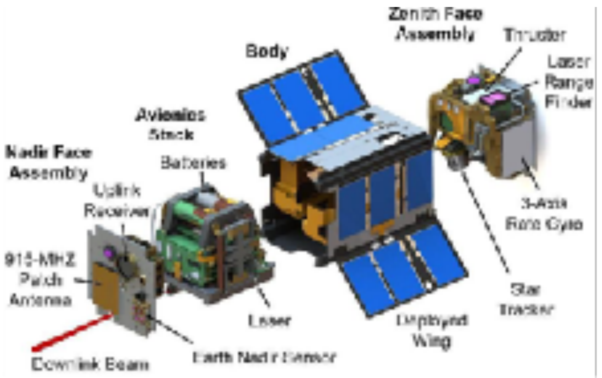


Z. Tang et al. Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite. Phys. Rev. Appl. 5, 054022 (2016)
A. Villar et al. Entanglement demonstration on board a nano-satellite. Optica 7, 734 (2020).

cubesat projects for QKD



- small sat are expanding the capabilities and leveraging on more refined component (pointing, sources, power, optics)
- Singapore and many countries in Europe endeavour developing Q-cubesats
  - CQuCoM
  - SpeQtre QUARC
  - ROKS
  - QUBE
  - NANOBOB/Q3sat



R. Bedington et al. Progress in satellite quantum key distribution. npj Quantum Inf. 3, 30 (2017)
J.S. Sidhu et al. Advances in space quantum communications. IET Quantum Commun. qtc2.12015 (2021)

EU Commission + ESA SAGA

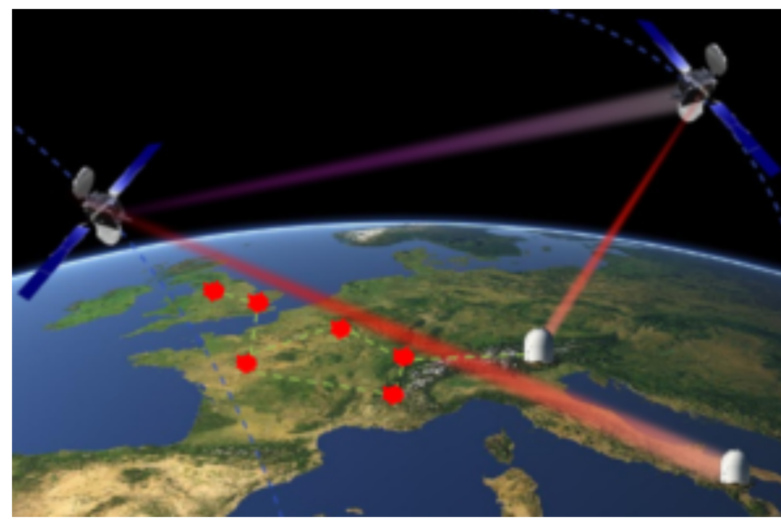
European Commission > Strategy > Shaping Europe's digital future > News >

Shaping Europe's digital future

DIGIBYTE | 13 June 2019

The future is quantum: EU countries plan ultra-secure communication network

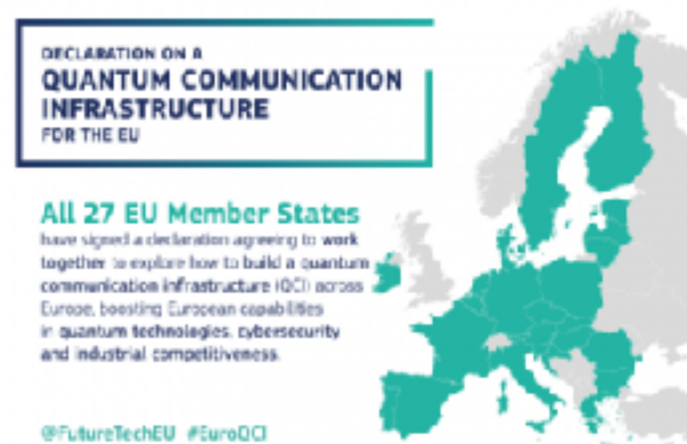
- Architecture of EURO-QCI
- Space Segment role
- Studies for specific applications
- Technology of QKD hardware
- Demonstration of QKD in orbit
- Links to the ground network (ground QCI)



OpenQKD: all EU QKD testbed

- OpenQKD EU demonstration project
- Demonstrate vertical supply chain from QKD (physical layer) to end-user (application layer)
- Many test sites across Europe to maximise impact
- Demonstration of more than 30 use-cases for QKD featuring:
  - realistic operating environments
  - end-user applications and support
- Secure and digital societies: Inter/Intra datacenter comm., e-Government, High-Performance computing, financial services, authentication and space applications, integration with post-quantum cryptography, securing time-transfer
- Healthcare: Secure cloud storage services and securing patient data in transit

38 Partners from 13 EU countries



https://openqkd.eu/objectives/
https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

intermodal QKD from free space to the fiber network

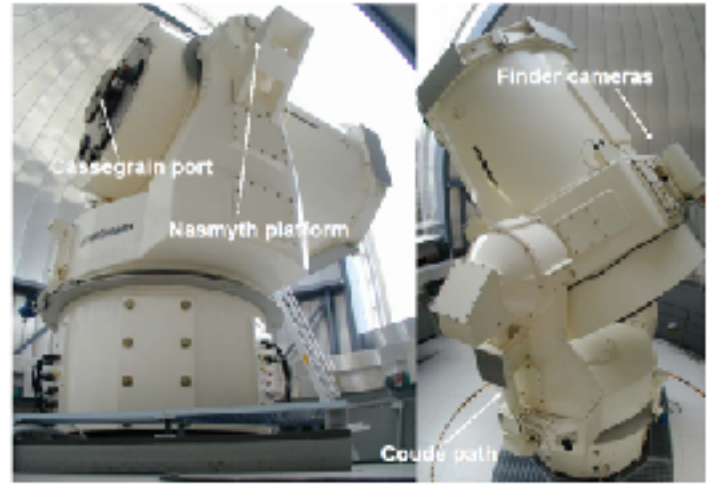
Avesani, M. et al. Resource-effective quantum key distribution: a field trial in Padua city center. Opt. Lett. 46, 2848 (2021).

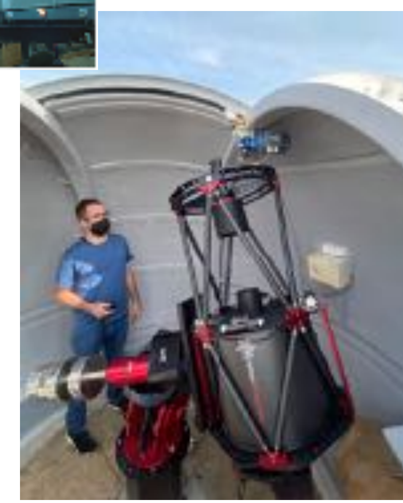
qtech.unipd.it
quantumfuture.dei.unipd.it
www.thinkquantum.com

QKD ground receivers

Telescope sizes for diverse uses:

- satellite-to-ground link on nodal points - meter class telescope (1.5m ASI- MLRO at Matera Italy and the 1 m OGS of ESA in Tenerife)
- operative user receiver, 40 cm class (GaliQEye - Padova)
- ground-to-ground free-space links night- and day-time with centimeter-class telescopes

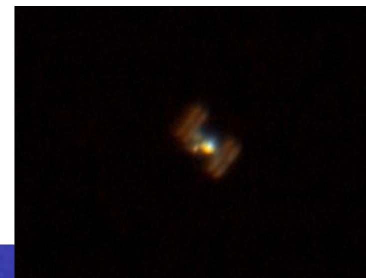


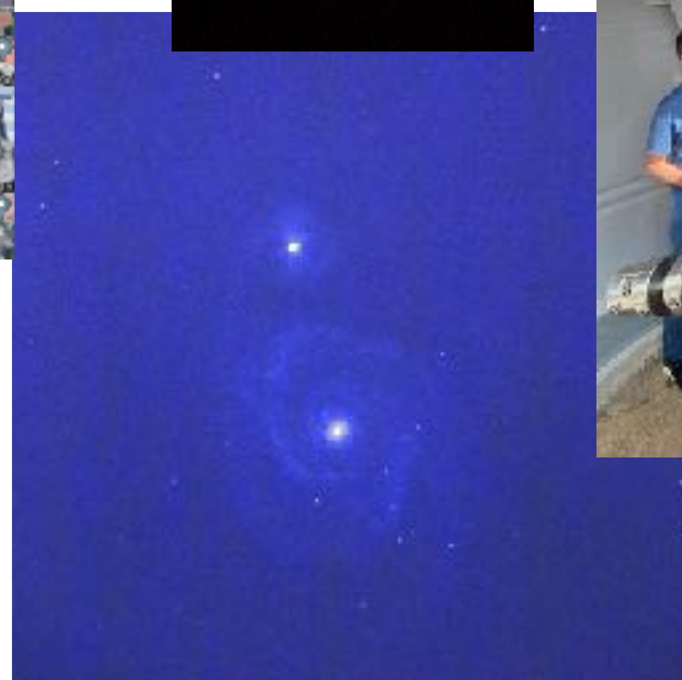


J. S. Sidhu et al. Advances in space quantum communications. IET Quantum Commun. qtc2.12015 (2021)

QuantumFuture GaliQeye
urban receiver for Space QKD @ UniPD

- 40 cm - class telescope
- wide wavelength range and protocols





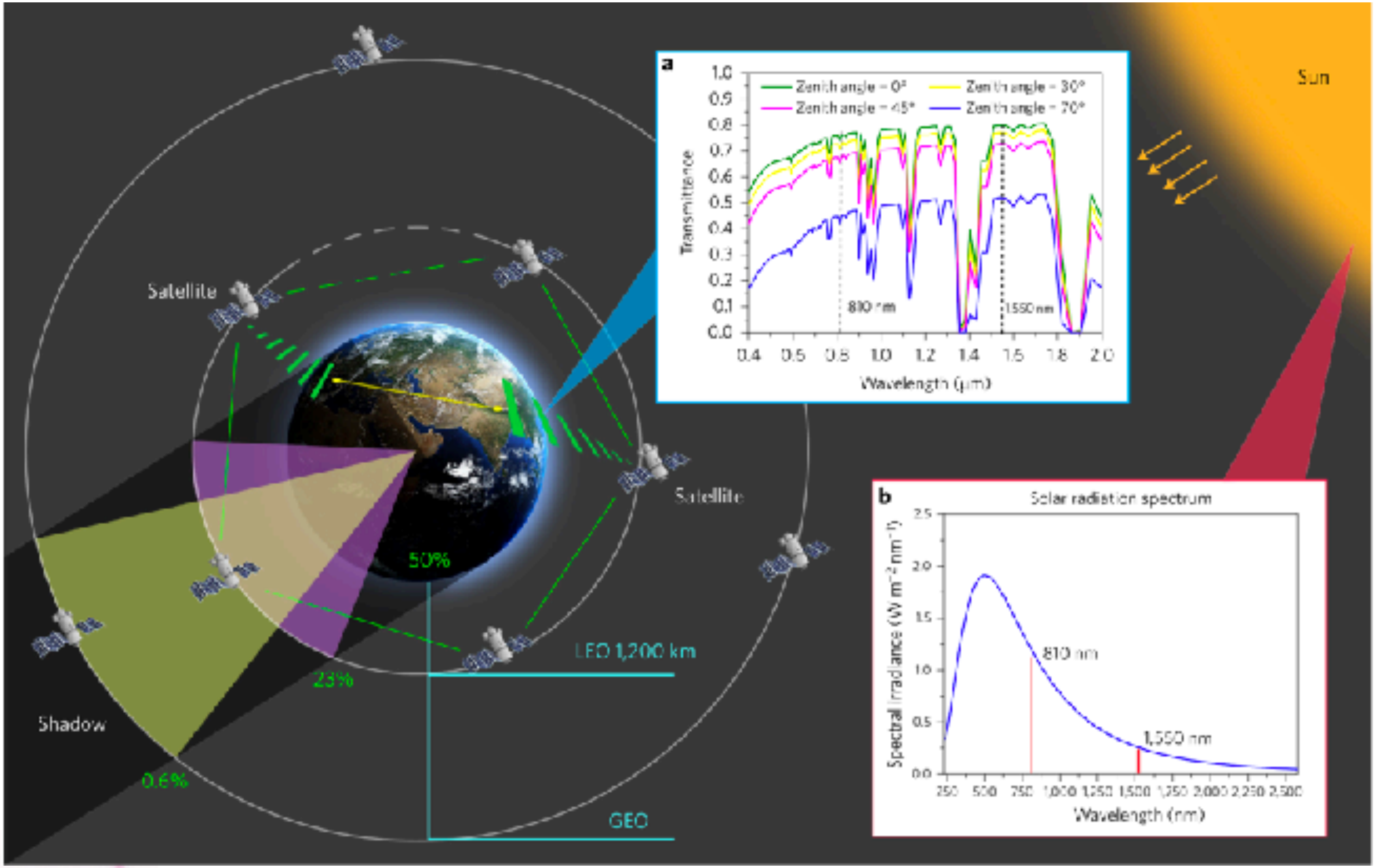
- the development of multiple ground networks is ongoing
- satellites for the QKD demonstration (first governmental and then commercial) are under realization
- ground stations need to be deployed
- new-space economy and secure communications will use QKD
- opportunities for applications and new schemes

standards and space QKD

- standardisation of QKD is ongoing
- the space part is in the development phase
- this will lead to standards to help a global operation

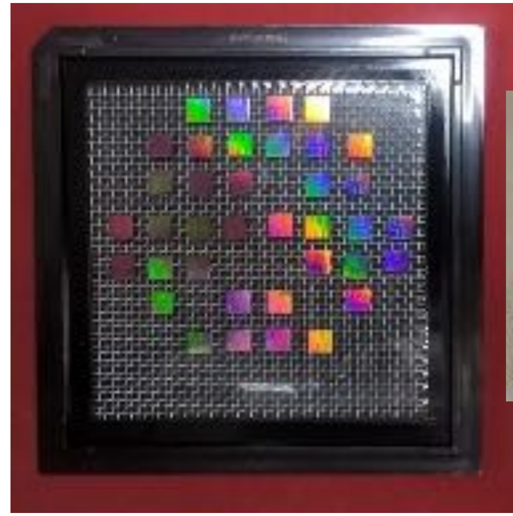
https://www.etsi.org/technologies/quantum-safe-cryptography

On daylight Space QComms

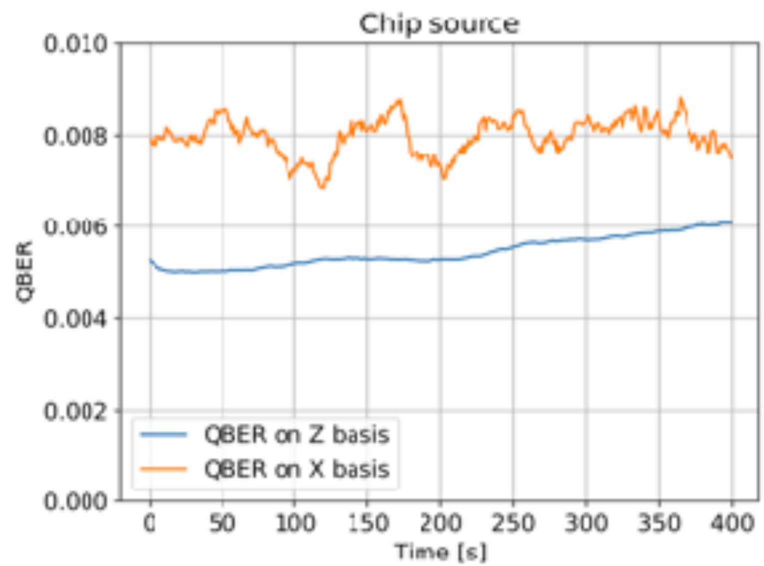


S.-K. Liao, *et al.,* Nat. Photonics **11**, 509 (2017)

Alice's compact transmitter with a PIC

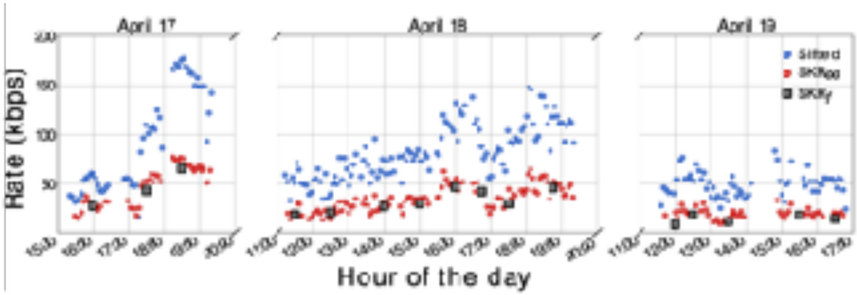


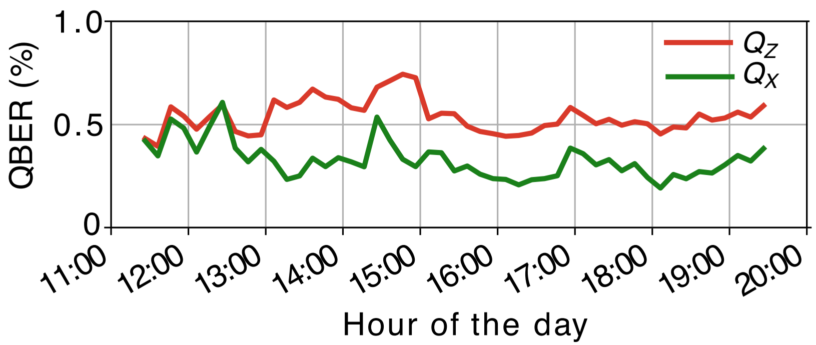
integrated photonic circuit (PIC) featuring a complete quantum state encoder for a space QKD system was realized at IMEC (image on the top right the produced batch).
We performed a full QKD-run in lab with the fiber-fiber configuration with both decoy and polarization modulations active at 50 MHz of repetition rate.
The QBER in the two measurement basis is represented in the figure on the bottom right.
We note that the integrated source shows a great polarization quality with a QBER which is lower than 1% for long time.



M. Avesani et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. npj Quantum Inf. 7, 93 (2021) - arxiv 1907.10039 (2019)

Results: full-daylight QKD with integrated source






11:30


12:00


13:00


14:30


16:30


19:30

- We reached an **extremely low QBER (~0.5%)** in both bases, with no active polarization stabilization
- The developed chip encoder is characterized by **an excellent polarization stability over time**
- **Integrated silicon photonics is very attractive for polarization-based QC (even with satellites)**
- **Highest in daylight at 1550 nm: max ~ 70 kbps**

M. Avesani et al. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. npj Quantum Inf. 7, 93 (2021) - arxiv 1907.10039 (2019)

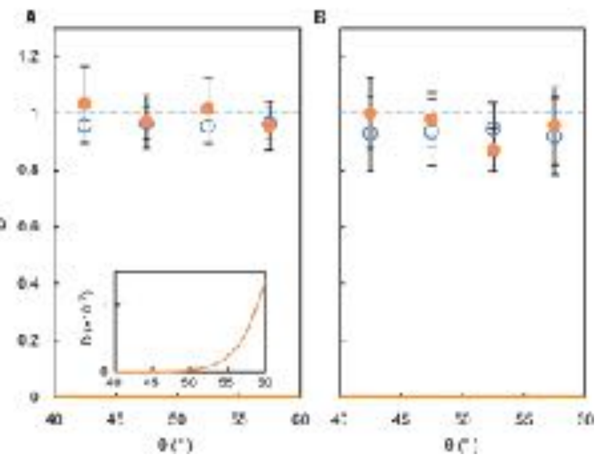
pathway to new science

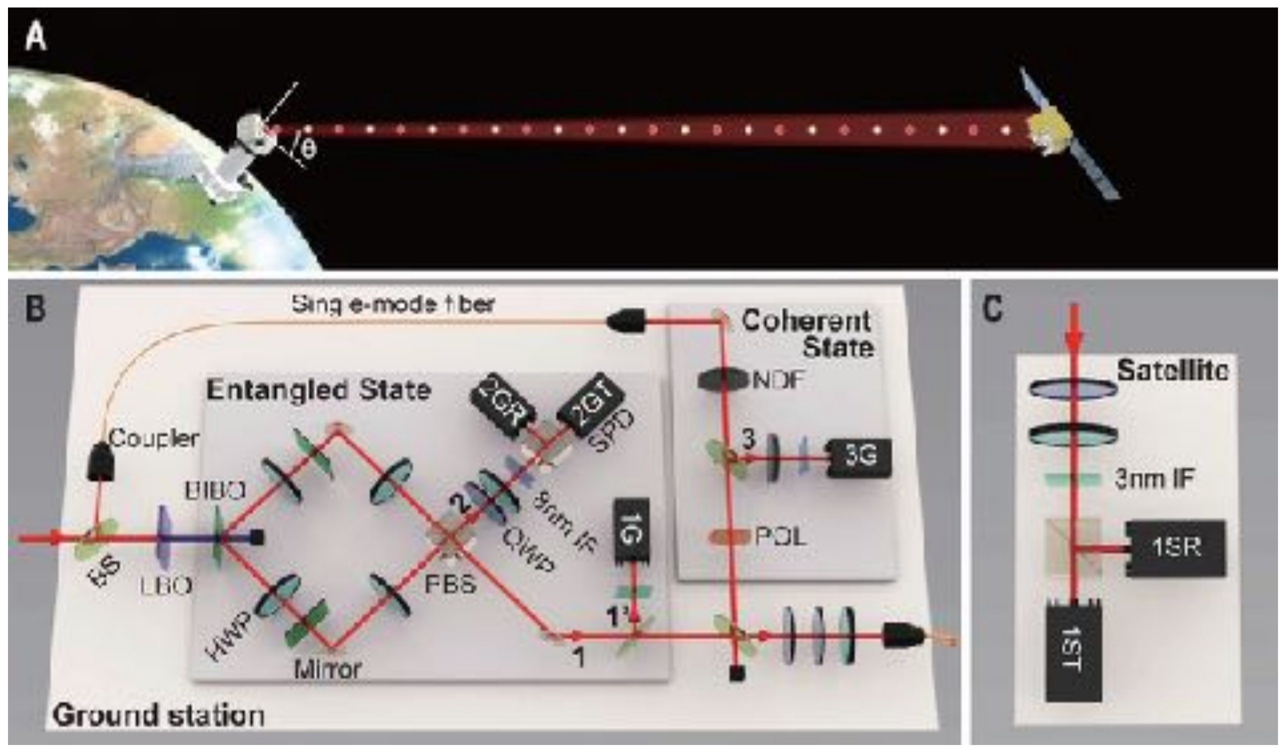
D. Rideout et al. Fundamental quantum optics experiments conceivable with satellites—reaching relativistic distances and velocities. Class. Quantum Gravity 29, 224011 (2012).
NASA L. Mazzarella et al. Deep Space Quantum Link (DSQL) mission concept Proc. SPIE 11835, 118350J (2021)
J. S. Sidhu et al. Advances in space quantum communications. IET Quantum Commun. qtc2.12015 (2021)

CAS: Satellite testing of a gravitationally induced quantum decoherence model

a pair of time-energy entangled photons are generated at a ground station. One photon of the pair is detected at the ground station and its entangled twin is sent to and detected at a satellite orbiting around Earth. **Event formalism predicts that in this setting the initially time-energy entangled pair of photons probabilistically decorrelate in time, which is different from the predictions of standard quantum theory**.

Observationally, the decoherence effect predicted by the event formalism will be the sum of these two effects. The probability of losing the time-energy entanglement, P , is characterized by the decorrelation factor, D , with D = 1 –P .





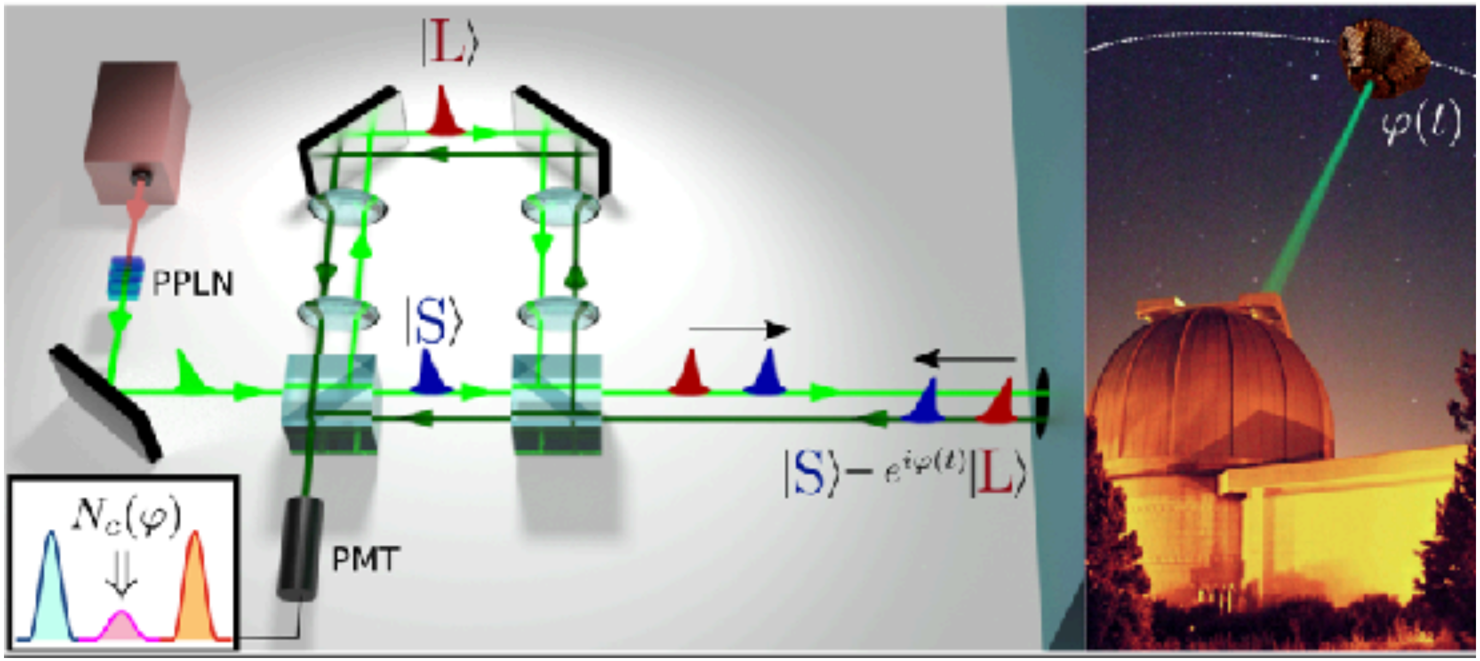
We then conclude that our experimental results are consistent with the descriptions of standard quantum theory and do not support the predictions of event formalism.

P. Xu *et al.*, *Science* 10.1126/science.aay5820 (2019)

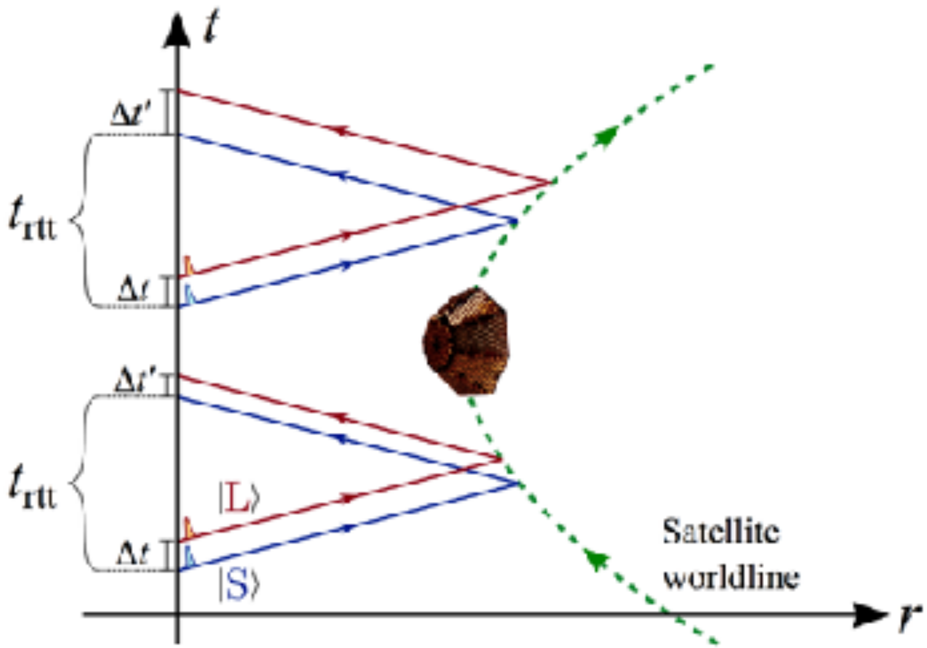
beyond polarization coding

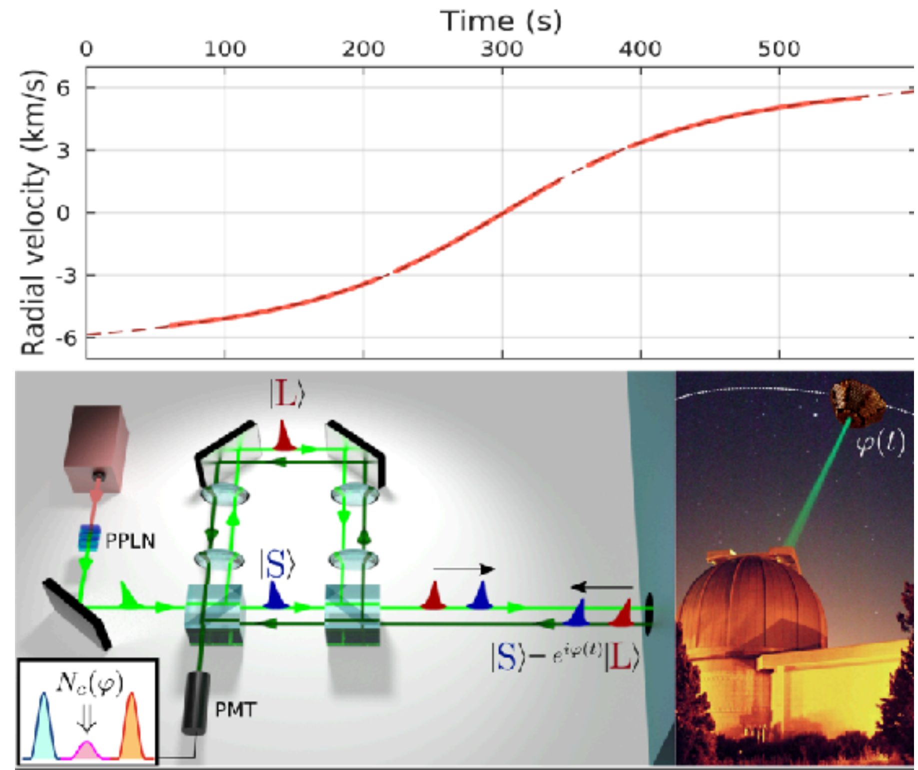
- Quantum interference arising from superposition of states is a striking evidence of the validity of Quantum Mechanics, for all DOF, confirmed in many experiments and also exploited in applications.

- single-photon interference at a ground station due to the coherent superposition of two temporal modes propagating to a satellite and back



returning qubit is modulated by a kinematic phase, sat-dependent





G. Vallone et al. Interference at the Single Photon Level Along Satellite-Ground Channels Physical Review Letters 116 253601 (2016) arXiv:1509.07855 (2015)

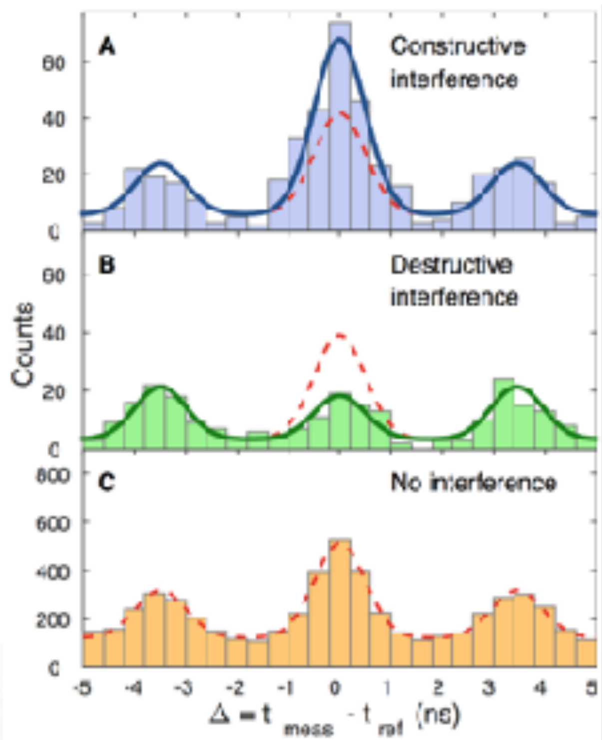
special relativistic derivation of the phase

- Special Relativity transformations to the CCR reference system and back, depending on β(t) = vr(t)/c.

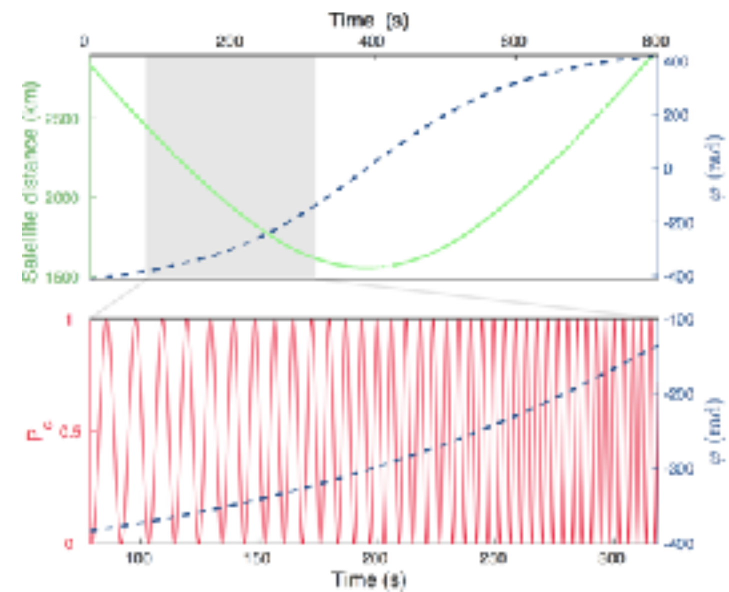
$$|\Psi_r\rangle = (1/\sqrt{2})(|S\rangle - e^{i\varphi(t)}|L\rangle)$$

- P_C probability of detecting the photon in the central peak

$$P_c(t) = \frac{1}{2}[1 - \mathcal{V}(t)\cos\varphi(t)]$$



$$\varphi(t) = \frac{2\beta(t)}{1+\beta(t)}\frac{2\pi c}{\lambda}\Delta t$$

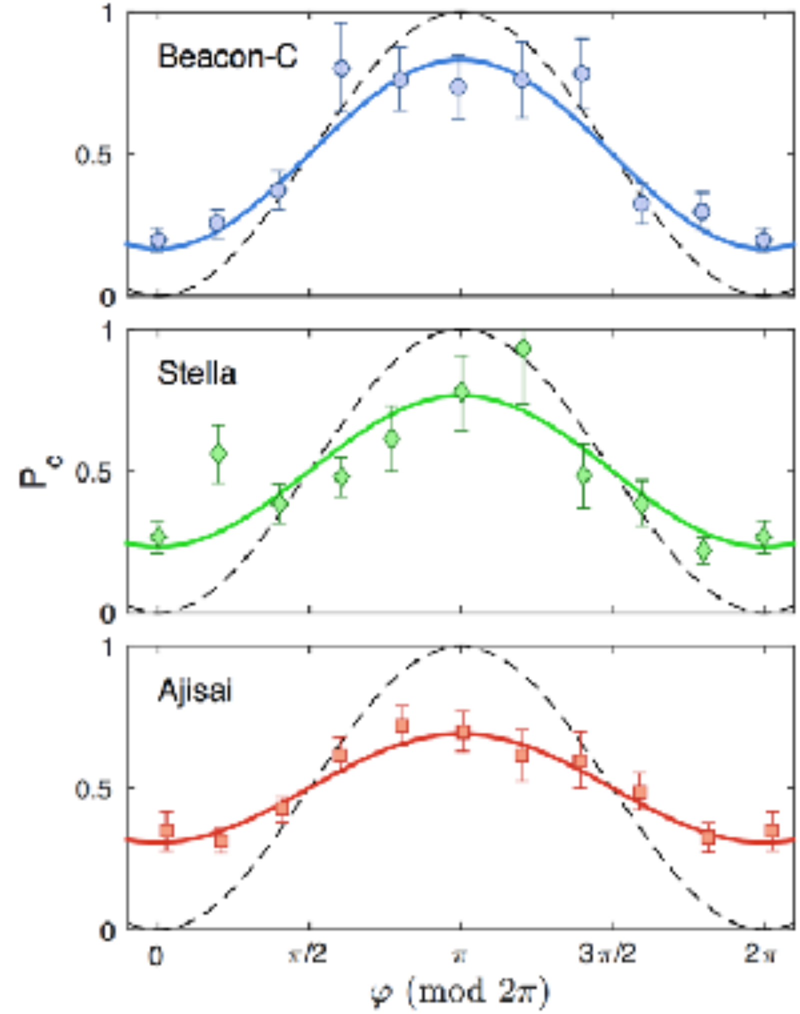


G. Vallone et al. Interference at the Single Photon Level Along Satellite-Ground Channels Physical Review Letters 116 253601 (2016) arXiv:1509.07855 (2015)

interference from the superposition visible with different satellites

V_{exp}=67±11% for Beacon-C

slanted distance 2500 km

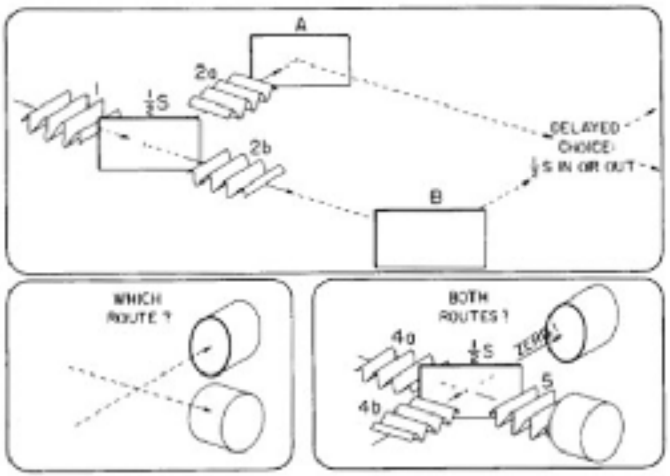


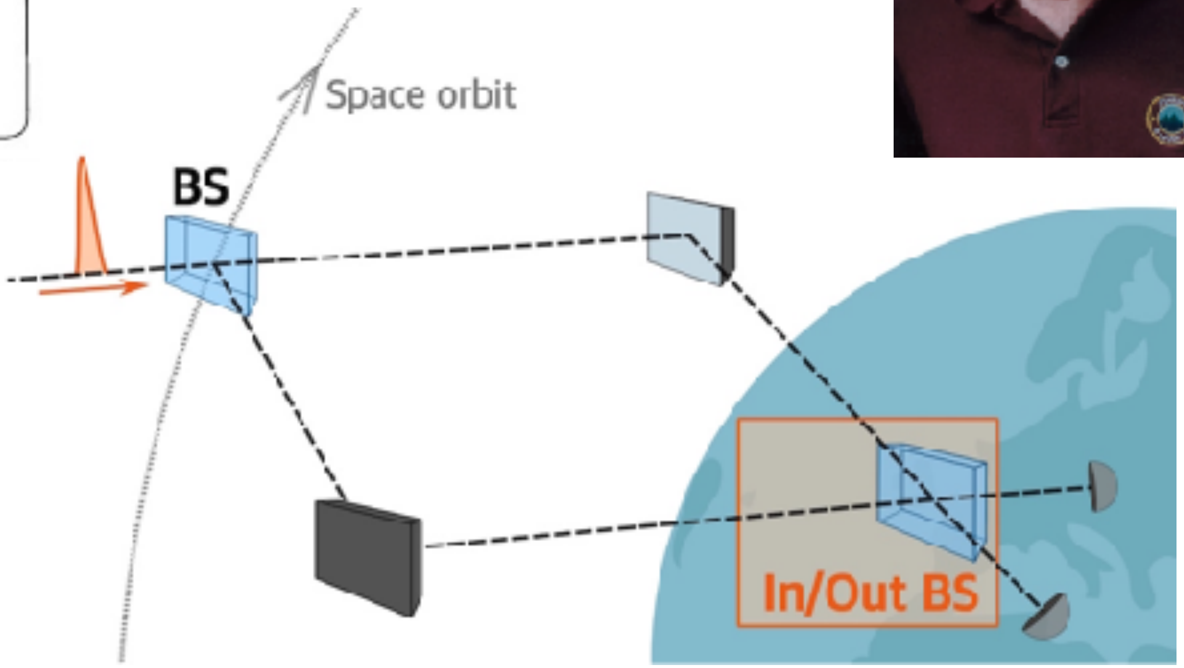
G. Vallone et al. Interference at the Single Photon Level Along Satellite-Ground Channels Physical Review Letters 116 253601 (2016) arXiv:1509.07855 (2015)

opportunity in combining pol and temp- qubits to extend the functions

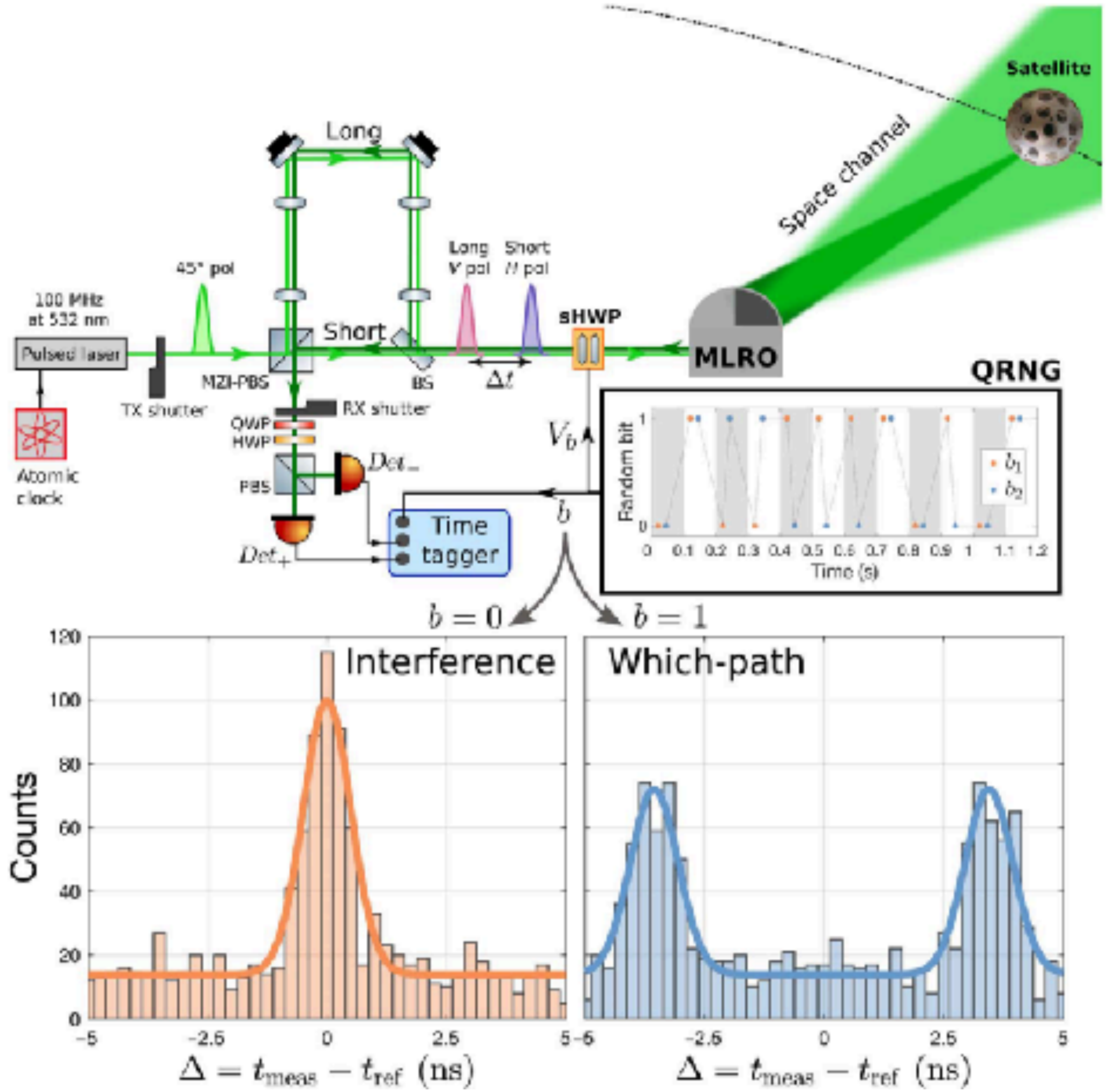
- suitable application in the space version of the John Wheeler Delayed-choice gedanken experiment
- wave-particle duality of quantum matter: impossibility of revealing at *the same time* both the wave-like and particle-like properties of a quantum object.
- Bohr: there is no difference "whether our plans of constructing or handling the instruments are fixed beforehand or whether we postpone the completion of our planning until a later moment"

Delayed-choice space experiment

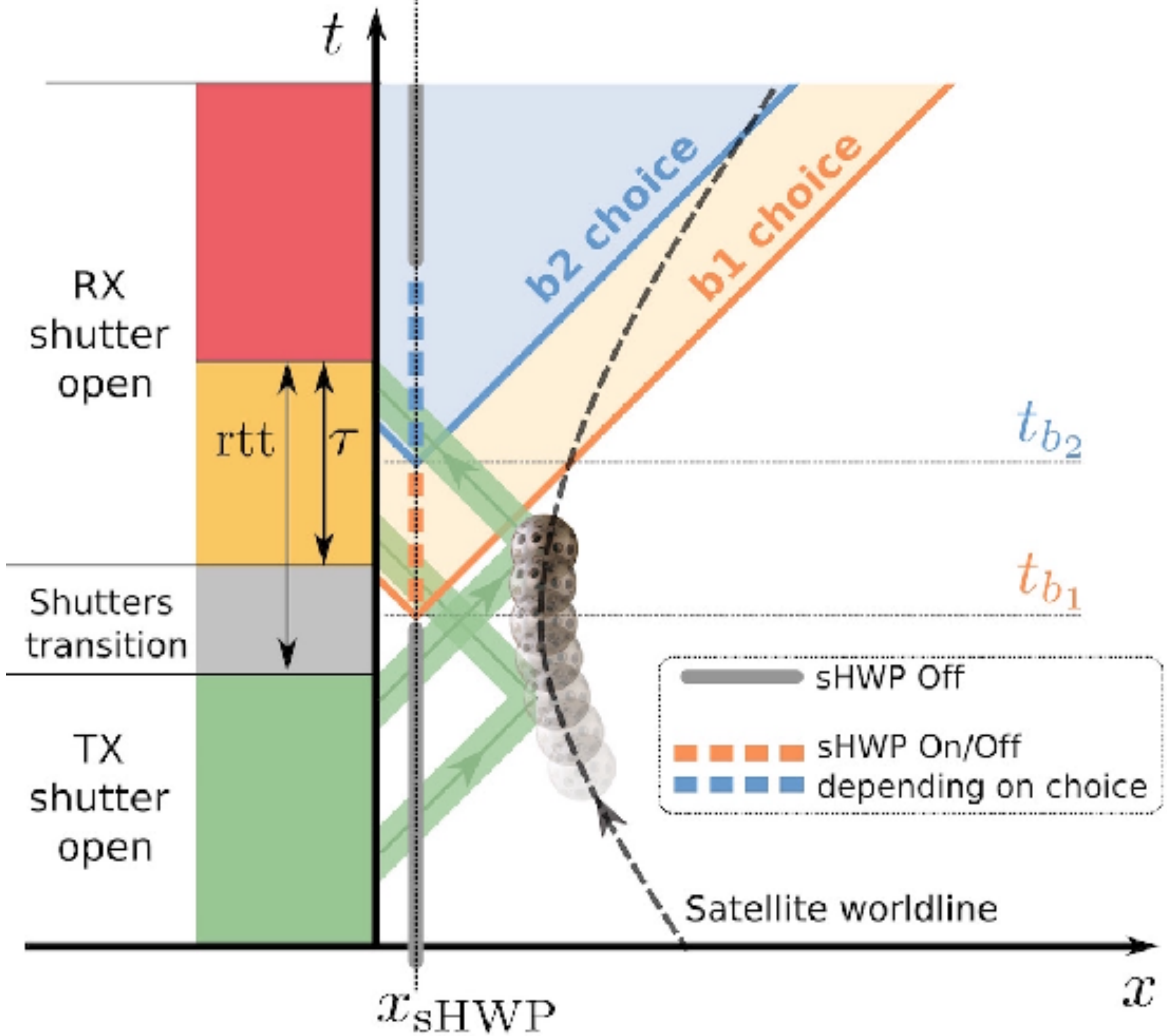




J.A. Wheeler **The “past” and the “delayed-choice” double-slit experiment**. Mathematical Foundations of Quantum Theory, Academic pp 9–48. (1978)



F. Vedovato et al. Extending Wheeler's delayed-choice experiment to space. Sci. Adv. 3, e1701180 (2017)



F. Vedovato et al. Extending Wheeler's delayed-choice experiment to space. Sci. Adv. 3, e1701180 (2017)

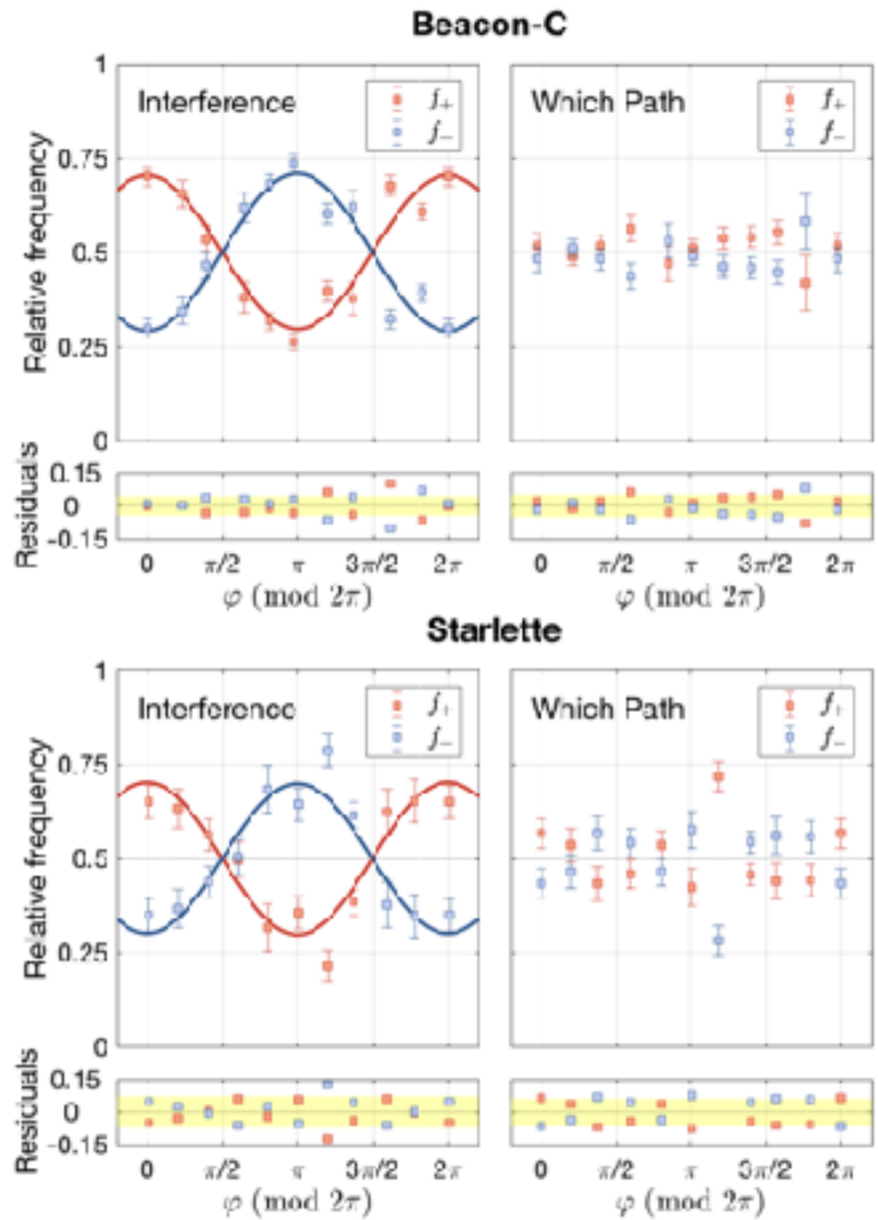
- wave-like: interference fringe visibility

$$f_{\pm}^{h=0} = \frac{N_{+}}{N_{+}+N_{-}}$$
$$\mathcal{V}^{\mathrm{Beacon-C}} = 41 \pm 4\%,$$
$$\mathcal{V}^{\mathrm{Starlette}} = 40 \pm 4\%$$

- particle-like: which-path information p_{wp} = 95 ± 1% (Starlette)

- ➔ excluding the objective viewpoint by 5σx

Our results extend the validity of the quantum mechanical description of complementarity to the spatial scale of LEO orbits (3500 km). Furthermore, they support the feasibility of efficient encoding by exploiting both polarization and time bin for high-dimensional free-space quantum key distribution over long distances



F. Vedovato et al. Extending Wheeler's delayed-choice experiment to space. Sci. Adv. 3, e1701180 (2017)

- wave-like

f

ν^{Bea}

ν^{Sta}

- particle-lik
95 ± 1% (S

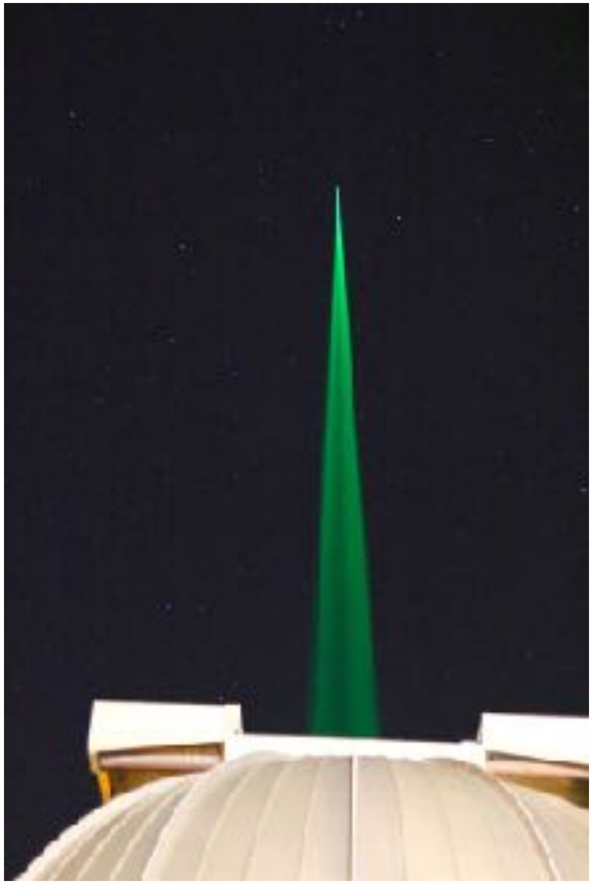
- ➔ excludi
5σx

Our results exter
mechanical de
spatial scale of
they support the
exploiting both
dimensional free
over long distan

F. Vedovato et al. Extending Wheeler's delayed-choice experiment to space. Sci. Adv. 3, e1701180 (2017)

conclusions

- the path to space QKD is clearly open and viable
- the growth and spreading of it depends on effective application demonstrations and concrete integrations with the ground networks
- so it's a crucial moment:
  - to act fast with IOVs
  - to propose concrete implementation solutions
  - to look ahead, to new uses and paradigm
- after all.. it's the most fundamental communication level ever conceived and at the largest possible scale!!



QuantumFuture on Space QComms and QRNG

FACULTY

P. Villoresi

G. Vallone

RtdA

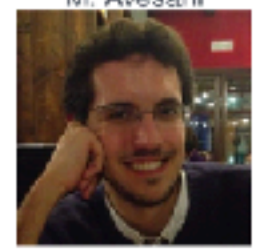
F. Vedovato

POST-DOC

C. Agnesi

M. Avesani

L. Calderaro



A. Stanco

New PhD students Elisa Bazzani and Matteo Padovan - we are hiring.. PhD Positions available!

PhD

A. Scriminich

G. Foletto

F. Picciariello

F. Santagiustina

F. Berra

T. Bertapelle

D. Scalcon

paolo.villoresi@dei.unipd.it
quantumfuture.dei.unipd.it
qtech.unipd.it
www.thinkquantum.com