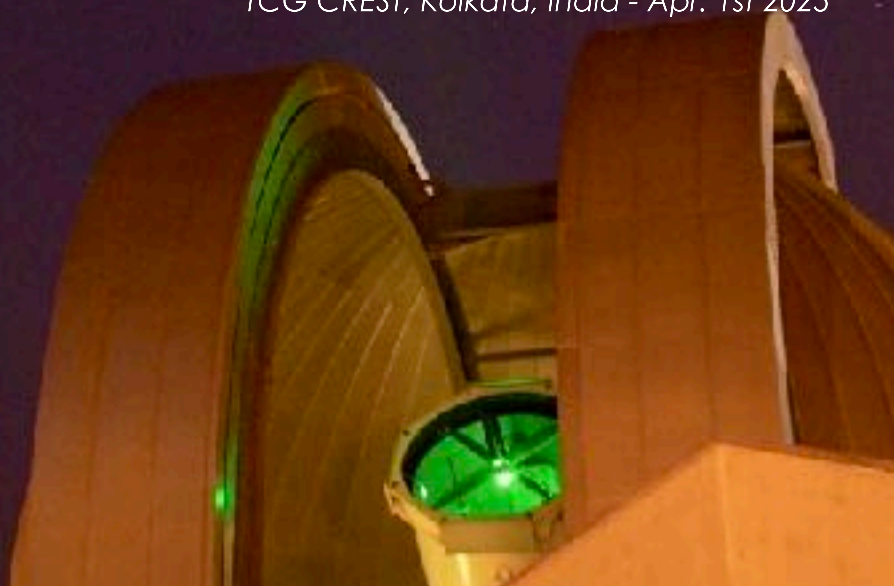
Quantum Communications developments on the ground and in space

Paolo Villoresi
QuantumFuture Research Group

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

International Year of Quantum Science & Technology (IYQ-2025)
International Symposium on Quantum Information and Quantum Communication
Centre for Quantum Engineering, Research, and Education (CQuERE),
TCG CREST, Kolkata, India - Apr. 1st 2025

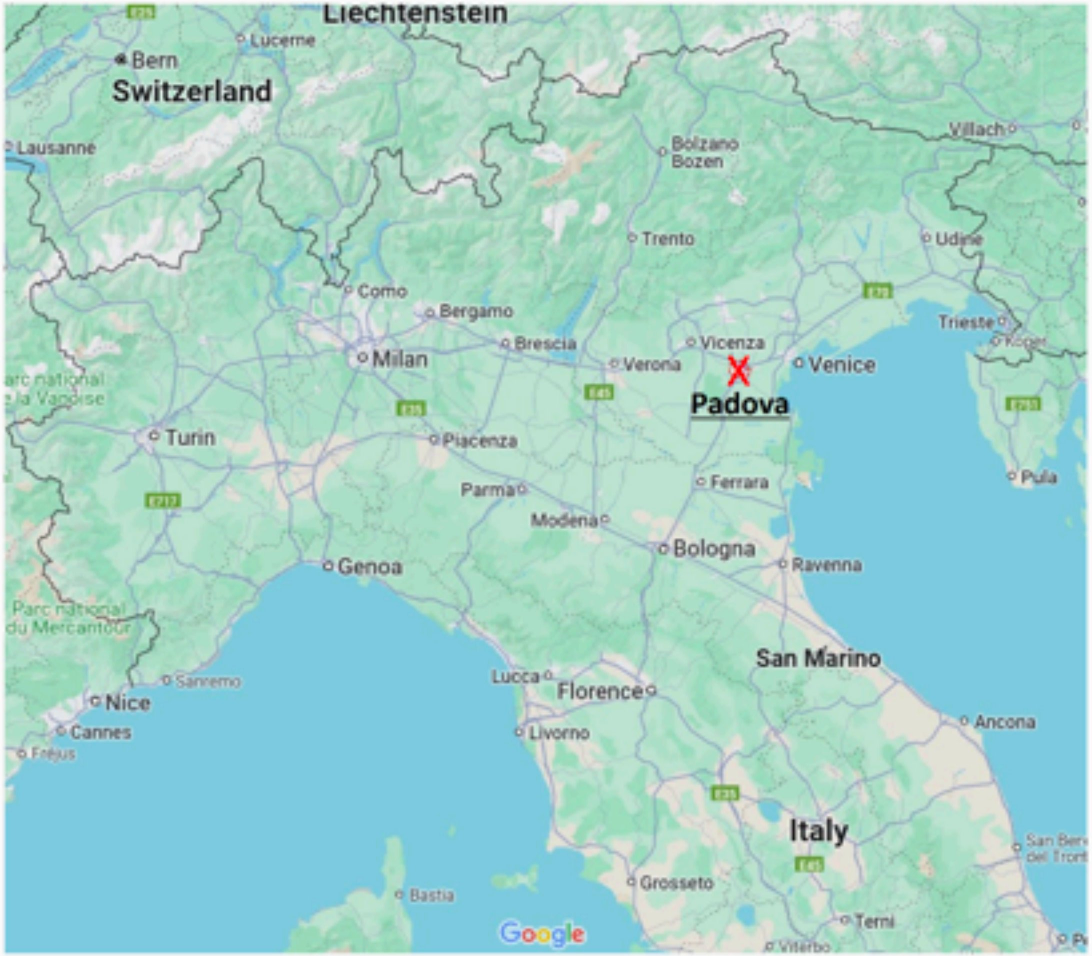


1222 · 2022 800 ANNI

Università degli Studi di Padova

PADUA Q TECH

Padua and its University, since 1222



Padua Quantum Technologies Research Center

PADUA QTECH

QTech primary objective is the **research in the field of quantum sciences** and the **deepening and dissemination of quantum technologies** in the field of computation, simulations, communications and information:
- promote, support and coordinate **research and teaching activities aimed at the study of quantum technologies;**
- to provide for the communication, integration and development of knowledge between **scholars of different scientific backgrounds**;
- acquire and manage **resources** to be used for the purposes of **research activities of specific interest to the Center.**

Director Paolo Villoresi (DEI),
ViceDirector Simone Montangero (DFA)
Executive Board: Director, ViceDirector, Giulio Giusteri (Math), Gaudenzio Meneghesso Director DEI, Flavio Seno Director DFA Physics, Bruno Chiarellotto Director Mathematics, Stefano Mammi Director DiSC Chemistry

about this talk

Some examples about the “advancements”

Novel techniques

Experiments on QM in space

EU perspectives

sharing quantum states

- when an elementary state of the microcosmos, a quantum state, is prepared with the purpose of its transmission for implementing a protocol, we have quantum communications.
- it is the most fundamental form of communication

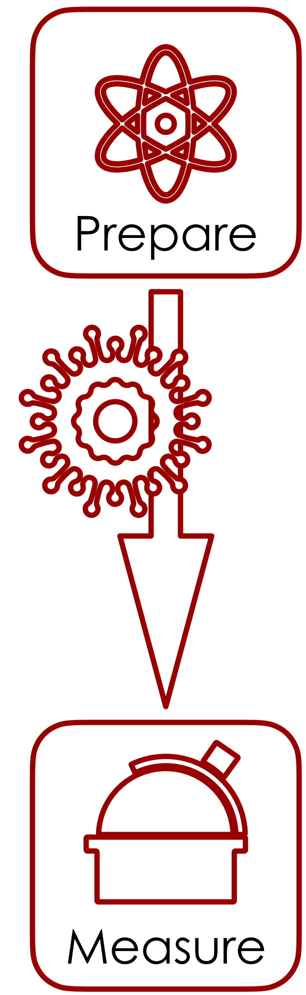
sharing quantum states

- the quantum channel is designed to protect the transmission
- however it also gives the opportunity to probe or exploit with the quantum state some interesting characteristics, as relativistic transformations or invariances

QComms are based on protocols

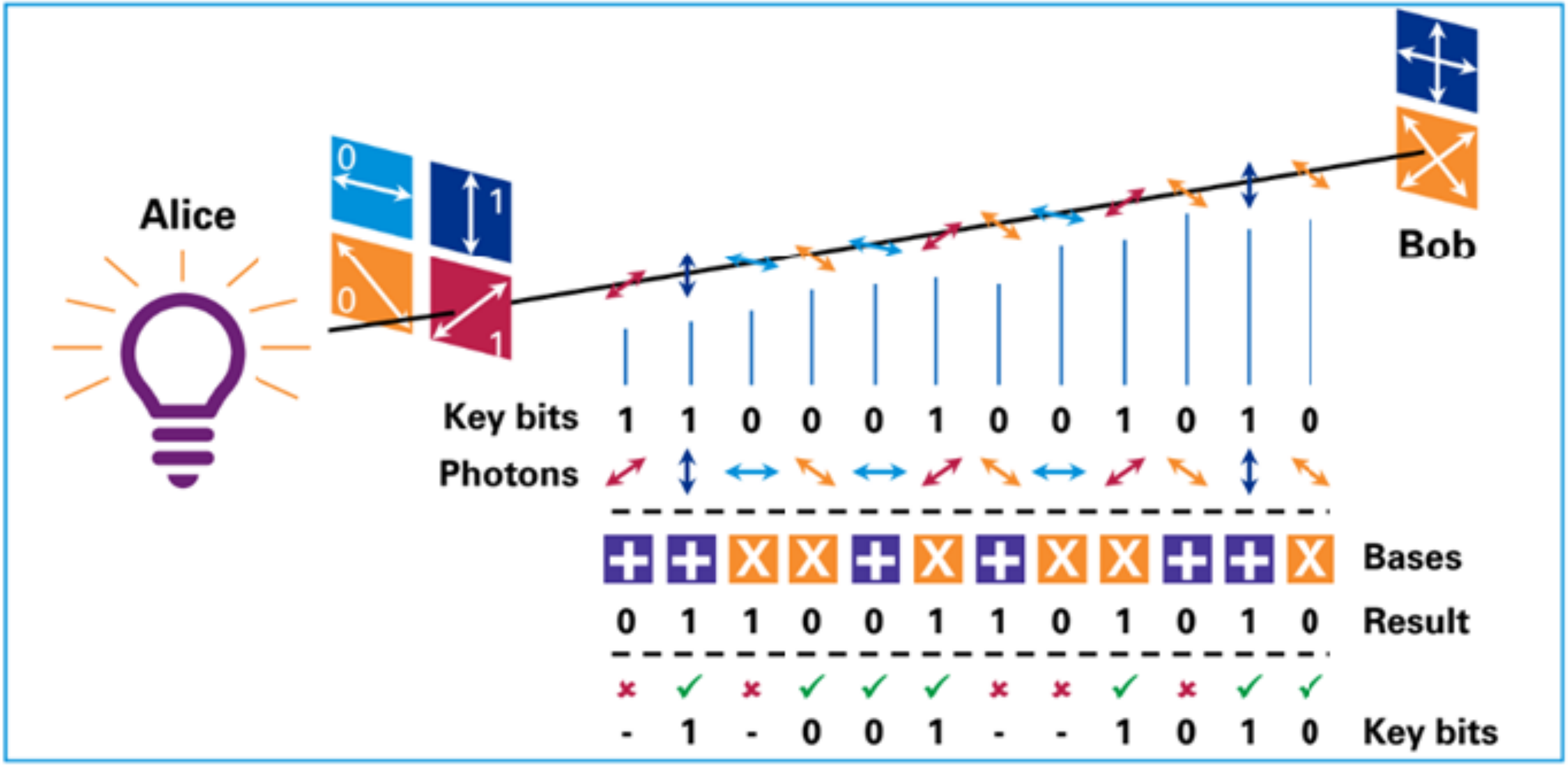
take for instance a generic "**prepare and measure" QKD protocol**:

- two main steps: **quantum communication followed by classical postprocessing**.
- During QComms, the sender (Alice) **encodes instances of a random classical variable a** into **nonorthogonal quantum states**.
- These states are **sent over a quantum channel** (optical fiber, free-space link)
- the channel is generally considered **under the control of an eavesdropper (Eve)**, who tries to steal the encoded information.
- The **linearity of quantum mechanics forbids the performance of perfect cloning**.
- Therefore **Eve can only get partial information** while disturbing the quantum signals.
- At the output of the communication channel, the **receiver (Bob) measures the incoming signals and obtains a random classical variable β.**
- **After a number of uses of the channel**, Alice and Bob **share raw data described by two correlated variables a and β.**



Pirandola et al Advances in quantum cryptography aop-12-4-1012 (2020)

QComms are based on protocols

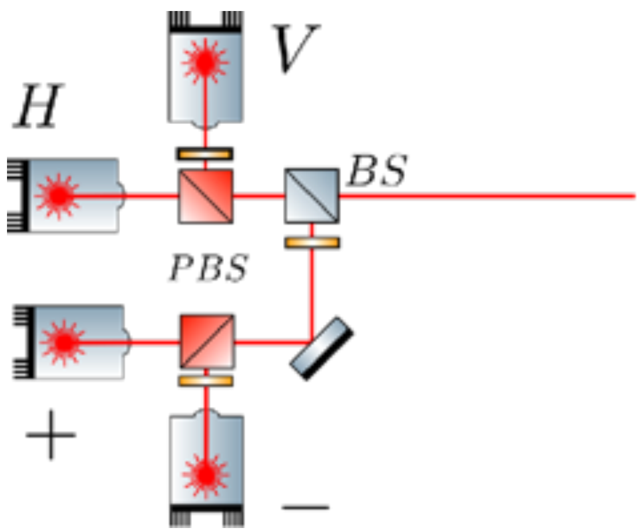


Bennett-Brassard 1984

Encoding				Decoding
basis	bit	state	Eve	after sifting
Z	$\begin{matrix} 0 \\ 1 \end{matrix}$	$\begin{matrix} \lvert 0\rangle \\ \lvert 1\rangle \end{matrix}$	$\nearrow \; Z\left\{\begin{matrix} \lvert 0\rangle \\ \lvert 1\rangle \end{matrix}\right. \longrightarrow$	$Z\left\{\begin{matrix} 0 \\ 1 \end{matrix}\right.$
			$\searrow \; X\left\{\begin{matrix} \lvert +,-\rangle \\ \lvert +,-\rangle \end{matrix}\right. \longrightarrow$	$Z\left\{\begin{matrix} ? \\ ? \end{matrix}\right.$
X	$\begin{matrix} 0 \\ 1 \end{matrix}$	$\begin{matrix} \lvert +\rangle \\ \lvert -\rangle \end{matrix}$	$\nearrow \; Z\left\{\begin{matrix} \lvert 0,1\rangle \\ \lvert 0,1\rangle \end{matrix}\right. \longrightarrow$	$X\left\{\begin{matrix} ? \\ ? \end{matrix}\right.$
			$\searrow \; X\left\{\begin{matrix} \lvert +\rangle \\ \lvert -\rangle \end{matrix}\right. \longrightarrow$	$X\left\{\begin{matrix} 0 \\ 1 \end{matrix}\right.$

initial QComms implementations required ideal encoder specs

example: discrete-variable polarization encoder based on multiple laser sources

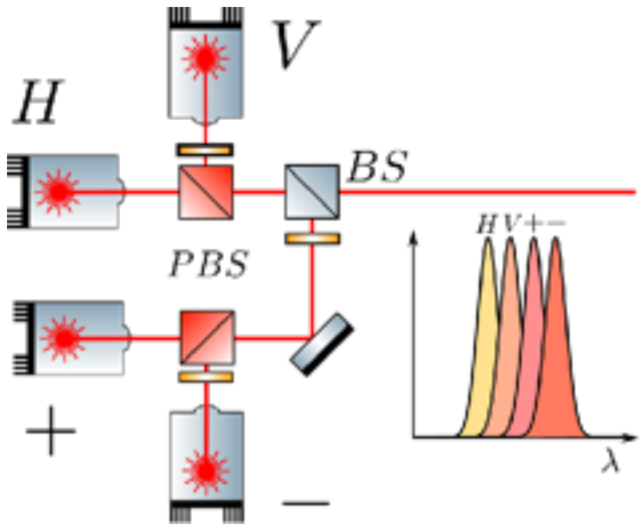


sequence of H V + - states

the only difference is the polarization orientation

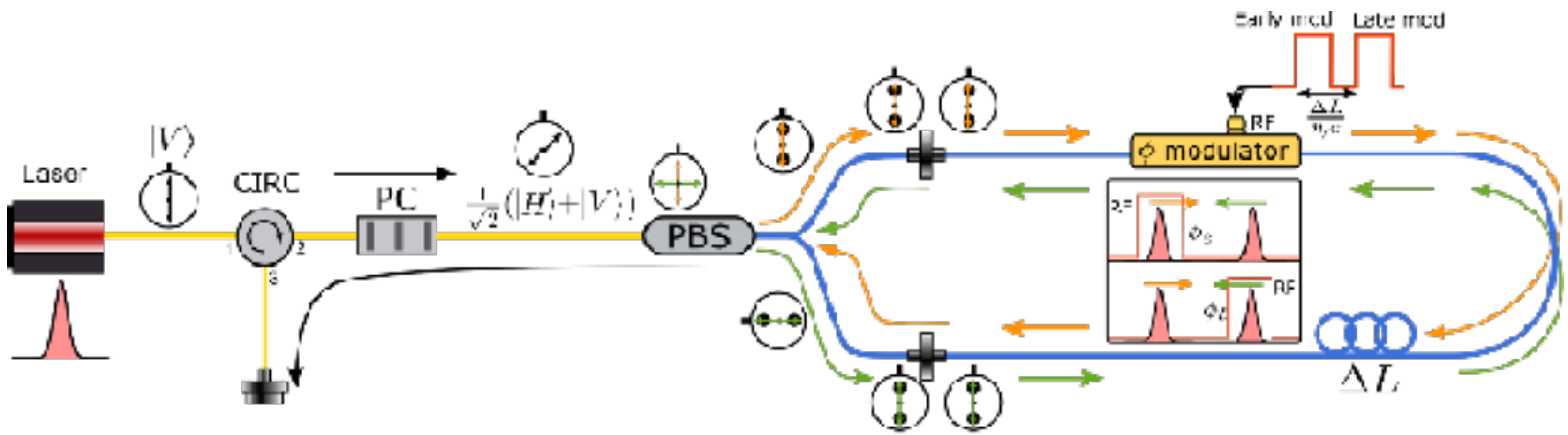
implementation non-idealities may be exploited by Eve

example: discrete-variable polarization encoder based on multiple laser sources



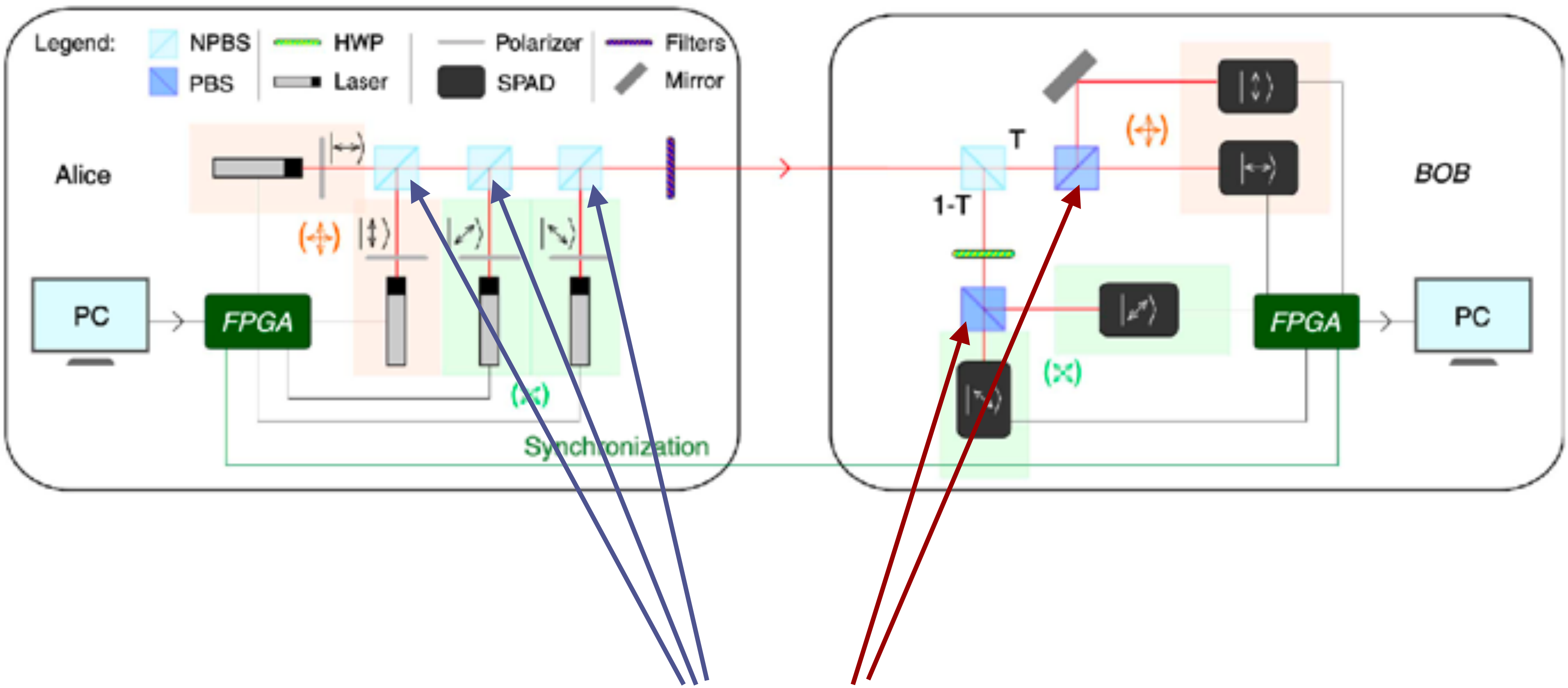
possible hacking due to mismatched spectra

novel schemes remove the issues



C. Agnesi et al. All-fiber self-compensating polarization encoder for quantum key distribution, Opt. Lett. 44 2398 (2019)

initial QComms implementations required very precise agreement on the Q-bases

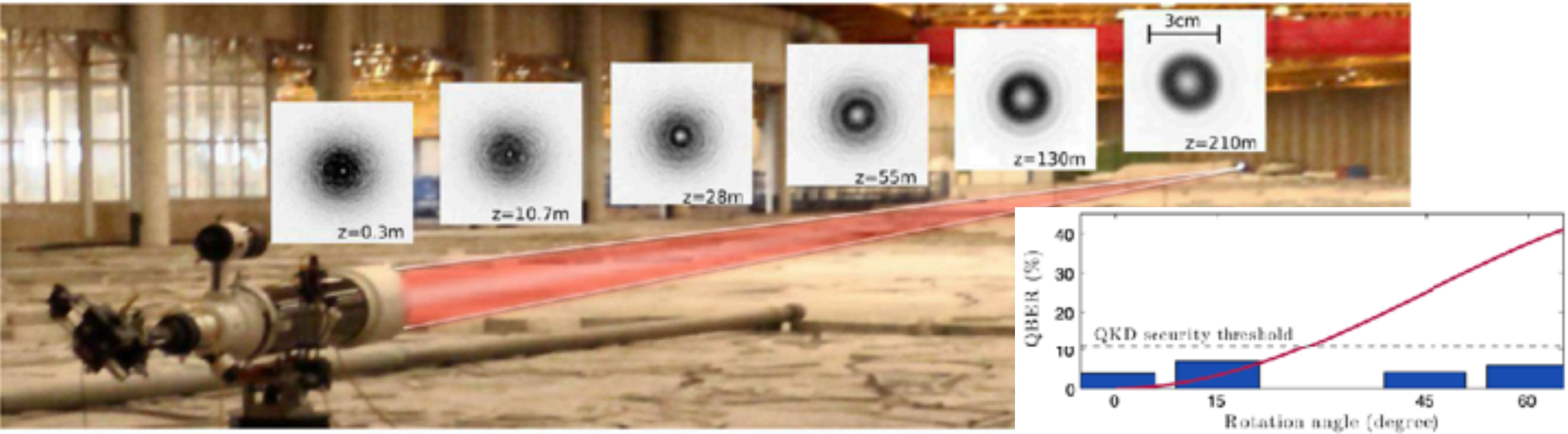


matching orientation

if one terminal rotates wrt the other, QBER rises

Bacco, D. et al. Experimental quantum key distribution with finite-key security analysis for noisy channels. Nat. Commun. 4:2363 (2013)

with a extra DoF - OAM - the rotation is allowed without rise on QBER



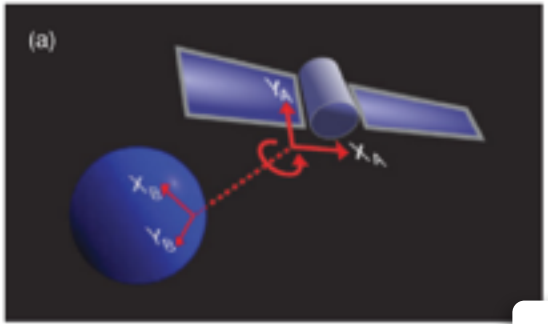
G. Vallone et al. Free-Space Quantum Key Distribution by Rotation-Invariant Twisted Photons, PRL 113, 060503 (2014)

Reference-frame-independent schemes to simplify QComms implementations

PHYSICAL REVIEW A 82, 012304 (2010)

Reference-frame-independent quantum key distribution

Anthony Laing,[1,*] Valerio Scarani,[2,3] John G. Rarity,[1,3] and Jeremy L. O'Brien[1,3]
[1]Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, BS8 1UB, United Kingdom
[2]Centre for Quantum Technologies and Department of Physics, National University of Singapore, Singapore
(Received 18 March 2010; published 7 July 2010)



Reference-Frame-Independent Quantum Key Distribution Using Fewer States

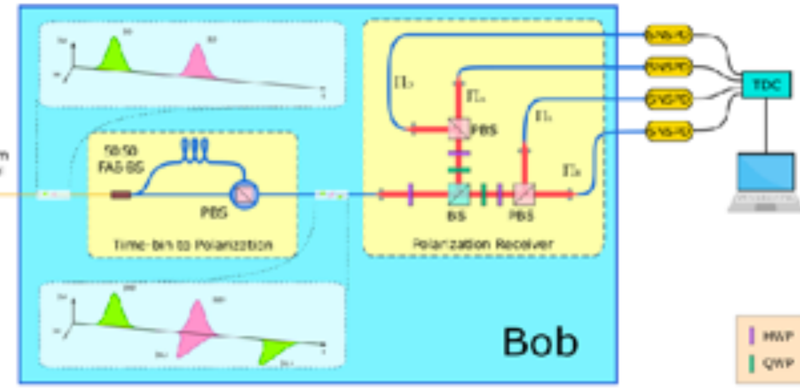
Hongwei Liu,[1,2,3,*] Jipeng Wang,[1,2,3] Haiqiang Ma,[1,†] and Shihai Sun[2,3,‡]
[1]School of Science and State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2]School of Physics and Astronomy, Sun Yat-Sen University, Zhuhai, Guangdong 519082, China
[3]College of Liberal Arts and Science, National University of Defense Technology, Changsha, Hunan 410073, China

Experimental Self-Characterization of Quantum Measurements

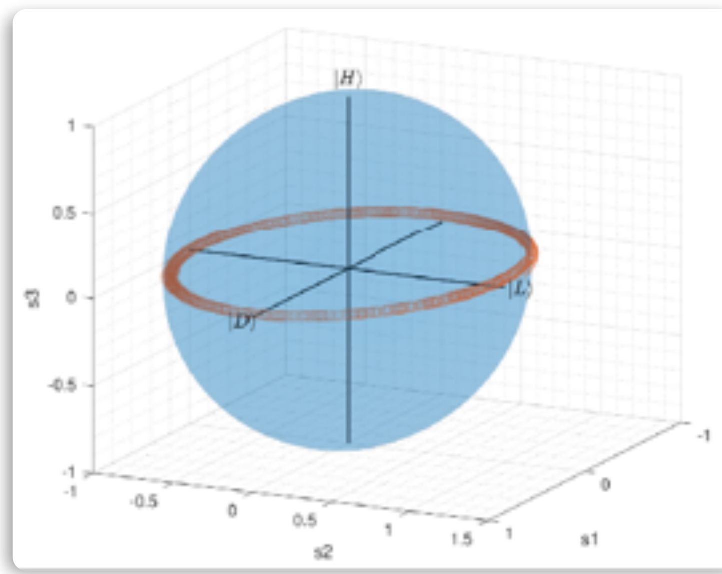
Aonan Zhang,[1,2,3] Jie Xie,[1,2,3] Huichao Xu,[1,2] Kaimin Zheng,[1,2] Han Zhang,[1,2] Yiu-Tung Poon,[3,4,5] Vlatko Vedral,[6,7,*] and Lijian Zhang[1,2,†]
[1]National Laboratory of Solid State Microstructures, Key Laboratory of Intelligent Optical Sensing and Manipulation (Ministry of Education), College of Engineering and Applied Sciences and School of Physics, Nanjing University, Nanjing 210093, China
[2]Collaborative Innovation Center of Advanced Microstructures, Nanjing University, Nanjing 210093, China
[3]Department of Mathematics, Iowa State University, Ames, Iowa 50011, USA
[4]Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China
[5]Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen, 518055, China
[6]Atomic and Laser Physics, Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, United Kingdom
[7]Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543, Singapore

Final numerical POVMs are computed by means of **dimensionality reduction** (principal component analysis) and **convex optimization** procedures, performed in post-processing

Passive and Self-Characterizing Cross-Encoded Receiver for reference-frame-independent QComms



- Allows to retrieve a realistic description of the measurement
  apparatus without performing a tomographic study
- The procedure is based on the reconstruction of the **accessible region of outcomes** at the disposal of the measurement device (**response range**)
- No precisely calibrated probe states are required
- Exploits the same photons used for security estimation (equatorial states)
- Final numerical POVMs are computed by means of **dimensionality reduction** (principal component analysis) and **convex optimization** procedures, performed in post-processing
- Send uncharacterized states in order to span the entire equator of the Bloch's sphere (X-Y bases)



M. Giacomin et al. A Passive and Self-Characterizing Cross-Encoded Receiver for Reference-Frame-Independent Quantum Key Distribution arxiv:2408.17304 (2024)

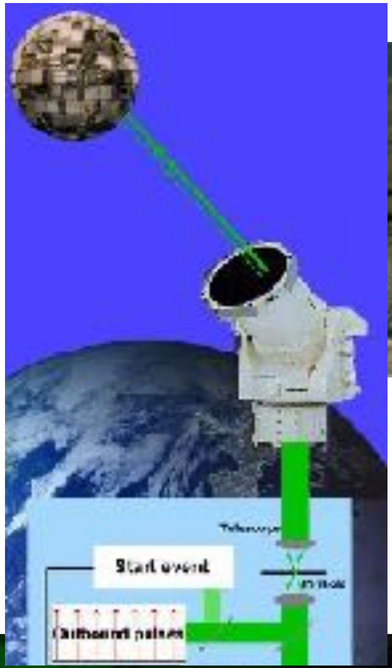
QComms venture along Space links

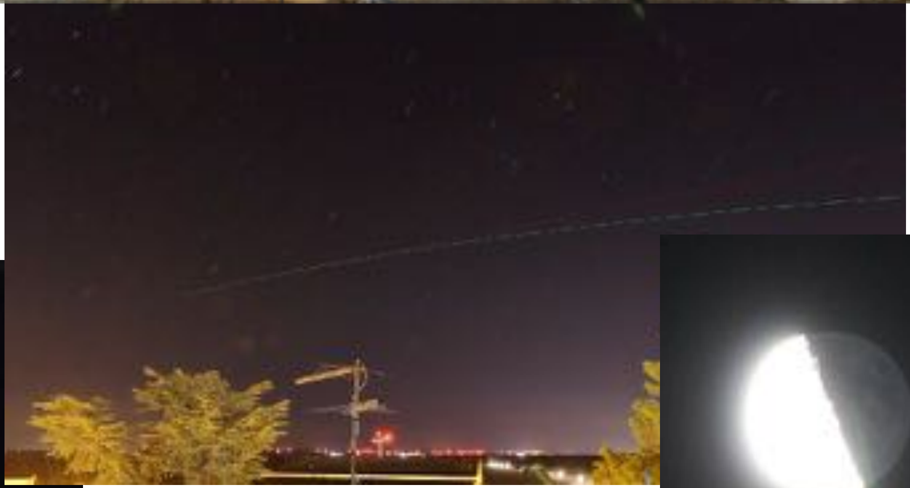
- QComms in Space are developing from
  - a scientific research subject in experimental Quantum Communications, and this still is going
  - in a phase for demonstrators of different realisations of protocols, as QKD,
  - to a technology for supporting cybersecurity at the planetary scale and beyond
- at present, strong support to space-QKD is provided by several Continents and Nations.
- Presently, the focus is on applications
- the scientific programs are needed but not well supported

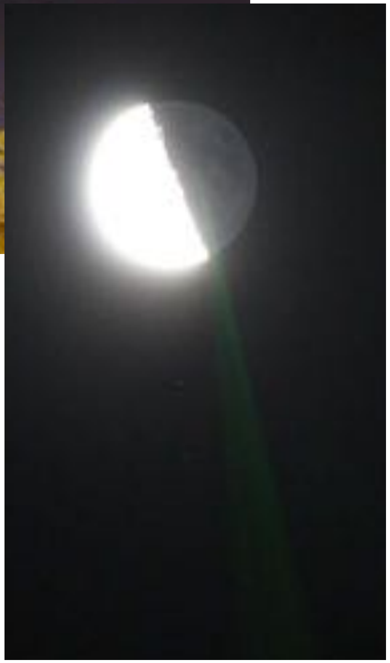
12756 km

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

Matera ASI-MLRO ground station







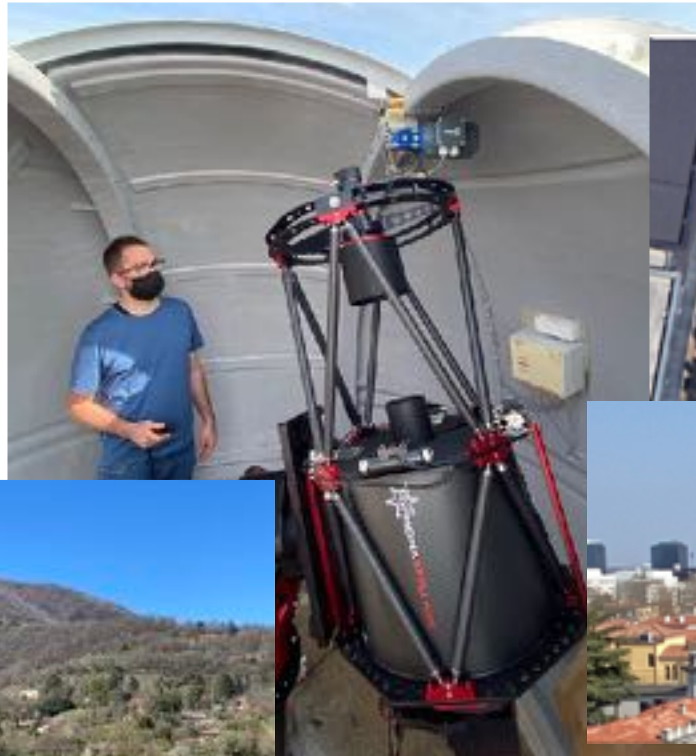
1.5 , telescope - Coudè - QComms since 2003

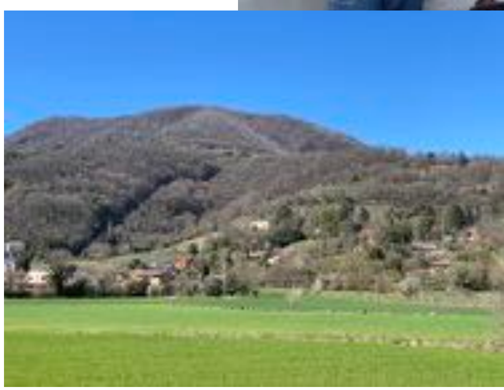
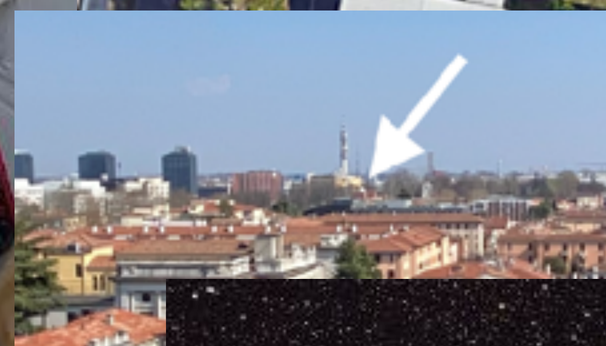
Lunar and satellite Laser Ranging facility - beacon - synch w atomic clock

polarization and timebin encoding - single photon exchange up to 20000 km

horizontal test path 10 km

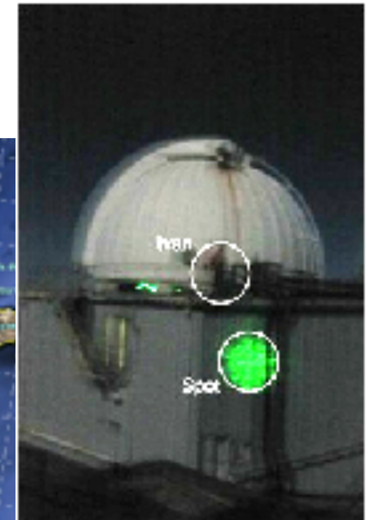
Padua GaliQEye ground station

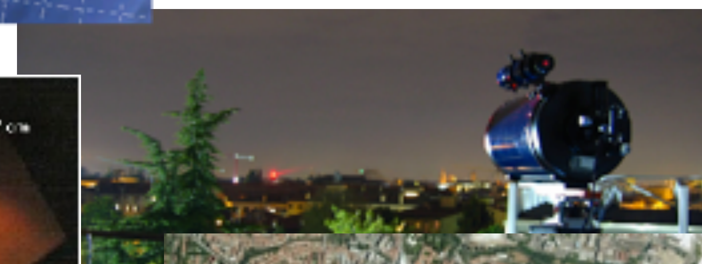


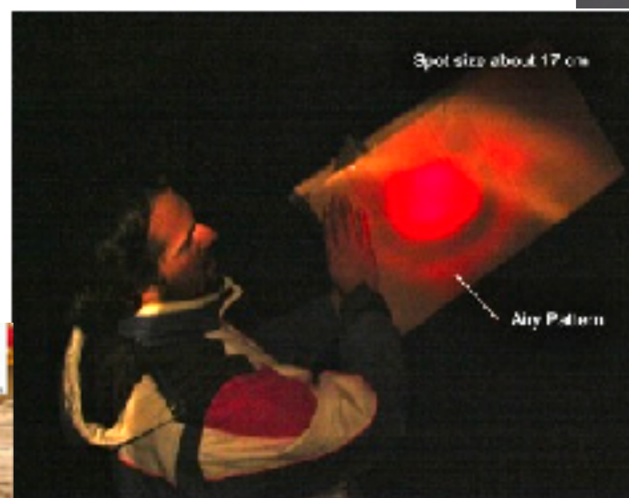



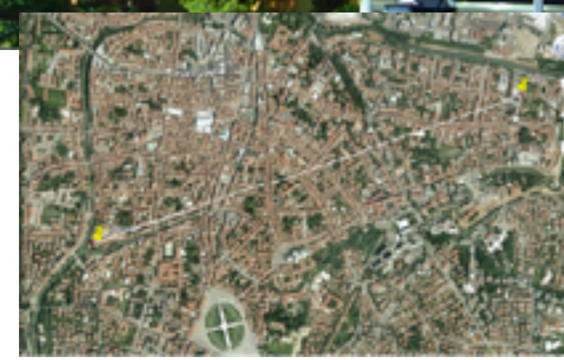
400 mm RC telescope with QKD receiver
tip tilt and adaptive optics 850 and 1550 nm
test links: city 600 m and sat simulation 18 km slanted
bundle of dark fibers to Padua MAN network and 16 SNSPD detectors

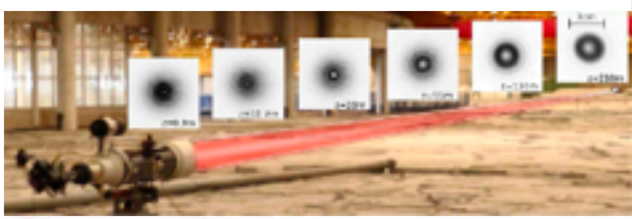
Horizontal links for QComms





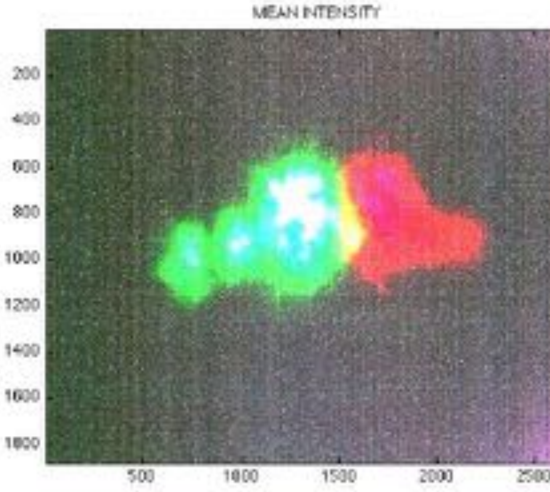




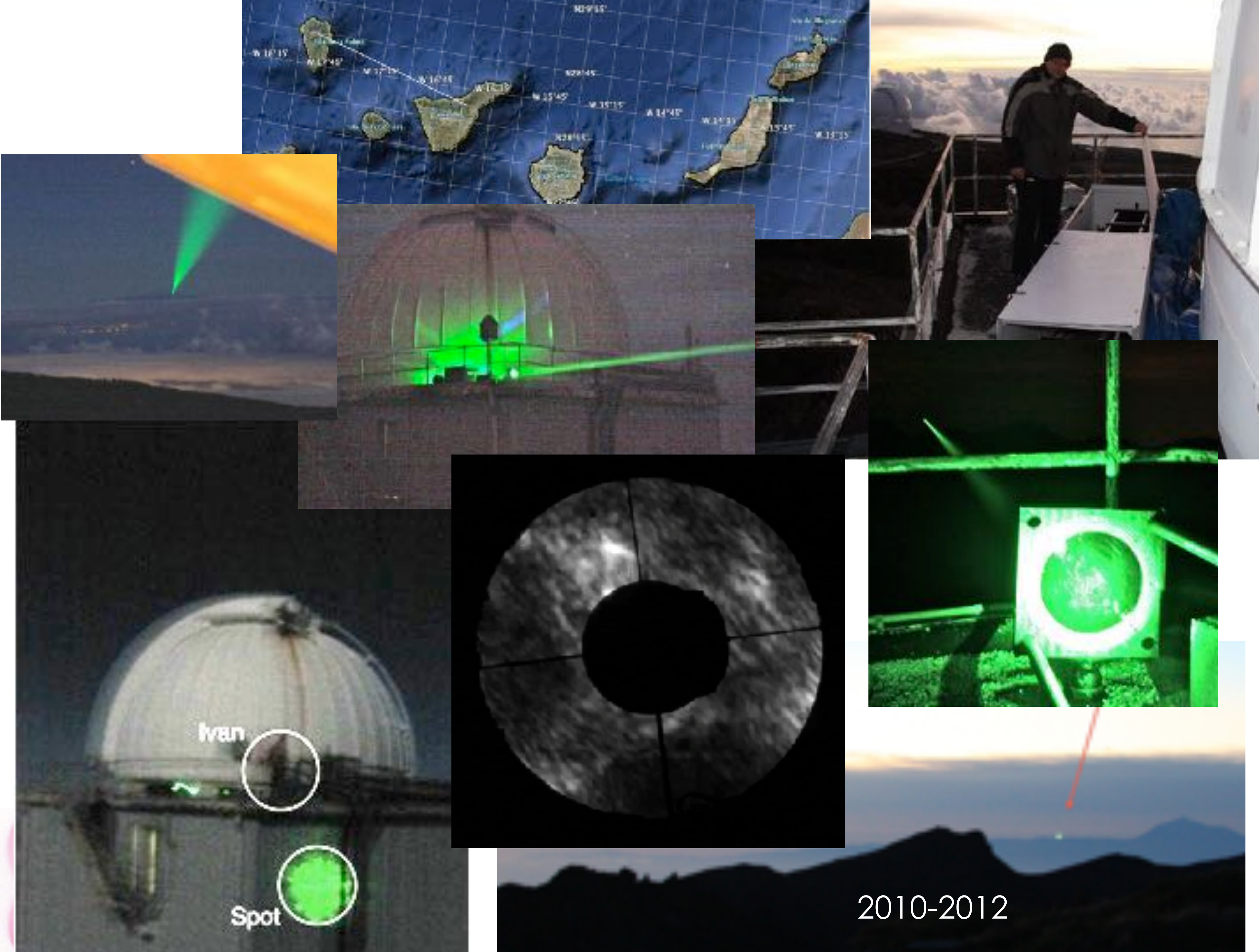


1. Capraro, I. et al. Impact of Turbulence in Long Range Quantum and Classical Communications. Phys. Rev. Lett. 109, 200502 (2012).
2. D. B., M Canale, M., Laurenti, N., Vallone, G. & Villoresi, P. Experimental quantum key distribution with finite-key security analysis for noisy channels. Nature Commun. 4, 2363 (2013).
3. Vallone, G. et al. Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels. Phys. Rev. A 91, 042320 (2015).
4. Vallone, G. et al. Free-Space Quantum Key Distribution by Rotation-Invariant Twisted Photons. Phys. Rev. Lett. 113, 060503 (2014).
5. Scriminich, A. et al. Optimal design and performance evaluation of free-space quantum key distribution systems. Quantum Sci. Technol. 7, 045029 (2022)

free-space quantum links in Asiago



2004-2010


Ivan
Spot
2010-2012

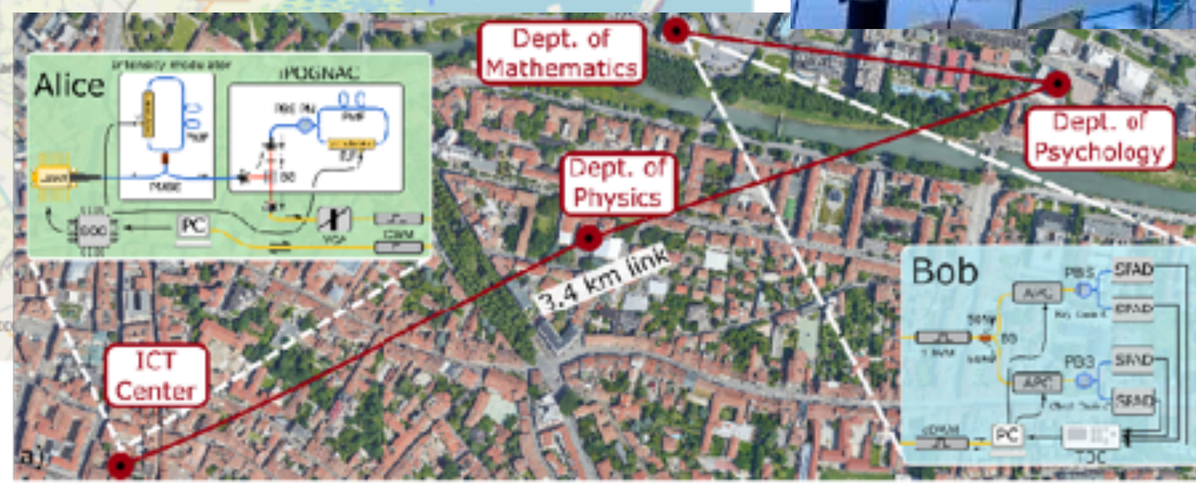
Ven-QCI

QSN PARTNERSHIP

Veneto Region quantum network

to be part of the Italian Backbone

serving governmental and infrastructures

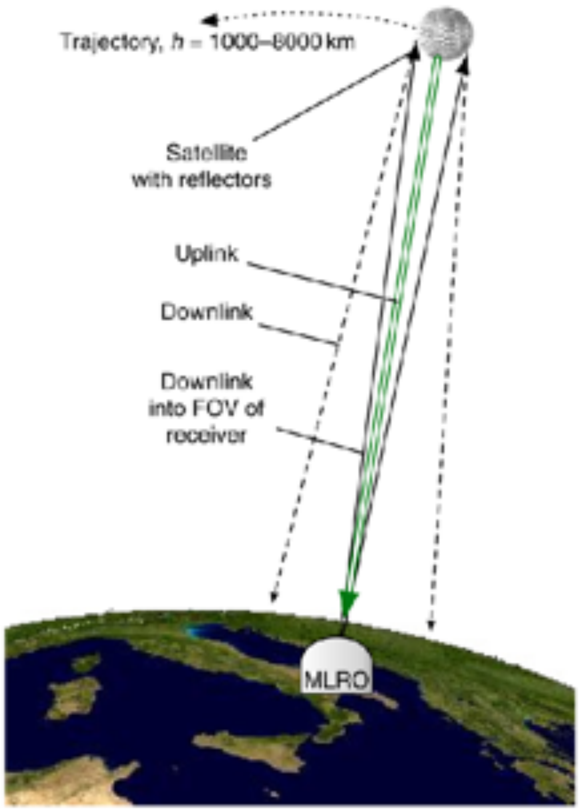


Italian, ESA and EU satellite projects

- Italian I-QKD satellite mission development, started in 2019
- ESA - SAGA PhA and PhB
- ESA - ARTES ground station development for QKD
- Horizon Europe missions and payload developments
- Marie Skłodowska-Curie Actions programmes
- Spinoff QKQ & QRNG ground and space

opening the space Q-channel

- UniPD funded project, started 2003-2008
- exploiting retroreflectors on orbiting satellite
- 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.



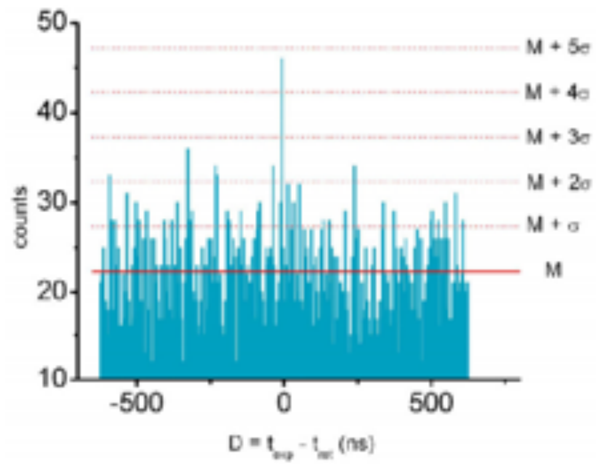
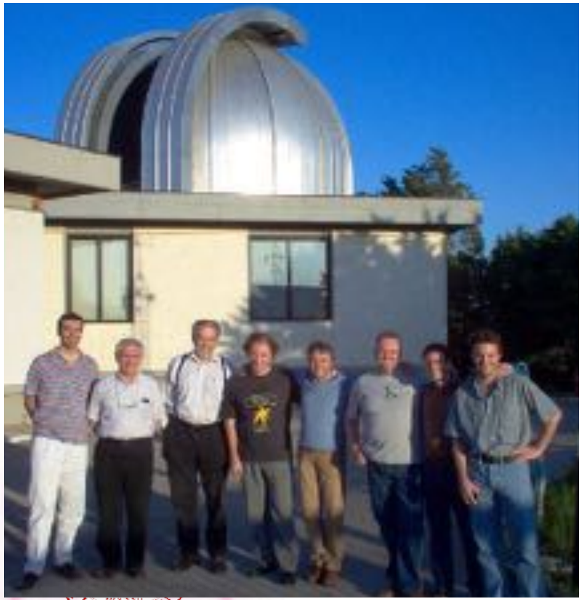


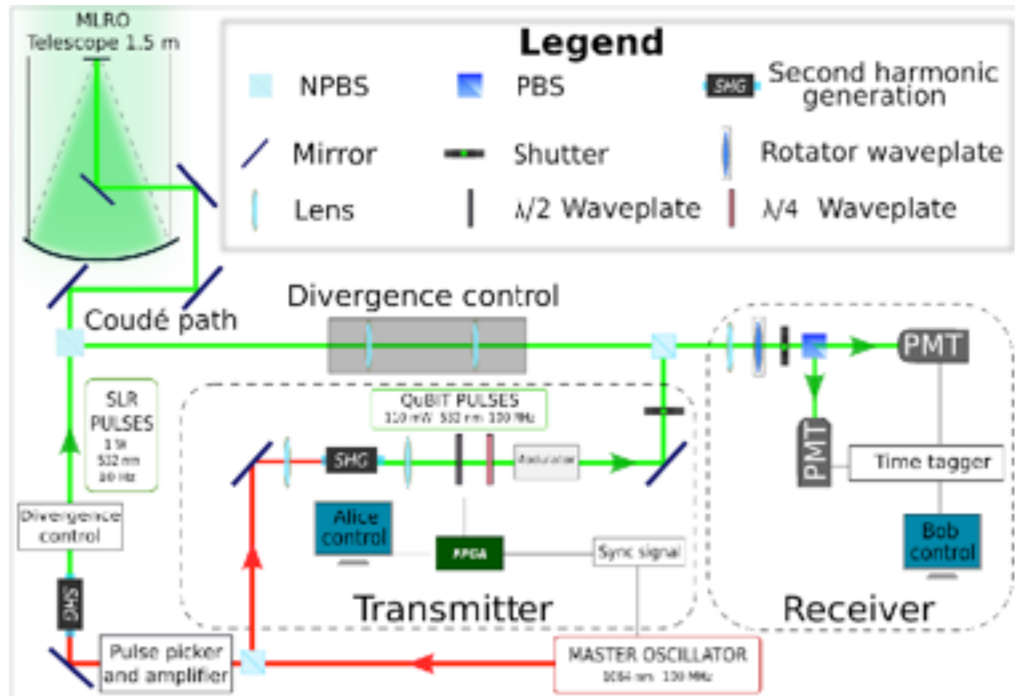
Figure 3. Histogram of the differences D between expected and observed detections for Ajisai satellite. The peak of the histogram is centered at $D = t_{exp} - t_{ret} = 0$ ns, as expected, and is larger than the mean value of the background counts by 4.5 standard deviations. The bin size is $\Delta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

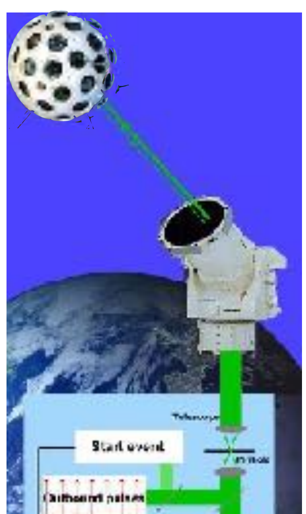


P. Villoresi et al. Experimental verification of the feasibility of a Q-channel between space and Earth. New J. Phys. 10, 033038 (2008)

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

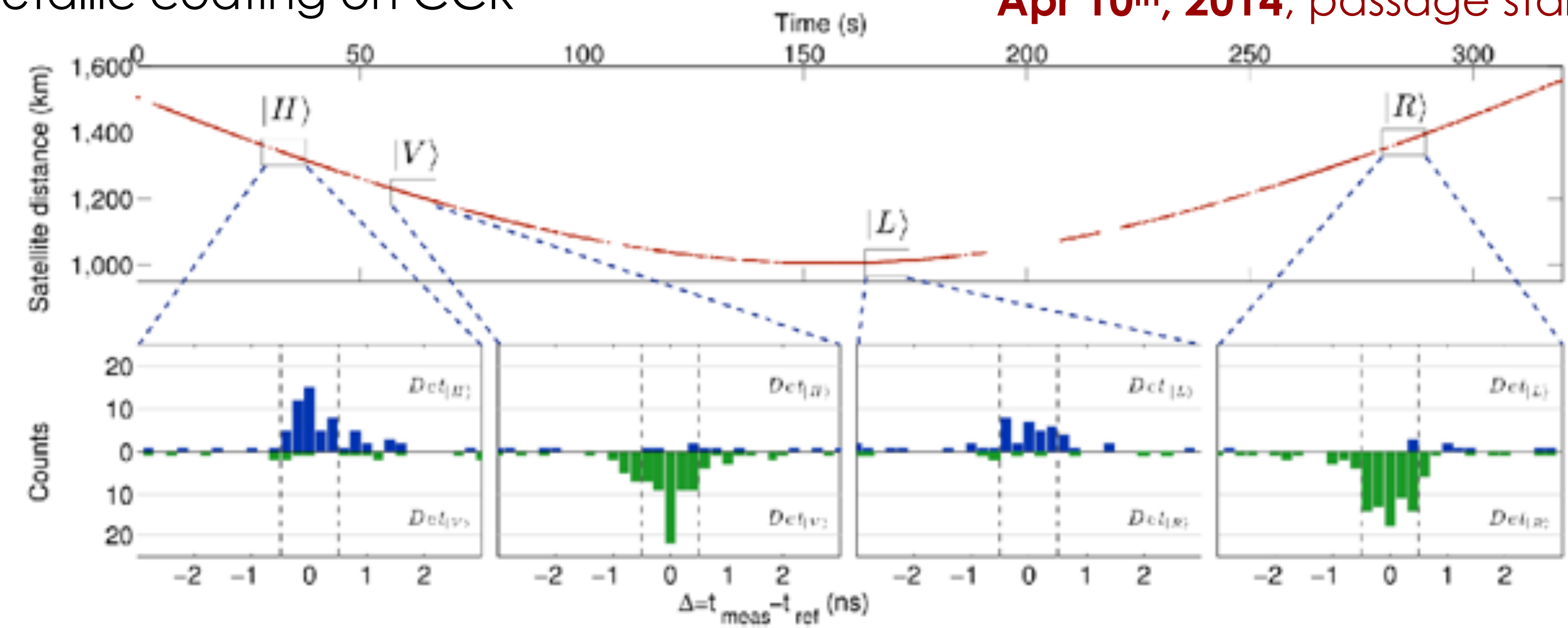




first results: LARETS

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

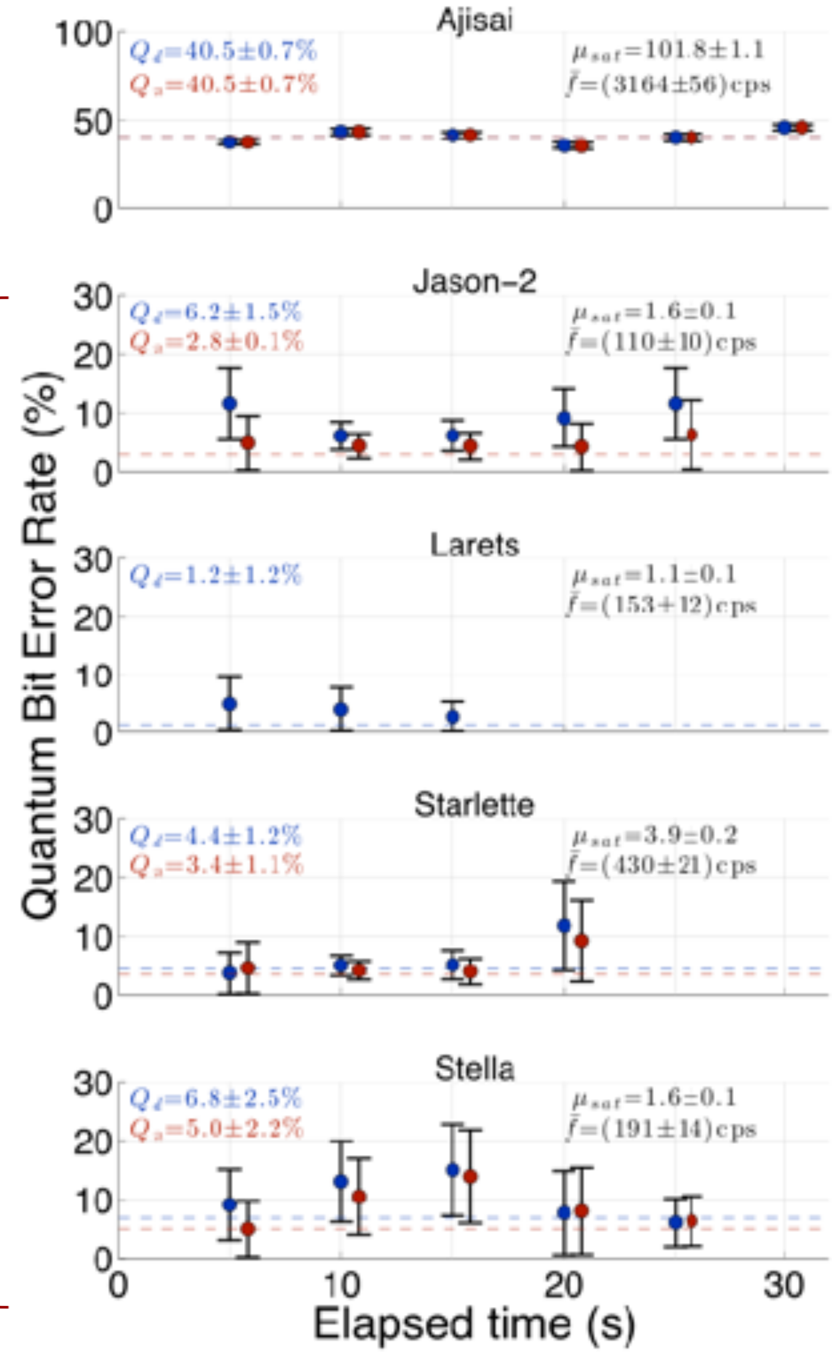
QBER

Non polarization maintaining CCR
Polarization QComms not possible

Polarization maintaining CCR

Polarization QComms with QBER compatible with applications

Demonstration of stable QBER over extended link duration



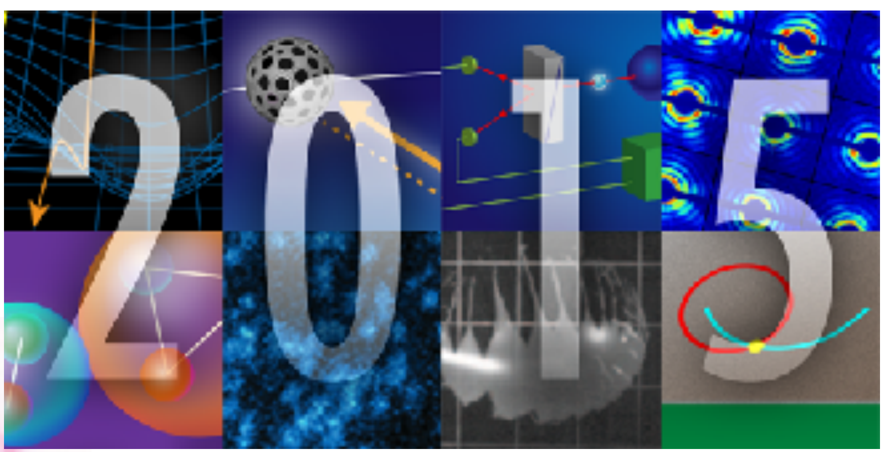
G. Vallone et al, ***Experimental Satellite Quantum Communications***, Phys. Rev. Lett. **115** 040502, 2015

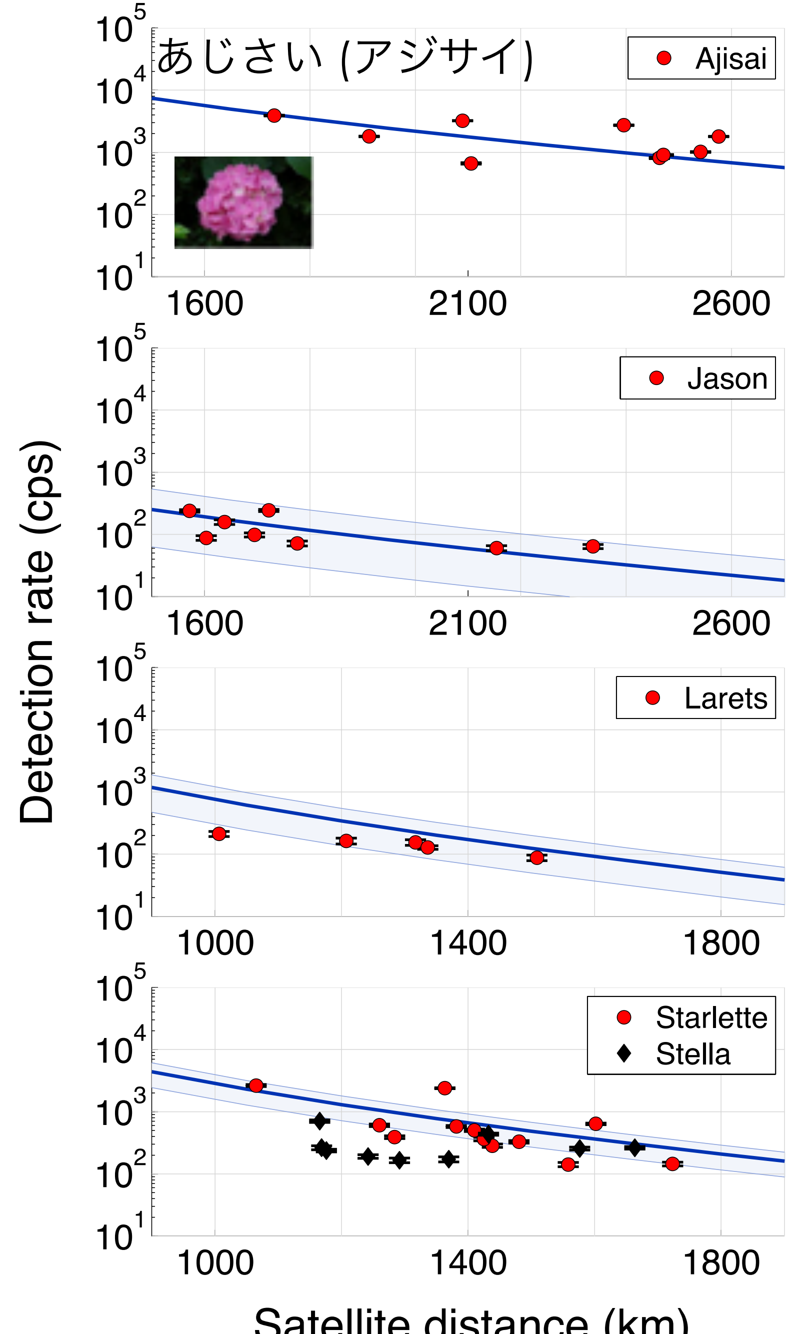
Link Budget and photon return rate

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.

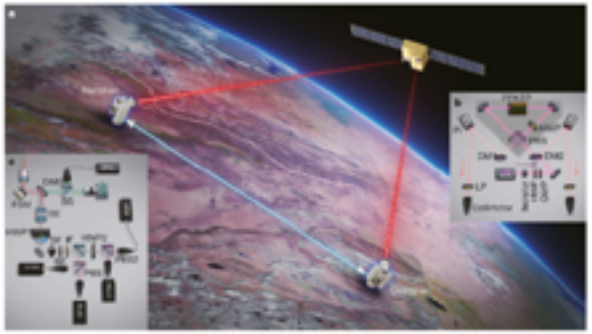


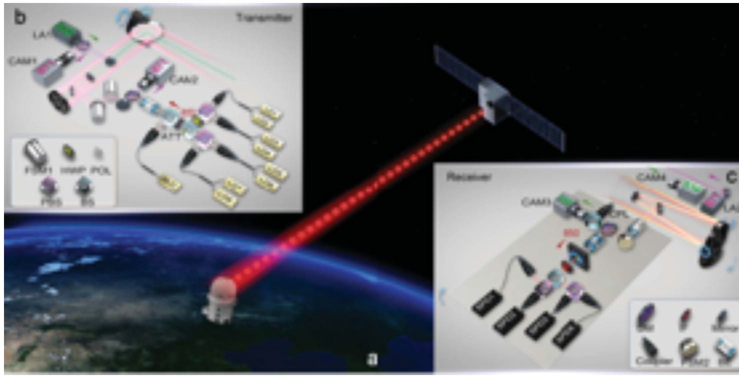


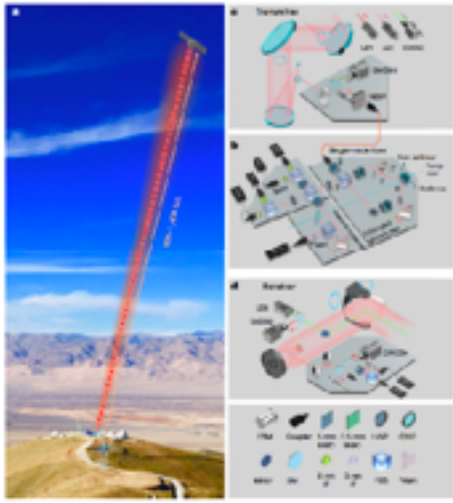
G. Vallone et al, ***Experimental Satellite Quantum Communications***, Phys. Rev. Lett. **115** 040502, 2015

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]







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

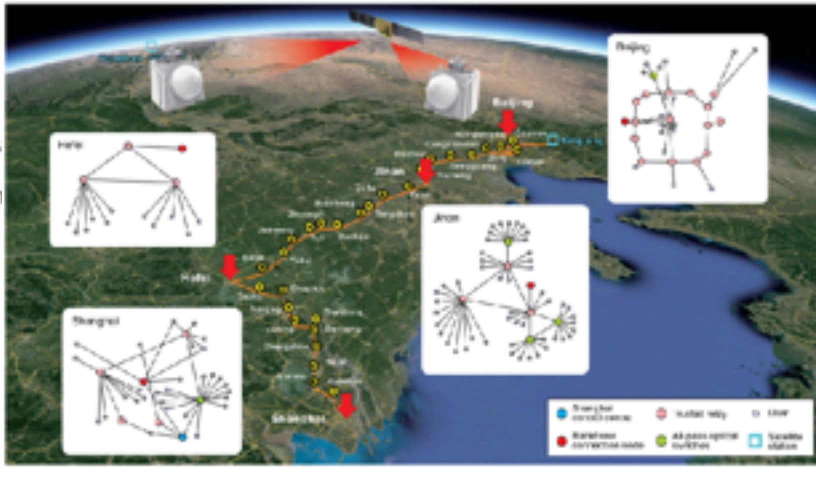
Published online: 15 June 2020

Juan Yin[1,2,3], Yu-Huai Li[1,2,3], Sheng-Kai Liao[1,2,3], Meng Yang[1,2,3], Yuan Cao[1,2,3], Liang Zhang[2,3,4], Ji-Gang Ren[1,2,3], Wen-Qi Cai[1,2,3], Wei-Yue Liu[1,2,3], Shuang-Lin Li[1,2,3], Rong Shu[2,3,4], Yong-Mei Huang[5], Lei Deng[6], Li Li[1,2,3], Qiang Zhang[1,2,3], Nai-Le Liu[1,2,3], Yu-Ao Chen[1,2,3], Chao-Yang Lu[1,2,3], Xiang-Bin Wang[2], Feihu Xu[1,2,3], Jian-Yu Wang[2,3,4], Cheng-Zhi Peng[1,2,3], Artur K. Ekert[7,8] & Jian-Wei Pan[1,2,3]

Ground-to-satellite quantum teleportation

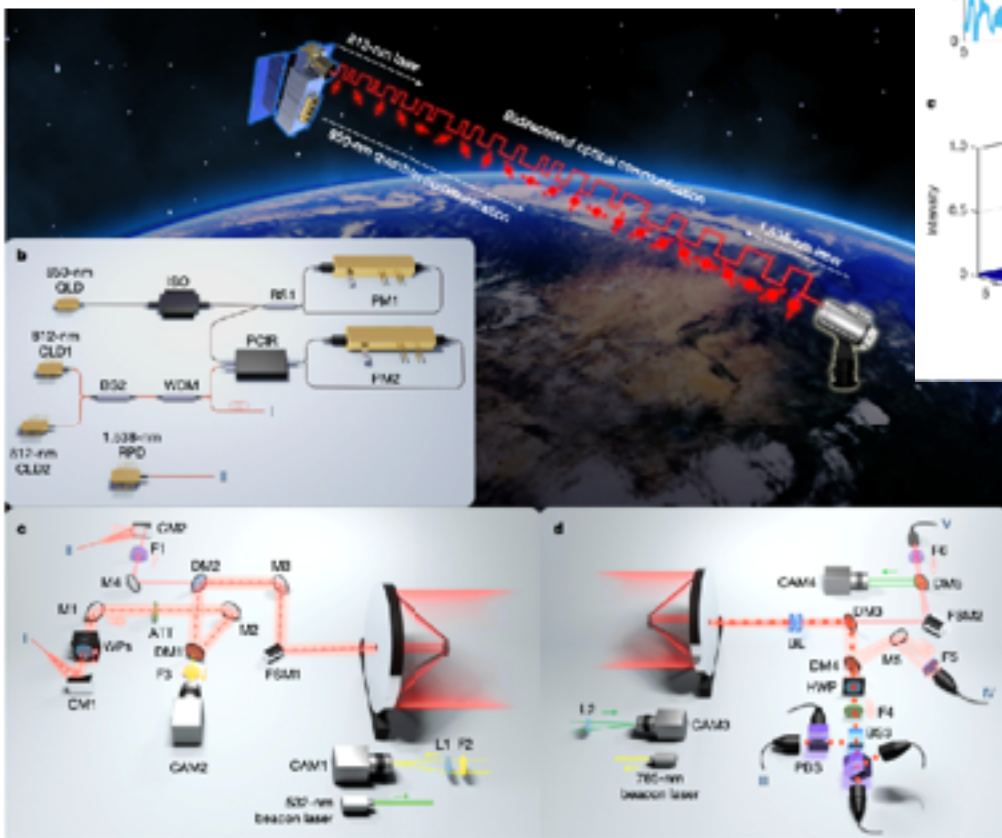
Ji-Gang Ren[1,2], Ping Xu[1,2], Hai-Lin Yong[1,2], Liang Zhang[2,3], Sheng-Kai Liao[1,2], Juan Yin[1,2], Wei-Yue Liu[1,2], Wen-Qi Cai[1,2], Meng Yang[1,2], Li Li[1,2], Kui-Xing Yang[1,2], Xuan Han[1,2], Yong-Qiang Yao[4], Ji Li[5], Hai-Yan Wu[5], Song Wan[6], Lei Liu[6], Ding-Quan Liu[3], Yao-Wu Kuang[3],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

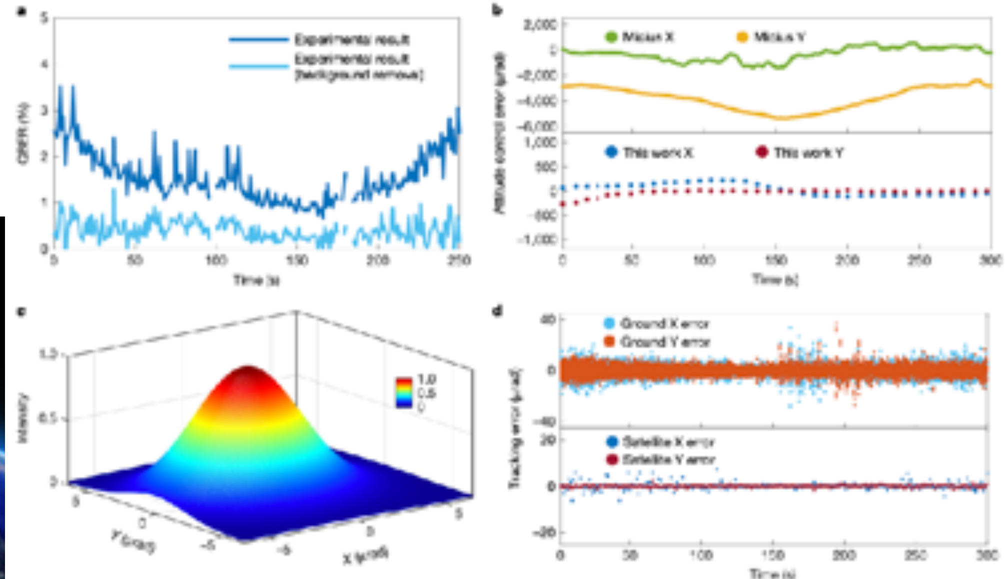
An integrated space-to-ground quantum communication network over 4,600 kilometres



Article

Microsatellite-based real-time quantum key distribution





Yang Li[1,2,3,14], Wen-Qi Cai[1,2,3,14], Ji-Gang Ren[1,2,3,14], Chao-Ze Wang[1,2,3], Meng Yang[1,2,3], Liang Zhang[3,4], Hui-Ying Wu[5], Liang Chang[5], Jin-Cai Wu[3,4], Biao Jin[6], Hua-Jian Xue[1,2,3], Xue-Jiao Li[1,2,3], Hui Liu[6], Guang-Wen Yu[1,2,3], Xue-Ying Tao[1,2,3], Ting Chen[5], Chong-Fei Liu[3,4], Wen-Bin Luo[1,2,3], Jie Zhou[6], Hai-Lin Yong[6], Yu-Huai Li[1,2,3], Feng-Zhi Li[1,2,3], Cong Jiang[7], Hao-Ze Chen[8], Chao Wu[8], Xin-Hai Tong[9], Si-Jiang Xie[9], Fei Zhou[7], Wei-Yue Liu[1,2,3], Yaseera Ismail[10,11], Francesco Petruccione[10,12,13], Nai-Le Liu[1,2,3], Li Li[1,2,3], Feihu Xu[1,2,3], Yuan Cao[1,2,3], Juan Yin[1,2,3], Rong Shu[3,4], Xiang-Bin Wang[7], Qiang Zhang[1,2,3,7], Jian-Yu Wang[3,4], Sheng-Kai Liao[1,2,3✉], Cheng-Zhi Peng[1,2,3✉] & Jian-Wei Pan[1,2,3✉]

https://doi.org/10.1038/s41586-025-08739-z

Received: 29 July 2024

Accepted: 4 February 2025

Published online: 19 March 2025

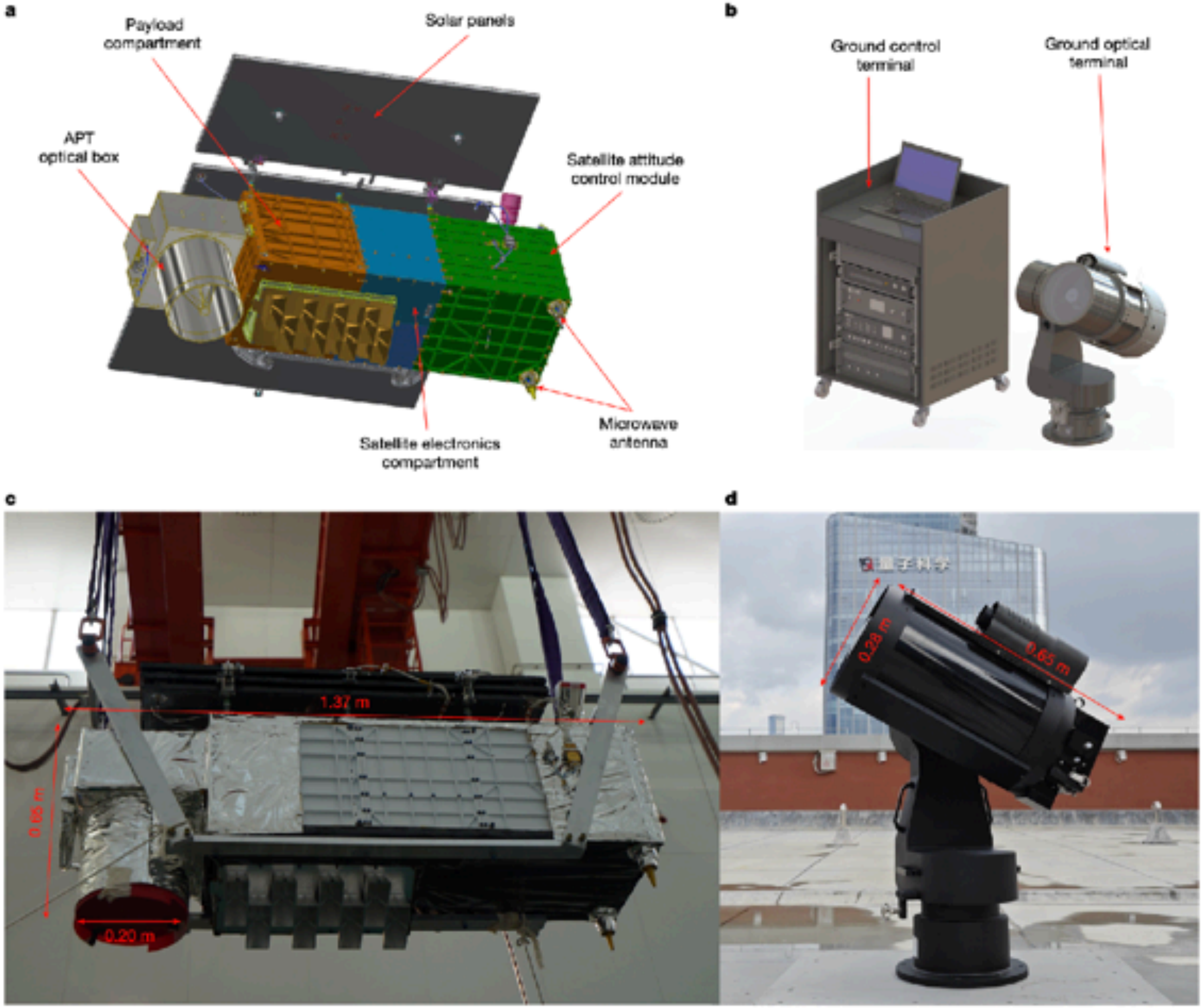


Fig. 3 | The microsatellite and the portable OGS. a, The satellite consists of an APT optical box, payload compartment, satellite electronics compartment, satellite attitude control module, microwave antenna and solar panels. **b**, The OGS consists of a control terminal and an optical terminal. **c**, Photo of the microsatellite before being assembled into the rocket. The satellite launch state envelope measures approximately 1.37 m × 0.49 m × 0.65 m, with a telescope aperture of 0.2 m. **d**, Photo of the portable OGS in the urban area of Jinan. The main telescope of the OGS has an envelope size of approximately 0.65 m × 0.28 m × 0.28 m.

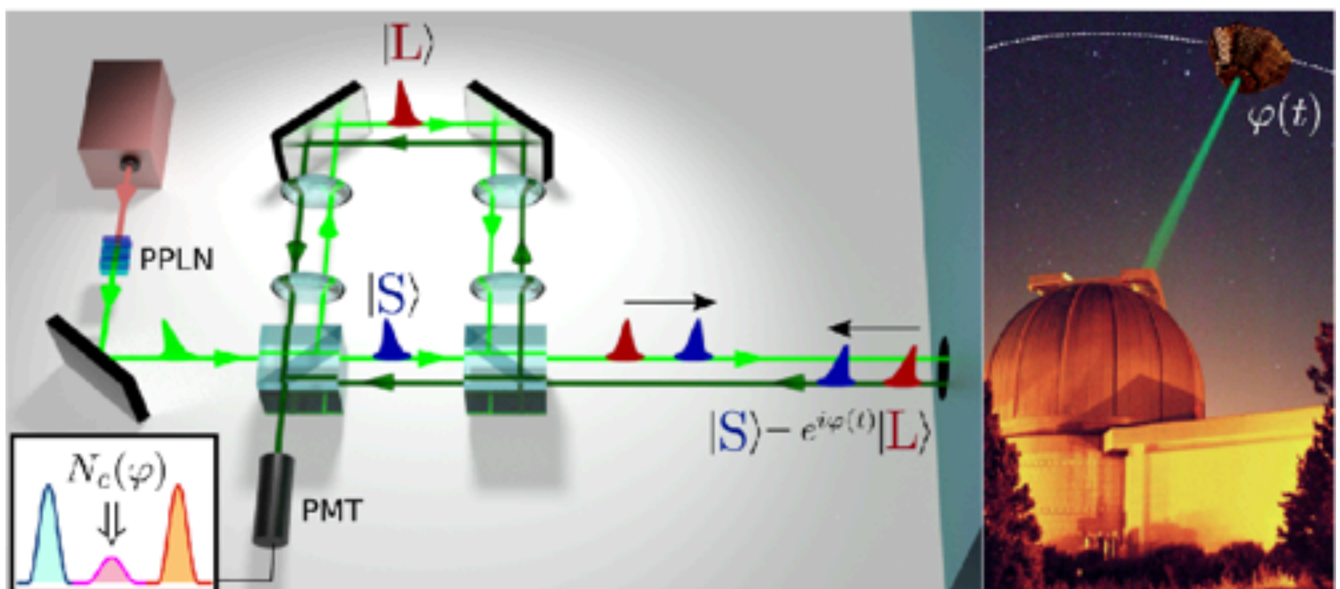
Quantum Information pioneers

Prof. Zeilinger talk extract

test of superposition principle using temporal modes of light

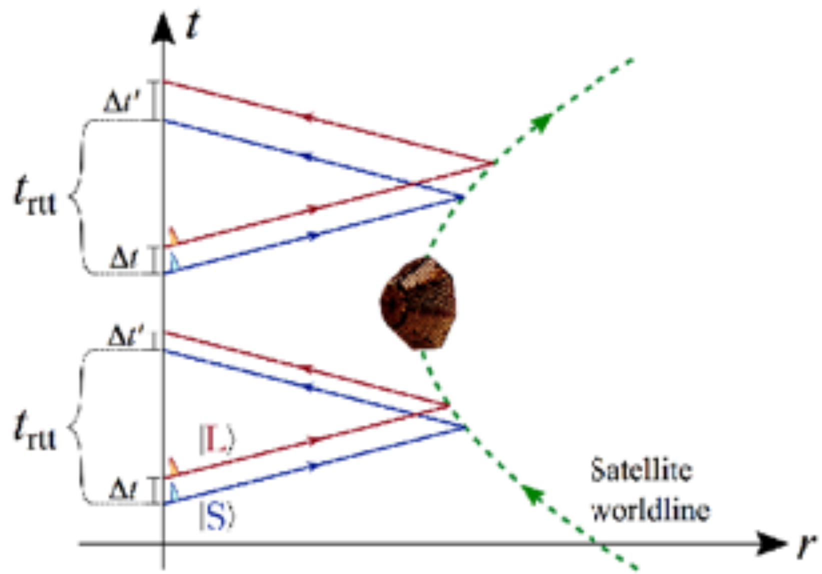
- Quantum interference arising from superposition of states is a striking evidence of the validity of Quantum Mechanics, confirmed in many experiments and also exploited in applications.

- The single-photon interference at a ground station is seen, due to the coherent superposition of two temporal modes reflected by a rapidly moving satellite thousand kilometres away.

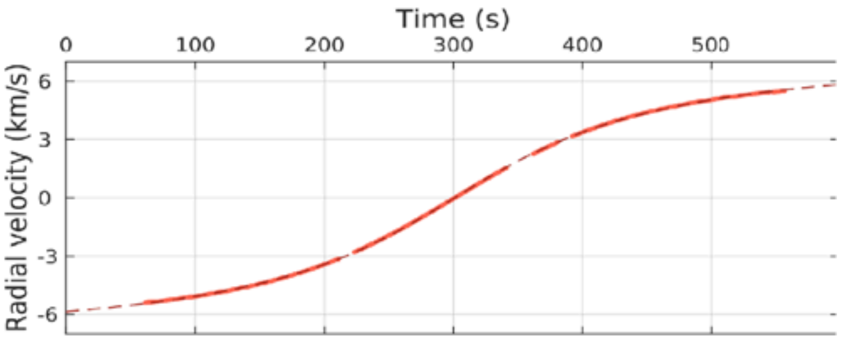


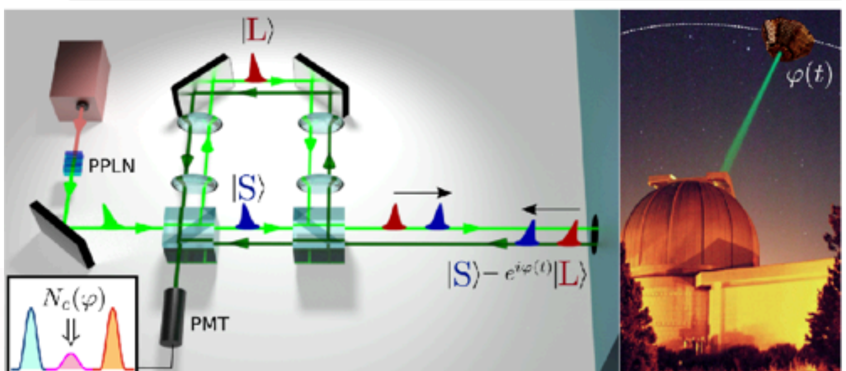
Kinematic Phase modulation by satellite relative motion

Relativistic effects on the photon interference



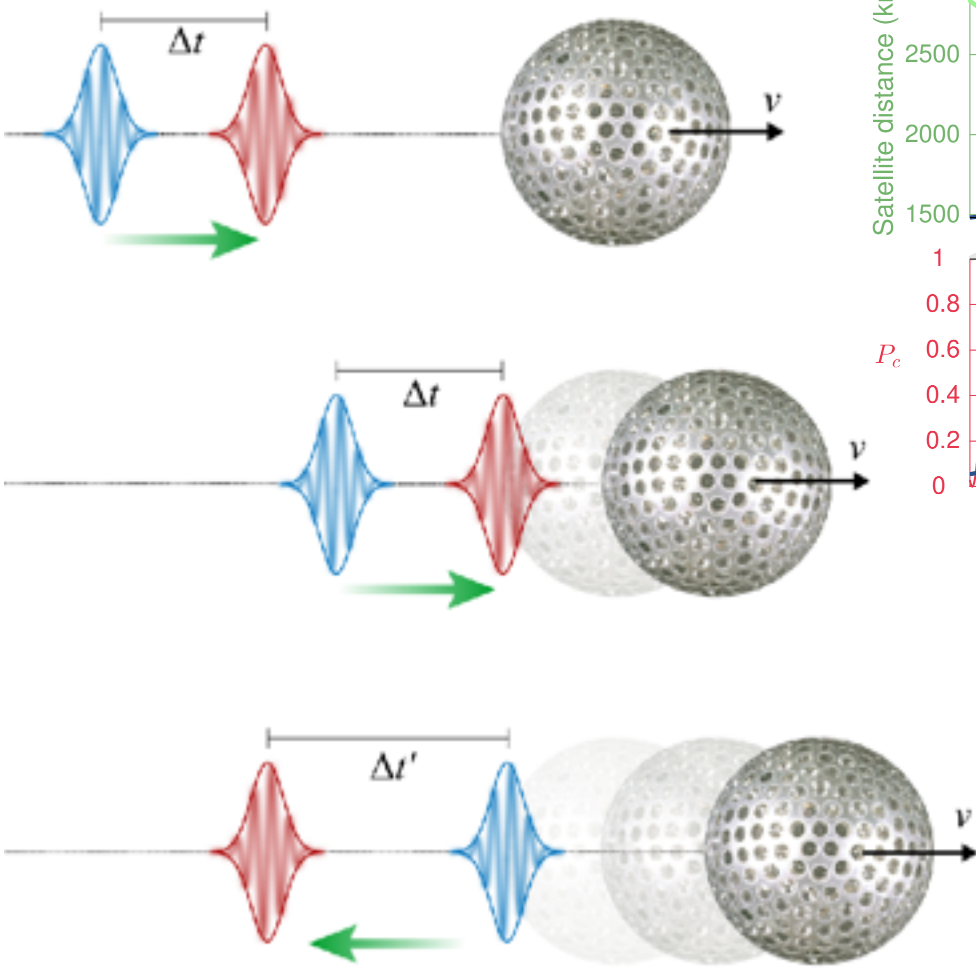
Beacon-C

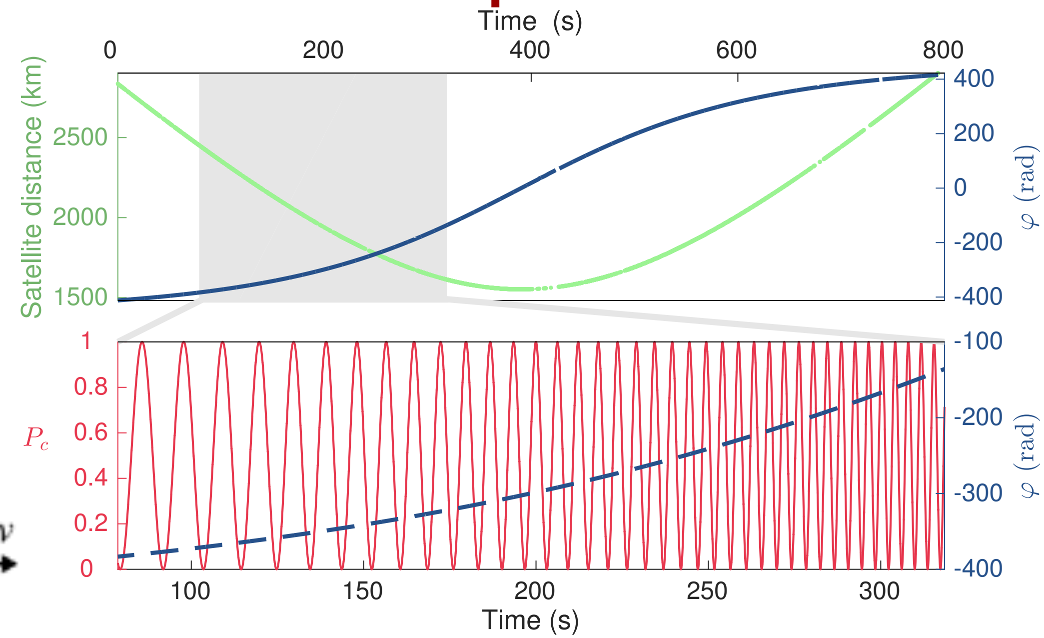




G. Vallone et al., **Interference at the Single Photon Level Along Satellite-Ground Channels**, Phys. Rev. Lett. **116** 253601 (2016)

Satellite-induced interference pattern





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

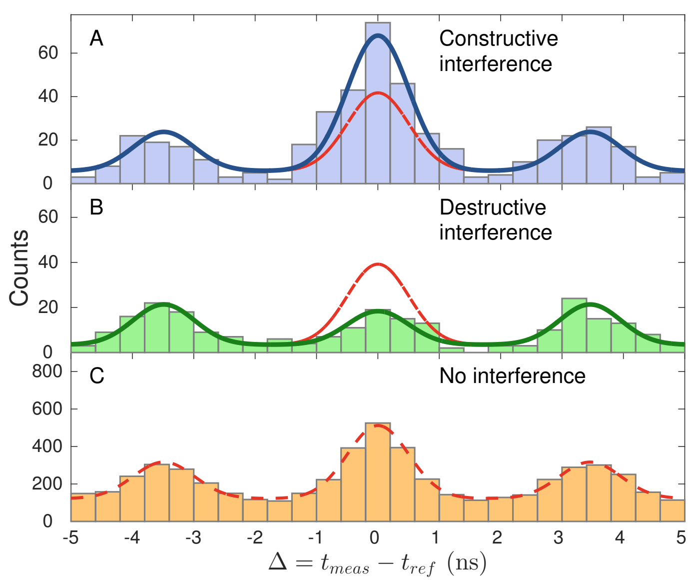
$$\mathcal{V}(t) = e^{-\frac{\lambda^2\varphi^2(t)}{8\pi c^2\tau_c^2}} \approx 1$$

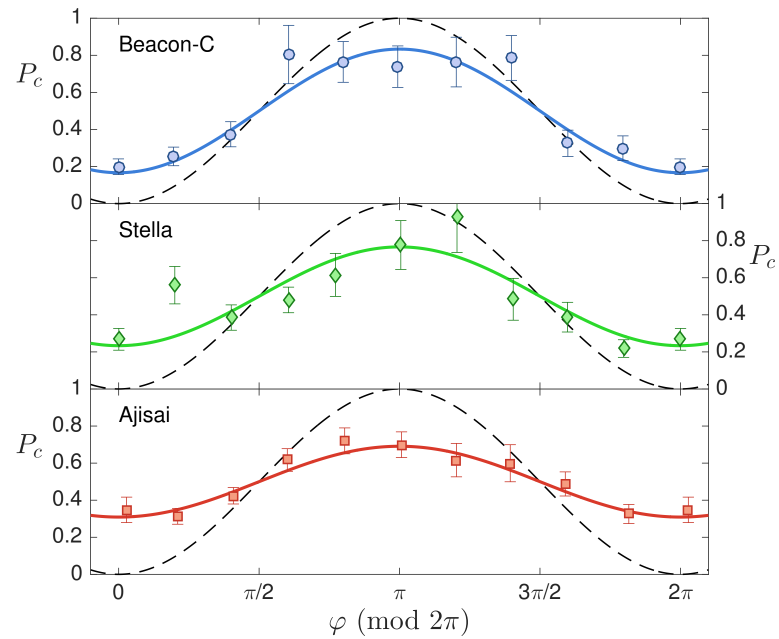
$$\varphi(t) = \frac{2\beta(t)}{1+\beta(t)}\frac{2\pi c}{\lambda}\Delta t \qquad \beta(t) := \frac{v_r(t)}{c}$$

G. Vallone et al., **Interference at the Single Photon Level Along Satellite-Ground Channels**, Phys. Rev. Lett. **116** 253601 (2016)

Experimental results

Since the radial velocity is continuously changing along the orbit, the detection probability in the central peak is varying accordingly

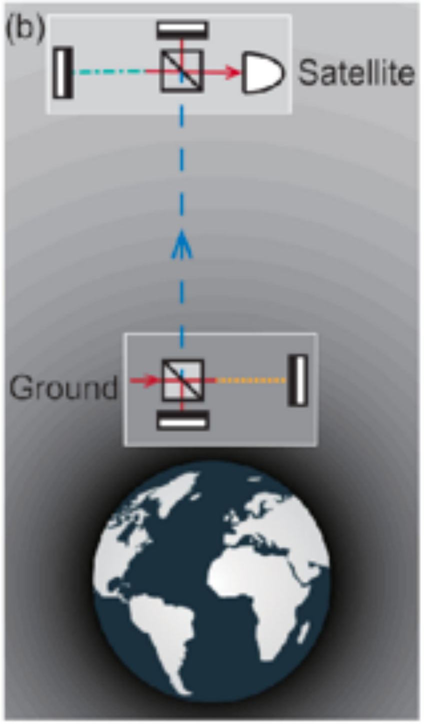




- We can **select single-photon detections** corresponding to phase-shift **for constructive and destructive interference.**
- **Without any data selection the interference is washed out**
- **We observed interference with 3 different satellites**
- **We** selected ten different values for the phase-shift and **reconstructed the interference pattern with visibility up to 67%**

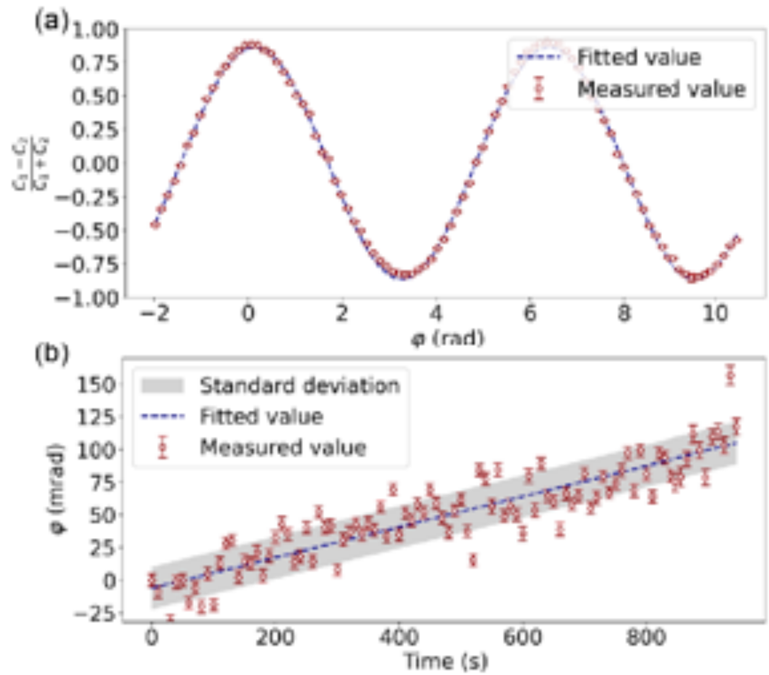
G. Vallone et al., **Interference at the Single Photon Level Along Satellite-Ground Channels**, Phys. Rev. Lett. **116** 253601 (2016)

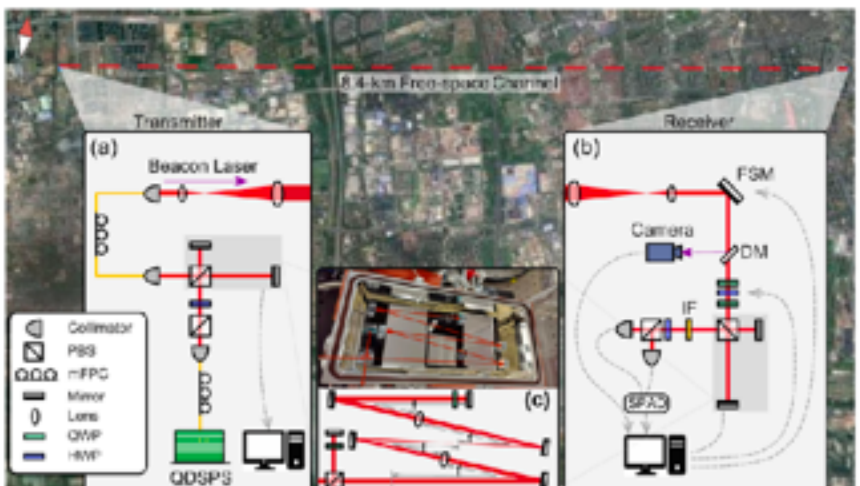
PHYSICAL REVIEW LETTERS **133,** 020201 (2024)



Single-Photon Interference over 8.4 km Urban Atmosphere: Toward Testing Quantum Effects in Curved Spacetime with Photons

Hui-Nan Wu,[*] Yu-Huai Li,[*] Bo Li, Xiang You, Run-Ze Liu, Ji-Gang Ren, Juan Yin, Chao-Yang Lu, Yuan Cao, Cheng-Zhi Peng, and Jian-Wei Pan





multimode interference. The measured multimode interference visibility $\mathcal{V} = 0.863 \pm 0.004$, indicates the effectiveness of the imaging system against atmospheric turbulence. By directly measuring the phase at a frequency of 0.1 Hz under fixed phase φ, we achieved a phase measurement precision of 35.8 mrad in Fig. 3(b). However, a long-term linear phase drift was observed and found to be 0.117 ± 0.006 mrad/s, which is shown as a blue dashed

Quantum Mechanics in Curved Spacetime

- reconciliation of gravity and quantum mechanics, started with QFTCS in the '70s

- **most tests are indirect**, as laboratory setting of analog gravity, or set in strong-field astrophysical processes

- opportunity to address direct tests in the actual channel - and weak-field regime, by means of **deployment of long-baseline quantum optical links**.

- Any Colella-Overhauser-Werner (COW) type test of the equivalence principle that touches upon quantum properties of photons will have the significance of being the first direct test of QFTCST.

QComms for fundamental tests in space

Mohageg et al. EPJ Quantum Technology (2022) 9:25
https://doi.org/10.1140/epjqt/s40507-022-00143-0

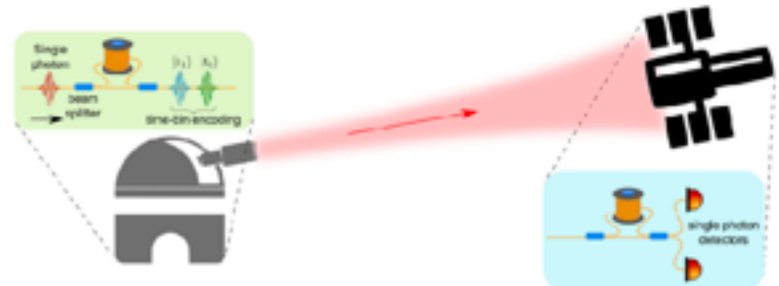
EPJ.org

EPJ Quantum Technology
a SpringerOpen Journal

REVIEW Ope

The deep space quantum link: prospective fundamental physics experiments using long-baseline quantum optics

Makan Mohageg[1*], Luca Mazzarella[1], Charis Anastopoulos[2], Jason Gallicchio[3], Bei-Lok Hu[4], Thomas Jennewein[5], Spencer Johnson[6], Shih-Yuin Lin[7], Alexander Ling[8], Christoph Marquardt[9], Matthias Meister[10], Raymond Newell[11], Albert Roura[10], Wolfgang P. Schleich[10,12,13], Christian Schubert[14,15], Dmitry V. Strekalov[1], Giuseppe Vallone[16,17,18], Paolo Villoresi[16,17], Lisa Wörner[10], Nan Yu[1], Aileen Zhai[1] and Paul Kwiat[2*]



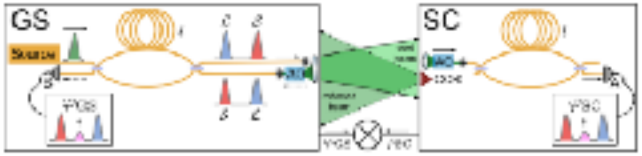
[1] D. R. Terno et al. Proposal for an optical interferometric measurement of the gravitational redshift with satellite systems. Phys. Rev. D 108, 084063 (2023) - arxiv in Nov. 2018.

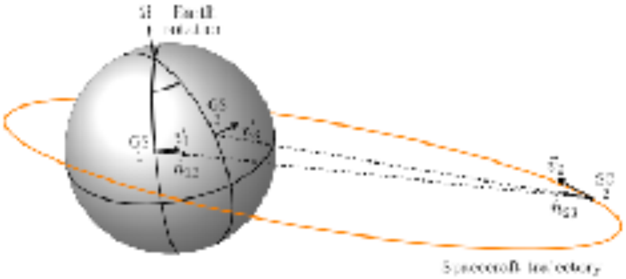
[2] D. R. Terno, G. Vallone, F. Vedovato, and P. Villoresi, “Large-scale optical interferometry in general spacetimes,” Phys. Rev. D, vol. 101, no. 10, p. 104052, May 2020.

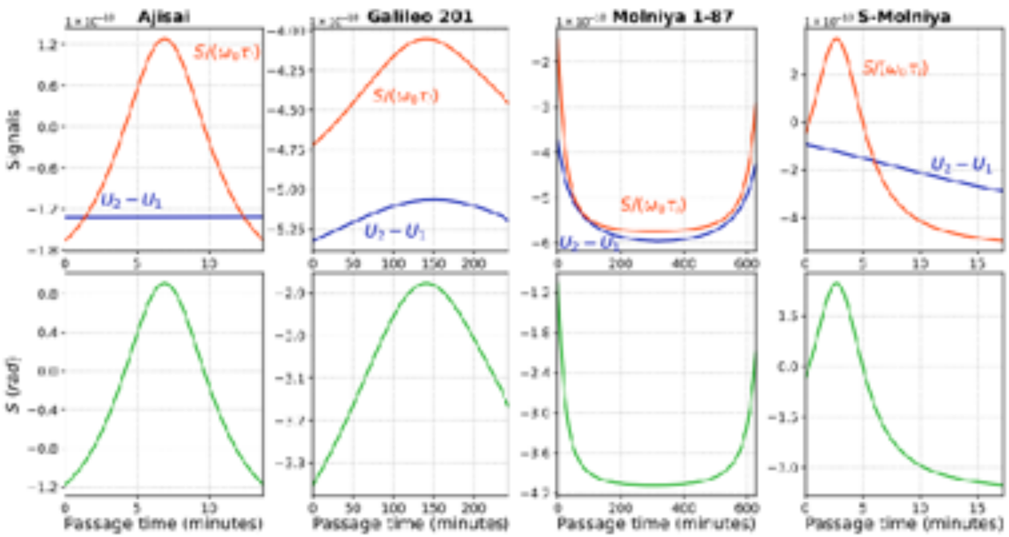
[3] M. Mohageg et al., “The deep space quantum link: prospective fundamental physics experiments using long-baseline quantum optics,” EPJ Quantum Technol., vol. 9, no. 1, p. 25, Dec. 2022.

Optical interferometric measurement of the gravitational redshift proposal

Addressing the redshift implied by the EEP, which affects the locally measured frequencies of a spectral line that is emitted at location 1 with the proper frequency ω_0 and then detected at location 2 with ω'







$$\frac{\Delta\omega}{\omega_0} = (1+\alpha)\Delta U + \mathcal{O}(c^{-3})$$

$$\varphi_{\mathrm{gr}} = \Delta U \omega_0 \tau_l \approx -\frac{gh}{c^2}\frac{2\pi}{\lambda} nl.$$

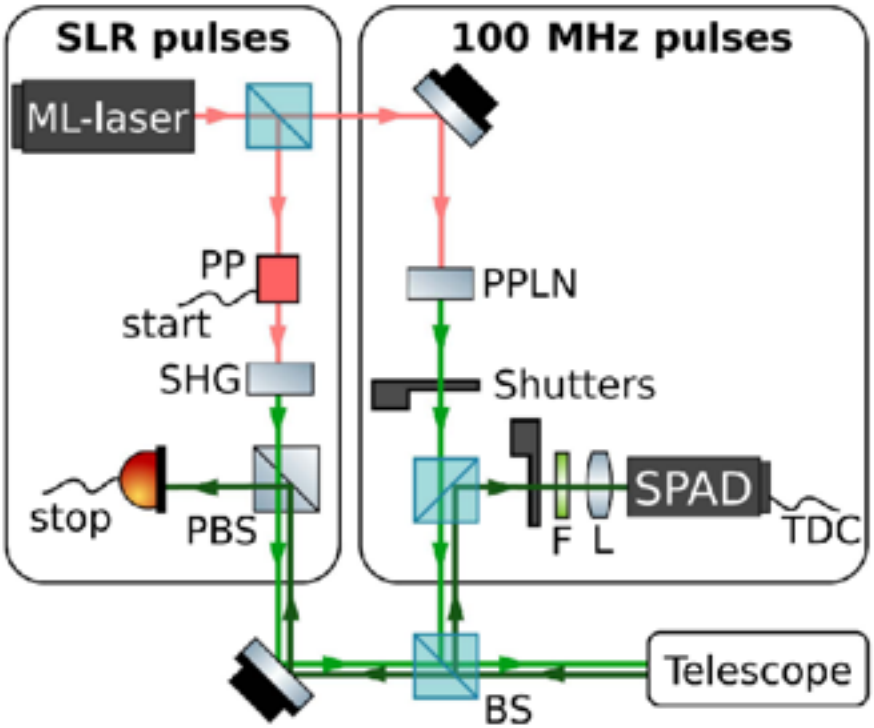
D. R. Terno et al.,"Proposal for an optical interferometric measurement of the gravitational redshift with satellite systems," Phys. Rev. D, vol. 108, no. 8, p. 084063 (2023 - initial arxiv 1811.04835)

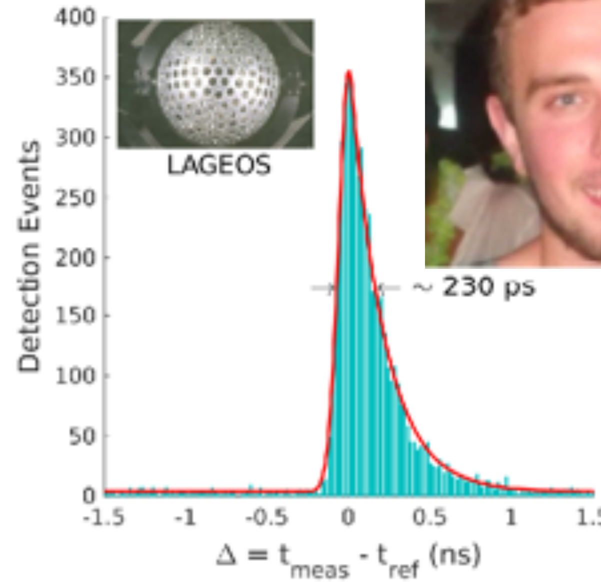
on the temporal resolution and clock rate

- **in QComms, the signal** - the gathered photons - as well as the secret key rate for QKD - **scales with the number of uses of the channel per second**
- 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
- values went from 100 MHz to 625 MHz of Jinan-1, to be increased.

single photon detection with 100 MHz probe

230 ps over 7000km (MEO)





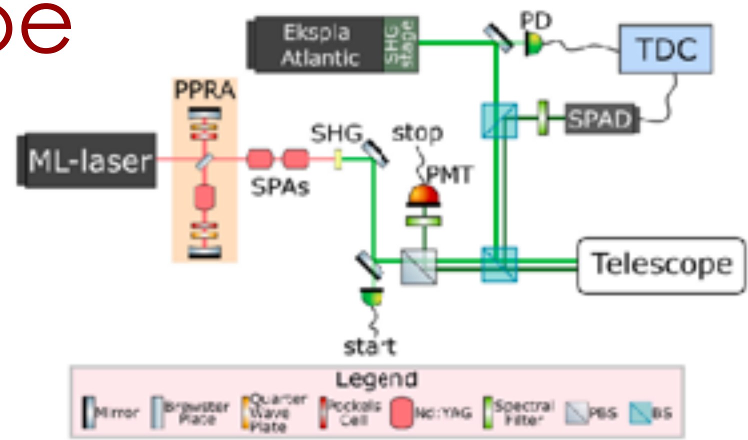
The 100-MHz pulse train is detected after a 50:50 BS to separate the outgoing and incoming beams and 3 nm spectral filter a silicon single photon avalanche detector SPAD (Micro-Photon-Devices Srl) with ≈ 50% quantum efficiency, ≈ 400 Hz dark count rate and 40 ps of jitter.

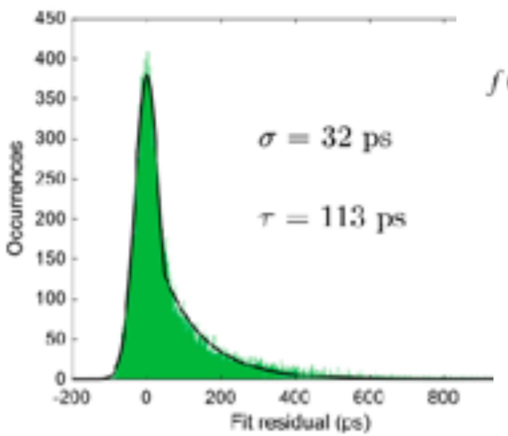
The time of arrival is tagged with 1 ps resolution (quTAG TDC from qutools GmbH)

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

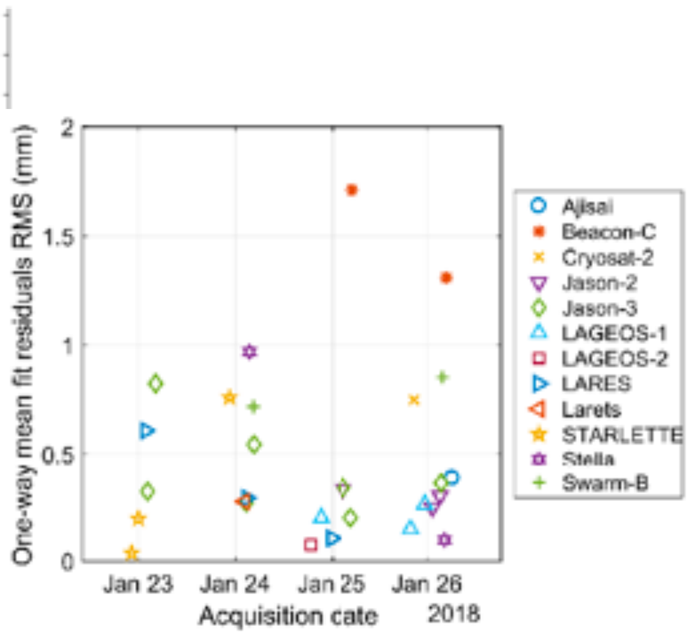
orbit ranging refinement with temporally structured probe

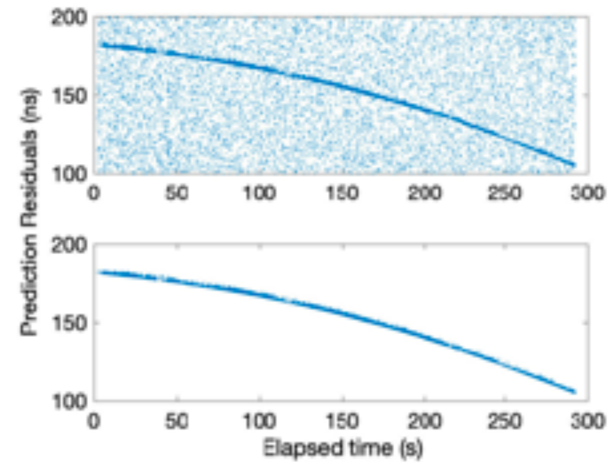
- combined lasers for ranging
- 10 Hz 40 ps 100 mJ + 100 kHz 10 ps 200 μJ
- linear PMT + SPAD 40 ps + 1 ps timetagging





$$f(t) = Ae^{-\frac{(t-t_1)^2}{2\sigma^2}}\,\Theta(t_1 - t) + Be^{-\frac{t-t_1}{\tau}}\,\Theta(t - t_1)$$





D. Dequal et al., "100 kHz satellite laser ranging demonstration at Matera Laser Ranging Observatory," J. Geod. **95**, 26, (2021).

The Qubit4Sync synchronization

- **encoding a suitable public string in the qubits before the start of the QKD allow to recover both the frequency and the absolute time, synchronizing the devices.**

•**No need of additional lasers, modulators and detectors for the synchronization**

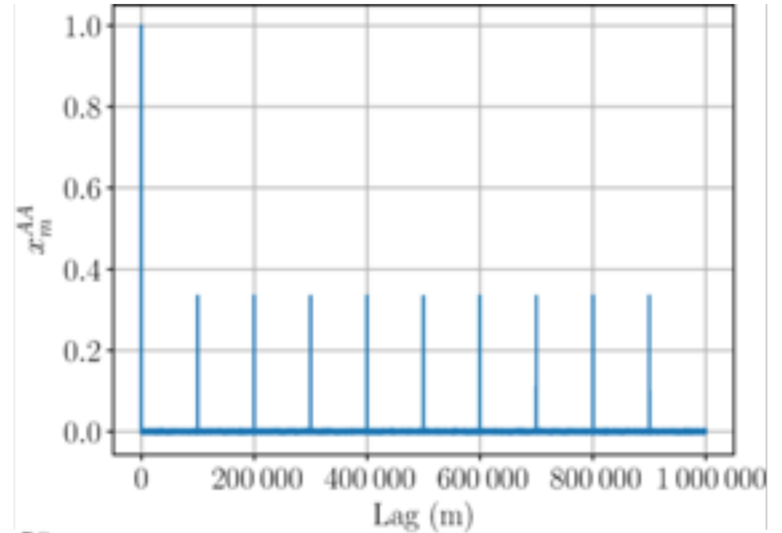
•Reduced numbers of channels and fibers used for the QKD, since no dedicated service-channel is needed for synchronization

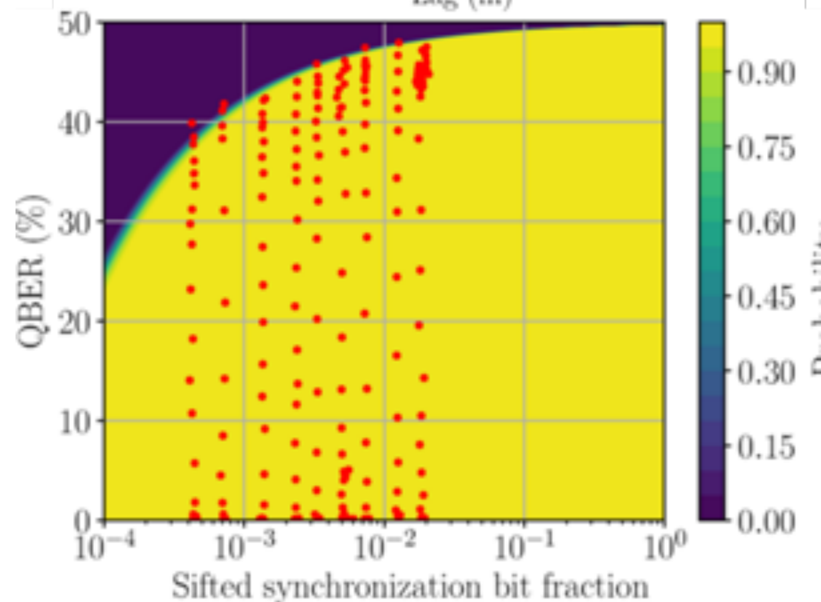
•Reduced complexity of transmitter and receiver: all the processing is done in software

•More flexible system, can be reconfigured in software without hardware changes

•The method is robust to losses: it tolerates losses higher than those necessary for the QKD

tested on the ground so far.





L. Calderaro et al., Phys. Rev. Appl., 13, 5, 054041 (2020)

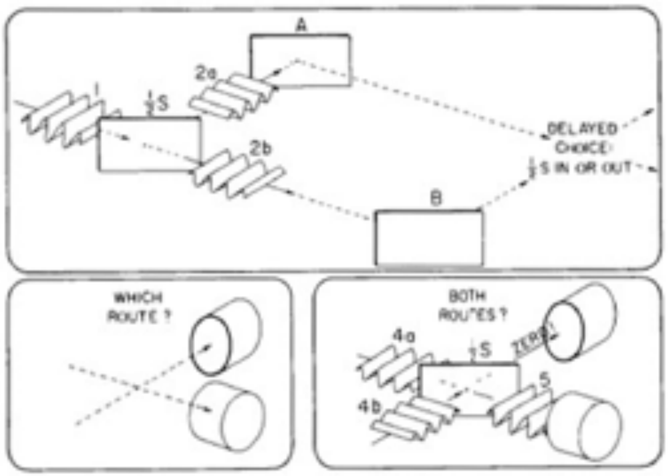
opportunity in **combining** pol- and temp-DoF to extend the functions

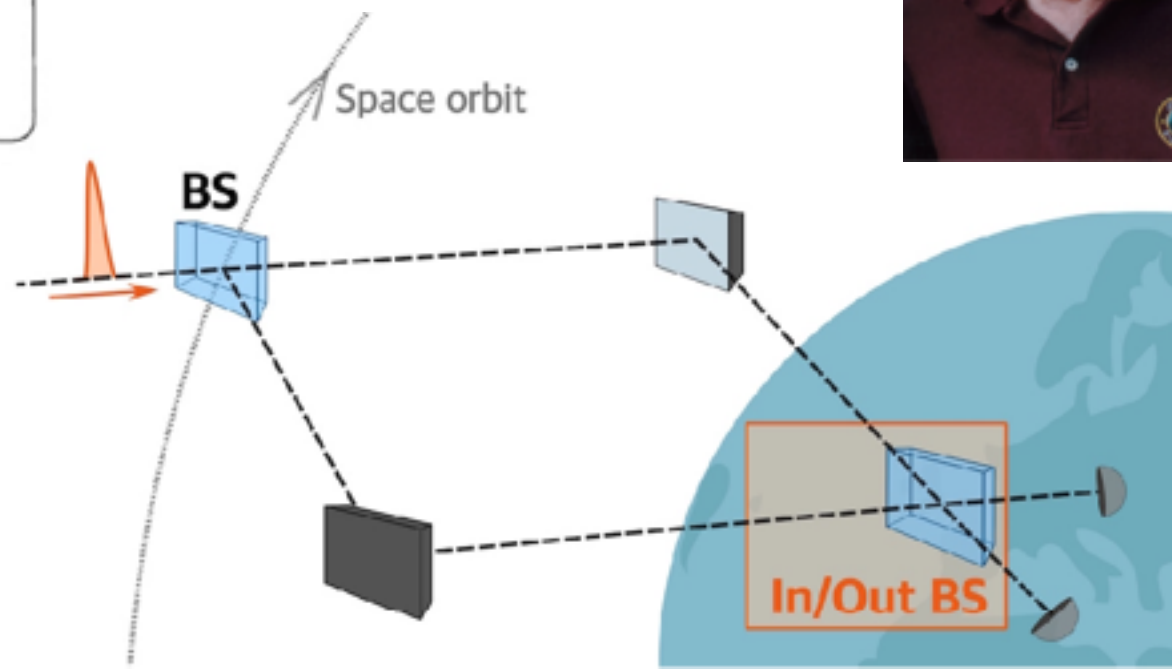
- suitable application in the space version of the John Wheeler Delayed-choice gedanken experiment

- 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.

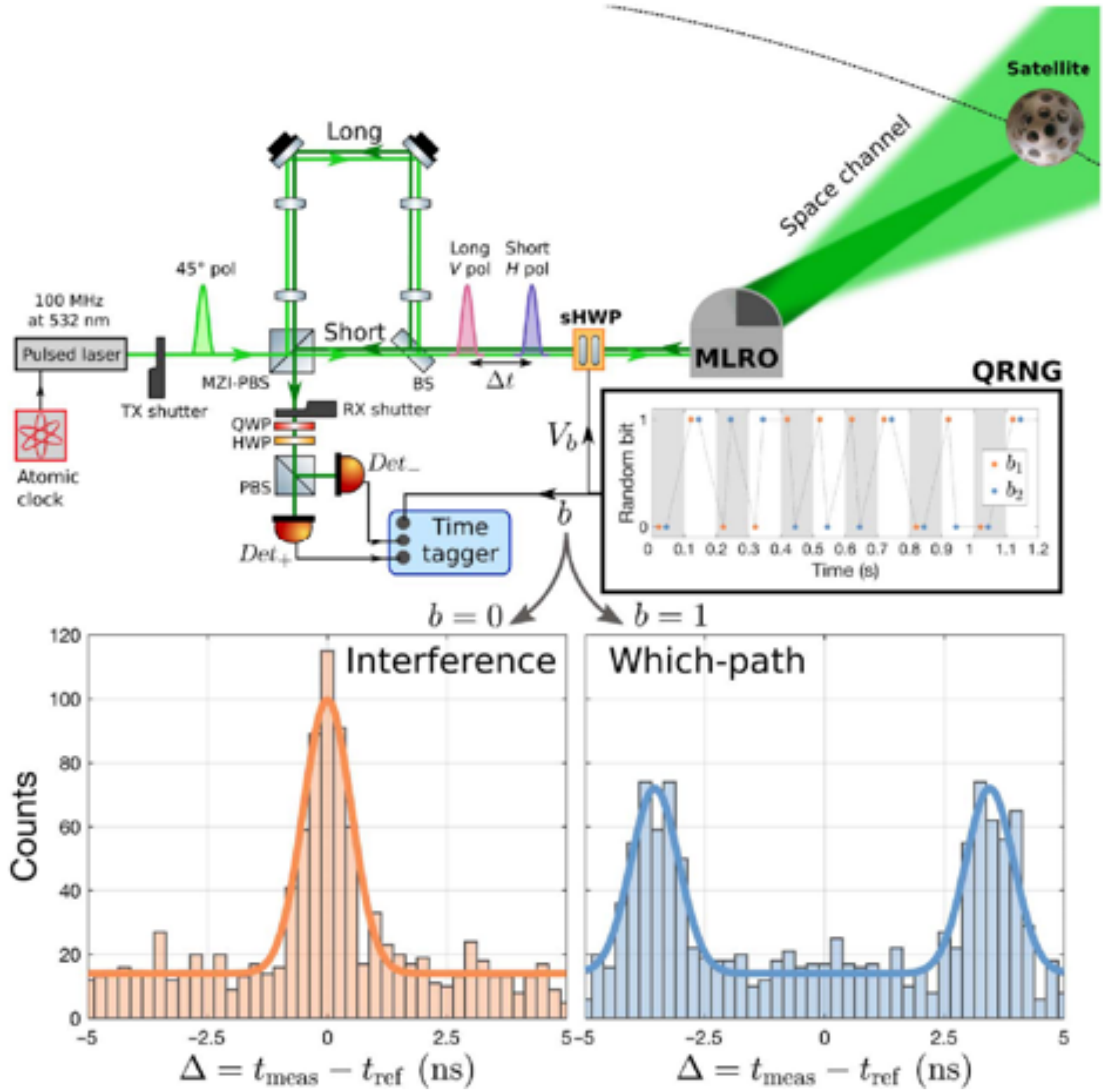
- Bohr: there is no difference "whether our plans of constructing or handling the instruments are fixed beforehand or whether we postpone the completion of our planning until a later moment"

Delayed-choice space experiment

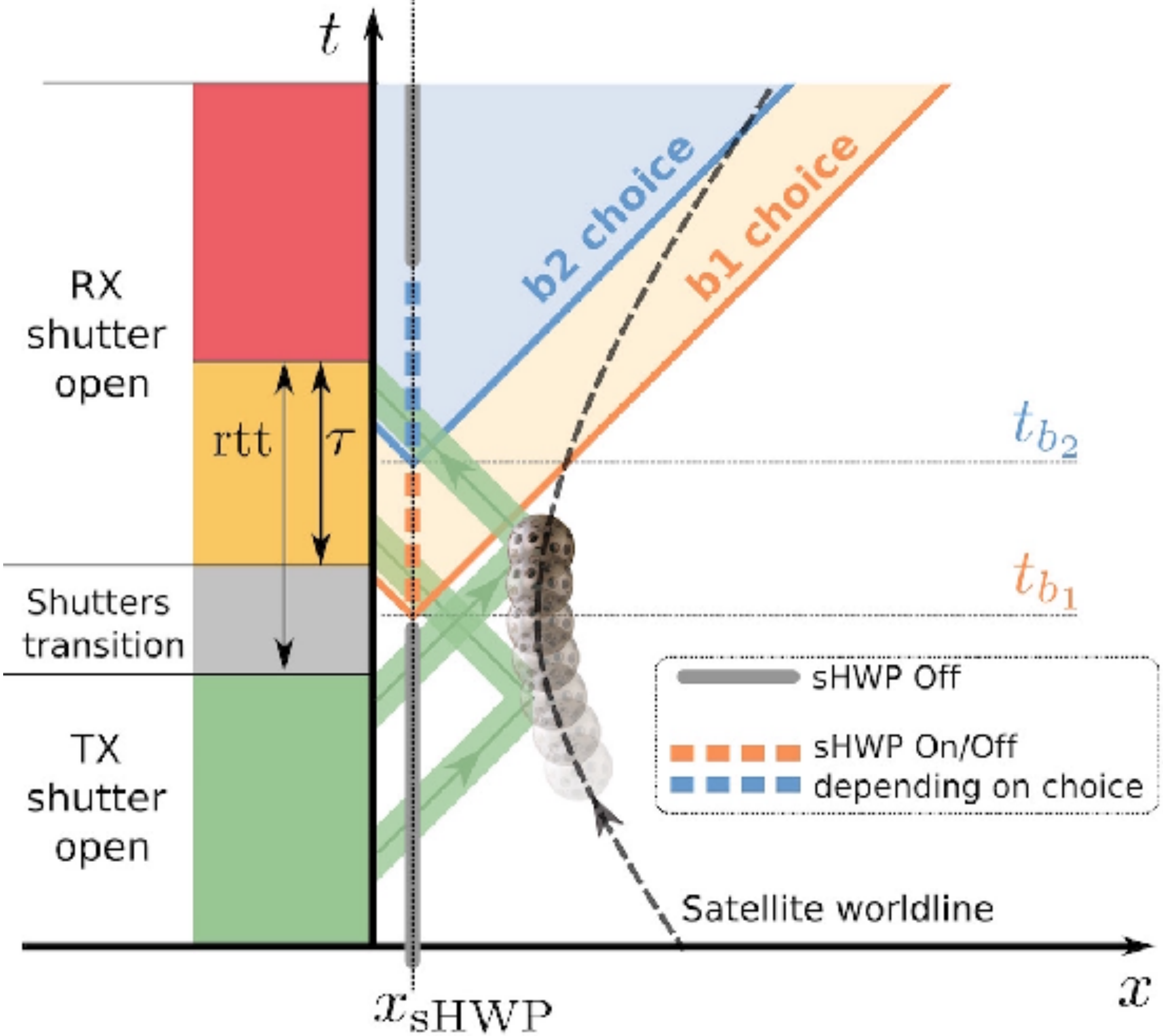




J.A. Wheeler **The “past” and the “delayed-choice” double-slit experiment**. Mathematical Foundations of Quantum Theory, Academic pp 9–48. (1978)



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



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

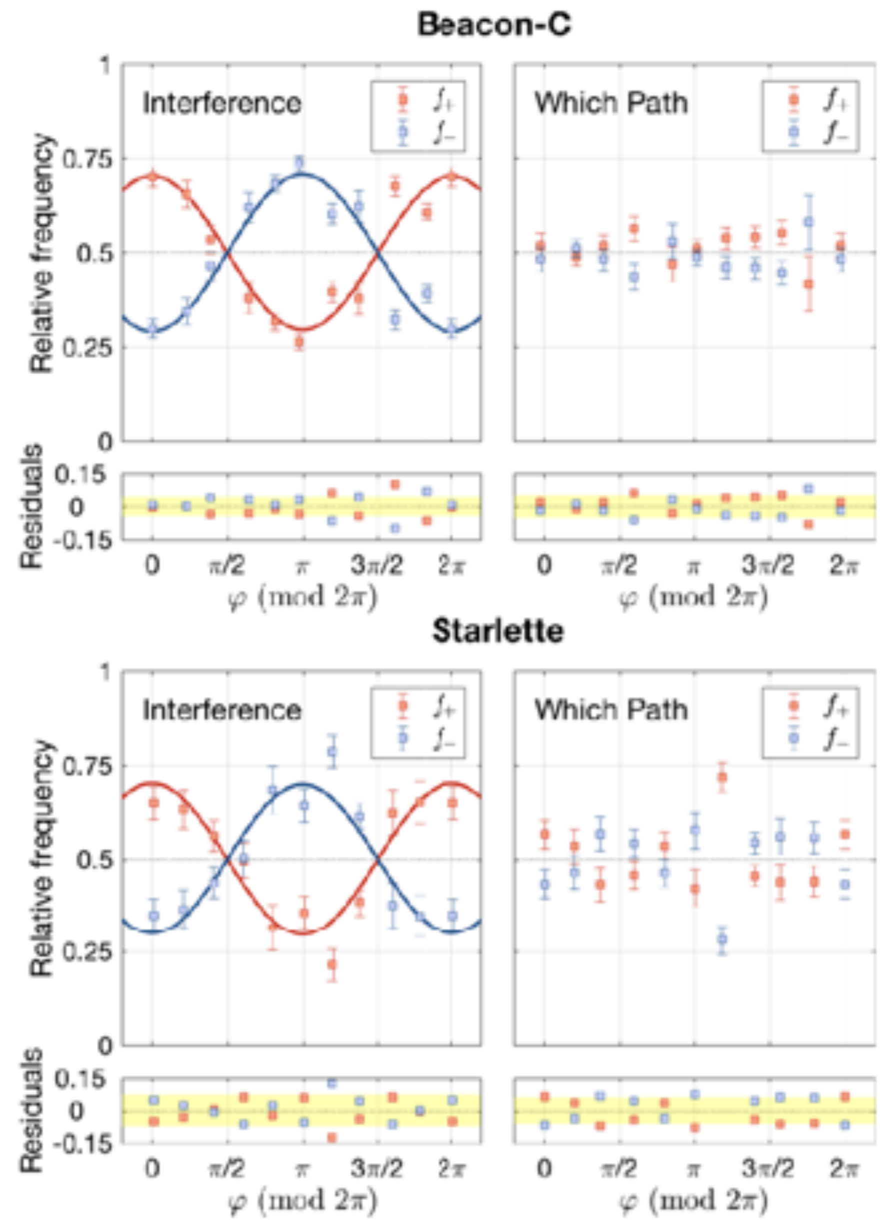
- wave-like: interference fringe visibility

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

- 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. Science Adv. 3, e1701180 (2017)

- wave-like

f

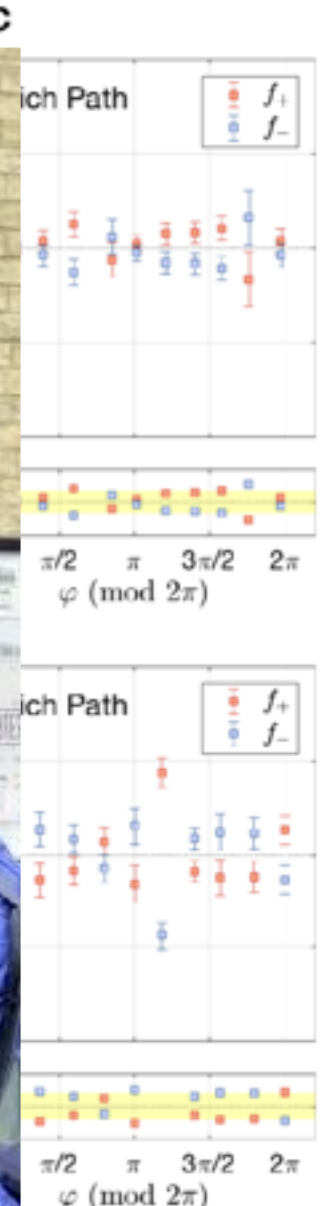
ν^{Bea}

ν^{Sta}

- particle-li
95 ± 1% (S

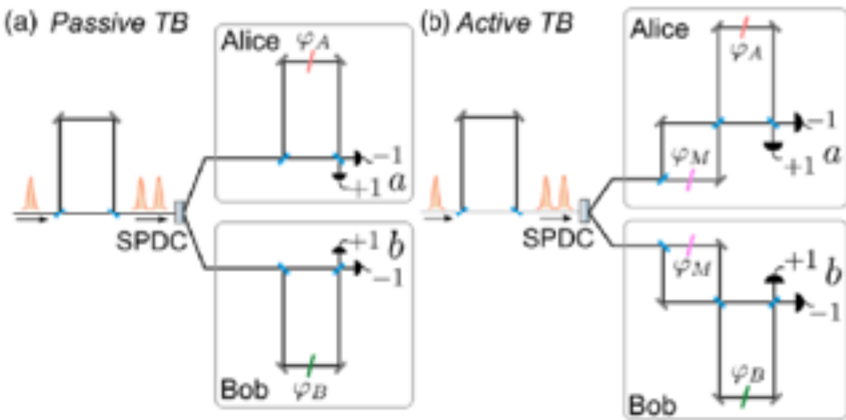
- ➔ excludi
5σx

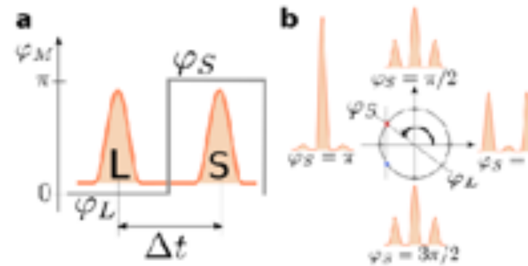
Our results exter
mechanical de
spatial scale of
they support the
exploiting both
dimensional free
over long distan



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

moving toward entanglement in time-bins:
*Bell test post-selection loophole-free with **genuine** time-bin entanglement*





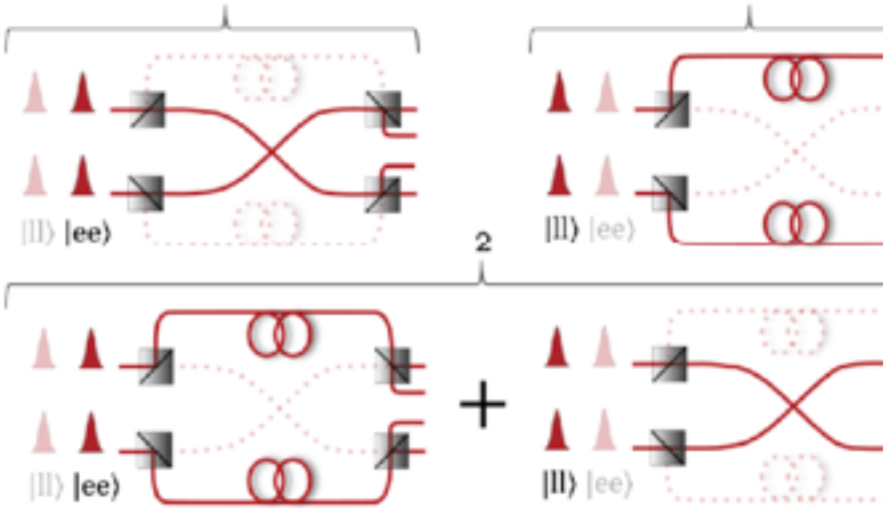
Franson type
Bell's test using
time-bin encoding

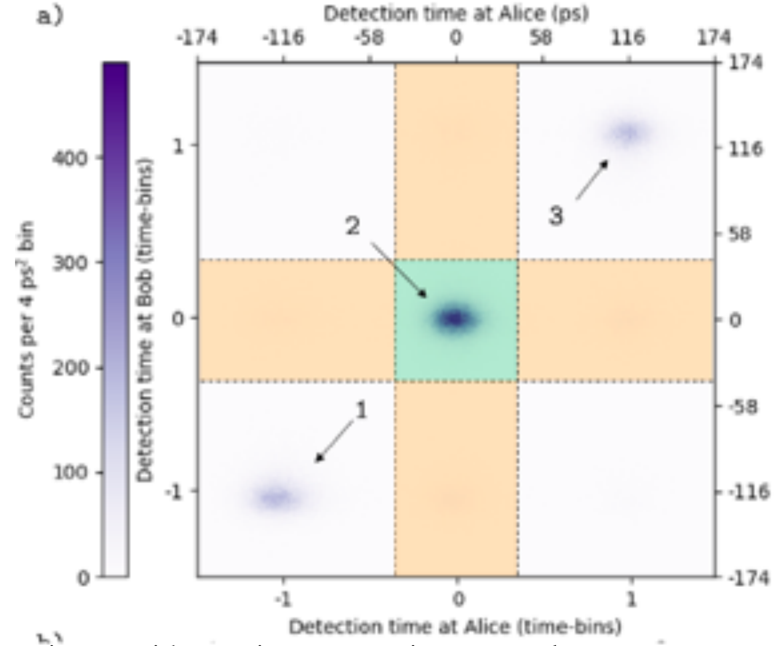
i) the *passive time-bin with post-selection;*
ii) the *passive time-bin with no post-selection;*
iii) the *active time-bin with no post-selection.*

Time-bin scheme	Δw	Post-Selection Loophole	$\mathcal{V}_{exp}$	S_{exp}	SD
i) passive	2.4 ns	Yes	0.95 ± 0.05	2.58 ± 0.03	18.3
ii) passive	8.1 ns	No	0.23 ± 0.02	0.67 ± 0.02	—
iii) active	8.1 ns	No	0.89 ± 0.03	2.30 ± 0.03	9.3

F. Vedovato et al. *Postselection-Loophole-Free Bell Violation with Genuine Time-Bin Entanglement*
Phys. Rev. Lett. **121** 190401 (2018)

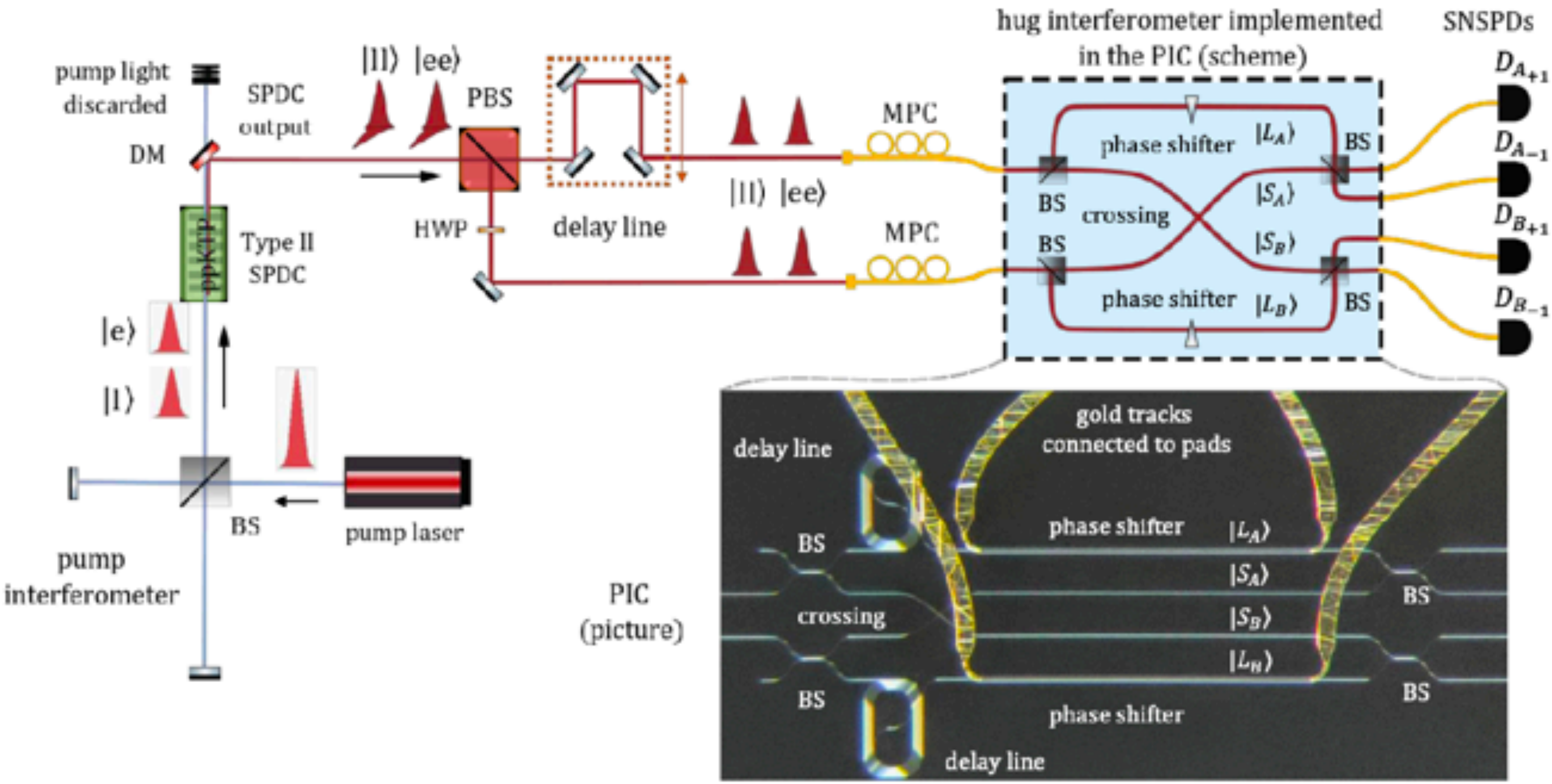
integrated solution by the hug interferometer





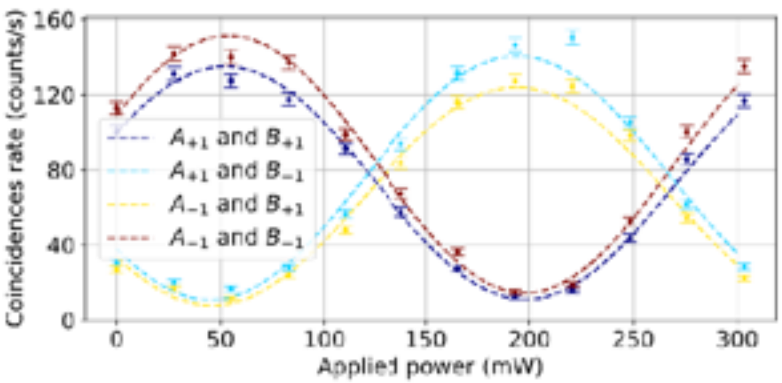
A. Cabello, A. Rossi, G. Vallone, F. De Martini, and P. Mataloni, Proposed Bell experiment with genuine energy-time entanglement, Phys. Rev. Lett. 102, 040401 (2009).

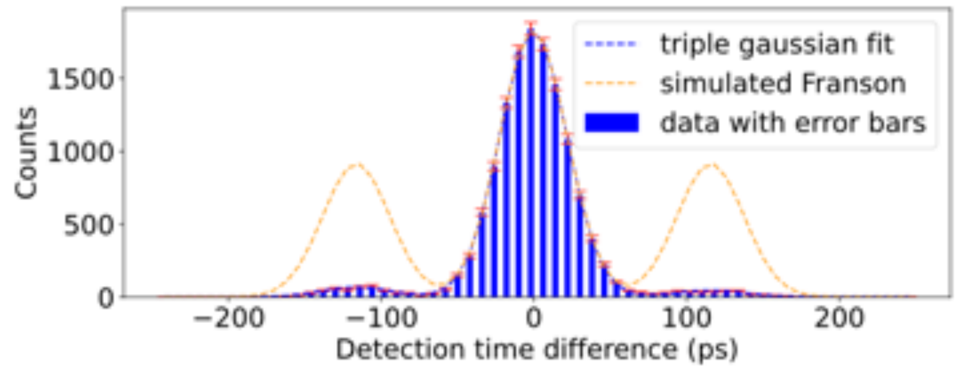
Integrated photonic general Bell-test chip for genuine TB and ET entanglement certification



F. B. L. Santagiustina et al. Experimental post-selection loophole-free time-bin and energy-time nonlocality with integrated photonics. Optica 11, 498 (2024).

Integrated photonic general Bell-test chip for genuine TB and ET entanglement certification





Histogram of detection time differences for arrivals at detectors $D_{A_{+1}}$ and $D_{B_{+1}}$ with bin-width of 8 ps.

First implementation of a hug interferometer inside a photonic integrated circuit (PIC)

usefulness as a certification tool for both genuine (i.e., post-selection loophole-free) energy-time (ET) and time-bin (TB) entanglement.

Using the PIC hug interferometer, **violation of a Bell inequality using genuine TB entangled photons and the hug configuration reporting a CHSH-Bell parameter of 2.42 ± 0.05.**

F. B. L. Santagiustina et al. Experimental post-selection loophole-free time-bin and energy-time nonlocality with integrated photonics. Optica 11, 498 (2024).

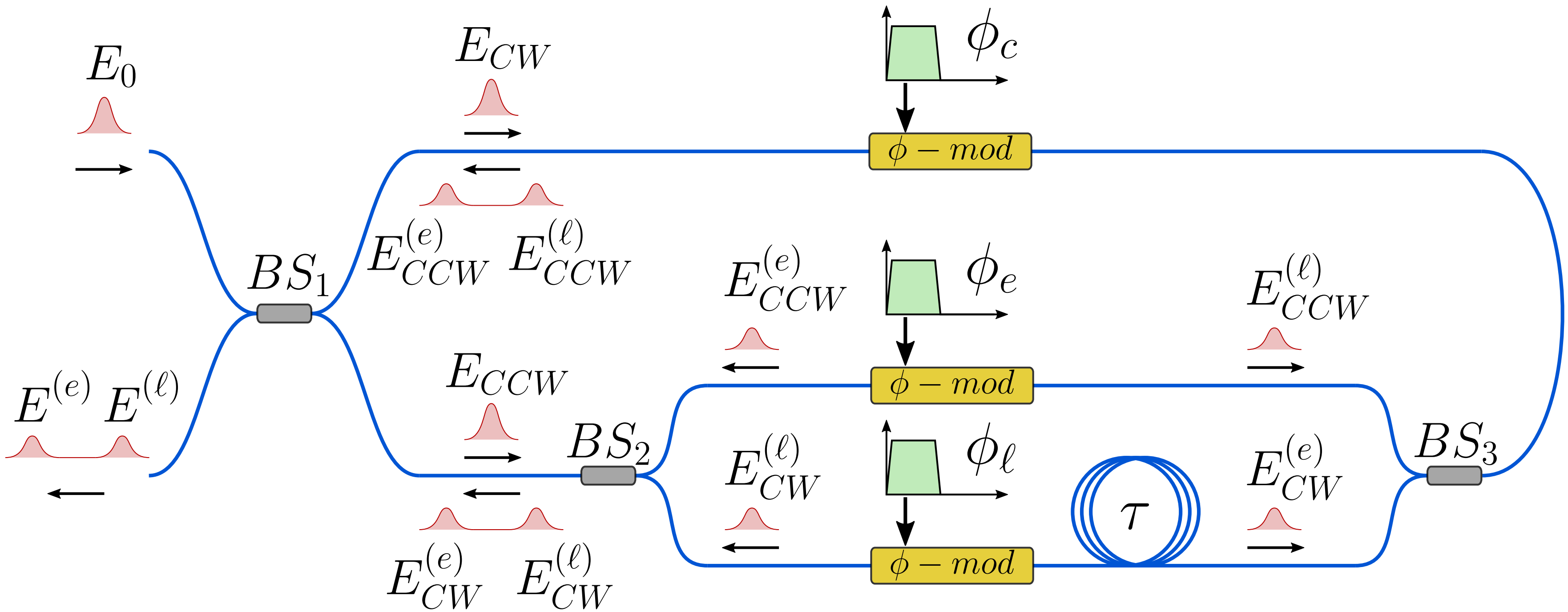
Evolution toward robust timebin source:
meet the **MacZac** Mach-Zehnder-Sagnac

- P&M DV QKD
- qubit generation and decoy in a single system
- intrinsic robustness to system instabilities
- low intrinsic qber
- design based on COTS

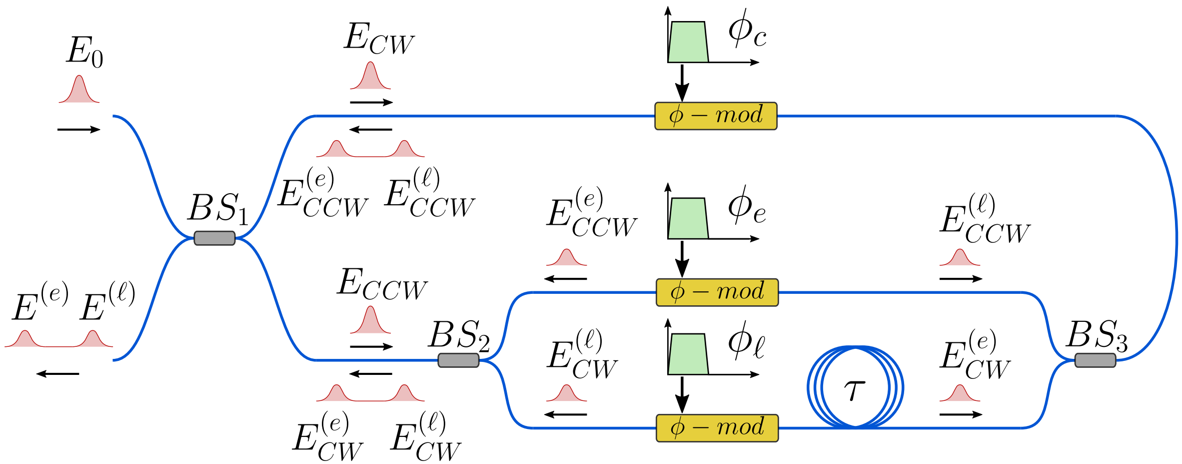
=> all-fiber-based and exploits a Mach-Zehnder interferometer nested in a Sagnac loop.. hence the name **MacZac**

Low-error encoder for time-bin and decoy states for quantum key distribution
Davide Scalcon, Elisa Bazzani, Giuseppe Vallone, Paolo Villoresi, Marco Avesani
npj Quantum Inf. https://doi.org/10.1038/s41534-024-00923-9 (2024) pat. app.

MacZac Mach-Zehnder-Sagnac



MacZac output



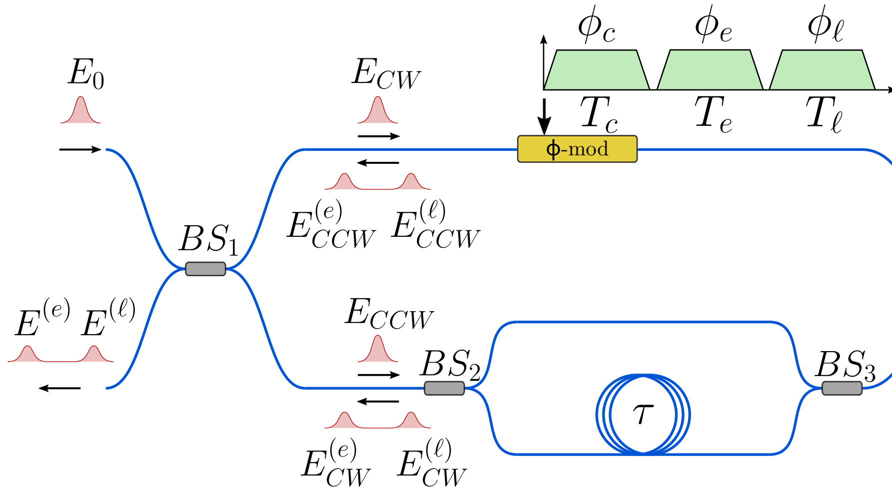
$$|\psi_{\text{out}}\rangle = \sqrt{T_e}\,|E\rangle - e^{i\delta\phi}\sqrt{T_\ell}\,|L\rangle$$

where $|E\rangle$ and $|L\rangle$ are the e and ℓ time-bins while

$$T_{e,\ell} = \frac{1}{4}\sin^2\frac{\phi_c - \phi_{e,\ell}}{2}\,, \qquad e^{i\delta\phi} = e^{i\frac{\phi_\ell - \phi_e}{2}}$$

The output quantum state can be controlled by properly setting the three phases φc, φe and φl.
All BSs with a splitting ratio of 1/2
$e^{i\omega\tau} = 1$, i.e. the relative phase imposed by the two arms is zero

simplified MacZac: 1 modulator

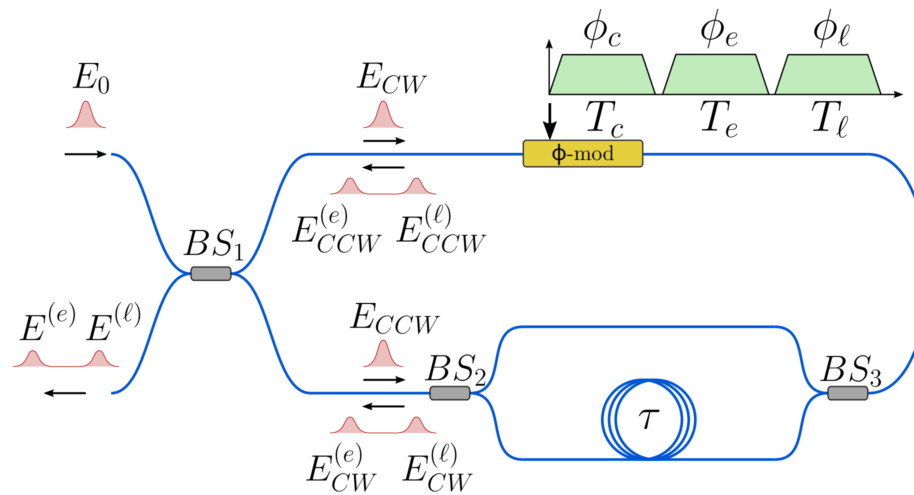


- By suitably changing the modulating voltage signal at different times, the phase modulator can set the phases φc, φe, and φl.
- to generate |E⟩ (|L⟩), the control electronics applies an electric pulse to the phase modulator when is travelled by the e (l) component of the CCW light.
- The |−⟩ state is produced by modulating the single CW laser pulse.

simplified MacZac: 1 modulator + decoy

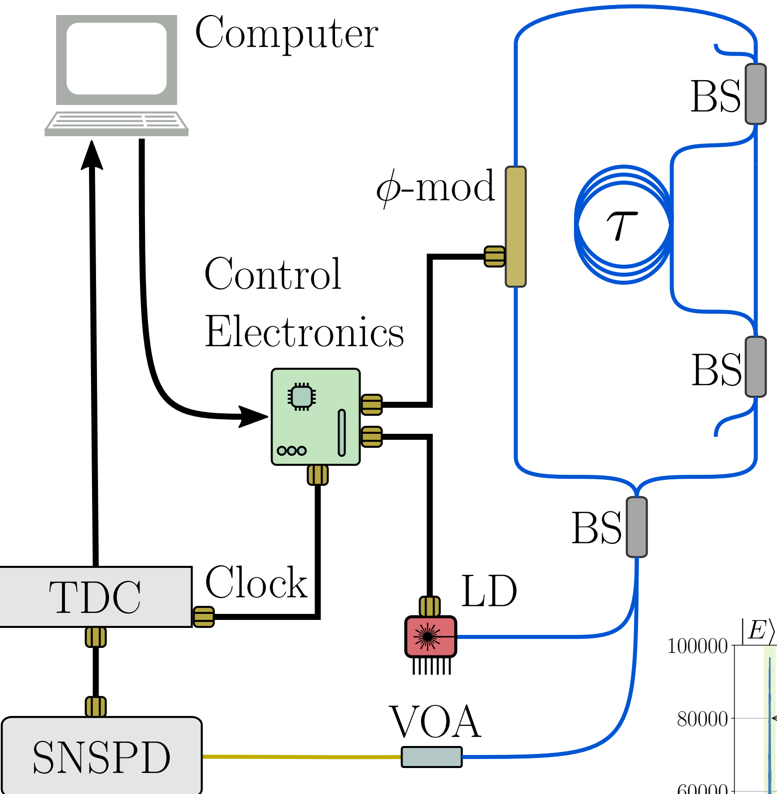
State	Decoy	Time slot	ϕ_c	ϕ_e	ϕ_ℓ
$\|E\rangle$	μ (decoy high)	T_E	0	α_μ	0
$\|E\rangle$	ν (decoy low)	T_E	0	α_ν	0
$\|L\rangle$	μ (decoy high)	T_L	0	0	α_μ
$\|L\rangle$	ν (decoy low)	T_L	0	0	α_ν
$\|-\rangle$	μ (decoy high)	T_-	β_μ	0	0
$\|-\rangle$	ν (decoy low)	T_-	β_ν	0	0

$$\sin^2\left(\frac{\alpha_\nu}{2}\right) = \frac{\nu}{\mu}\sin^2\left(\frac{\alpha_\mu}{2}\right)$$

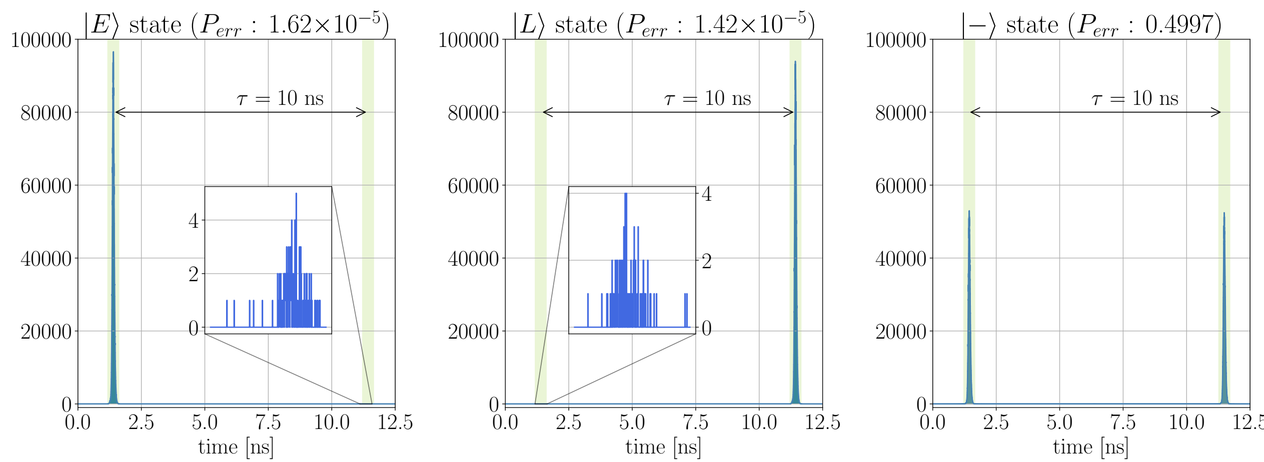


- Amplitude and time position of the pulses generated by the control electronics for all possible state to be prepared.
- Time instant TE (TL) means that the output is triggered when the early (late) component of the counterclock- wise signal crosses the phase modulator, T- specifies that the output instant coincides with the time in which the clockwise pulse goes through the phase modulator.

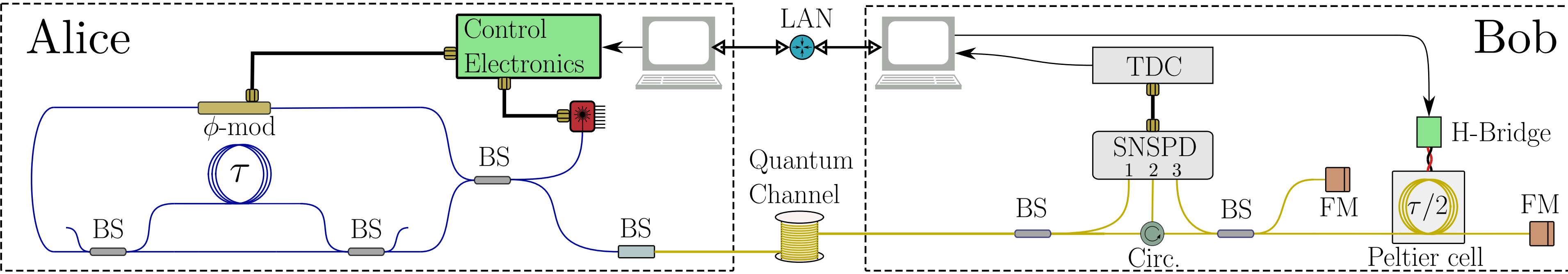
MacZac at test: QBER and extinction ratio

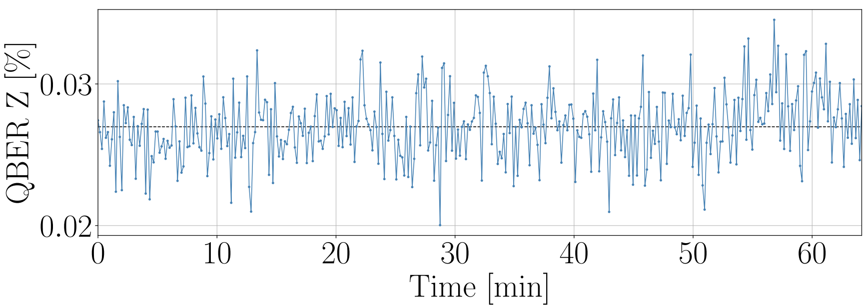


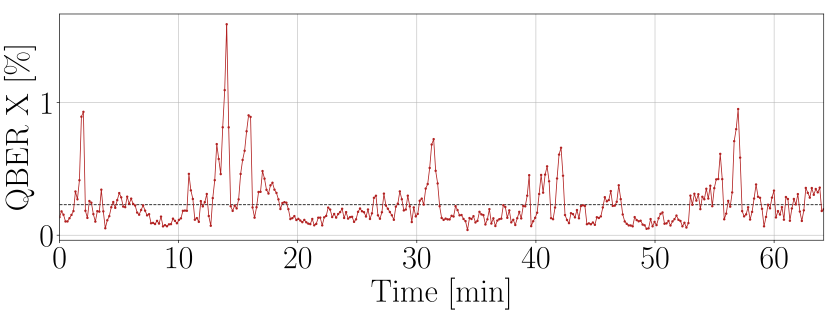
- Perr = 1.62 10^{-5} ± 1.4 10^{-6} (ER = 47.9±0.4dB) for early state
- Perr = 1.42 10^{-5} ± 1.3 10^{-6} (ER = 48.5±0.4dB) for late state



MacZac for QKD

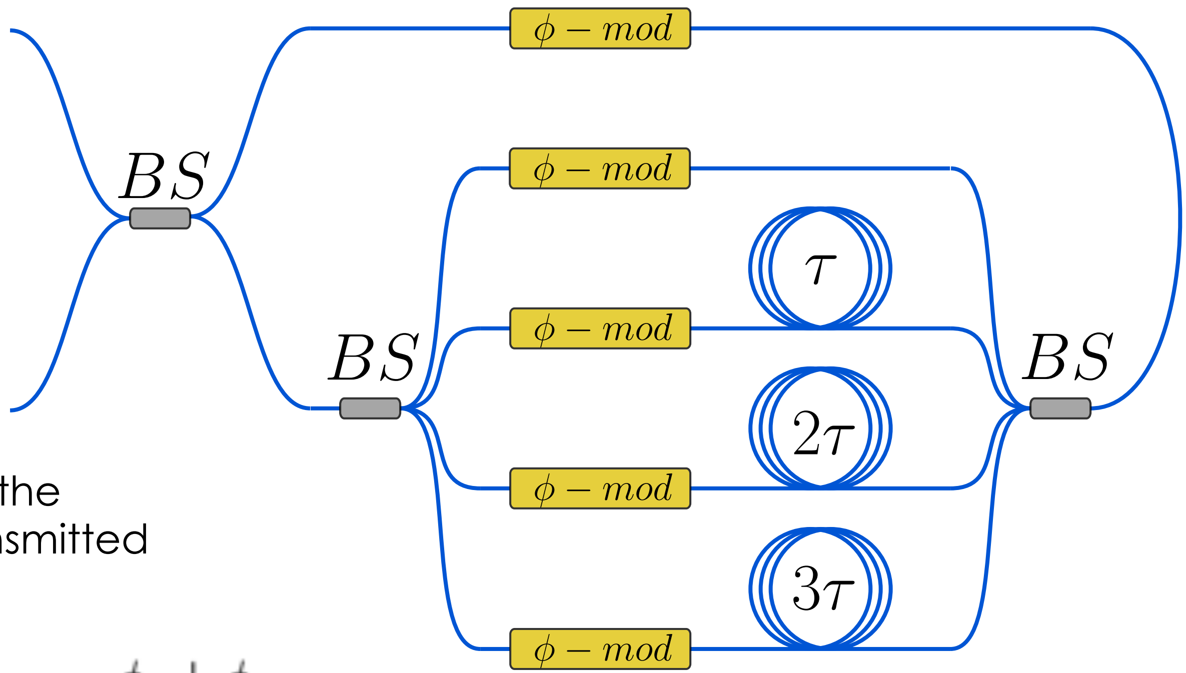






	mean	std
QBER Z [%]	0.027	0.012
QBER X [%]	0.23	0.29
SKR [kbps]	19.3	1.5
Sifted [kbps]	80.4	1.2
Detection rate [kHz]	112.9	1.7

MacZac for **qudits**



Assuming BS splitting as 50/50, the complex amplitude of the transmitted light in the k–th time slot is:

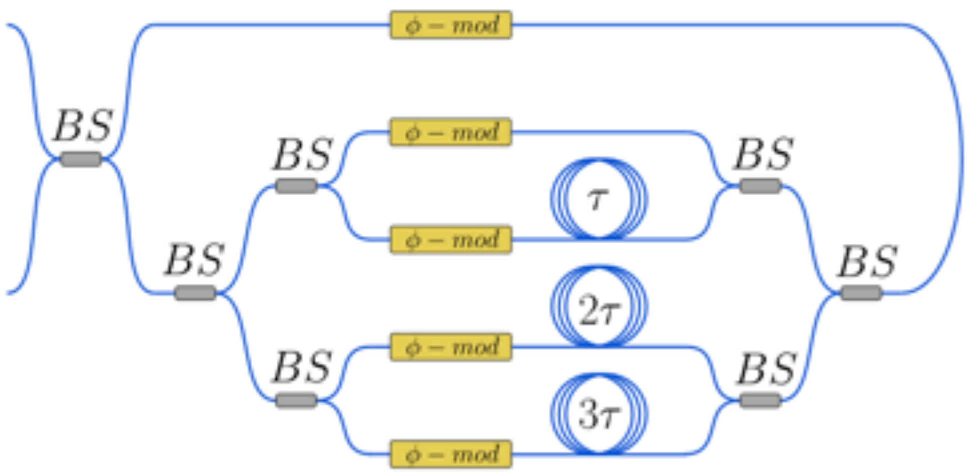
$$E^{(k)} = \frac{iE_0}{d} e^{\phi_+^{(k)}} \sin \phi_-^{(k)} \,, \quad \phi_\pm^{(k)} = \frac{\phi_c \pm \phi_k}{2}$$

while the corresponding transmittance is

$$T_{\phi_c,\phi_k}^{(k)} = \frac{|E_{out}^{(N)}|^2}{|E_{in}|^2} = \frac{1}{d^2} \sin^2 \left(\frac{\phi_c - \phi_k}{2} \right)$$

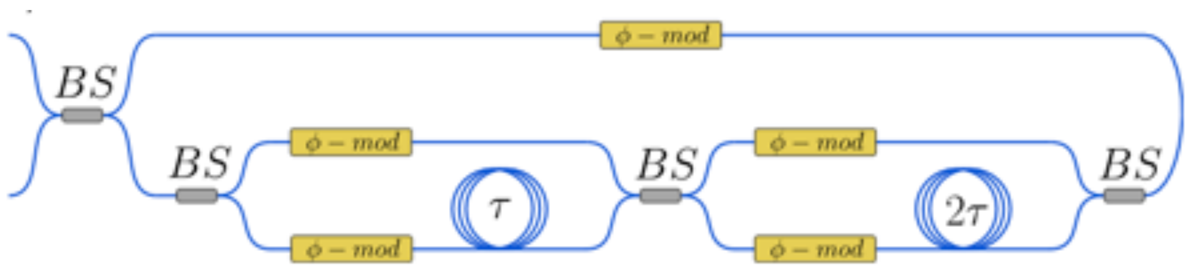
M-Z beamsplitters N+1

variants in the MacZac for qudits



Scheme for the generation of four dimensional states **using two by two beamsplitters** in a series of two interferometers

Using instead two interferometers in parallel



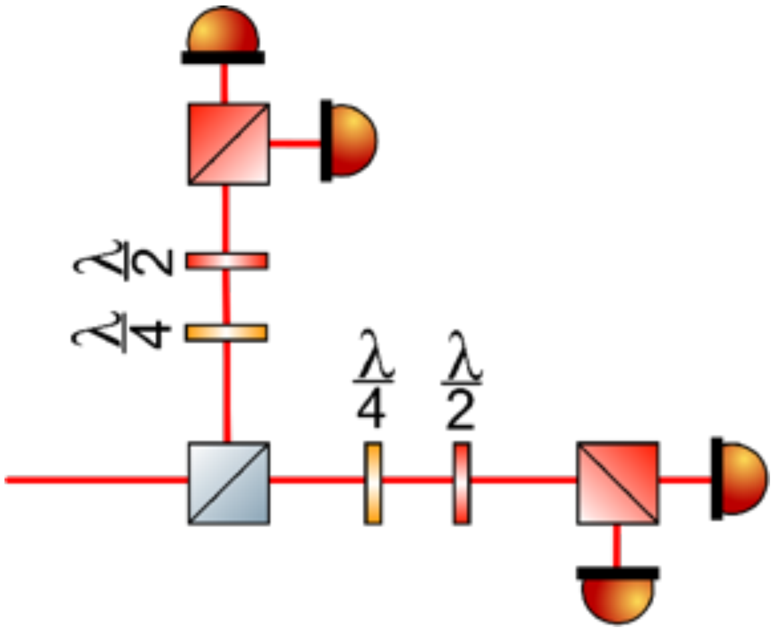
Low-error encoder for time-bin and decoy states for quantum key distribution
Davide Scalcon, Elisa Bazzani, Giuseppe Vallone, Paolo Villoresi, Marco Avesani
npj Quantum Inf. https://doi.org/10.1038/s41534-024-00923-9 (2024) pat. app.

rationale for pol-coded space QKD

- Simple state decoding
- Unperturbed atmospheric propagation
- Kinematic effects can be easily corrected
- **Compatible with fiber-based networks on ground**
  - **reduce the number of Bobs**
  - **dislocate the QKD receiver from the telescope**
  - **intermodal QKD networks OpenQKD user case (Padua)**

rationale for pol-coded space QKD

- **Simple state decoding**
  - Developed with HWP, QWP, PBS
  - Requires no “fine tuning” that depends on the transmitter



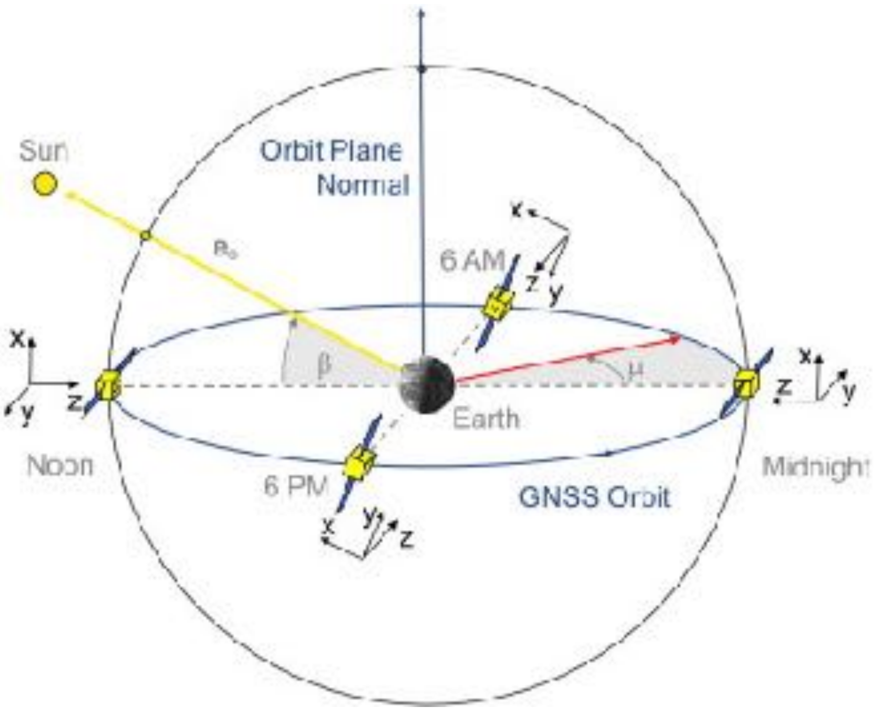
rationale for pol-coded space QKD

- Simple state decoding
- **Unperturbed by atmospheric propagation**
  - Perturbations on the polarization of an electromagnetic wave due to turbulence, scattering processes or Faraday effect account for about 0.001rad

- C. Bonato et al., "Influence of satellite motion on polarization qubits in a Space-Earth quantum communication link," Opt. Express **14** 10050(2006)
- G. Vallone et al., "Experimental Satellite Quantum Communications," Phys. Rev. Lett. **115** 040502 (2015)

rationale for pol-coded space QKD

- Simple state decoding
- Unperturbed atmospheric propagation
- **Kinematic effects can be easily corrected**
  - Dependent on the relative rotation between ground station and satellite
  - Can be predicted beforehand
  - Correction only requires a HWP

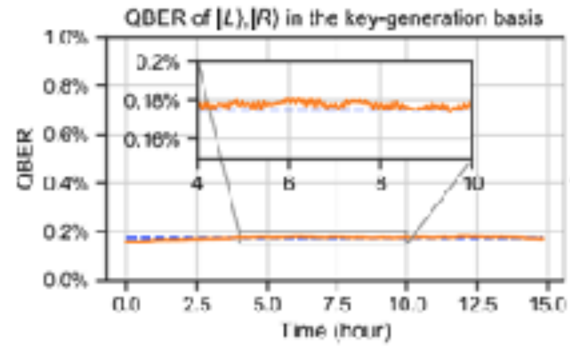


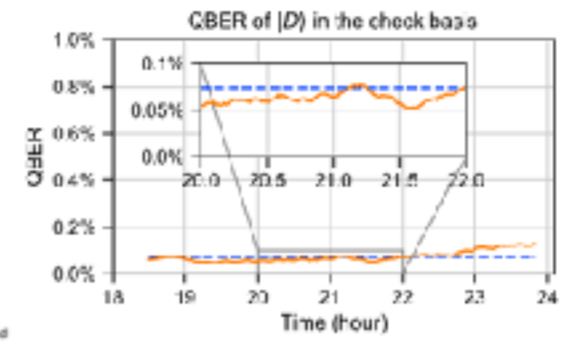
- C. Bonato et al., "Influence of satellite motion on polarization qubits in a Space-Earth quantum communication link," Opt. Express **14** 10050(2006)

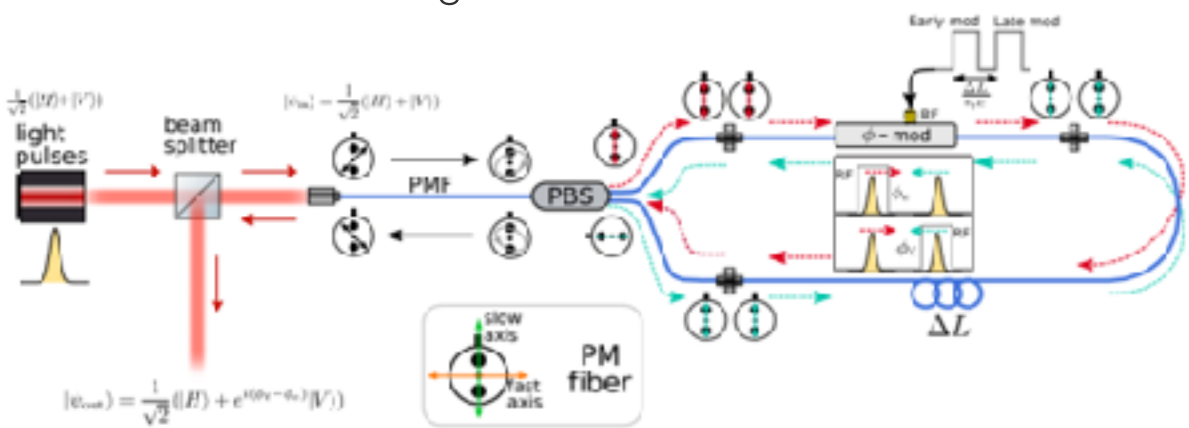
The I-POGNAC polarization encoder

aiming at stability and low noise

- Only one laser
- Self-compensating Sagnac interferometer: no need for stabilization and long term stability
- Record-low QBER: <0,2%
- PM input fiber: does not require calibration
- Can generate 3 states of polarization with only binary signals
- Requires lower modulation voltages than other solutions





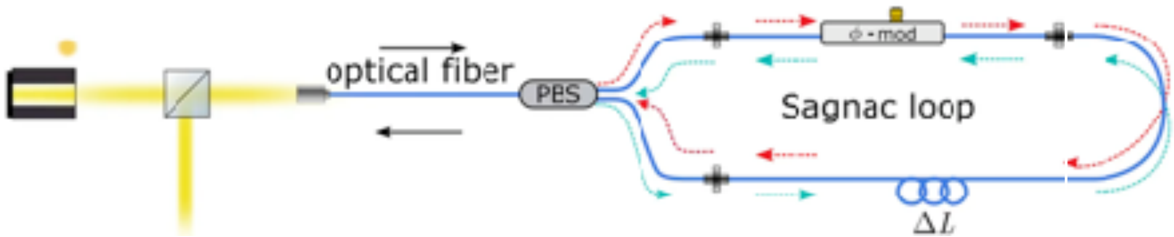


M. Avesani, et al., Opt. Lett. 45, 4706-4709 (2020)
patented

rationale for Alices's pol-coded qubit gen i-POGNAC

- Relative phase between orthogonal polarization components can be individually addressed based on time of arrival at the modulator.
- Sagnac Loop compensates fluctuations and PMD.
- Free-space input and output removes need for calibration and guarantees a fixed polarization output state.
- One laser only.
- Only phase is modulated.

$$|H\rangle + e^{i\phi}|V\rangle$$



$$\{|L\rangle, |R\rangle\} \quad |D\rangle$$

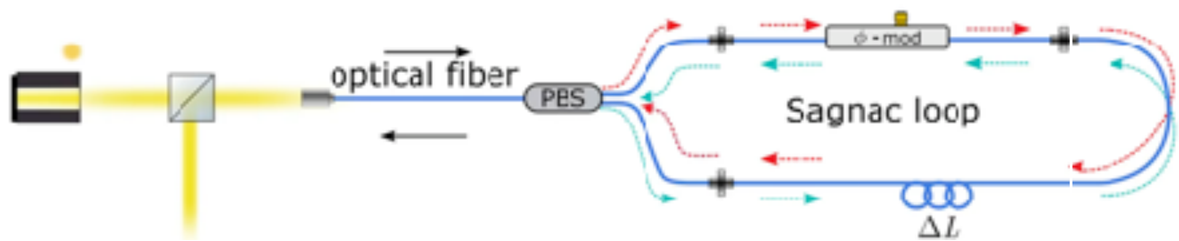
M. Avesani, C. Agnesi, A. Stanco, G. Vallone, and P. Villoresi, "Stable, low-error, and calibration-free polarization encoder for free-space quantum communication," Opt. Lett. **45** 4706 (2020)

rationale for Alices's pol-coded qubit gen i-POGNAC

$$|H\rangle + e^{i\phi}|V\rangle$$

Performances:

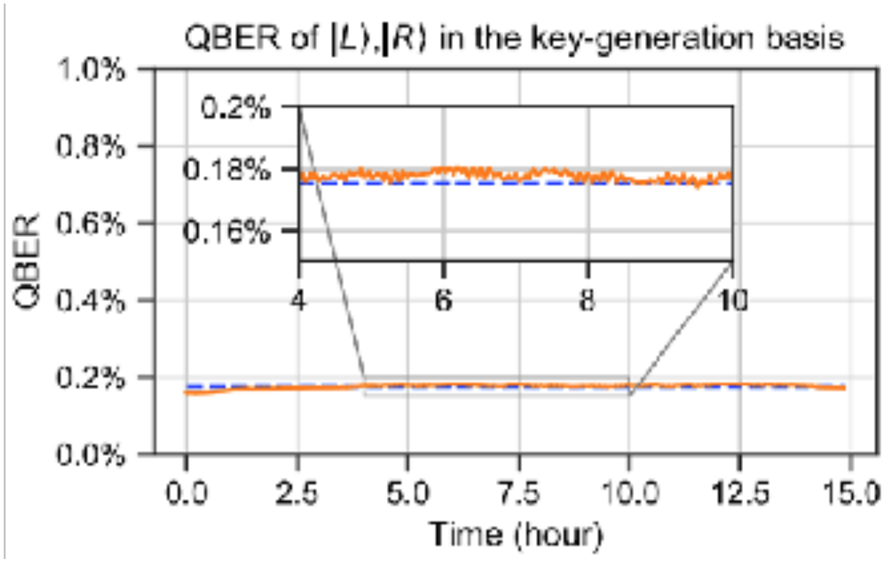
- No side-channel that can be exploited by Quantum Hackers ✓
- Stable performances ✓
- No calibration required before use ✓
- Well-defined polarization output states ✓
- Low intrinsic QBER ✓

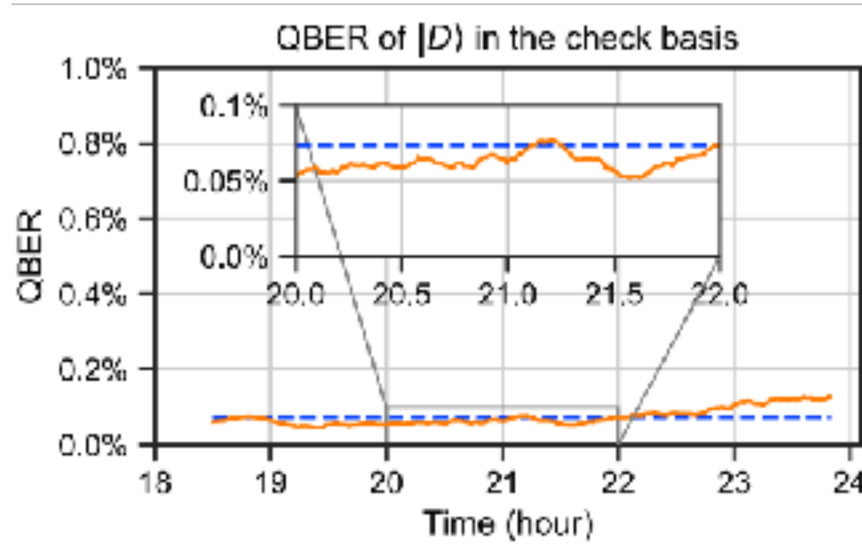


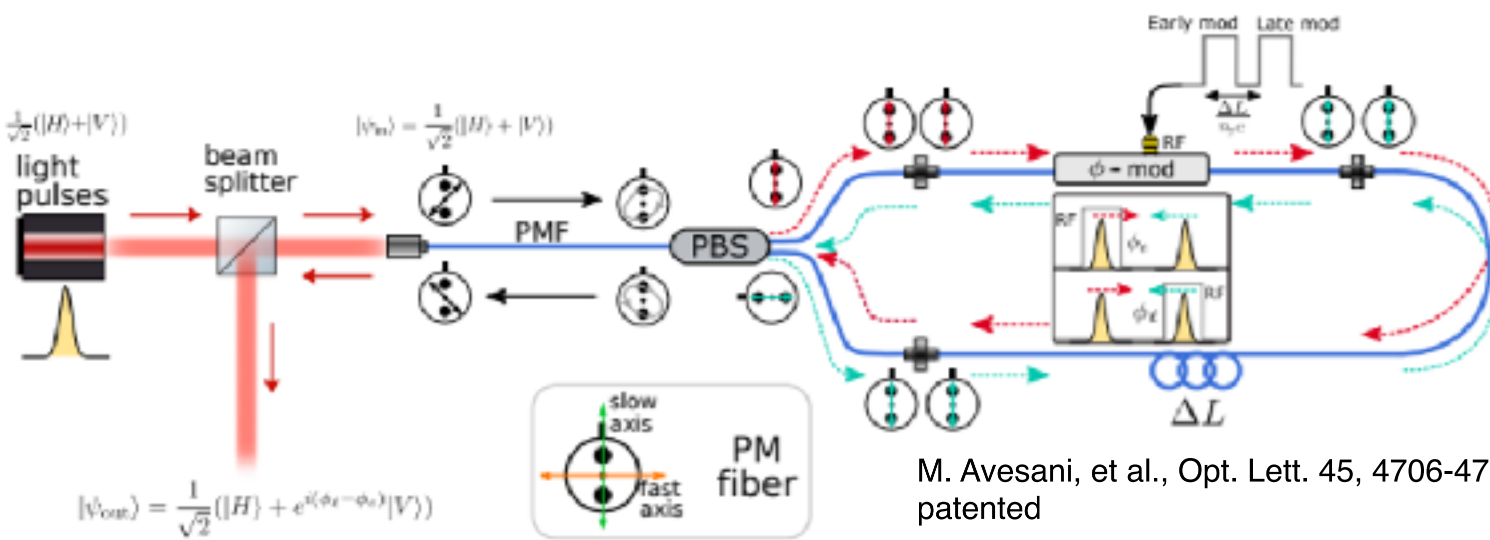
$$\{|L\rangle, |R\rangle\} \quad |D\rangle$$

Pat. ITA-102019000019373 (21.10.2019), PCT/EP2020/079471
Licensed to **ThinkQuantum srl**

i-POGNAC performances

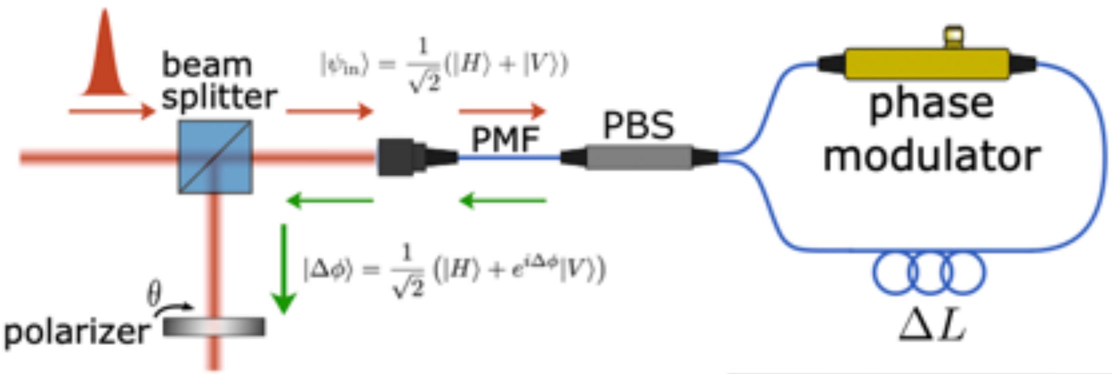


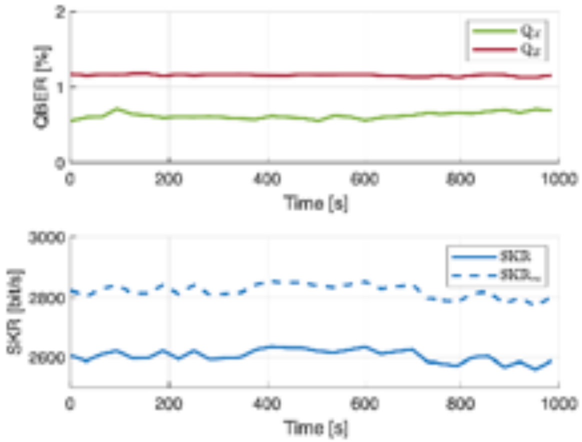


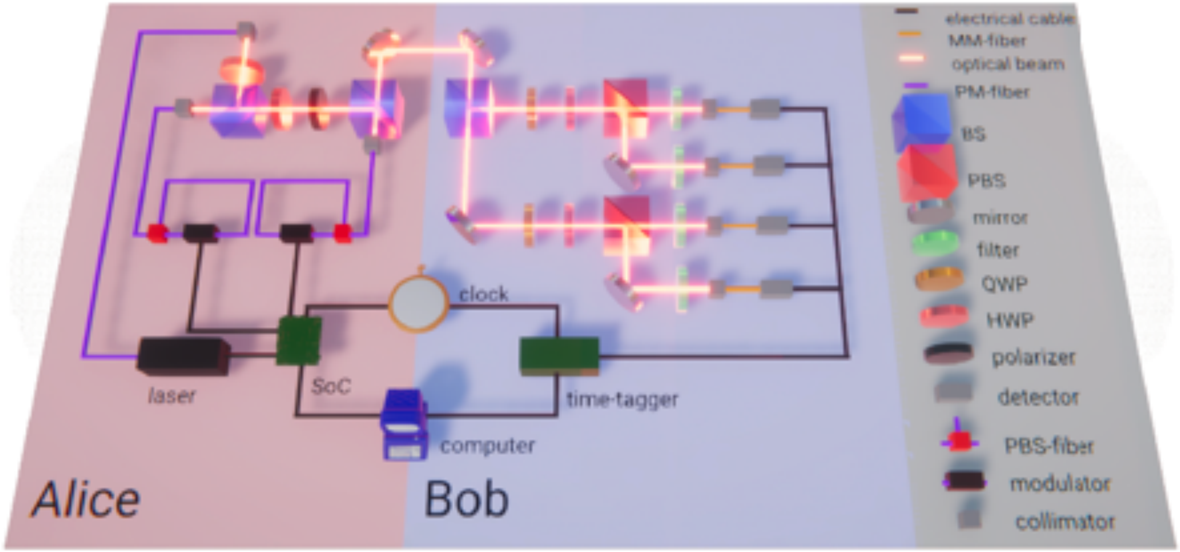


M. Avesani, et al., Opt. Lett. 45, 4706-4709 (2020)
patented

modular i-POGNAC: intensity and polarization modulation at 800 nm for complex payload

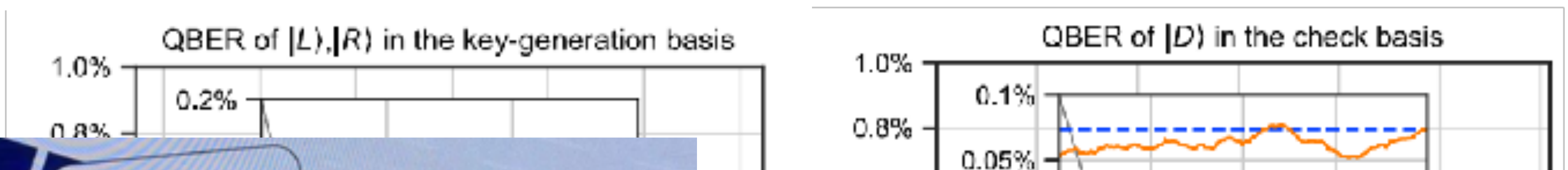






F. Berra et al. Modular source for near-infrared quantum communication. EPJ Quantum Technol. 10, 27 (2023).

i-POGNAC performances



IPA 2021

INTELLECTUAL PROPERTY AWARD CEREMONY

The award dedicated to the excellence of Italian Public Research

Save the date

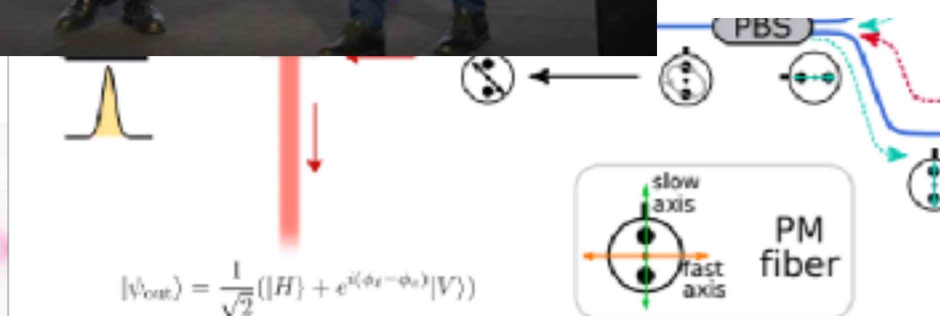
Dubai, Italy Pavilion, Amphitheatre

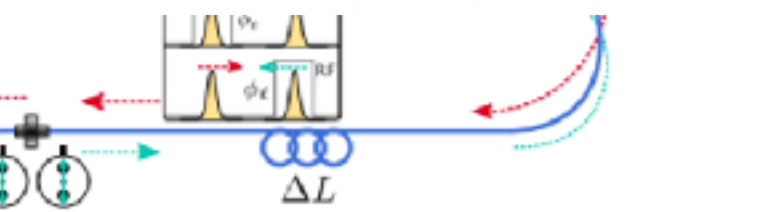
28th February - 1st March 2022

10.30 am – 03.00 pm (GMT+4) / 07.30 am - 12.00 pm (CET)

The event will be streamed on the following channels:

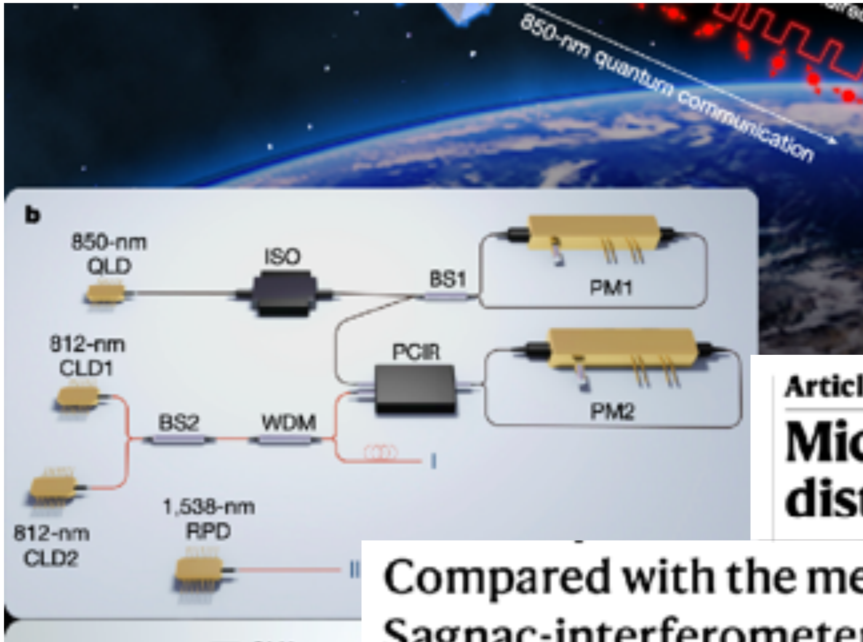
YouTube Italy Expo | Facebook Italy Expo

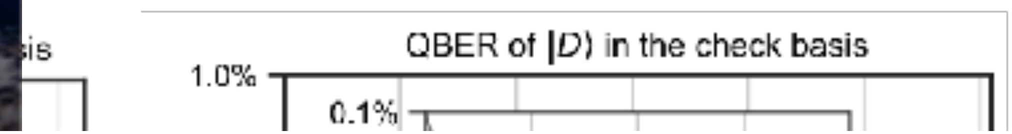




M. Avesani, et al., Opt. Lett. 45, 4706-4709 (2020)
patented

mances

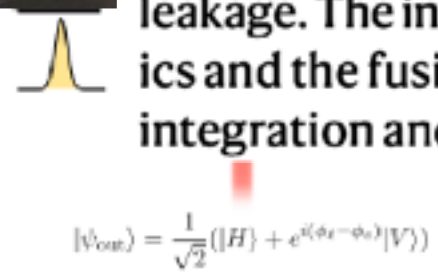




Article

Microsatellite-based real-time quantum key distribution

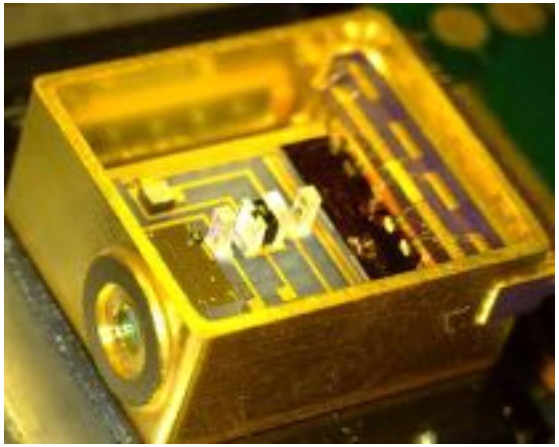
Compared with the method employing multiple laser diodes[6], this Sagnac-interferometer-based modulation scheme enables a much higher repetition rate while ensuring inherent robustness for complex spaceborne applications. The ground-test results showed an extinction ratio of approximately 29 dB and an average polarization contrast ratio of approximately 25 dB. By utilizing a single laser diode and outputting through a single-mode fibre (SMF), the inherent uniformity across other photon dimensions, such as space, time and frequency can be ensured, effectively mitigating the risk of potential side-channel information leakage. The integrated design of optical components, drive electronics and the fusion of optical-fibre components contribute to the high integration and light weight of the QKD light source.



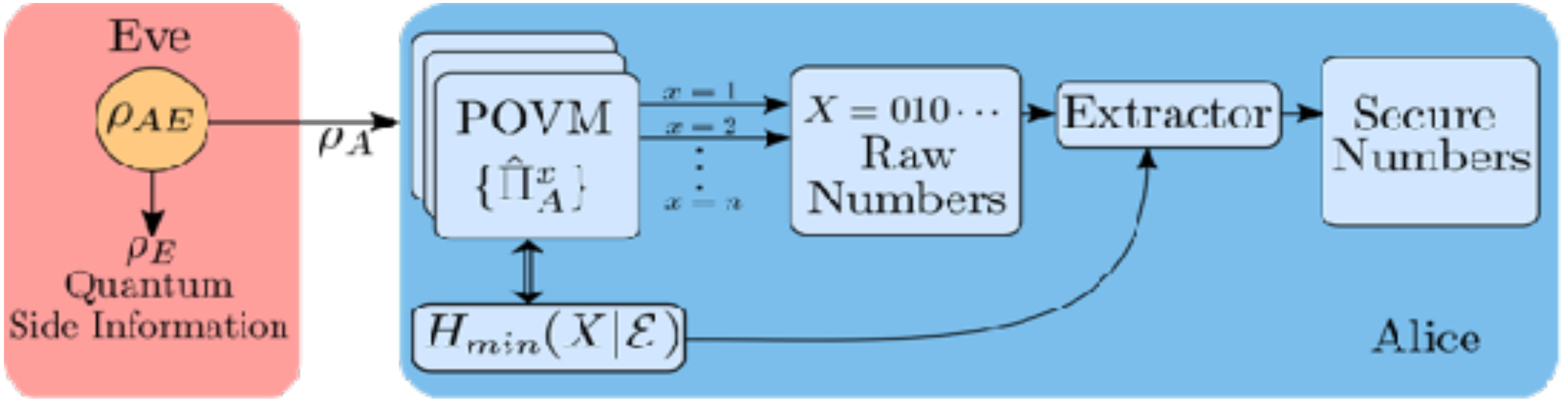
M. Avesani, et al., Opt. Lett. 45, 4706-4709 (2020) patented

Alice needs genuine random numbers..

- QKD starts from random numbers - as in the case of many applications
- their unpredictability is crucial for secure comms
- here: QRNG protocols are based on Uncertainty Principles



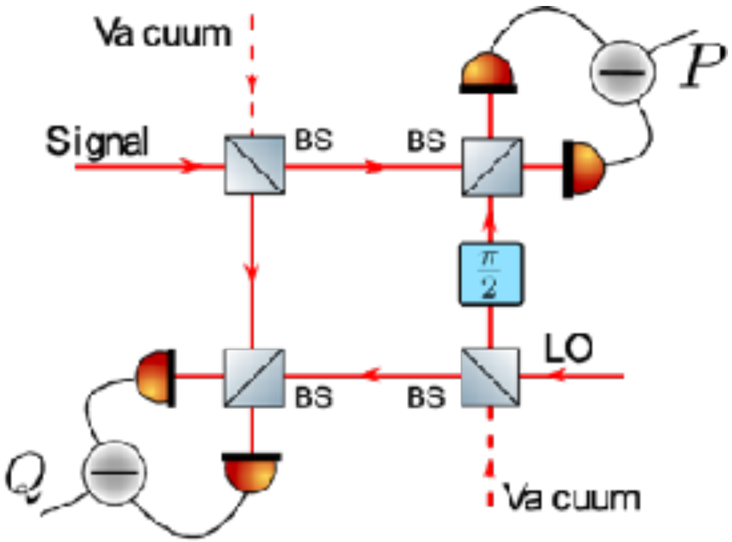
QRNG: Source Device-Independent scenario: the protocol

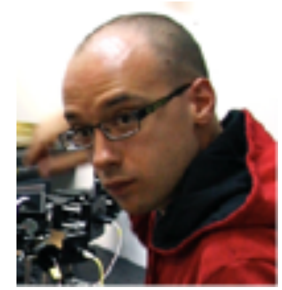


- Eve has full control on the source: she and Alice can share any bipartite sates at each round
- Valid for any set of generalized measurements (POVM) implemented by Alice
- The POVM are trusted, but don't need to be ideal
- The key element is the quantum conditional min-entropy, :
- It takes into account quantum side-information for a single-shot of the protocol
- Use the Leftover Hashing Lemma to get the secure numbers

1. Vallone, G., Marangon, D. G., Tomasin, M. & Villoresi, P. Quantum randomness certified by the uncertainty principle. Phys. Rev. A 90, 52327 (2014).
2. Marangon, D. G., Vallone, G. & Villoresi, P. Random bits, true and unbiased, from atmospheric turbulence. Sci. Rep. 4, 5490 (2015).
3. Marangon, D. G., Vallone, G. & Villoresi, P. Source-Device-Independent Ultrafast Quantum Random Number Generation. Phys. Rev. Lett. 118, 060503 (2017).
4. Michel, T. et al. Real-Time Source-Independent Quantum Random-Number Generator with Squeezed States. Phys. Rev. Appl. 12, 034017 (2019).

QRNG: Heterodyne Source-DI QRNG





Heterodyne POVM = $\Pi = \frac{1}{\pi}|\alpha\rangle\langle\alpha|$

Overcomplete set POVM, projection on coherent states

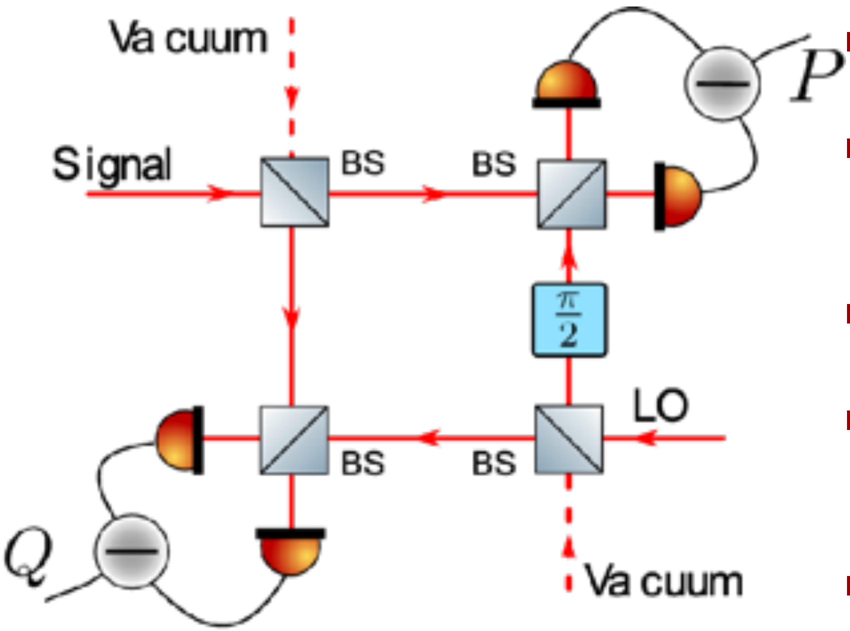
The outcome of the measured quantum state ρ_A is modelled as a random variable X with probability density function Q(q, p)

- The attacker cannot guess the outcome with a probability larger than $1/\pi$

$$P_{guess}(X|\mathcal{E}) \leq \max_{\alpha,\tau_W \in \mathcal{H}_A} Q_{\tau_W}(\alpha) = \frac{1}{\pi}$$

M. Avesani et al., **Source-device-independent heterodyne-based quantum random number generator at 17 Gbps** Nature Comm 9, 5365 (2018)

QRNG: Heterodyne Source-DI QRNG

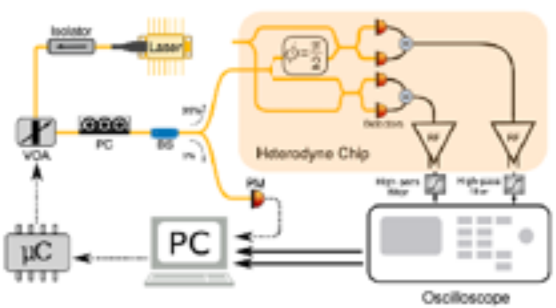


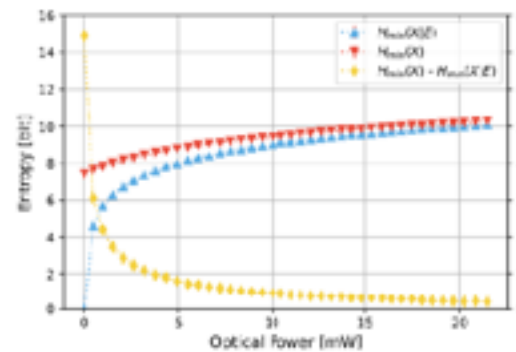
- No initial seed needed
- POVM such that no need for update the QBER and the extraction param.
- All passive design - no switches
- Speed scales with electronic performances - fits to actual needs
- Integrated & bulk versions ready

M. Avesani et al., **Source-device-independent heterodyne-based quantum random number generator at 17 Gbps** Nature Comm 9, 5365 (2018)

A Si-Phot QRNG for Space Applications: ASI QNRG project

- We are developing with the Italian Space Agency, an integrated, secure and high speed Source-DI QRNG on a silicon-photonics chip





- double homodyne measurement via a 4×4 MMI - the output optical signals are then detected by two balanced detectors pairs endowed with 20GHz of bandwidth - the generated photo-currents, proportional to the two EMF q, p quadratures, are readily amplified by a custom developed 3-stage fully-differential amplifier board, integrated inside the QRNG package.

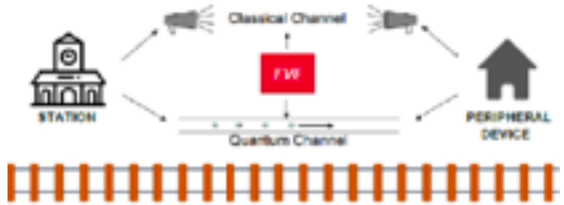
- We are able to **generate random bits at more than 20 Gbps** with offline post-processing,

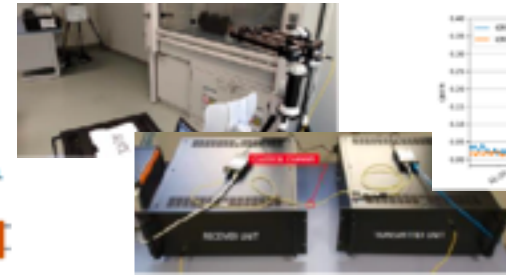
- 2Gbps with online postprocessing on the FPGA

T. Bertapelle et al, Optica Quantum **3** 111 (2025 - arXiv:2305.12472)

QKD applications with diverse players

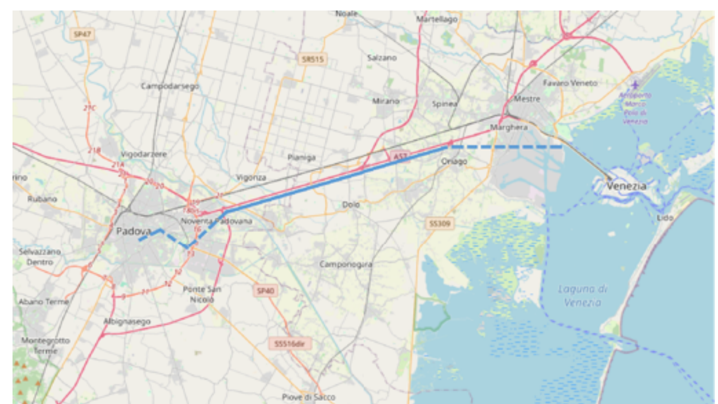
- Italian Railways RFI
  - M. Ermini et al WCRR2022





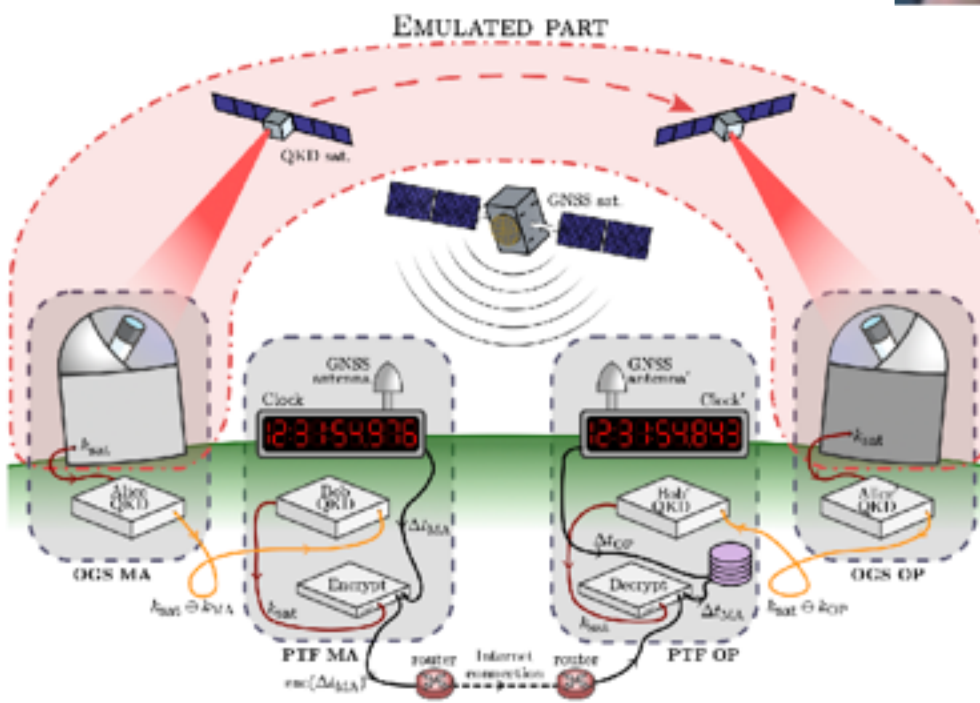
- Intermodal in Vienna and Padua
  - Hubel et al OFC 2023

- Veneto Region QCI:
  - multi wavelengths on single fiber Foletto et al. - TNC2023
  - Motorways, Region, UniPD
- Energy distribution networks



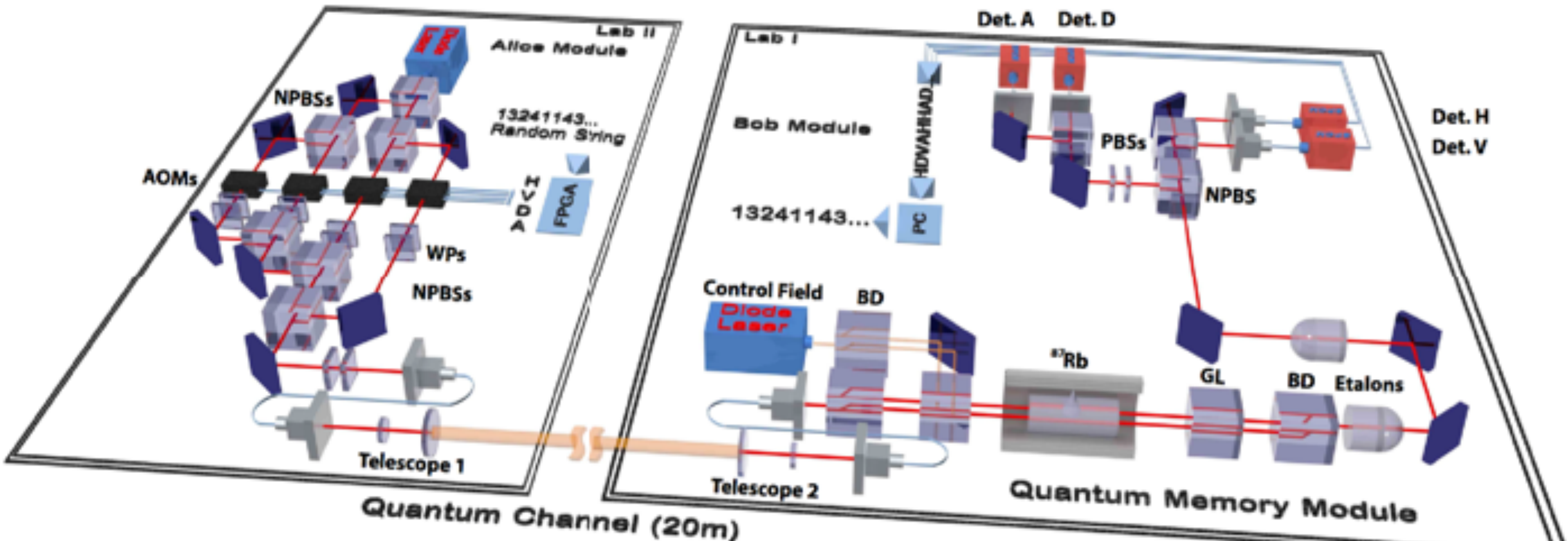
Quantum Application for Galileo GNSS

- Securely transmitting clock difference data needed for synchronization of clocks of two distant **Precise Timing Facilities PTF**
- **The security and integrity of the communication between PTFs is of paramount importance: if compromised, it could lead to disruptions to the GNSS service.**
- demo between **German Aerospace Center** (Deutsches Zentrum fur Luft- und Raumfahrt, DLR) in **Oberpfaffenhofen** (OP); the second is located at the **Matera Laser Ranging Observatory** (MLRO) of the **Italian Space Agency in Matera** (MA)



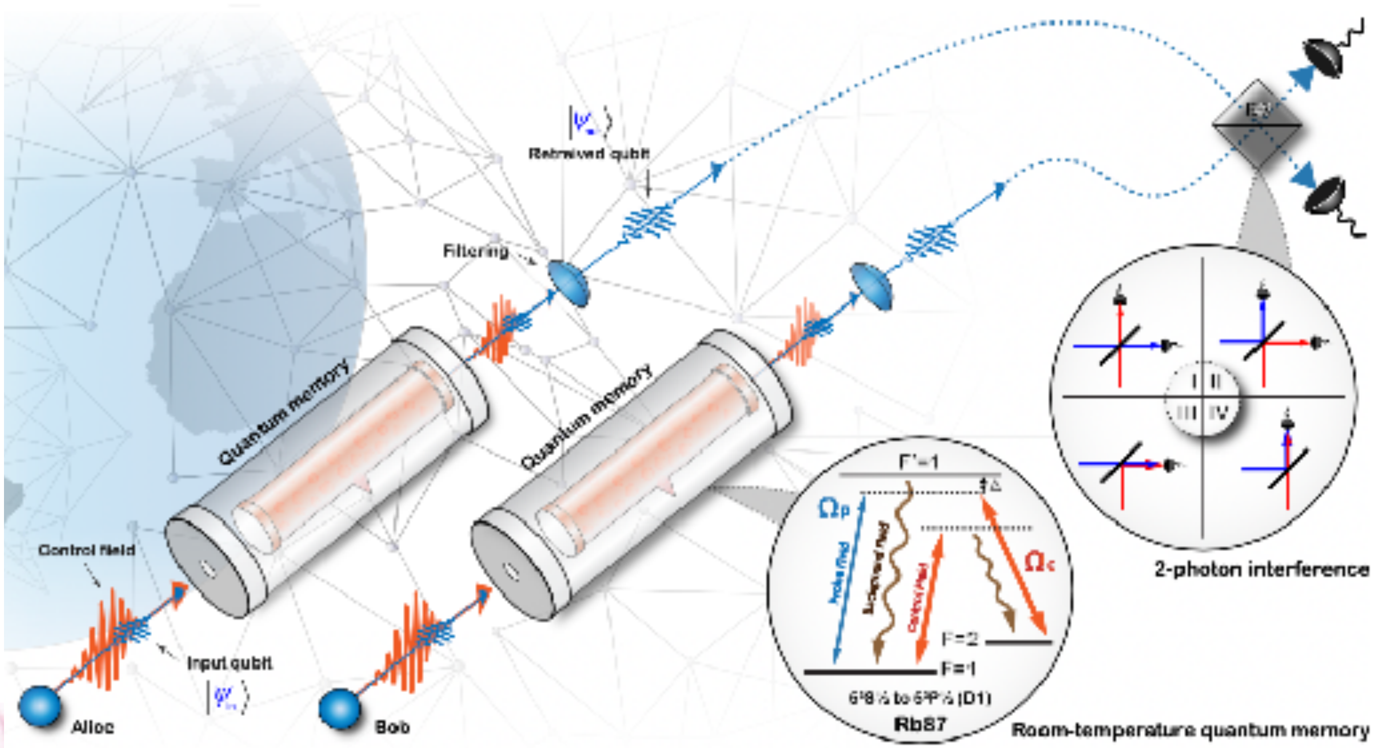
F. Picciariello et al. *International time transfer between precise timing facilities secured with a quantum key distribution network*, GPS Solutions **28** 48 (2024)

Rb memory for free-space BB84 QKD



M. Namazi et al,
Free space quantum communication with quantum memory
Phis. Rev. Applied 8, 064013 (2017)

Hong-Ou-Mandel interference of polarization qubits stored in independent room-temperature quantum memories



Mael Flament, Sonali Gera, Alessia Scriminich et al. arXiv:1808.07015v2
NPJ Quantum Information **10** 10 2024 10.1038/s41534-024-00803-2

postselection-free time-bin entanglement scheme1550 nm

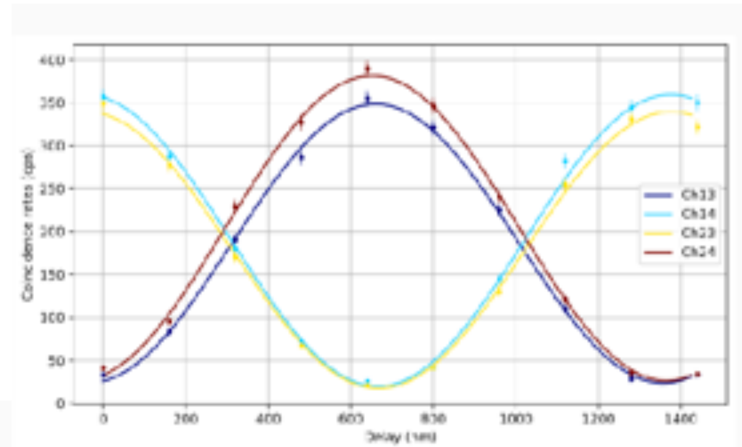
Kannan Vijayadharan

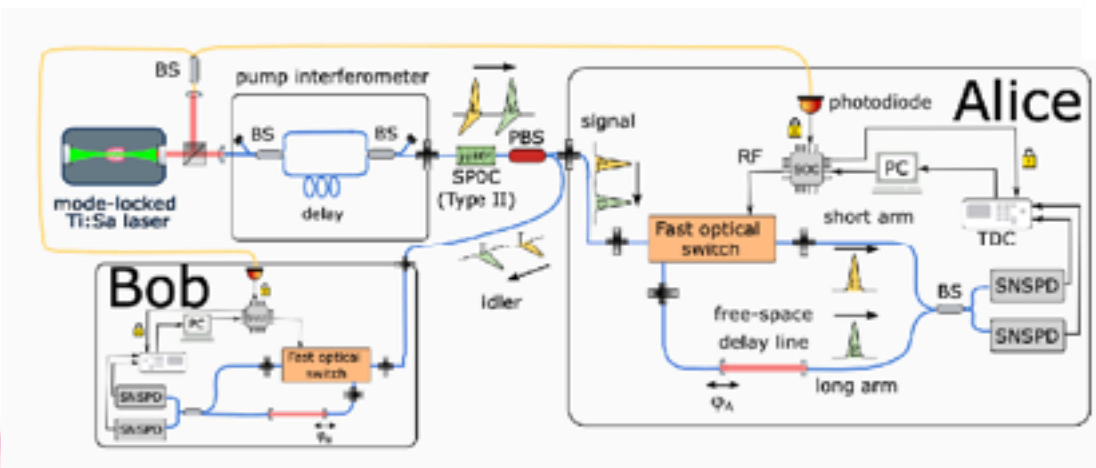
All fiber design with most COTS parts

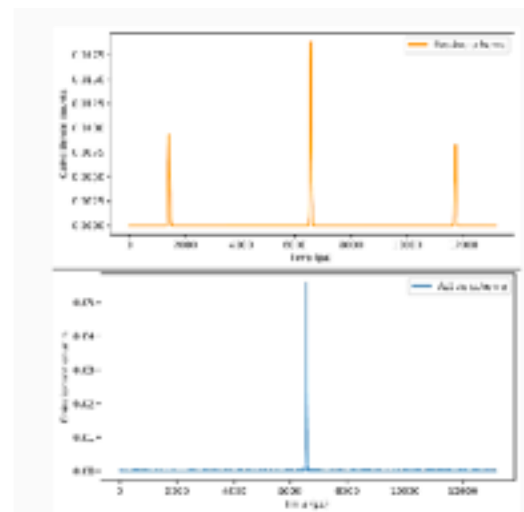
Improve the receiver interferometer design to have higher phase stability and extinction ratio

Improved visibility and Bell violation S= 2.65

Very high switch extinction ratio of up to 30 dB (99.9%)

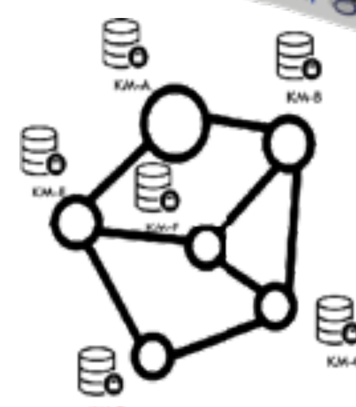






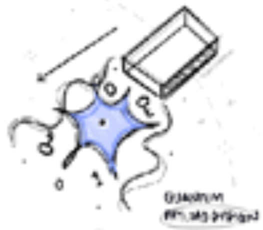
QKD Applications by spinoff

- The i-Pognac and the SDI-QRNG patents were the basis for spin out the applications on large scale
- ThinkQuantum formed in 2021, from part of the QuantumFuture group @ UniPD and Officina Stellare spa
- QKD systems Polarization-based encoding using the IPOGNAC;
  - Integrated proprietary QRNG; Compatible with ETSI 04, 014, SKIP, 2U system
  - Secret Key Rate 2.2/4.4 kb/s (13dB) [InGaAs], 18 kb/s (13dB) [SNSPD]
  - Max losses 24dB / >33dB
- QRNG Source-device independent, post-processed rate: 330 Mbps
- Key Management System [KMS], creation of virtual links through the use of trusted nodes. Exposes APIs to grant access to the generated key to applications/services, compatible with ETSI GS QKD 14, ETSI GS QKD 4 standards, SKIP,…



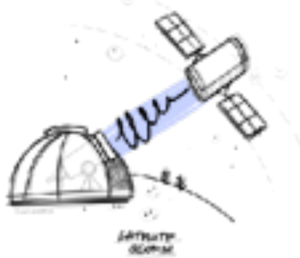
QKD Applications by spinoff

Space-domain & Free-Space Solutions



QKD Payload

- Design and assembly of QKD payload



Optical Ground Station

- Automatic Pointing-Acquisition-Tracking
- Free-space coupling (optional fiber-coupling with Adaptive Optics)

Free-space optical link

- Ground-to-ground link
- Common technologies/challenges of OGS
- Daylight operation

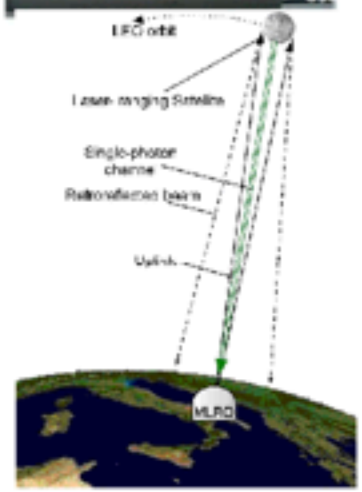
ThinkQUANTUM

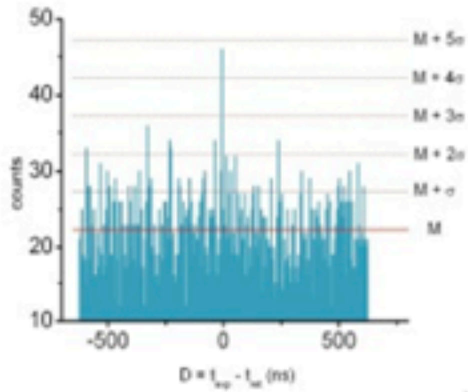
QUDICE
QUantum Devices and subsystems for Communications in spacE

Italian Space Quantum Communications

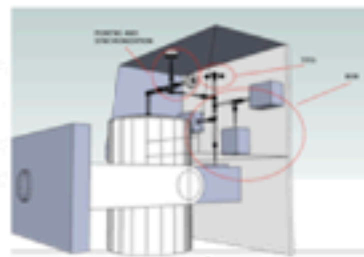
Exchanging quantum states, or quantum communications, allows for the realization of Quantum Information protocols as Quantum Teleportation and Q Key Distributions.

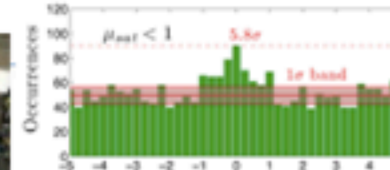
QuantumFuture Research Group of University of Padova, operated since **2003** at ASI **Matera Laser Ranging Observatory,** using its **1.5 m telescope with millimeter resolution in Satellite Laser Ranging.**

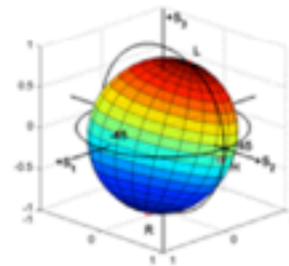




P. Villoresi et al.
New J. Phys.
10 033038 (2008)







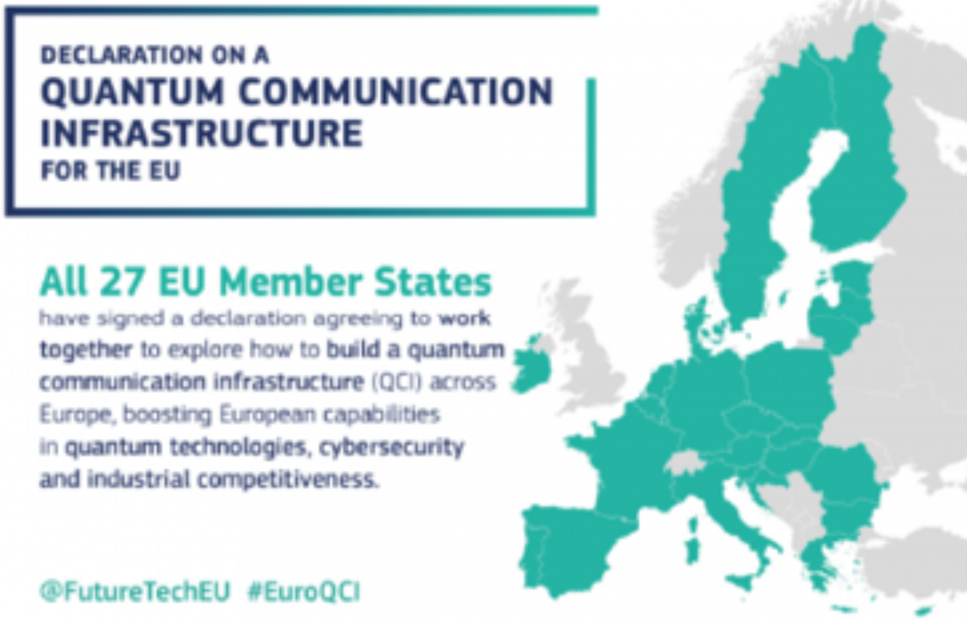
G. Vallone et al. Phys. Rev. Lett. vol 115 040502 (2015)

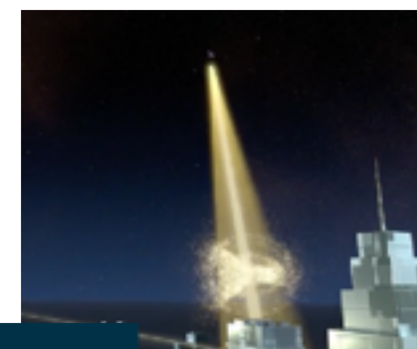
SpaceQ project together with Prof. Anton Zeilinger Group (2003-2008)

first Space QComm as APS highlight of the year

F. Vedovato et al. - Science Adv. 3 e1701180 (2017) Wheeler Delayed Choice Exp to Space

Q-Comms in Europe: fibers and satellites






QSN
PARTNERSHIP
Long Term Goal
Quantum Secure Networks
1|
Advanced technology for quantum secure communication networks against the ever increasing power of computers and sophistication of algorithms (even for quantum computers)
2|
Integration of quantum cryptography technology at component, system and network levels, also into classical communication
3|
Quantum-safe critical governmental infrastructures, private telecommunication market sector and future quantum internet

Quantum Cryptography & Beyond

Secure multi-party computation

Long-term secure storage (LTSS) based on proactive secret sharing and QKD

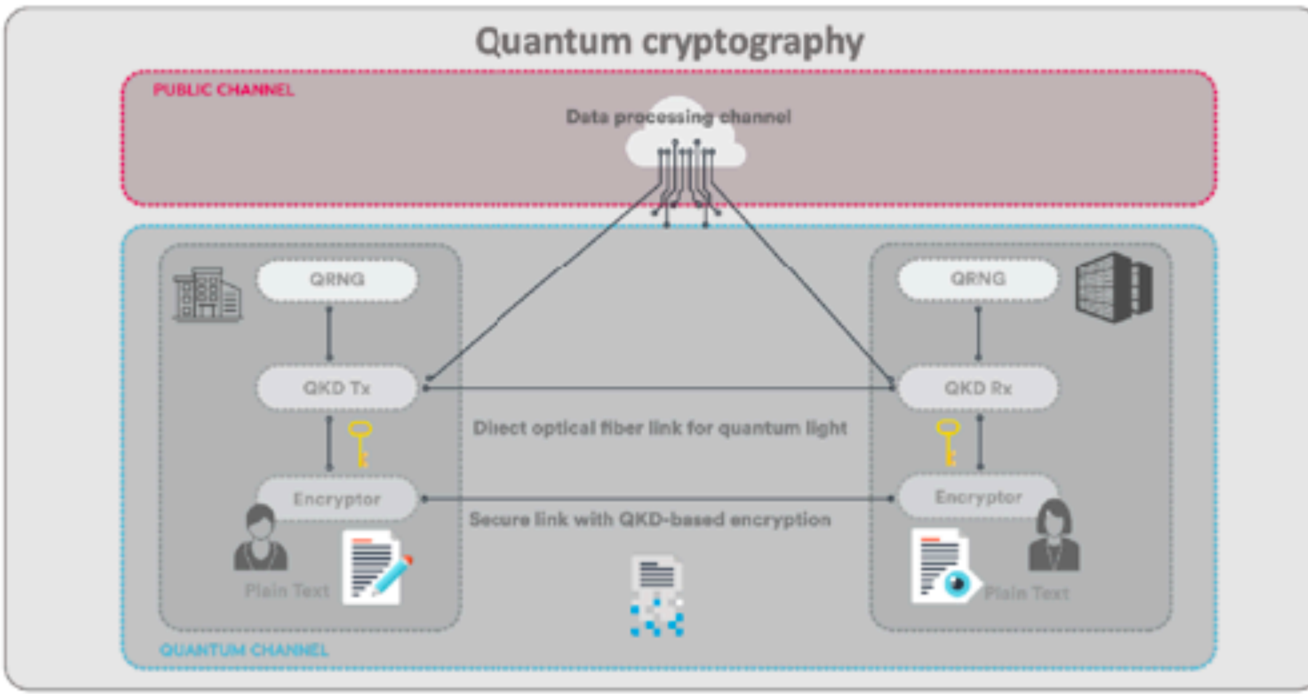
Quantum distance-bouncing

Secured distributed quantum metrology and sensing

Key establishment with performance beyond QKD in weaker security models

Quantum comm with super-aditive quantum receiver

Unforgeable quantum cryptograms for e-payment networks

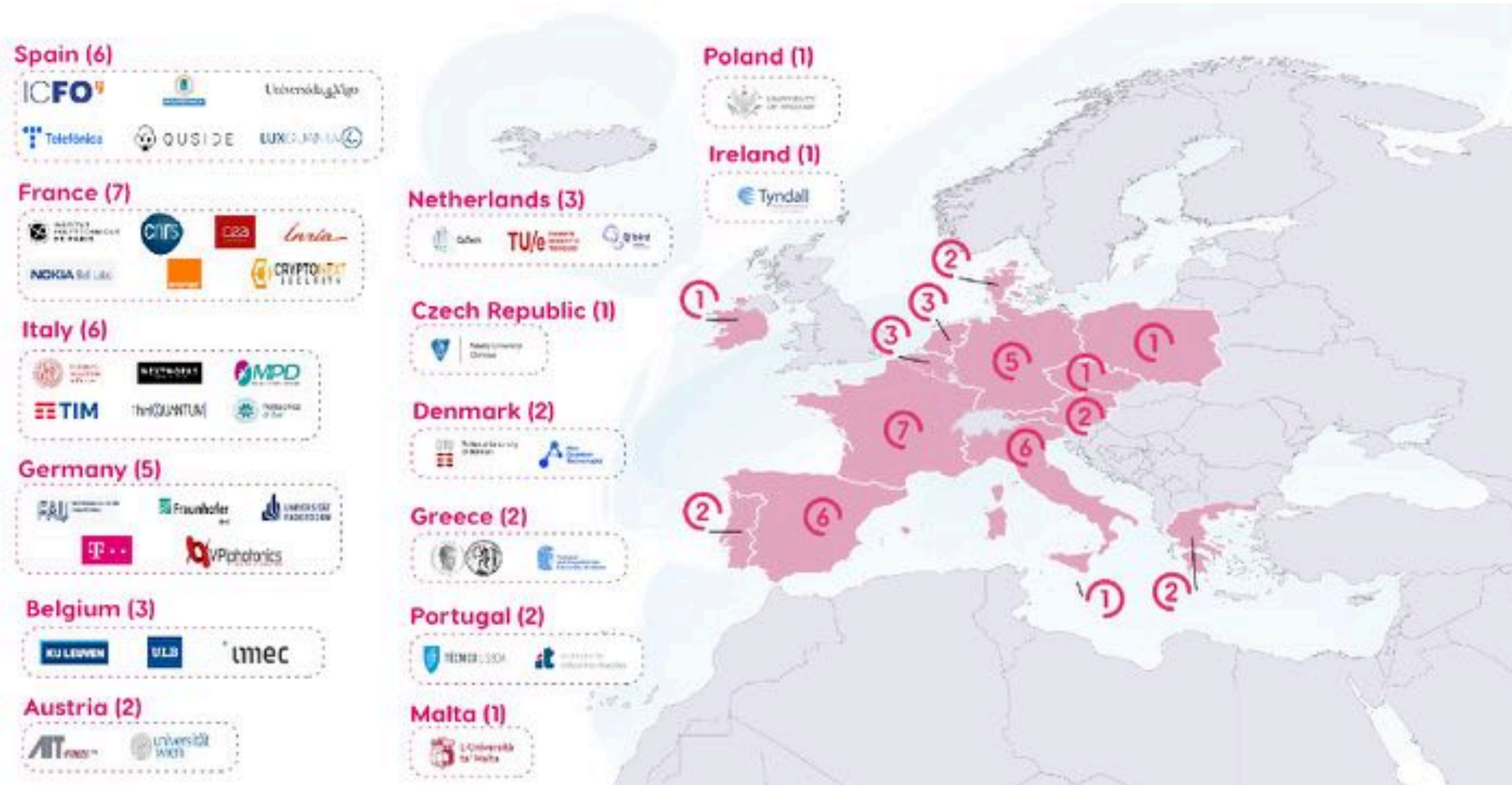


QSN PARTNERSHIP

Funded by the European Union

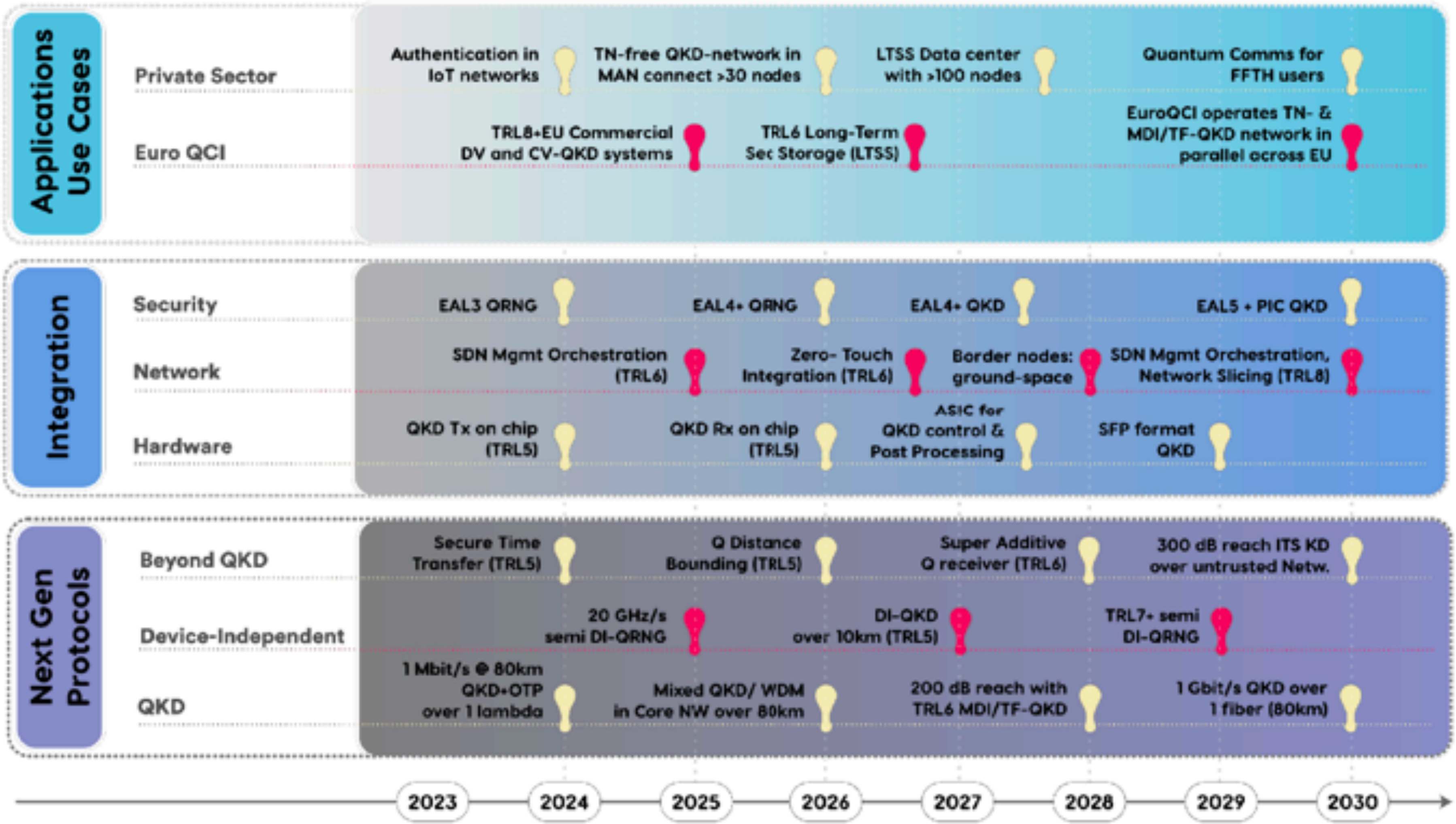
This project has received funding from the European Union's Horizon Europe research and innovation programme under the project "Quantum Secure Networks Partnership" (QSNP, grant agreement № 101114043)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission-EU. Neither the European Union nor the granting authority can be held responsible for them.



This project has received funding from the European Union’s Horizon Europe research and innovation programme under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No 101114043).

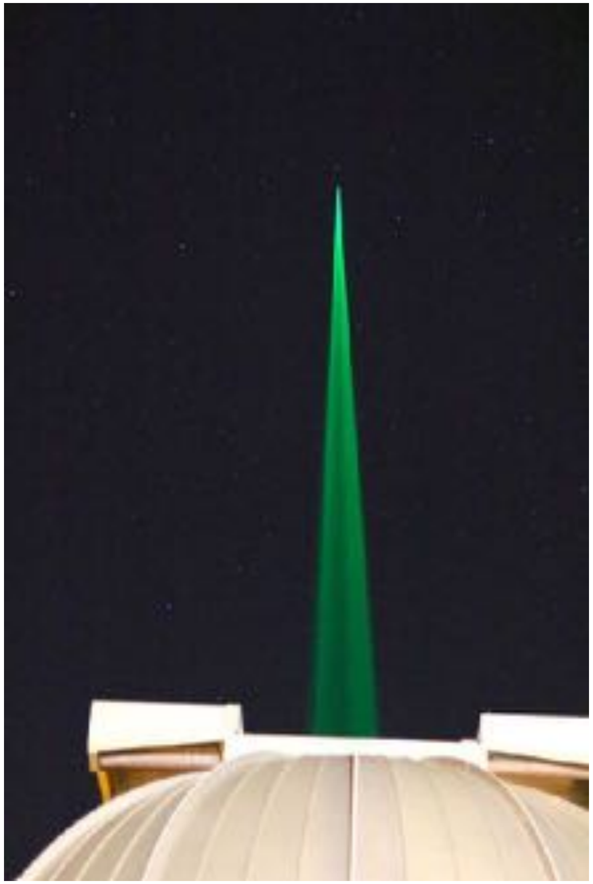
Roadmap



This project has received funding from the European Union's Horizon Europe research and innovation programme under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No 101114043).

conclusions

- Space QComms established with a variety of protocols
- QKD demonstrations have drawn investments and deploy over continental scale
- the speed of development now depends on effective application demonstrations and concrete integrations with the ground networks
- while supporting the QKD demonstration in the transition to industrial implementation..
- the scientific developments are very much needed!
- after all.. it's the most fundamental communication level ever conceived and at the largest possible scale!!



QSN PARTNERSHIP

Funded by
the European Union

This project has received funding from the European Union's Horizon Europe research and innovation programme under the project "Quantum Secure Networks Partnership" (QSNP, grant agreement № 101114043)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission-EU. Neither the European Union nor the granting authority can be held responsible for them.

Space QComms: not limits but horizons