University of Strathclyde Science

# UK Space Quantum Technology Activities & SatQKD

Dr Daniel Oi
CNQO, SUPA Dept of Physics, University of Strathclyde
Friday 31st March 2023

X THE FACULTY OF SCIENCE

# International Network in Space Quantum Technologies

- UKRI EPSRC Funded 3-years (Q1 2022- Q1 2025)
- Over 60 Members from 20 Countries (25 from UK)
- Promote cooperation and collaboration in Space Quantum Engineering
- Develop Roadmap for the Space Quantum Internet


https://www.insqt.ac.uk/

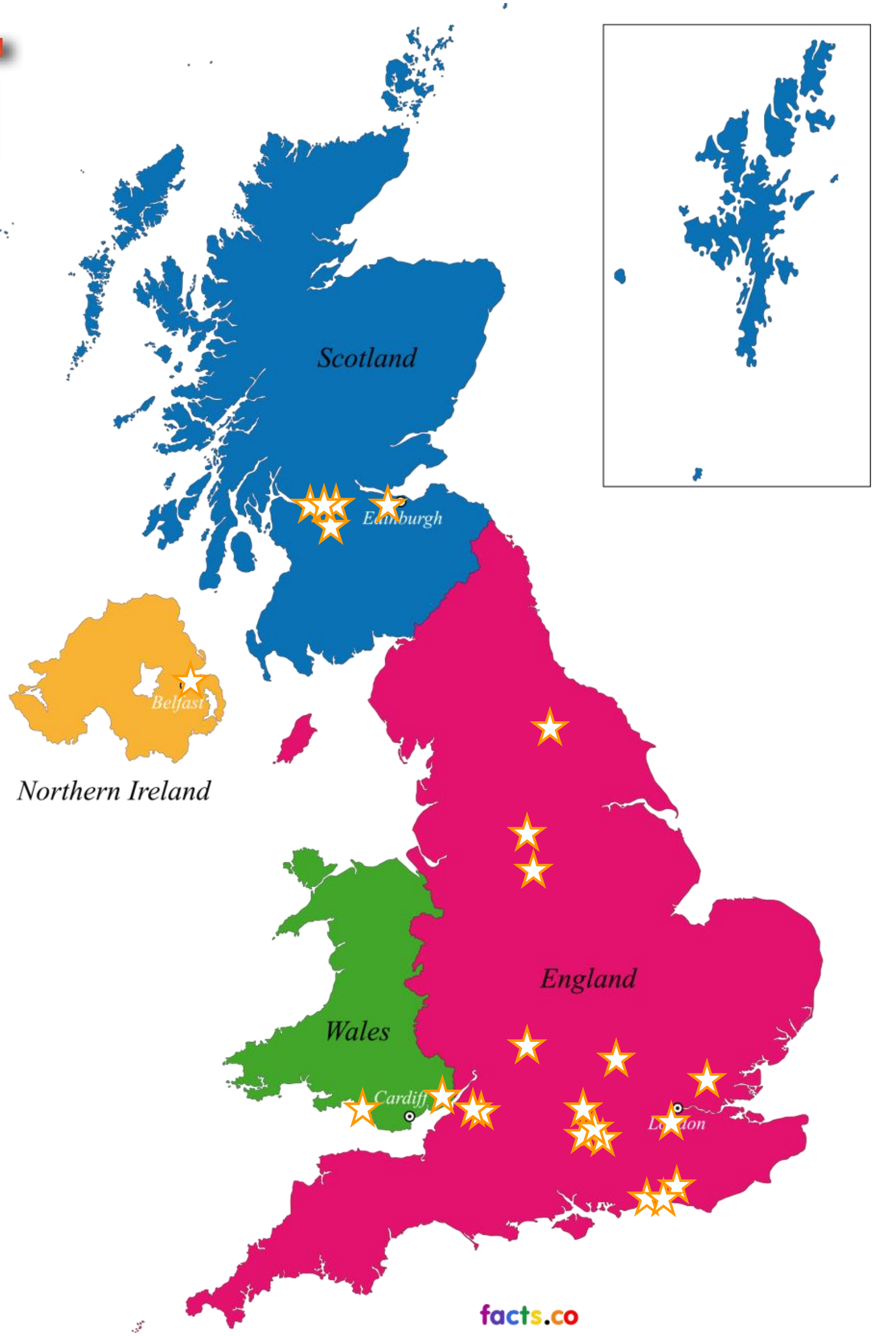
# UK Members of INSQT

- Academic
  - U Birmingham, Kai Bongs, Yeshpal Singh
  - U Oxford, Artur Ekert
  - Queens University Belfast, Mauro Paternostro, Matteo Carlesso
  - Swansea University, James Bateman
  - U Bristol, John Rarity, Siddarth Joshi
  - U Leeds, Mohsen Razavi
  - U Strathclyde, Daniel Oi, Paul Griffin
  - U Southampton, Hendrik Ulbricht, Corin Gawith
  - U York, Rupesh Kumar, Marco Lucamarini
  - Heriot-Watt University, Ross Donaldson, Alessandro Fedrizzi, Gerald Buller
  - U Warwick, Animesh Datta
  - U Glasgow, Adtunmise Dada

*Not yet members (but interested):*

- *Toshiba*
- *Quantum Dice*
- *Crypta Labs*
- *TAS UK*
- *…*

- Public Sector
  - RAL Space, Tristan Valenzuela
  - National Physical Laboratory, Patrick Gill
  - Satellite Applications Catapult
- RTO
  - Fraunhofer Centre for Applied Photonics
- SME
  - Archangel Lightworks, Owain Pryce-Jones
  - Craft Prospect Ltd, Steve Greenland
  - Zero Point Motion Ltd, Ying Lia Li
  - Aquark Technologies, Andrei Dragomir
  - Covesion, Stuart Coomber
  - Aegiq Ltd., Maksym Sich, Scott Dufferwiel, Thomas Lyons
- Industrial
  - Teledyne e2v
  - Airbus
  - Arqit Ltd, Alex Koehler-Sidki, Carlo Page



# UK Space Quantum Technology Activities

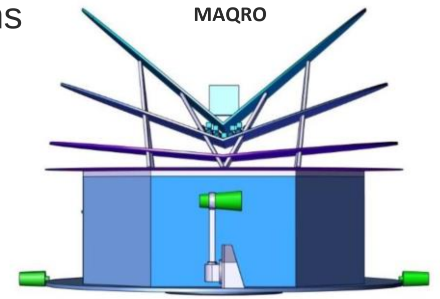
TELEDYNE e2v Everywhereyoulook™

CASPA-ADM

- Cold Atoms/Ions for Space
  - Clocks, PNT
  - Inertial Sensors, Gravimetry
  - Electric and Magnetic Field Sensing
  - Fundamental Tests, e.g. STE-QUEST

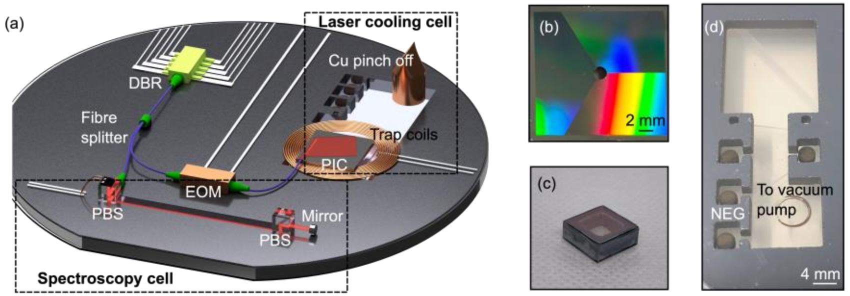
- Satellite QKD
  - Commercial & Research Missions
  - Theory/Modelling

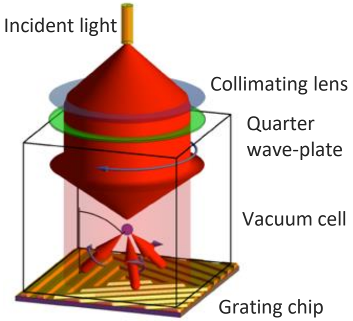
MAQRO

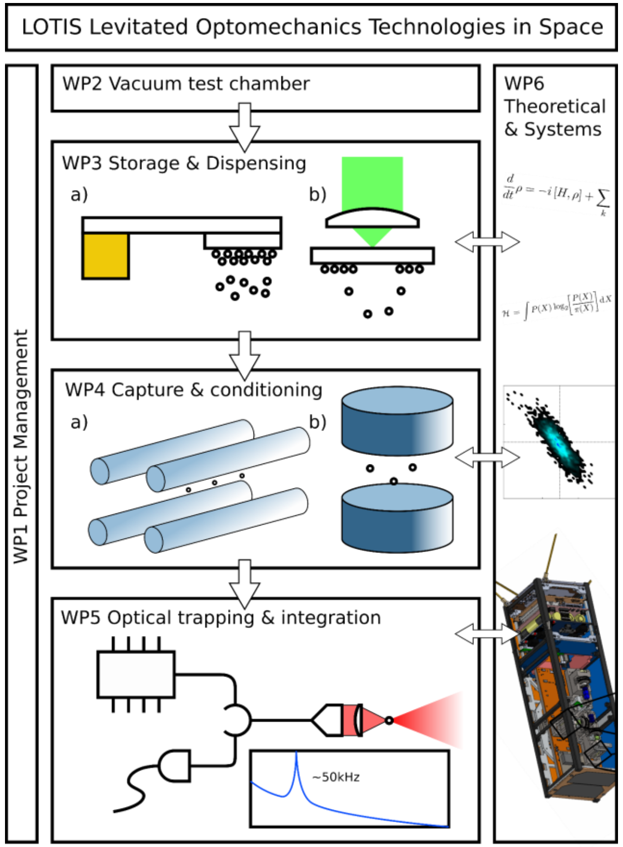


- Levitated Optomechanics
  - MAQRO partner
  - Sensing

Grating MOT



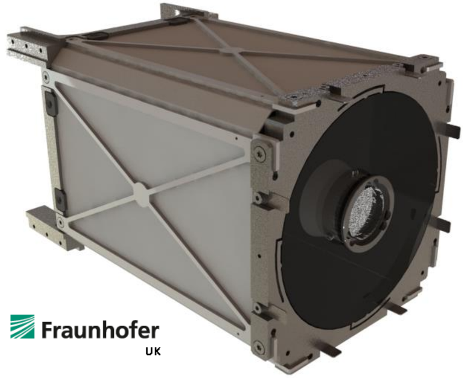




- Device, Components, Subsystems
  - Lasers/muLEDs/Photonics
  - Optics
  - QRNGs
  - Etc.

Crypta Labs

QUANTUM DICE

CubeSat Telescope



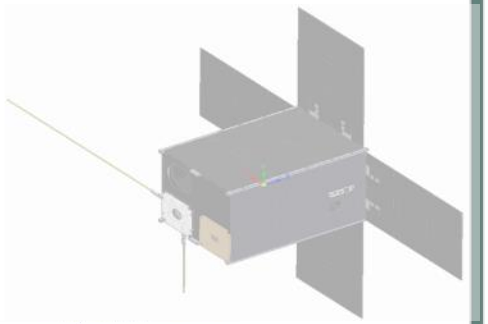
Fraunhofer UK

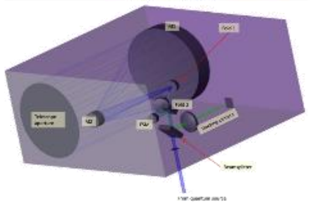
# Worldwide distances

- Quantum communications across oceans and between continents can utilise satellites. R&D is underway worldwide.
- Until satellites support memories, repeaters and entanglement distribution, they form trusted nodes for communications.

# Worldwide distances

- The Hub is undertaking an in-orbit demonstration (launch 2024) of QKD from a CubeSat (supplier ISISPACE) to an optical ground station (Errol Airfield, Scotland).
- Other UK missions: ROKS, SPEQTRE.
- Other Hub-related activity e.g. Canadian QEYSSat mission: UK-Canada QT programme downlink source ReFQ; Hub PRF project uplink entangled source.






QUANTUM COMMUNICATIONS HUB

UK NATIONAL QUANTUM TECHNOLOGIES PROGRAMME

UKRI Engineering and Physical Sciences Research Council

# What next for UK “quantum in space”?

- We will learn a lot from the current Hub, ROKS and SPEQTRE CubeSat missions, plus international collaborations.
- Given current EU/ESA and other worldwide activity, along with UK exclusion from EU security R&D, it is important for the UK to further develop our “quantum in space” R&D.
- What next? Further CubeSat missions? A larger satellite, with multiple quantum payloads?
- Who pays?

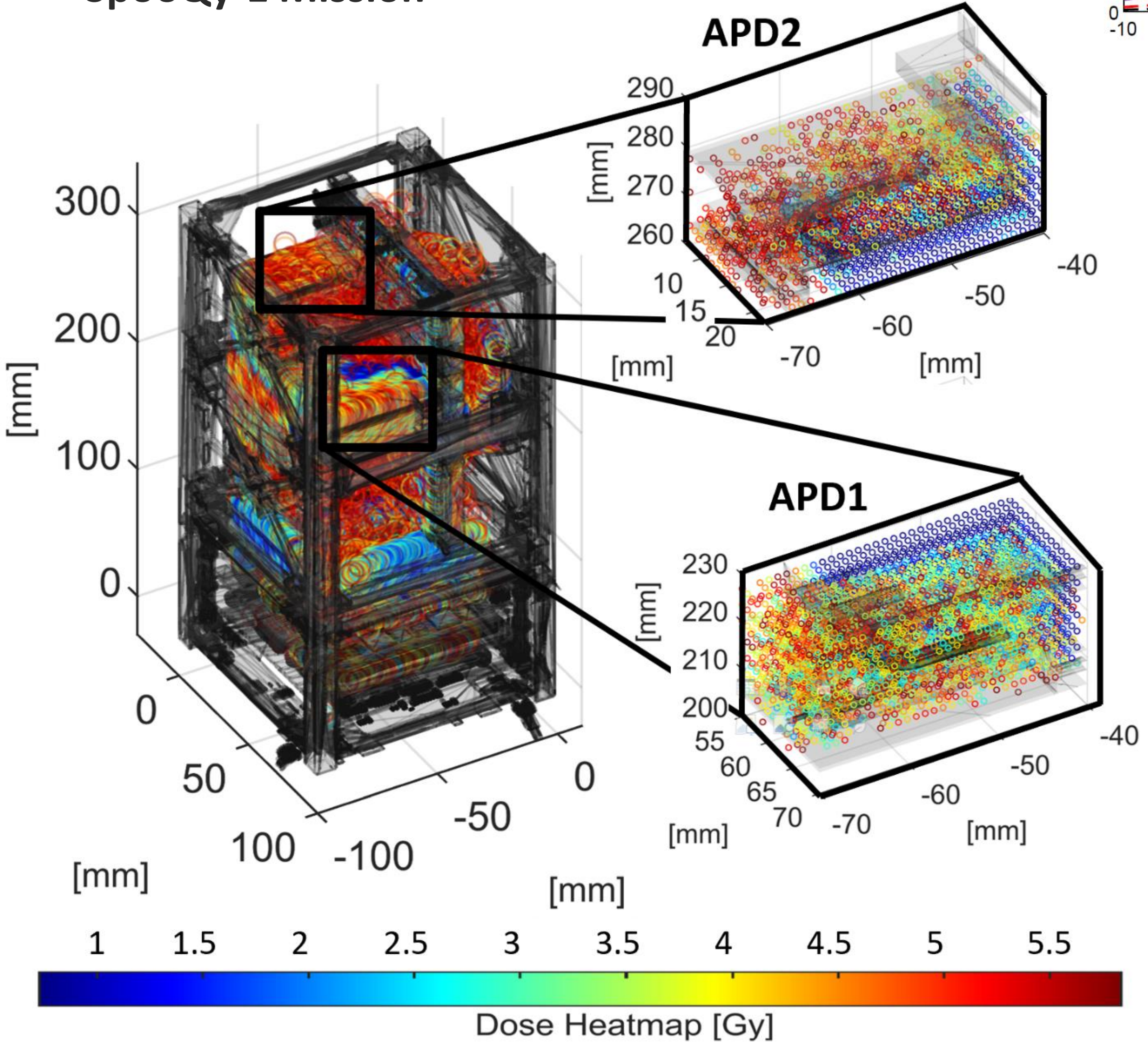
The time is right to start addressing these questions.

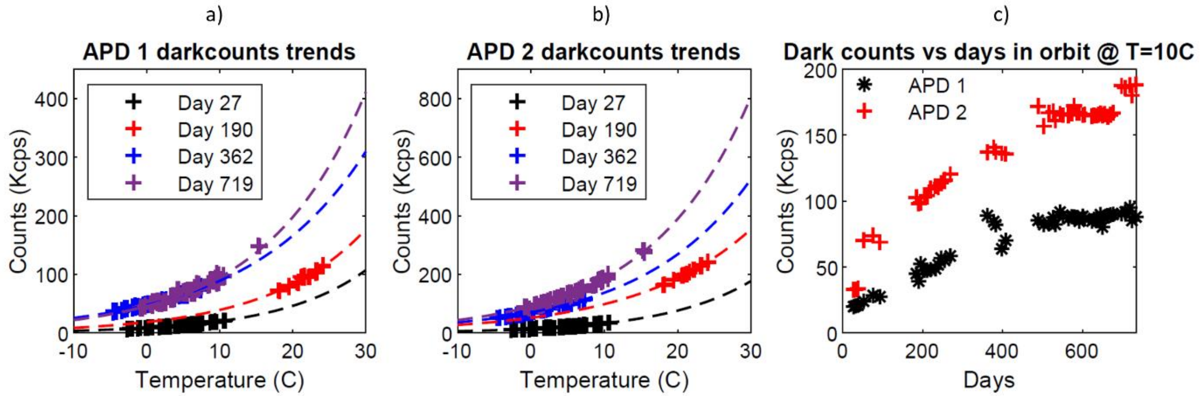
arXiv:2209.00408

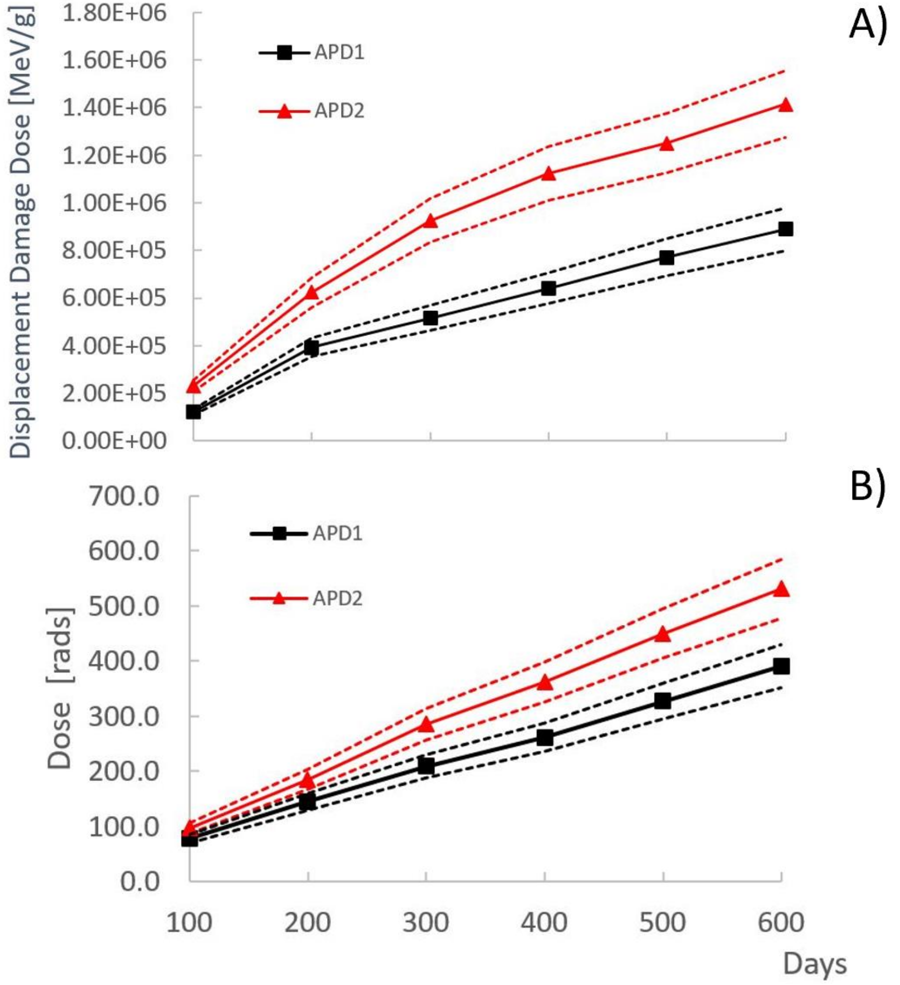
# Space Radiation

Arpad Lenart, Prof Bernhard Hidding et al.

## SpooQy-1 Mission



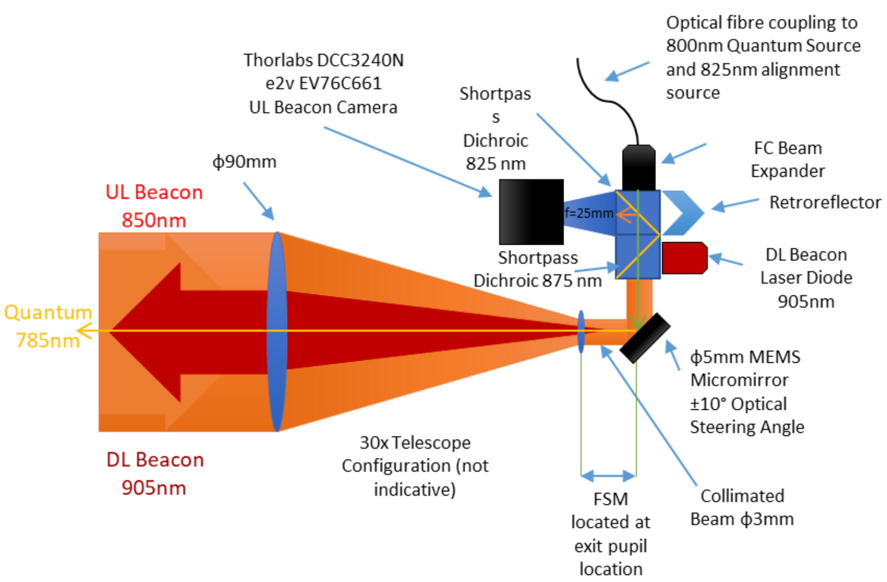

X THE FACULTY OF SCIENCE

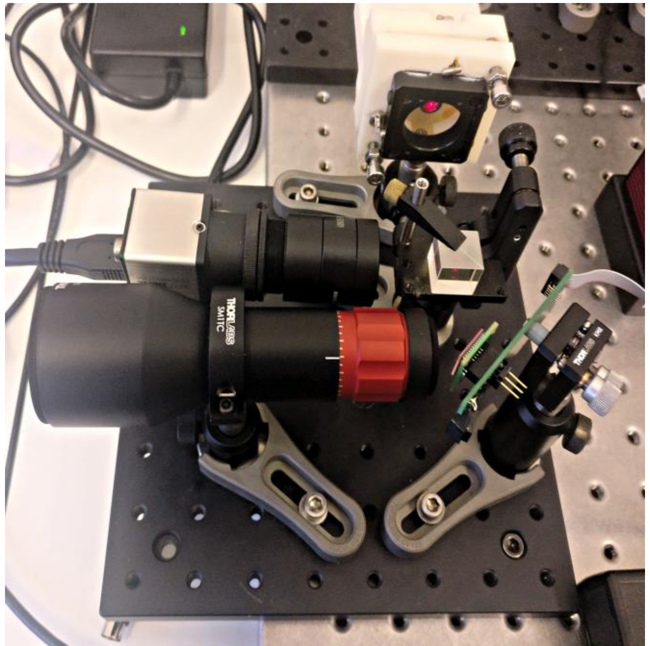
Centre for Quantum Technologies

THE FACULTY OF SCIENCE

# Quantum Research CubeSat QUARC

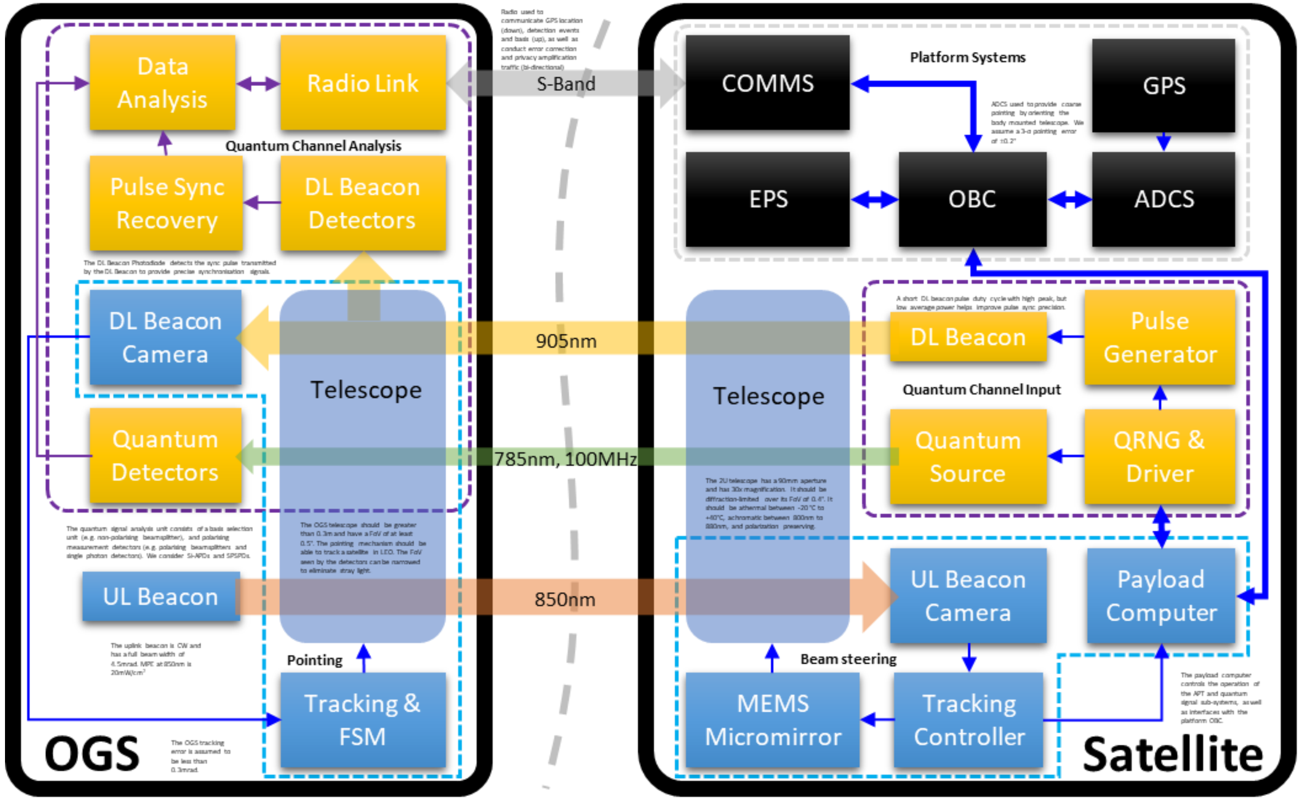
Offspring of CQuCoM H2020-FET Proposal, 6-Nations

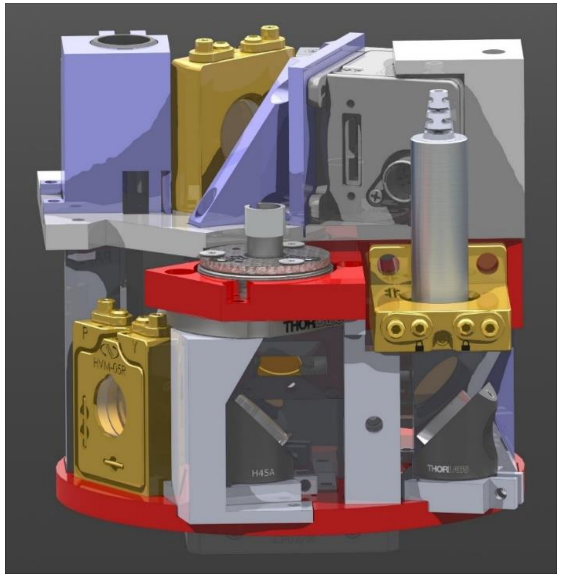


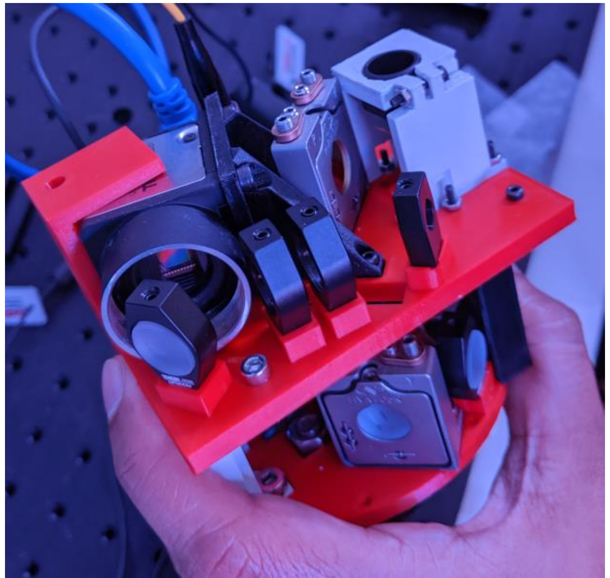
APT Proof of Concept

System Design



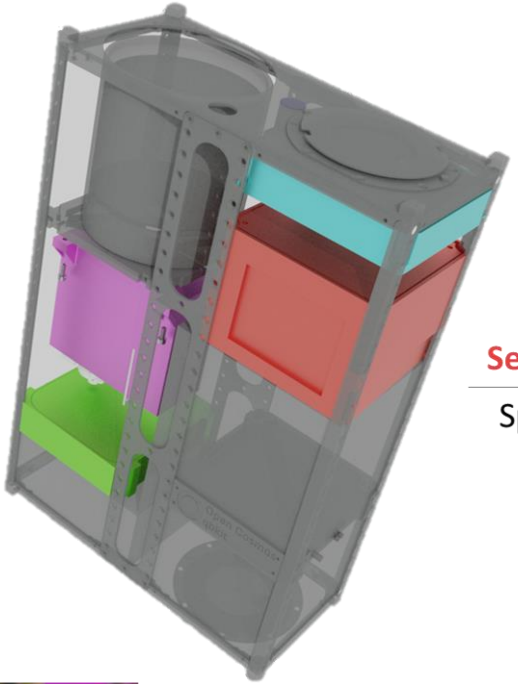



APT Concept Design



APT Mockup

# ROKS QKD Mission



**Optical beamsteering**

Optical laser communications

**Quantum key laser source**

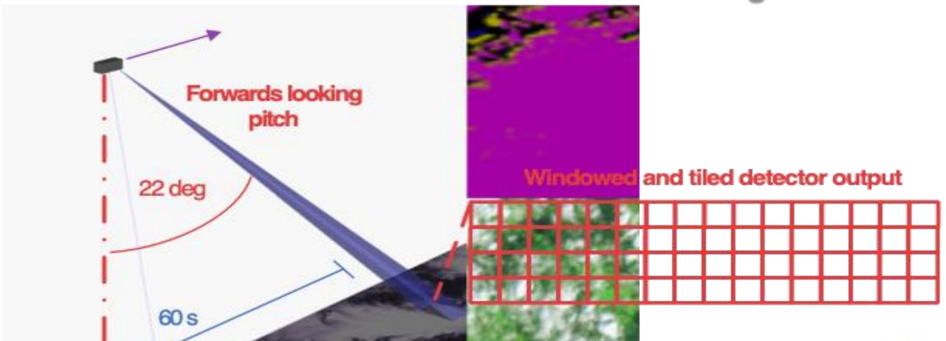
Global encryption services

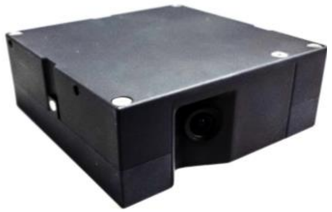
**Low power real-time AI**

Onboard intelligence

**Secure assured computing**

Space countersecurity

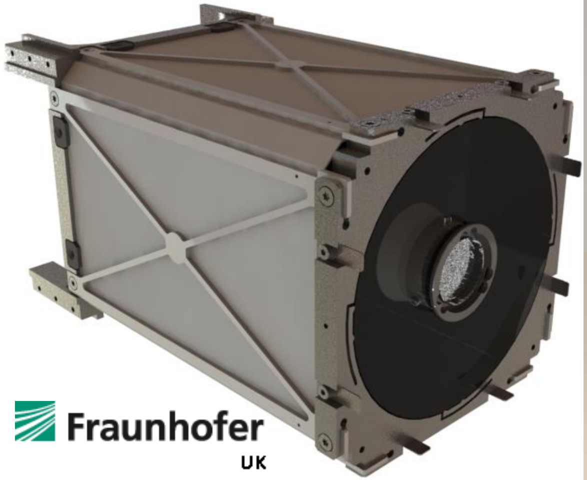


6U CubeSat

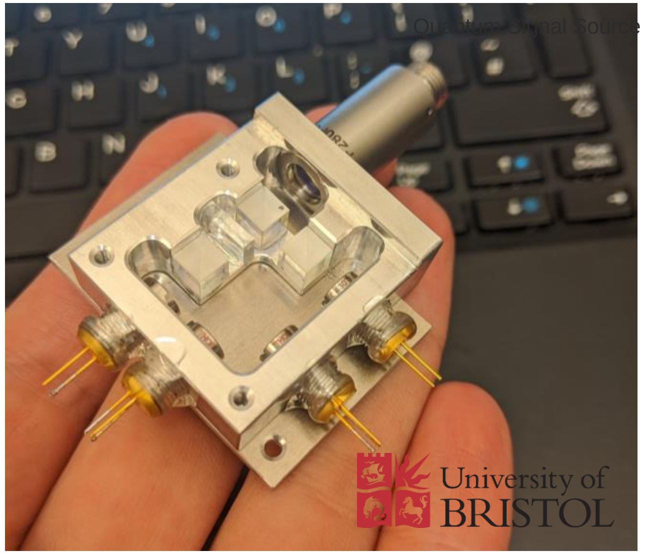
X THE FACULTY OF SCIENCE

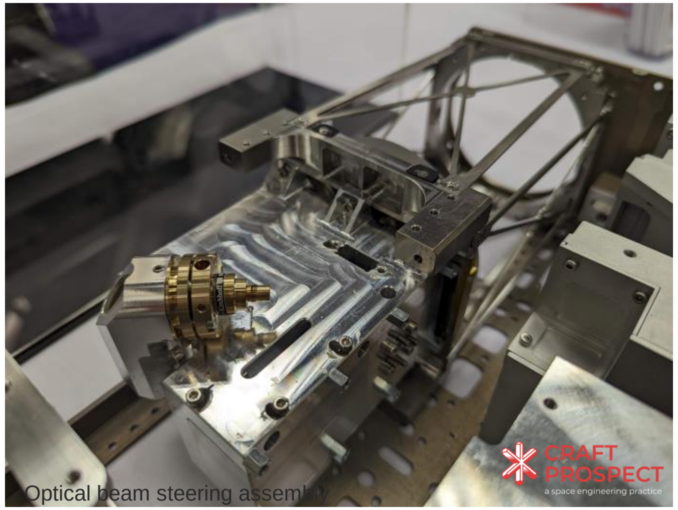
CRAFT PROSPECT

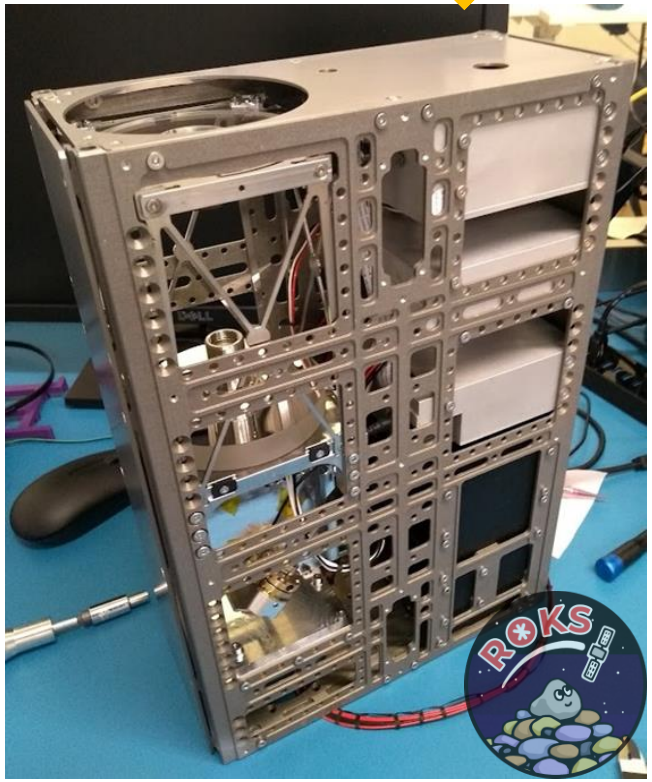

Fraunhofer
UK

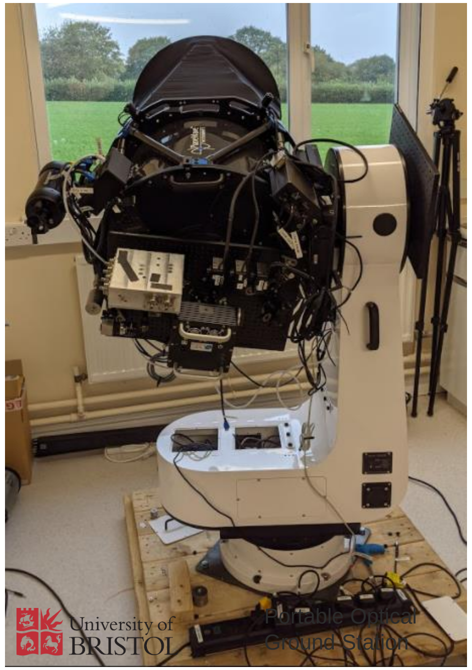

Telescope


Quantum Signal Source and Control
Electronics
CRAFT PROSPECT
a space engineering practice

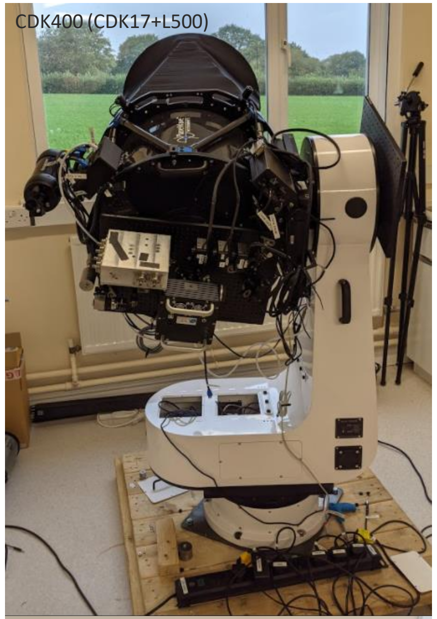

University of
BRISTOL

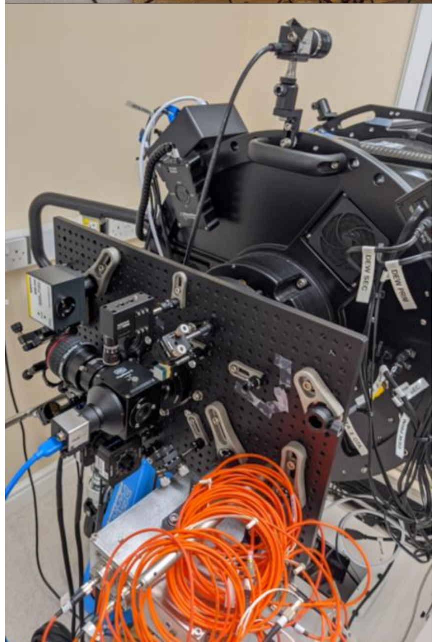

Optical beam steering assem
CRAFT PROSPECT
a space engineering practice


ROKS

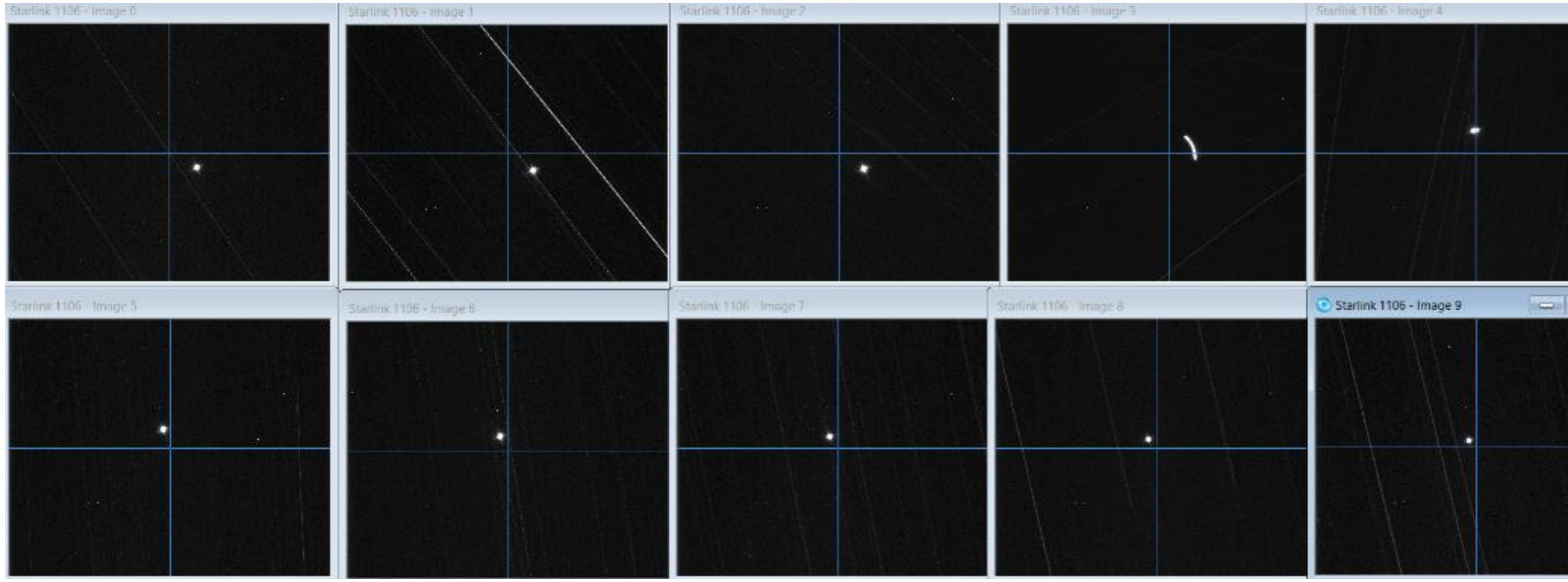

University of
BRISTOL
Portable Optical
Ground Station

# Mobile Optical Ground Stattion



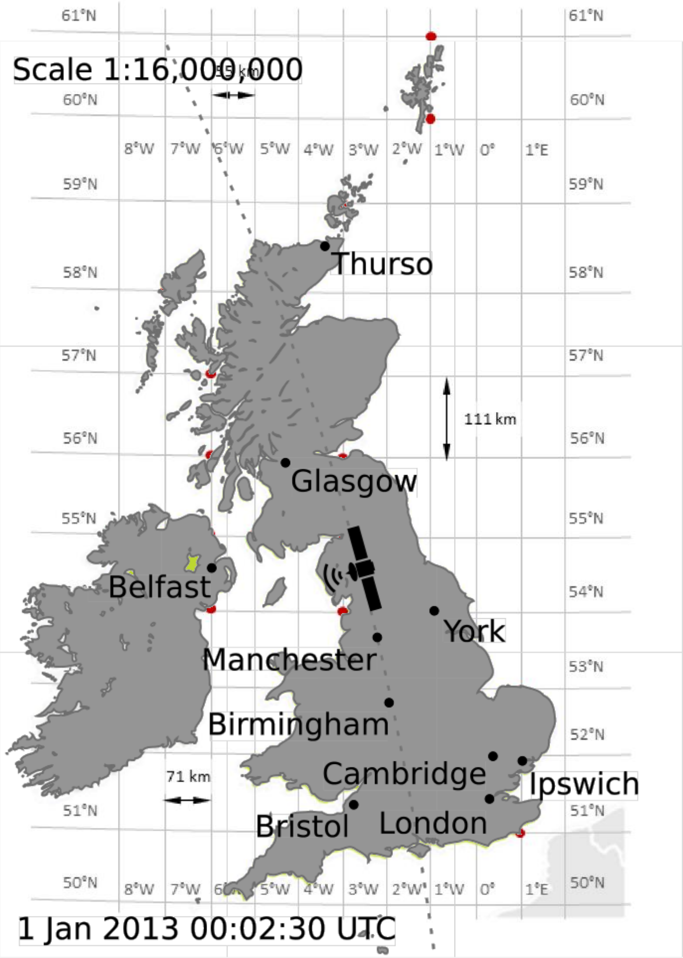
LEO Satellite Tracking



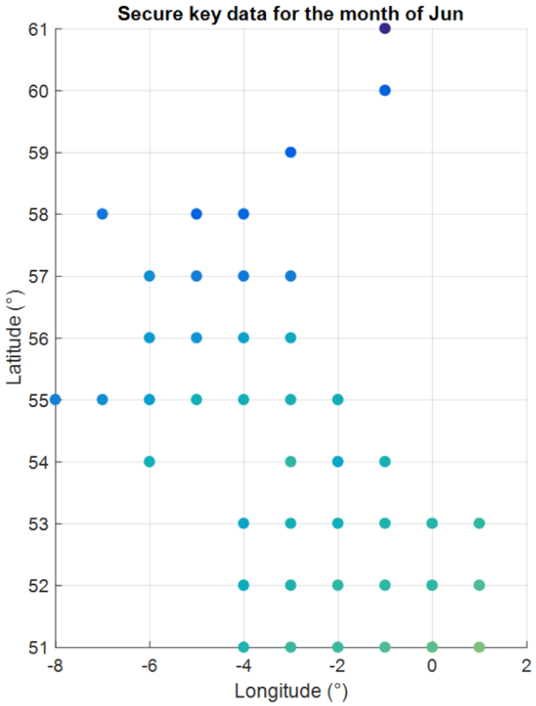

Tracking the ISS

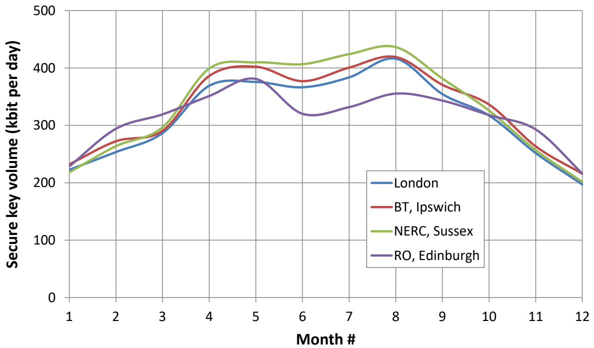
# QKD Modelling

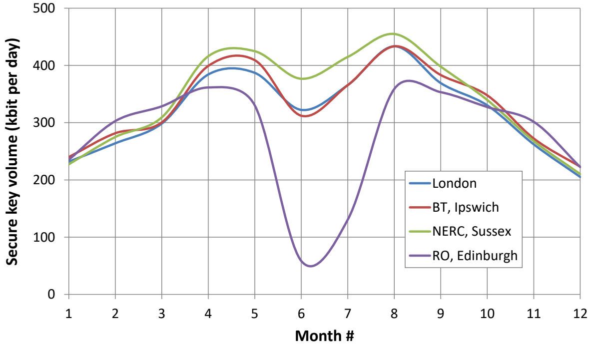
- Finite-key
- Seasonal/weather

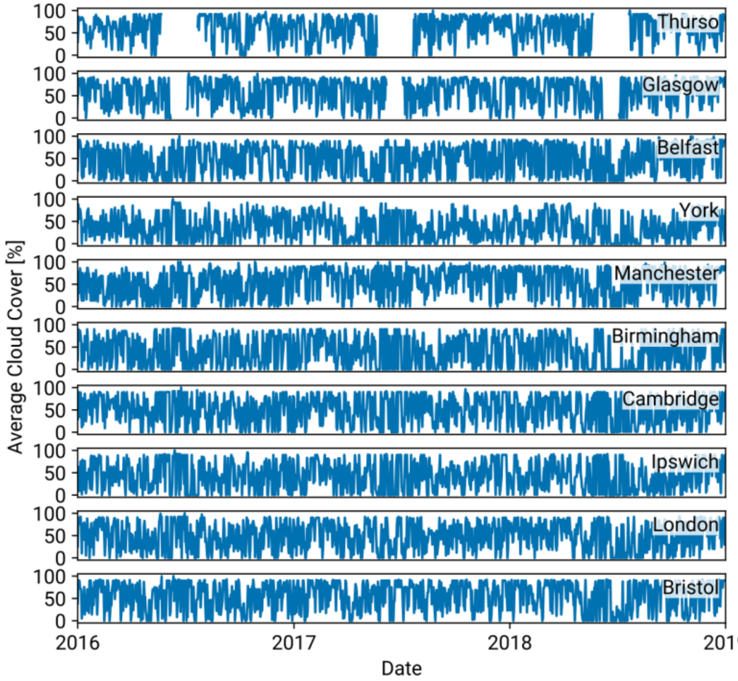


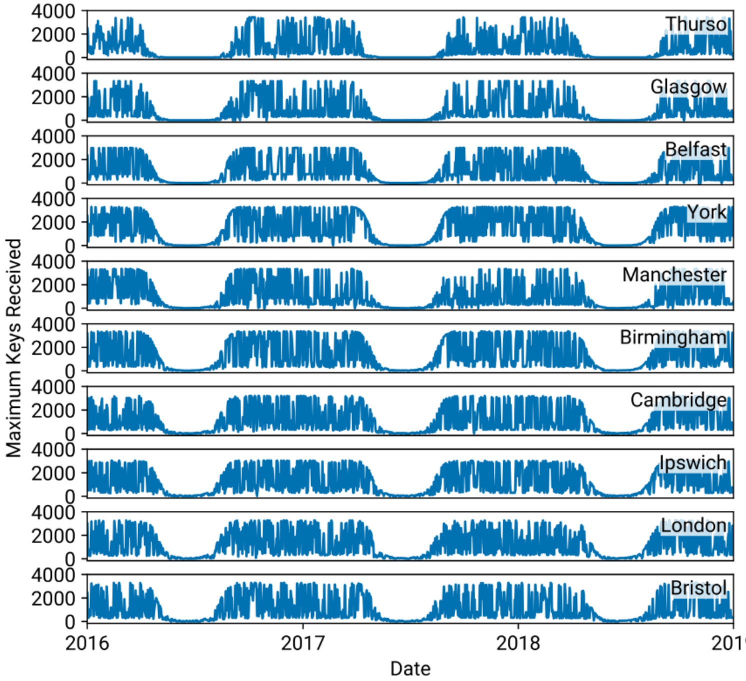

With MAE (Dr Annalisa Riccardi et al.)




Mazzarella L, et al., QUARC: Quantum Research Cubesat—A Constellation for Quantum Communication. Cryptography 4, 7 (2020) https://doi.org/10.3390/cryptography4010007

Polnik M, et al., Scheduling of space to ground quantum key distribution. EPJ Quantum Technology 7, 3 (2020), https://doi.org/10.1140/epjqt/s40507-020-0079-6

X THE FACULTY OF SCIENCE

https://github.com/cnqo-qcomms/SatQuMA

X THE FACULTY OF SCIENCE

# Finite Size Effects in SatQKD

Efficient BB84 WCP DS
X basis for key
Z basis for parameter estimation

Lim, C. C. W., et al., Concise security bounds for practical decoy-state quantum key distribution. Phys. Rev. A 89, 022307 (2014)

## QKD Security requires reliable bounds

Lower bounds on vacuum and single photon yields
Upper bound on phase error rate
Upper bound on error correction leakage
Composable security, correctness and secrecy

## Parameter Estimation

Observed statistics, true means unknown
Random fluctuations, statistical uncertainty
Tail bounds to constrain failure probability

## Secret Key Rates/Lengths

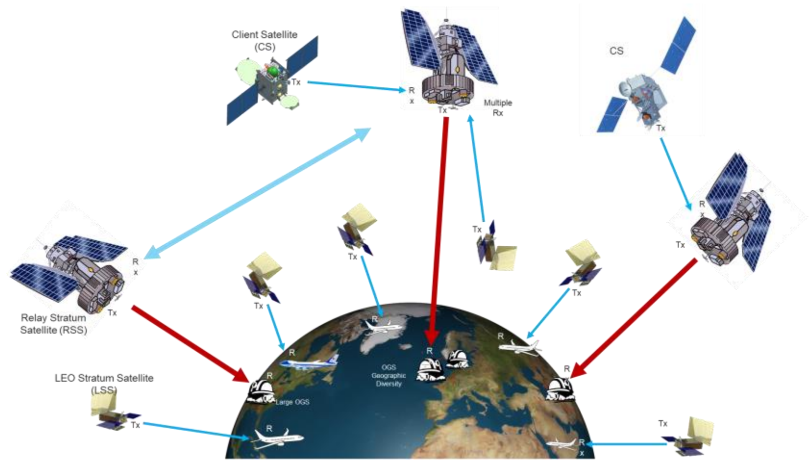
Uncertainty increases required PA for security
Approaching asymptotic regime require large blocks
Error correction efficiency block size dependent
Threshold effect, boom or bust

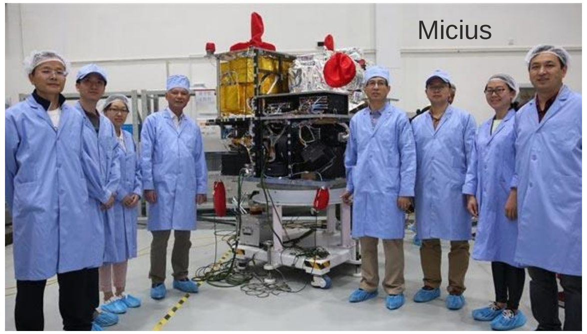
## Operational flexibility

Generate key directly from single overpass, ideally
Avoid storage of raw key from several passes/satellites
Reduce post-processing, communications, management
Smaller satellites/OGSs

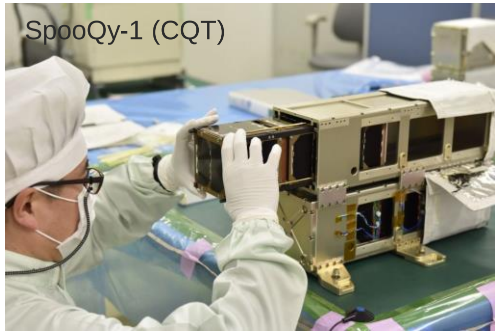
Vacuum Yield / Single Photon Yield / Phase Error / Error Correction Leakage / Security / Correctness

$$\ell = \left\lfloor s_{X,0} + s_{X,1}(1 - h(\phi_X)) - \lambda_{\mathrm{EC}} - 6\log_2 \frac{21}{\epsilon_s} - \log_2 \frac{2}{\epsilon_c} \right\rfloor$$

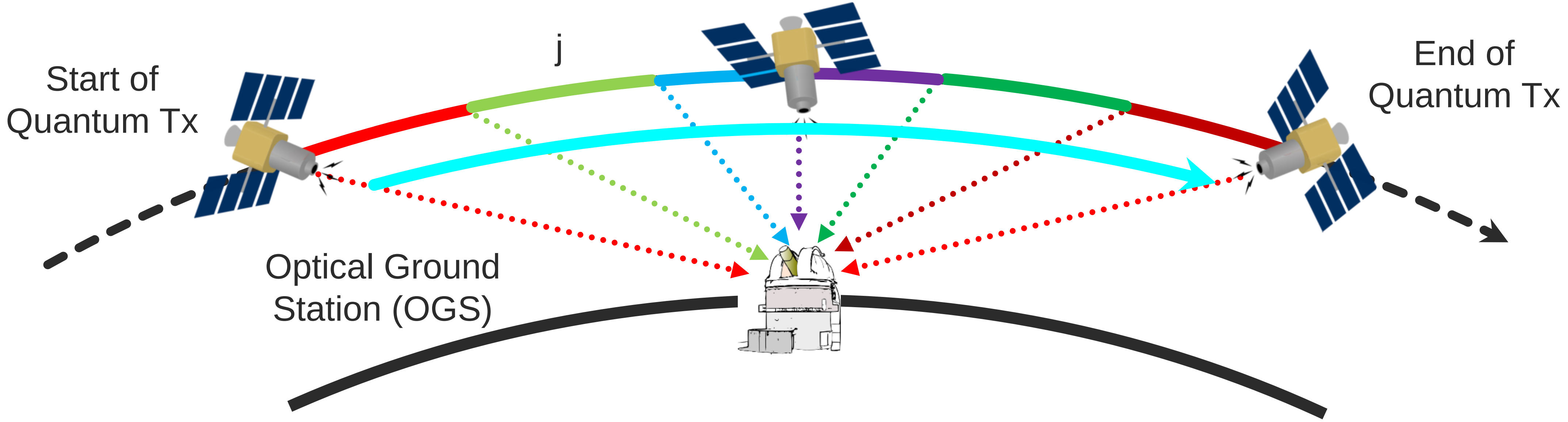



vs



# Key Accumulation




## Continuous or Blockwise

$$\mathrm{SKL}_{\infty}^{\mathrm{Cont.}} = \int_{t_{\mathrm{start}}}^{t_{\mathrm{end}}} \underbrace{\mathscr{R}_{\infty}(t)}_{\text{Instantaneous}} dt,$$

Asymptotic Rates

$$\mathrm{SKL}_{\infty}^{\mathrm{Block}} = \sum_j \underbrace{\mathscr{R}_{\infty}^{(j)}}_{\text{Block}} \mathcal{L}_j,$$

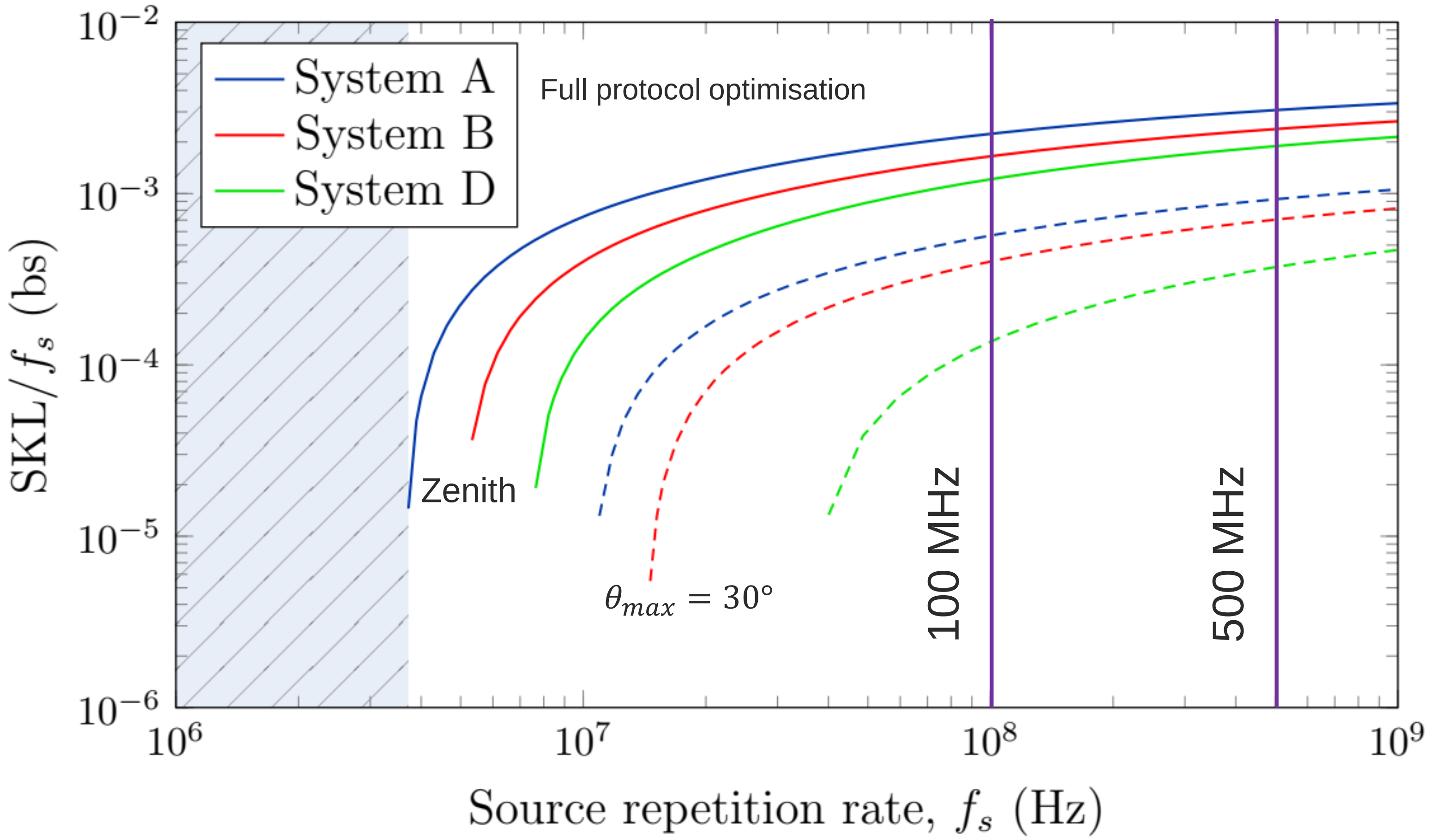
- Treat entire block together
  - Block click statistics
  - Finite statistical uncertainties
  - Composable security framework

$$\mathrm{SKL}_{\mathrm{finite}} = \mathrm{SKL}\left(\overbrace{\{n_k^{\mu}, m_k^{\mu}\}}^{\text{Observed counts}}\right)$$

# Source Rate Scaling

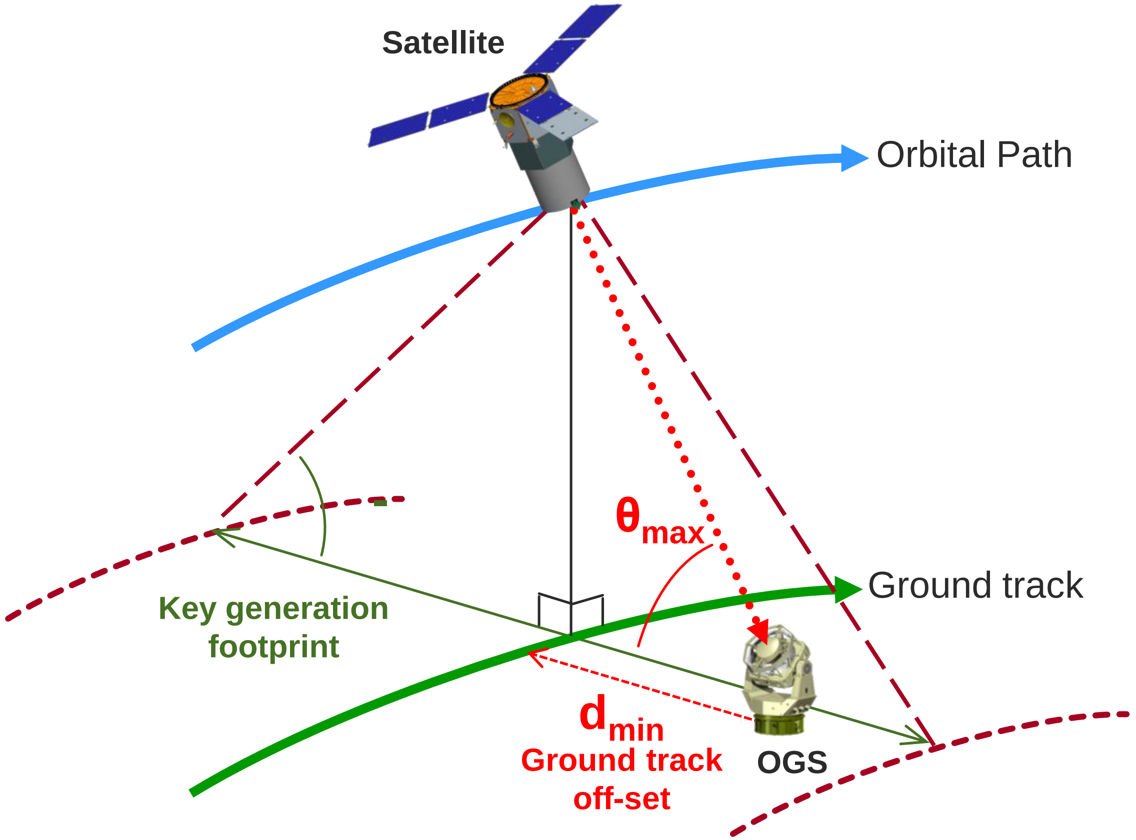
Figure 3. **Finite key efficiency vs source rate**. Source rate normalised SKL as a function of $f_s$ for overpasses with $\theta_{\max} = 90°$ (solid lines) and 30° (dashed lines), for three system configurations $\{QBER_I, p_{ec}\}$: A = $\{0.1\%, 1\times10^{-8}\}$, B = $\{0.5\%, 1\times10^{-8}\}$, and D = $\{0.5\%, 1\times10^{-7}\}$. The critical $f_s$ value corresponds to the transition of zero and non-zero finite SKL. The shaded blue region illustrates the key suppression region for System A with $\theta_{\max} = 90°$ where statistical fluctuations in estimated parameters overwhelm key generation due to finite available statistics. The vertical line is at $f_s$ = 500 MHz which we consider for the remainder of the paper.

Source Rate Normalised Efficiency




Sidhu, JS., et al, Finite key performance of satellite quantum key distribution under practical constraints, arXiv:2301.13209

# SKL vs Overpass Geometry



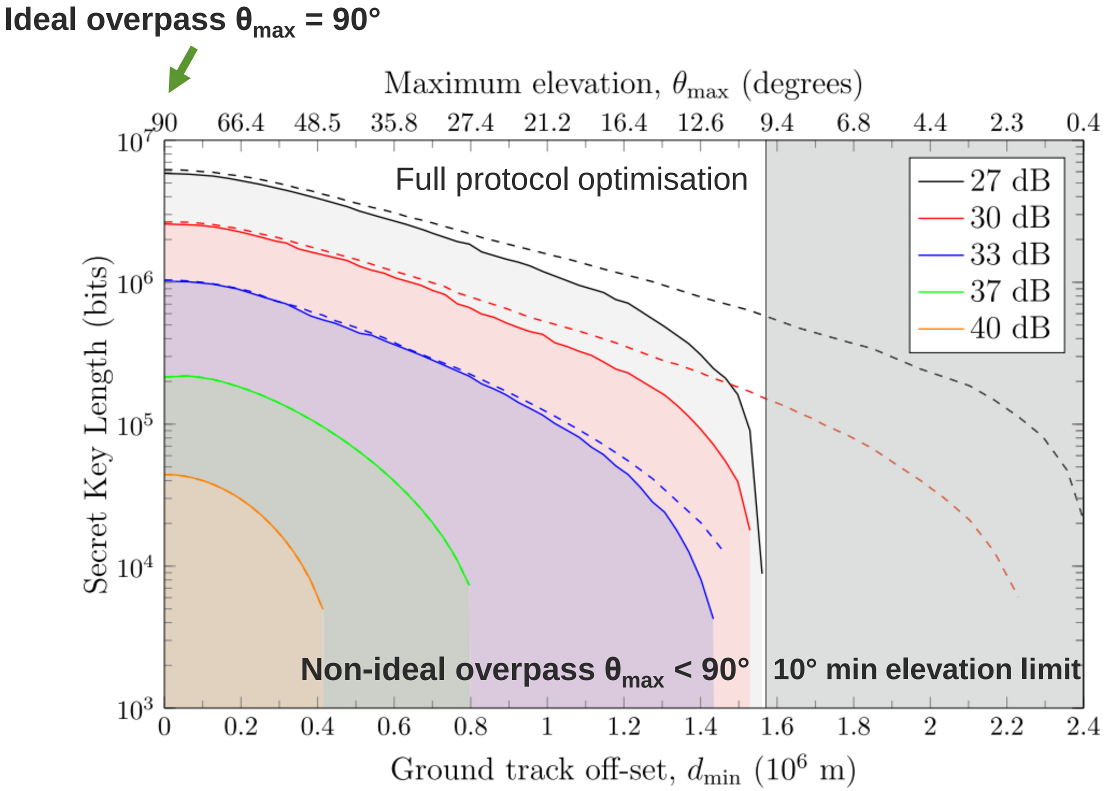




**Fig. 5 SKL vs ground track off-set.** $p_{ec} = 5 \times 10^{-7}$ and $QBER_I =$ 0.5%. The key generation footprint is given by the maximum $d_{min}$ with non-zero SKL. Solid lines correspond to imposing $\theta_{min} = 10^\circ$ (indicated by dark grey region on the right) and dashed lines to no elevation limit. The shaded areas under the curves determine the expected annual SKL for different $\eta_{loss}^{sys}$. Imposing $\theta_{min} = 10^\circ$ reduces the area, and hence the expected annual SKL, by 18.82%, 13.37%, and 3.58% at 27 dB, 30 dB, and 33 dB, respectively.

- Sun synchronous orbit Noon-Midnight
- h=500km altitude
- Downlink at night
- $\eta_{loss}^{sys} = 27 - 40dB$ (Micius-CubeSat)
- $f_s$=100MHz
- $QBER_I$=0.5%
- $p_{ec}=5*10^{-7}$
- >10° elevation limit

Sidhu JS, et al., Finite key effects in satellite quantum key distribution. npj Quantum Information 8,18 (2022)

# Annual SKL

## Assuming

Sun-synchronous (near polar)

Low to moderate OGS latitude

No Earth synchronism

Randomly distributed ground track offsets

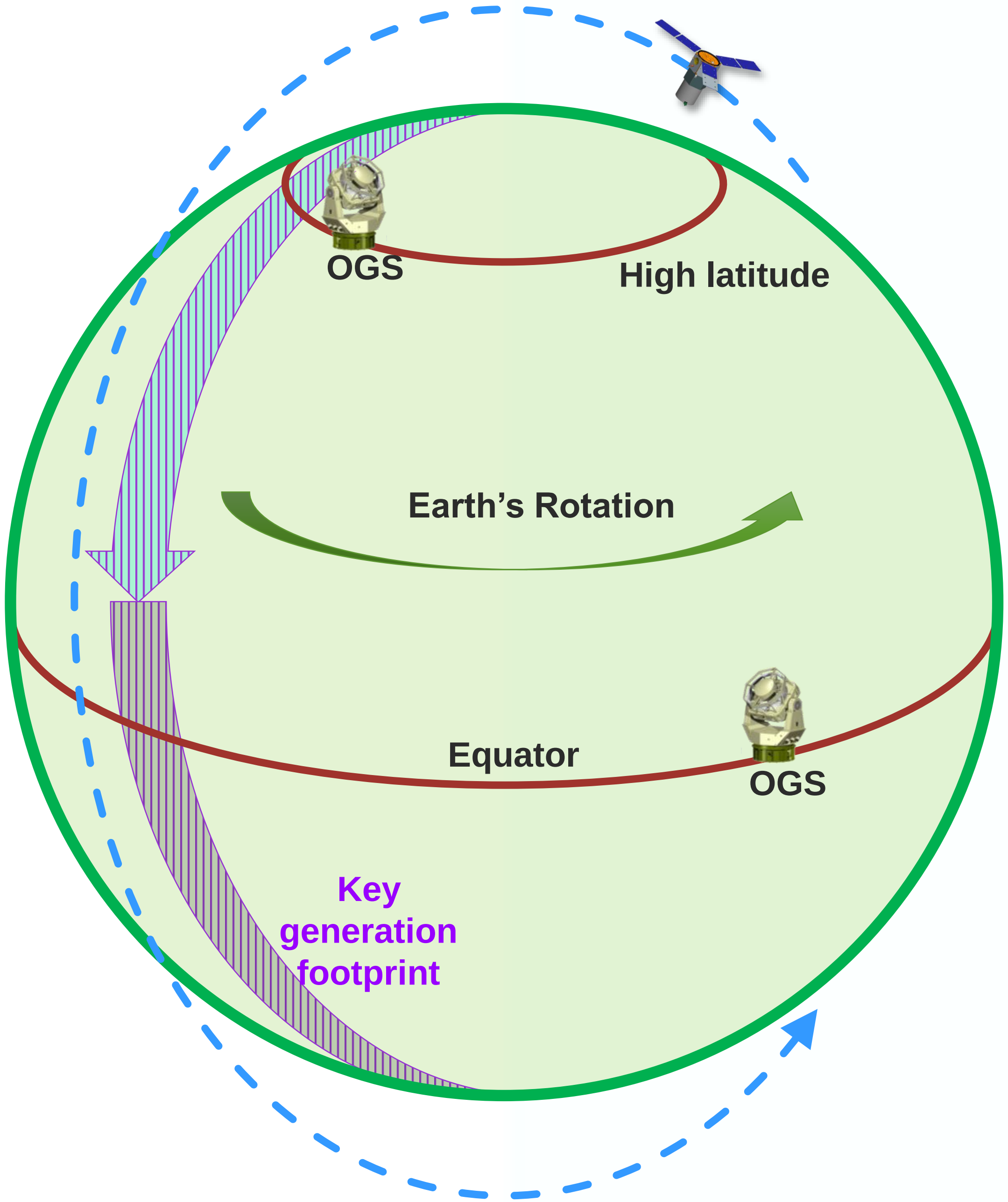
Only night downlinks

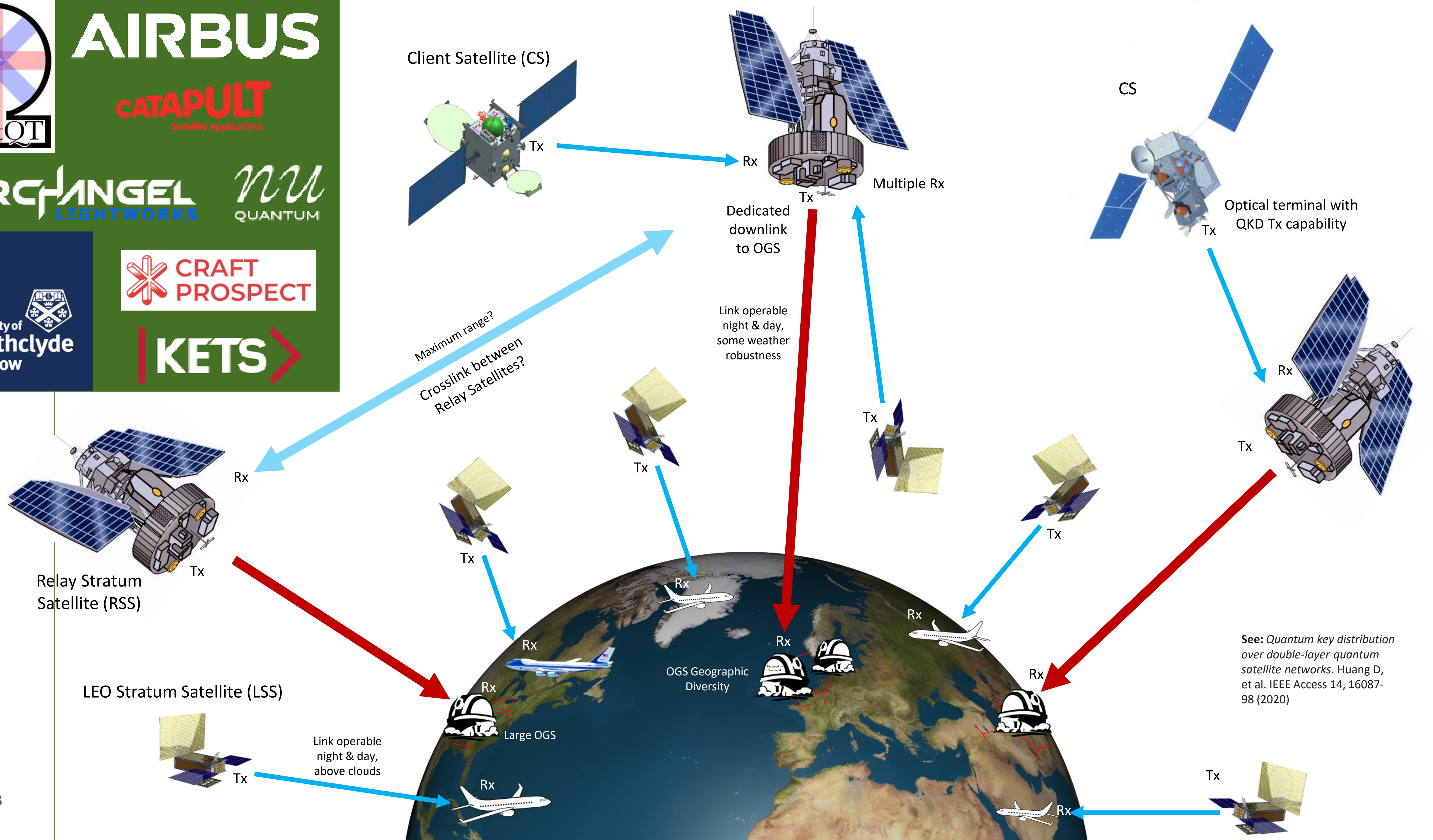
Area under SKL vs $d_{min}$ curve

$$\overline{\mathrm{SKL}}_{\mathrm{year}} = N^{\mathrm{year}}_{\mathrm{orbits}} \frac{\mathrm{SKL}_{\mathrm{int}}}{L_{\mathrm{lat}}},$$

Number of orbits per year

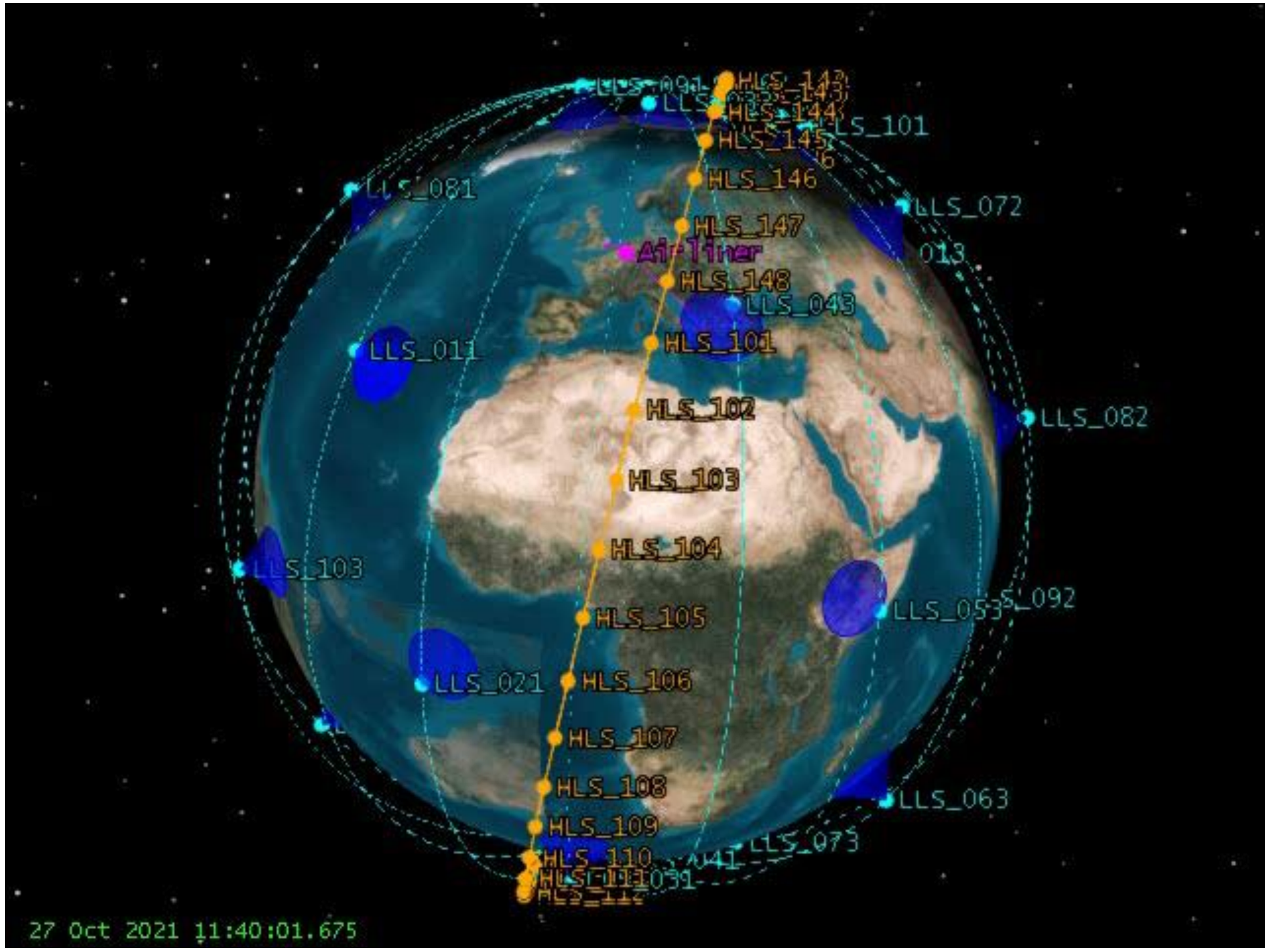
Distance around line of latitude at OGS position





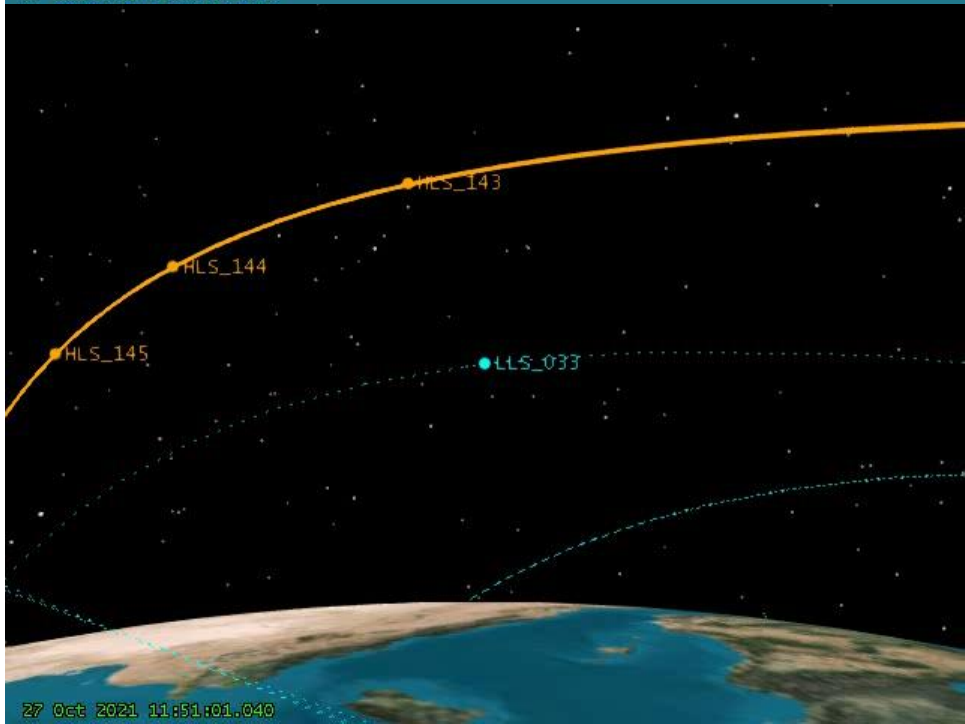

**See:** *Quantum key distribution over double-layer quantum satellite networks*. Huang D, et al. IEEE Access 14, 16087-98 (2020)

# SatQKD Constellation




Satellite-Aircraft QKD

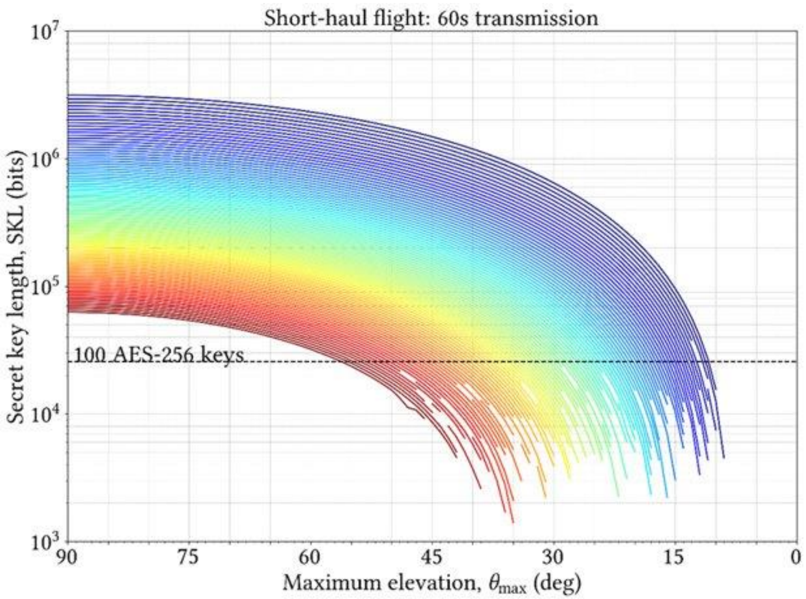

Satellite-Aircraft QKD

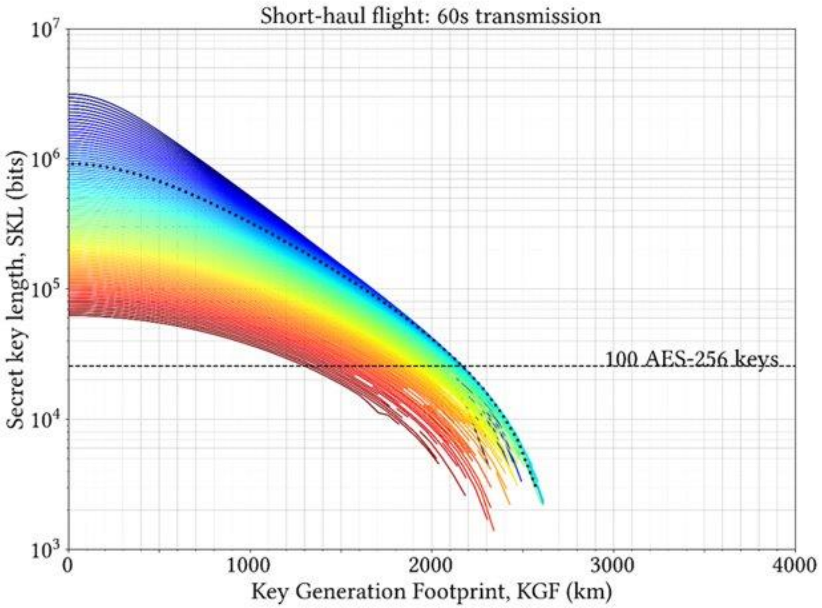



Intersatellite QKD Relay

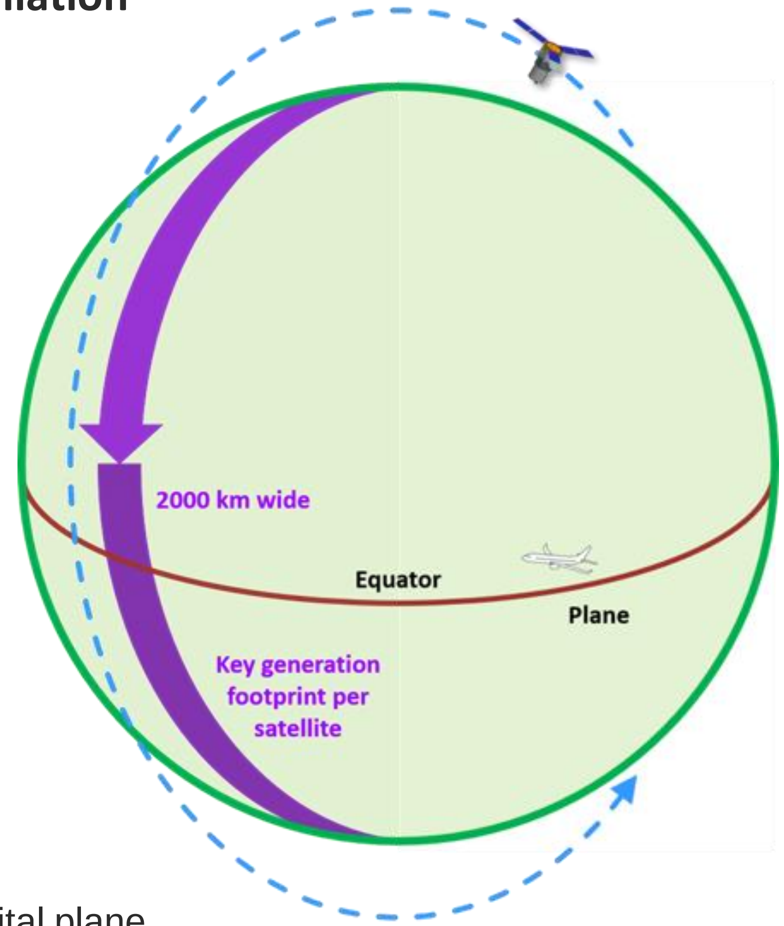
Innovate UK

# Constellation Design and Optimisation




**ViSatQT Dual-Layer Constellation**
**Low-LEO Stratum (LLS)**




## LLS Constellation

- 10 Orbital planes, 3 per orbital plane
- Circular polar orbits 530 km
- Key Generation Footprint 2000 km
- Revisit time 30 mins

# Spaceborne QMs

Proposal for space-borne quantum memories for global quantum networking

*npj Quantum Inf* **7,** 128 (2021)

Mustafa Gündoğan[1✉], Jasminder S. Sidhu[2], Victoria Henderson[1], Luca Mazzarella[2], Janik Wolters[3,4], Daniel K. L. Oi[2] and Markus Krutzik[1]

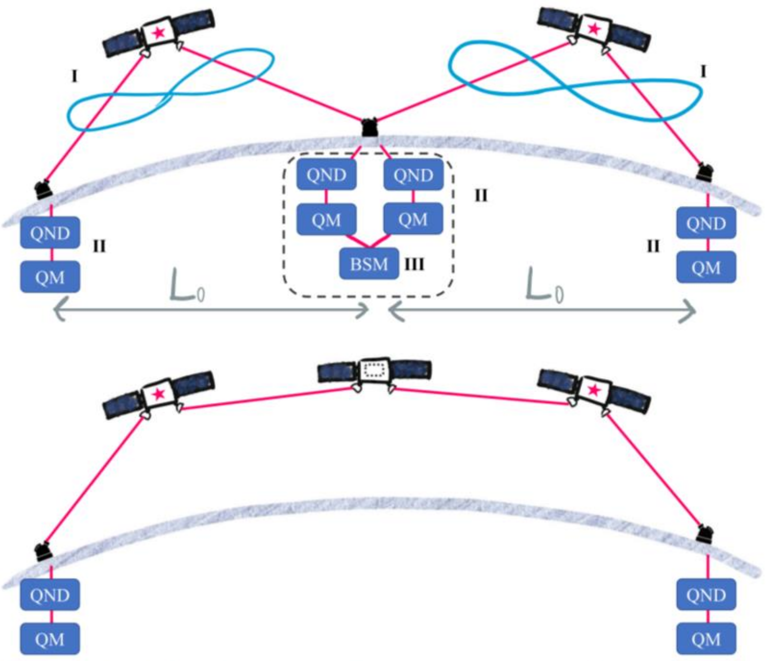



**Fig. 1 Comparison of hybrid and fully space-based quantum repeater architectures.** Top: Hybrid QND-QR protocol, following[37] with nesting level, $n = 1$ and segment length, $L_0$. Entangled photon pairs are created by on-board sources (red stars) and sent to ground stations (I). After a QND detection heralds the arrival of the photons they are loaded to QMs (II). BSM is performed between the memories to extend entanglement between end stations (III). Bottom: New architecture where the QND and QMs are also located on-board an orbiting satellite.

See Also:

- Liorni C, et al. Quantum repeaters in space. New Journal of Physics 23, 053021 (2021)
- Boone K, et al. Entanglement over global distances via quantum repeaters with satellite links. PRA 91, 052325 (2015)
- Khatri S, et al. Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet. npj QI 7, 1-5 (2021)

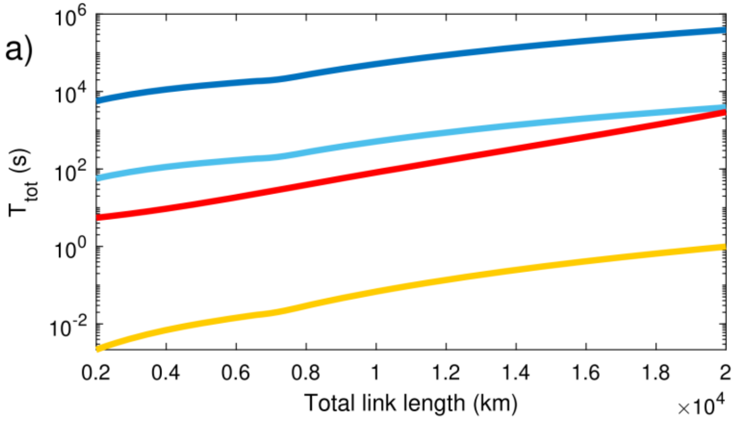



**Fig. 2 Time to distribute an entangled pair as a function of different parameters. a** total distance, **b** beam divergence and **c** memory efficiency. Within each plot: DLCZ with single (dark blue) or 100 mode (light blue) memory, hybrid-QND (red) and space-QND protocols (orange). The nominal assumed parameters (when not varied) are nonideal Gaussian beams with divergence $\Delta\theta = 4\,\mu rad$, $L = 20{,}000$ km and $\eta_r\eta_w \equiv \eta_{mem} = 0.9$, with $\eta_r = \eta_w$. We fix $\eta_q = 0.9$, $\eta_s = 1$, $R_s = 20$ MHz and an average fcc = 0.54.

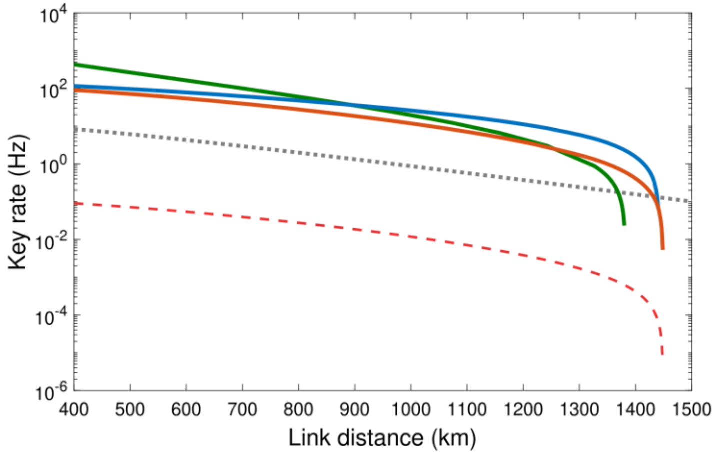



**Fig. 4 Comparison of MA-QKD schemes with ent-QKD (no memory) protocol.** Grey dotted: ent-QKD ($R_s = 20$ MHz); blue: uplink configuration with storage time 5 ms; solid (dotted) red: downlink configuration, with $N = 1000$ (single) temporal modes with storage time 7.5 s; green: downlink with $N = 1000$ temporal modes and $m = 100$ memory pairs with storage time 100 ms.

- Challenges
  - Cryogenics
  - Detectors
  - Wavelength conversion
  - Heralding, Loading/Extraction efficiency
  - Storage times/fidelity
  - Coupling, Rate, #Modes …

Ma Y, et al. One-hour coherent optical storage in an atomic frequency comb memory. Ncomms 12, 1-6 (2021)

Se also: Time-delayed single quantum repeater node for global quantum communications with a single satellite, arXiv:2303.04174

# UK Space Quantum Technology Opportunities

- Diverse Quantum Technology Portfolio
- UK Investment in Quantum Technology (recent £2.5B injection)
- Several missions under development
- Quantum and Space expertise
- Strong Space Industry, Primes and SMEs
- Small Satellite/CubeSat strengths, rapid space development
- International Focus, Collaboration/Cooperation/Coordination

X THE PLACE OF USEFUL LEARNING

University of Strathclyde Science