ENTANGLED-PHOTON SOURCE DEVELOPMENT FOR QUANTUM KEY DISTRIBUTION

Fraunhofer Centre for Applied Photonics

Loyd J. Mcknight, Head of Quantum Technologies Business Unit

22nd April 2024

Fraunhofer UK

Fraunhofer Centre for Applied Photonics

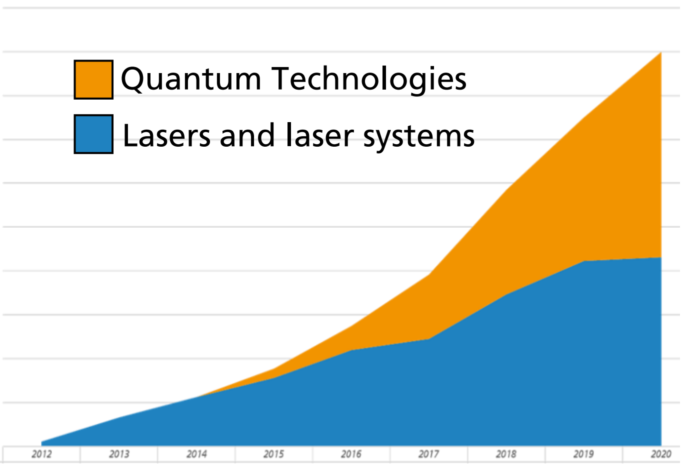
- Founded in 2012 in Glasgow, Scotland, UK
  - Non-for-profit RTO
  - Part of the Fraunhofer network
- Currently 70 staff including 25 PhD/EngD students
- Supporting industry
  - Contract R&D
  - Innovations in photonics
  - >100 funded company partners
- Two Business Units
  - Laser and Laser Systems
  - Quantum Technologies

Scottish photonics and quantum cluster

- Scotland has a photonics sector with a turnover greater than £1Bn
- More than 60 companies with 5500 highly skilled jobs
- Over 50% of quantum technologies Innovate UK funded activities include a Scottish organisation
- Fraunhofer CAP participate in 30% of the UK's Quantum Technology Innovation Programme

"Glentanglement"

Business Units, markets and technical themes



- Both business units continue to grow serving a wide range of markets and funding sources.

SPACE	HEALTHCARE
ENERGY	MANUFACTURE
LIFESCIENCE	DEFENCE

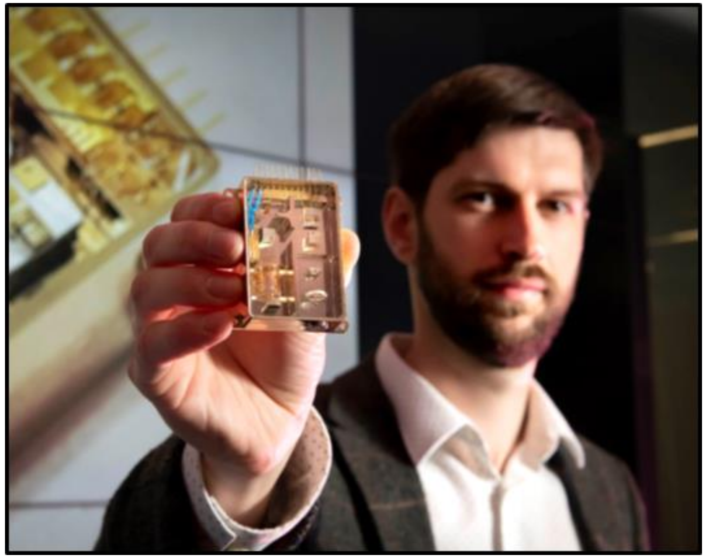
- Technical expertise and facilities are shared between teams and staff work across themes.

Lasers and Laser Systems

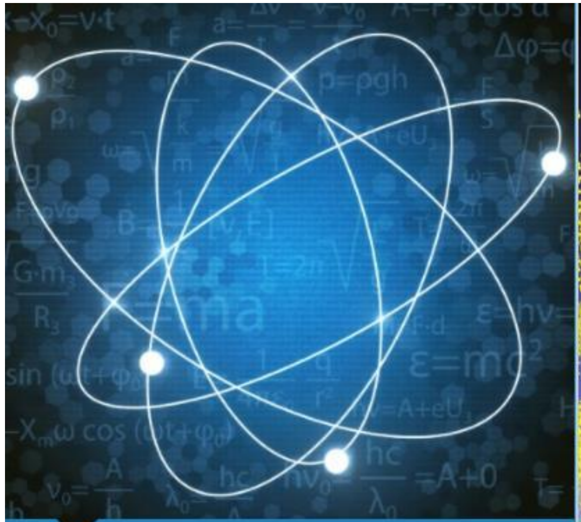
- Chemical sensing
- Lidar
- Laser instrumentation
- Asset monitoring

Quantum Technologies

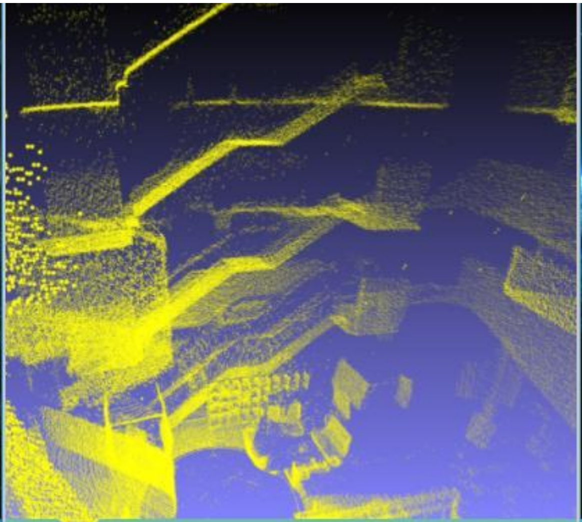
- Sensing
- Communications
- Imaging, Lidar, Spectroscopy
- Computing



Quantum technology themes at Fraunhofer CAP

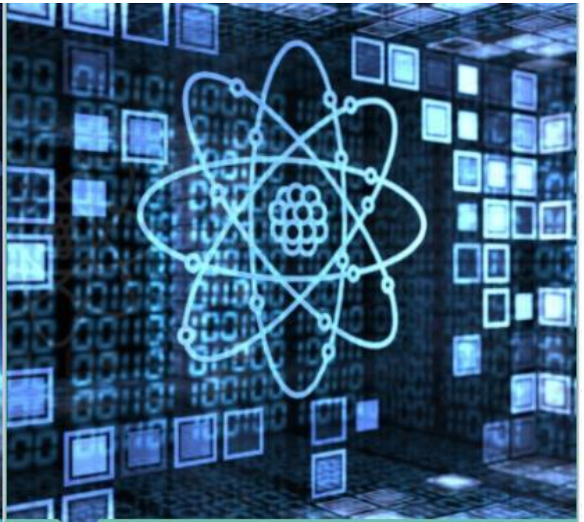


Quantum Sensing



Quantum imaging LiDAR and spectroscopy

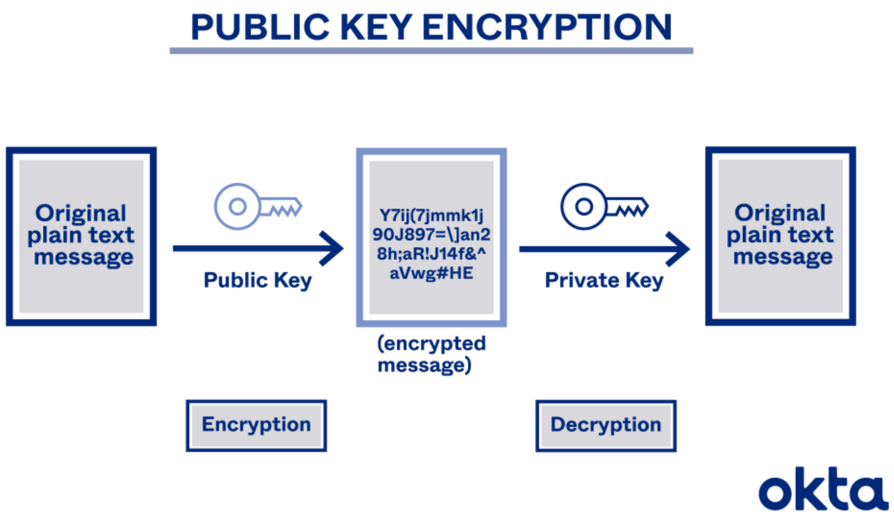
Quantum Communications



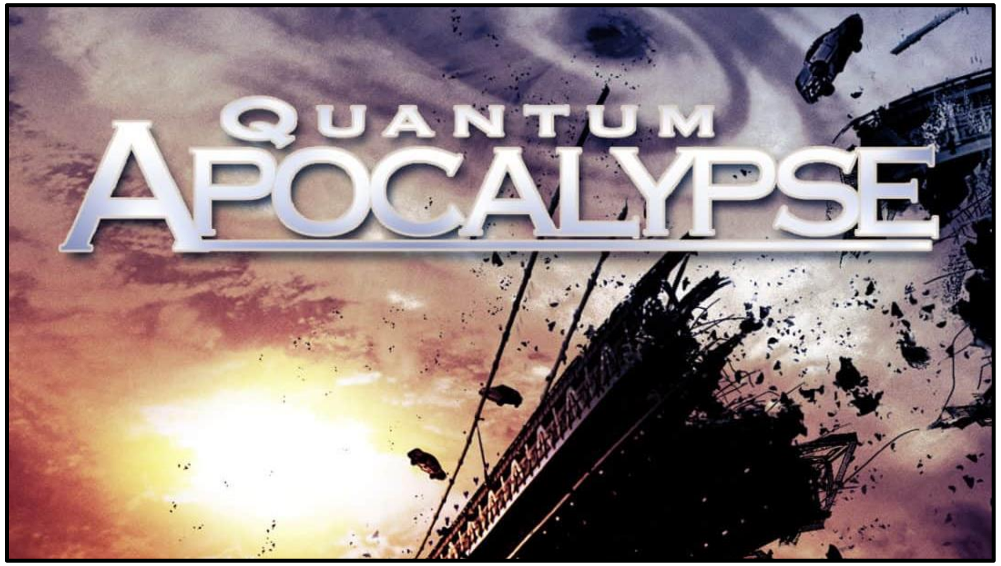
Quantum Computing

Introduction to quantum networking

Motivation: Protection against future threats



- Public Key cryptography could be broken by quantum computers when they are sufficiently powerful.
- All valuable information from businesses, states and individuals will be accessible to those with sufficient computing power.
- Information collected today can still be valuable in 20+ years.
- Post quantum cryptography is still immature.



The CISA report said, "including some scenarios as wide-ranging as the adversary possessing a theoretical quantum computing capability to break public-key cryptography." ***April 2024***

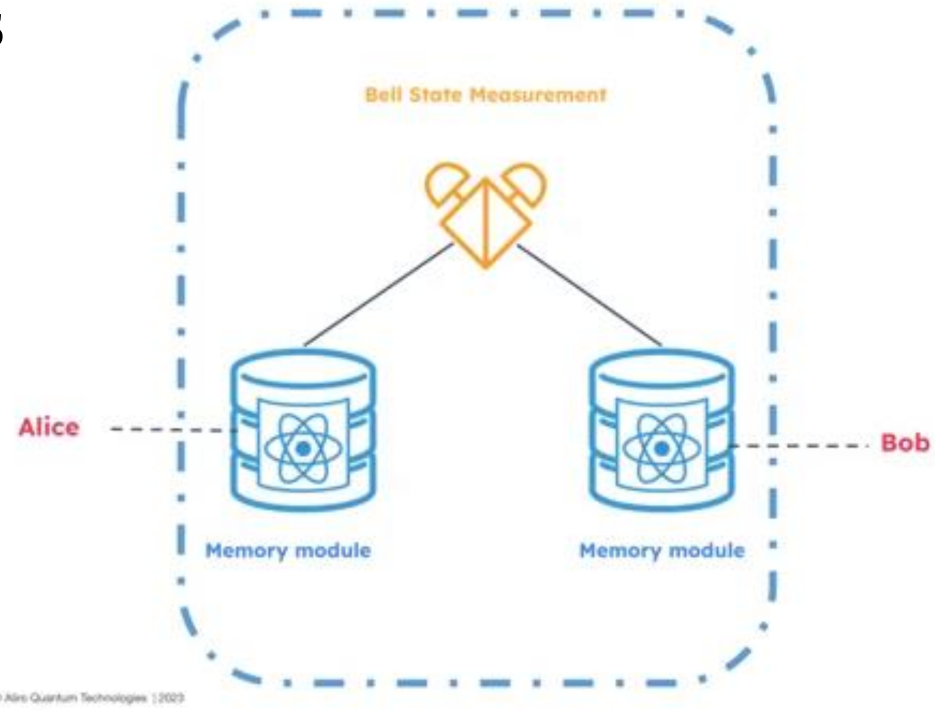
Motivation: Protection of critical infrastructure

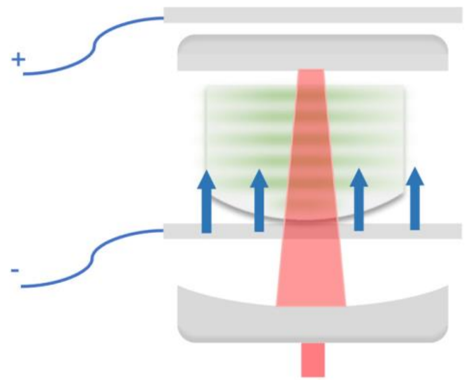
- Assumption is the cost of QKD deployment will initially prohibit mass adoption by consumers therefore high-value applications will be the market.
- Modern society relies on several types of critical infrastructure to function.
  - Energy, Communications, Financial services, Transport, Healthcare, Government
- These critical infrastructure facilities represent a large risk to public safety and economic activity.

"A water utility in Pennsylvania and other U.S. water utilities and organizations involved in water distribution confirmed cyberattacks throughout November and December. The top cybersecurity agency in the U.S. told reporters in December that it was tracking a small number of impacted water utilities and reaching out directly to operators that may have been affected." **February 2024**

Motivation: Application of quantum networks

- Using entanglement swapping extended quantum networks “the quantum internet” can be realised.
  - Hybrid computing methods.
  - Broad geographic distribution.
  - More efficient use of resource.
  - Blind quantum computing.
- Routes to scalable quantum computing
  - Limited capacity of dilution fridge
  - Access to quantum memory
  - Take advantages of different qubit architectures

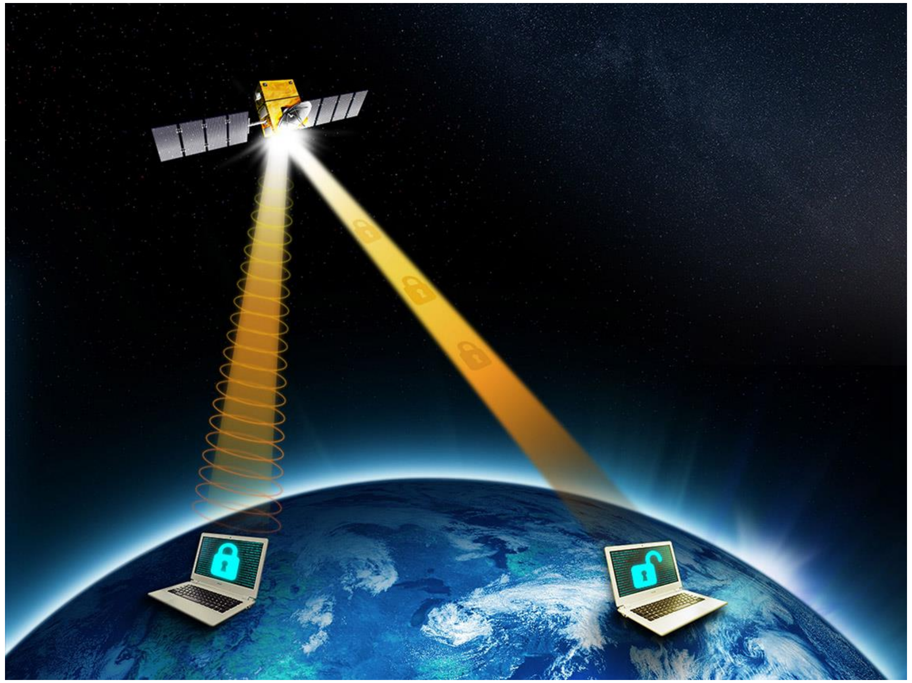




Fraunhofer UK

Motivation for QKD from space

- Global coverage
  - Lower propagation losses
  - No need for nodes and repeaters
  - Access to any facility/customer
- Enhanced security
  - Harder to disrupt
- Demonstrations have been made:



Article

Entanglement-based secure quantum cryptography over 1,120 kilometres

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

Received: 15 July 2019

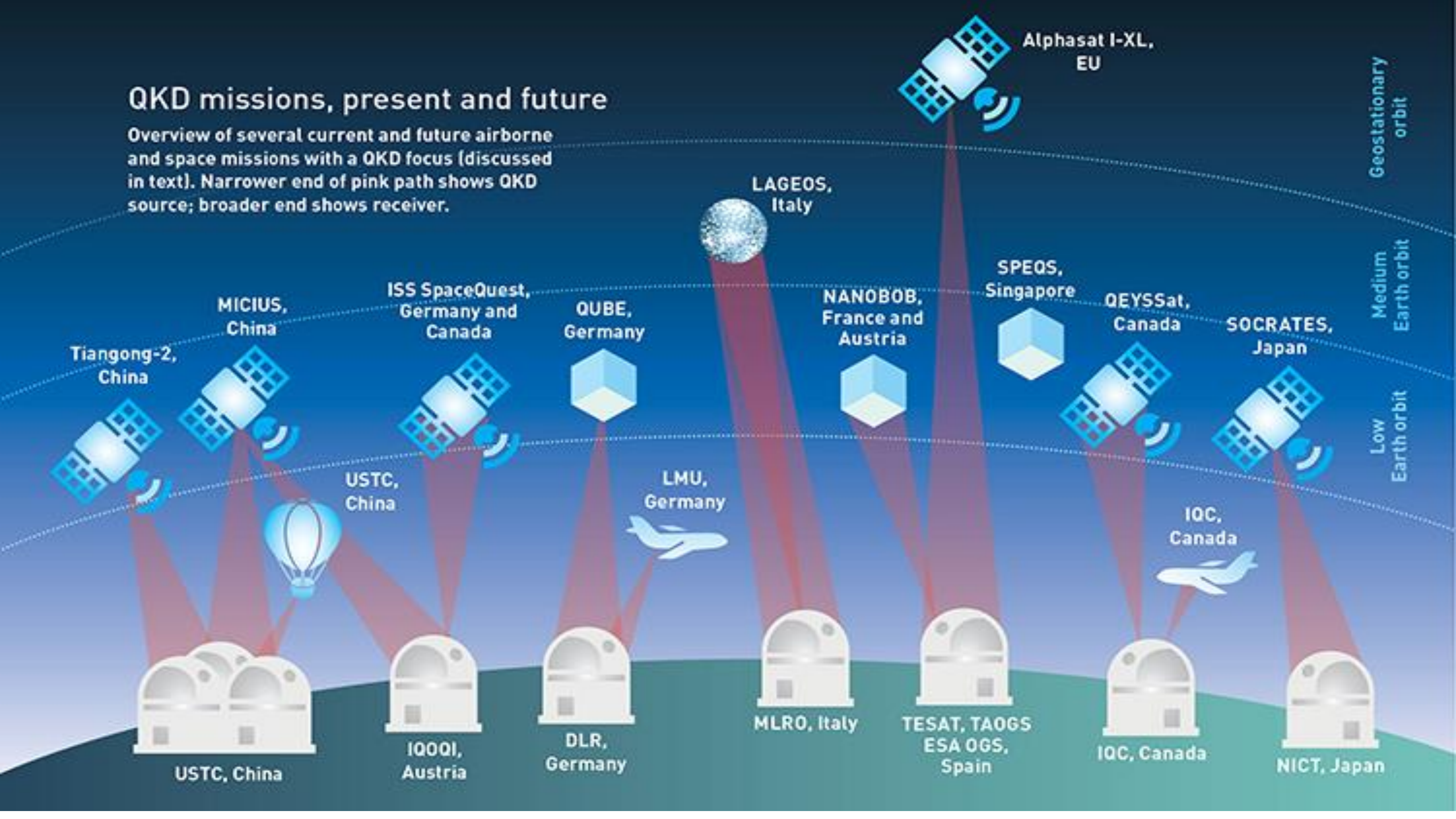
Accepted: 13 May 2020

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] ✉

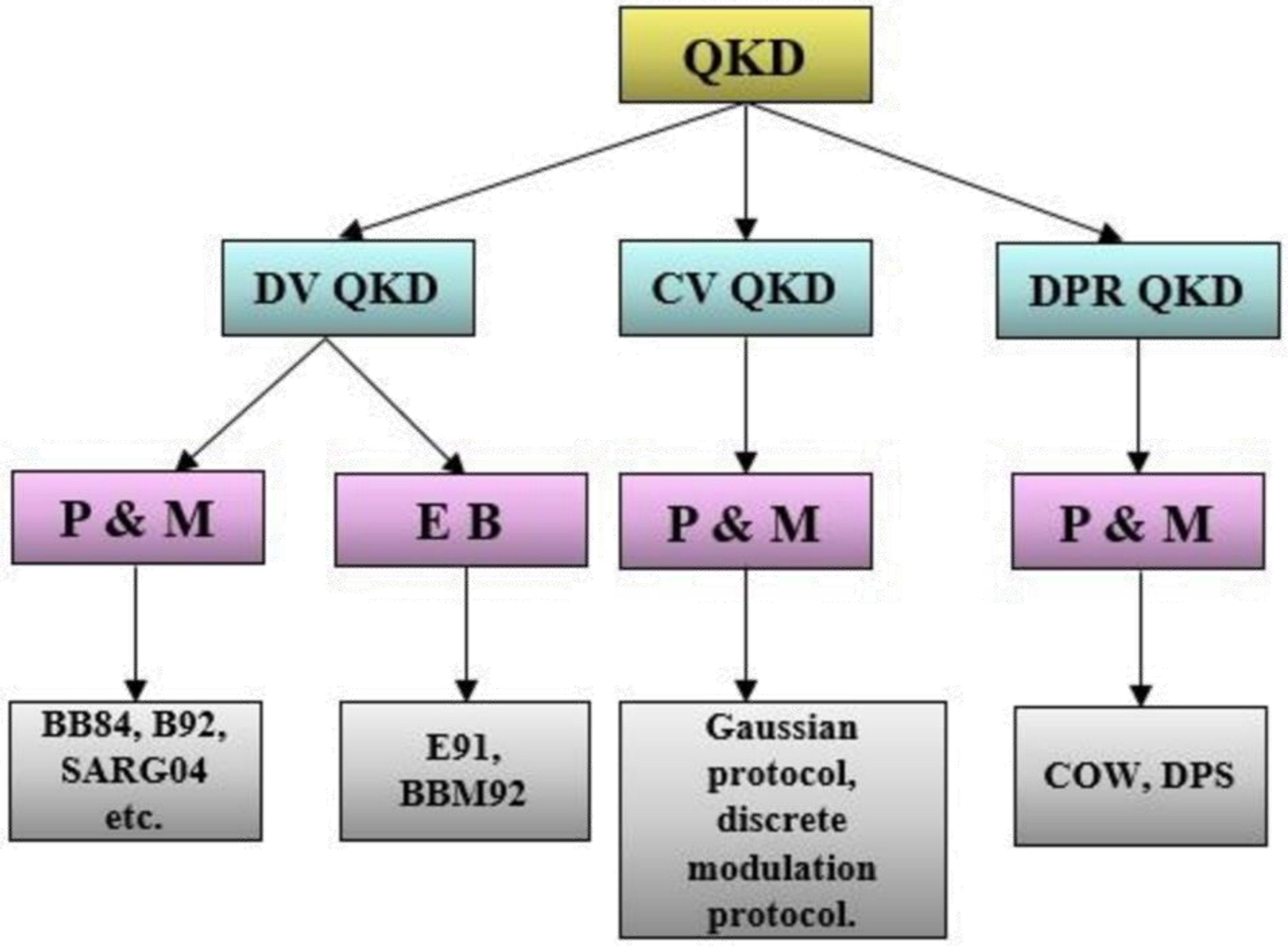
- Micius satellite demonstration
  - 5.9×10^6 entangled photon pairs/s
  - A finite secret-key rate of 0.12 bits/s
  - Link maintained over ~5 minutes
  - 372-bit secret key

Fraunhofer UK


QKD missions, present and future
Overview of several current and future airborne and space missions with a QKD focus (discussed in text). Narrower end of pink path shows QKD source; broader end shows receiver.
Alphasat I-XL, EU
Geostationary orbit
LAGEOS, Italy
Medium Earth orbit
SPEQS, Singapore
NANOBOB, France and Austria
QEYSSat, Canada
SOCRATES, Japan
ISS SpaceQuest, Germany and Canada
QUBE, Germany
MICIUS, China
Tiangong-2, China
Low Earth orbit
USTC, China
LMU, Germany
IQC, Canada
USTC, China
IQOQI, Austria
DLR, Germany
MLRO, Italy
TESAT, TAOGS ESA OGS, Spain
IQC, Canada
NICT, Japan

Types of quantum key distribution

- Discrete variable
  - Prepare and measure
  - Entanglement based
- Continuous variable
- Distributed phase reference



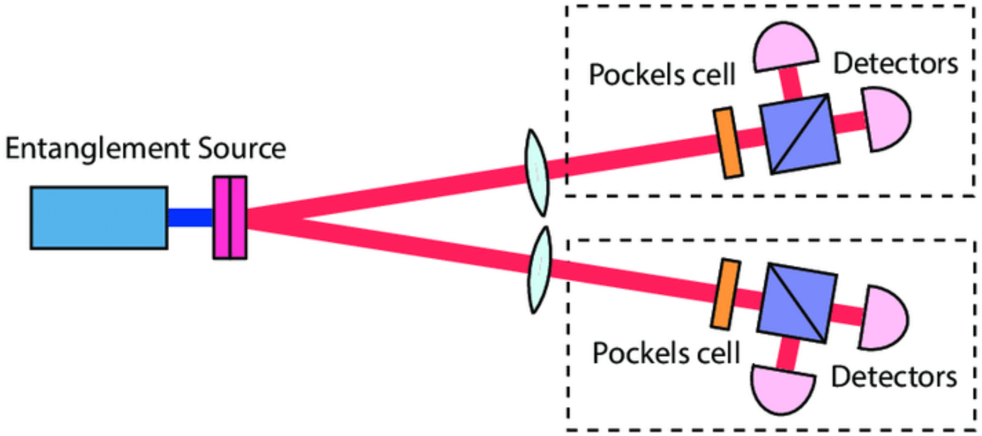
https://arxiv.org/html/2401.00146v1

Entanglement-based QKD

- Reduced complexity and trust required at the point of key generation.
- Potential for higher key rates over longer distances. Primarily limited by components available for prepare and measure.
- Prepare and measure QKD is more susceptible to certain eavesdropping attacks, such as photon-number-splitting attacks, which can exploit vulnerabilities in the transmission of individual quantum states.
- Entanglement swapping opens up opportunities for quantum networks by linking together quantum computers.

Prepare and measure

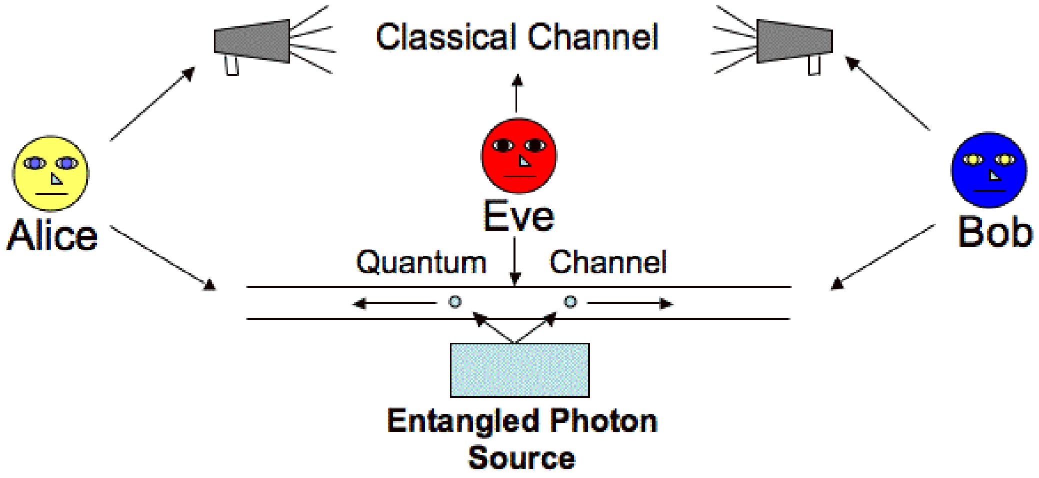
Entanglement-based

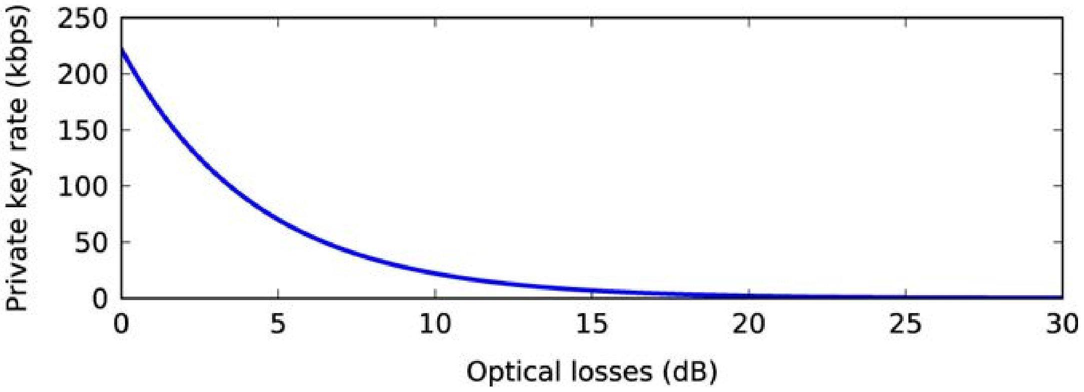


Introduction: QKD system components

Each system will have some basic elements

- Transmitter
  - Source of photons
  - Means to encode (for prepare and measure)
- Receiver
  - Single photon detectors (for discrete)
  - Heterodyne detectors (for continuous variable)
- Scheme/protocol
- Transmission link
  - Fibre
  - Telescopes and beam steering system
- A classical link





Fraunhofer UK

Discrete variable: Types of photon sources for

- True single photons
  - Triggered and indistinguishable (e.g. quantum dots and diamond colour centres)

  A triggered single photon source will produce a single photon ‘on demand’. This is practical for synchronisation. If the photons have the same properties (indistinguishable) they may be interfered with each other which can be useful in computing applications.

  - Heralded (spontaneous parametric downconversion or four-wave mixing)

  A heralded photon source is one in which a pair of photons are produced at the same time. This photon pair may be generated statistically rather than on demand. The presence of one can be used in order to look for the other which helps with synchronisation.

  - Entangled (e.g. in polarisation, time, or frequency)

  The property an individual photon will be related to the other but is otherwise unknown until checked. Entangled photons can be used for different QKD schemes that may be more secure.

- Attenuated lasers
  - Basic QKD schemes can rely on the statistical probability of having a single photon but this method is usually considered less secure.

Entangled-Photon Source Development for Quantum Key Distribution

A collaboration including:

CRAFT PROSPECT
a space engineering practice

ALTER
TECHNOLOGY

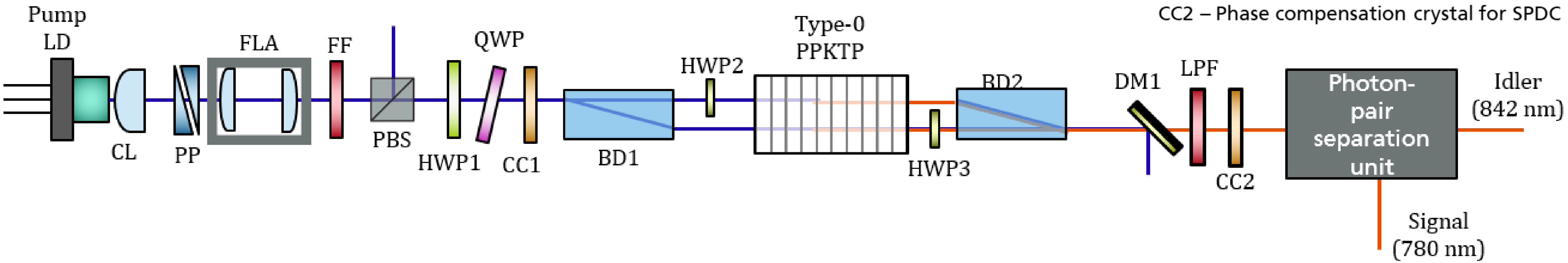
In memory of Una Marvet

Fraunhofer UK

Design of source

- Motivated by
  - Variation of a published (proven) approach
  - Single nonlinear crystal
  - Maturity of components
  - 800 nm wavelength for compatibility with silicon SPADs
  - Possibility for a compact unit
  - Linear scheme for a simple mounting approach

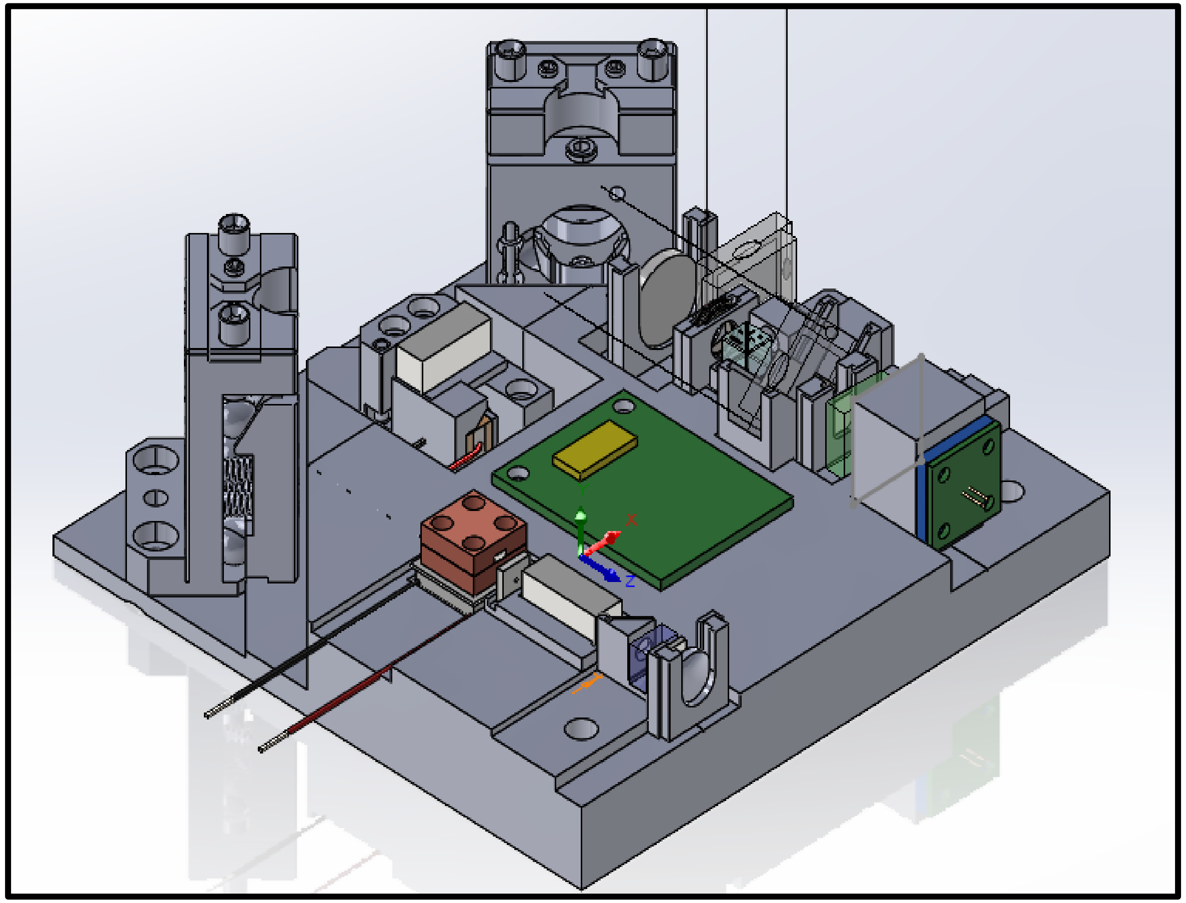
LD – Laser diode
CL – Pump collimating lens
PP – Prism pair (Wedge)
FLP – Pump focussing lens pair
FF – Pump fluorescent filter
PBS – Polarizing beam splitter
HWP1 – Pump half-wave plate
QWP – Pump quarter wave plate
CC1 – Pump phase compensation crystal (YVO4)
BD1 – Beam displacer for pump
HWP2 – Half-wave pate for pump (at 45°)
HWP3 - Half-wave pate for SPDC (at 45°)
BD2 – Beam displacer for SPDC
DM1 – Pump dichroic mirror
LPF – Long pass filter
CC2 – Phase compensation crystal for SPDC

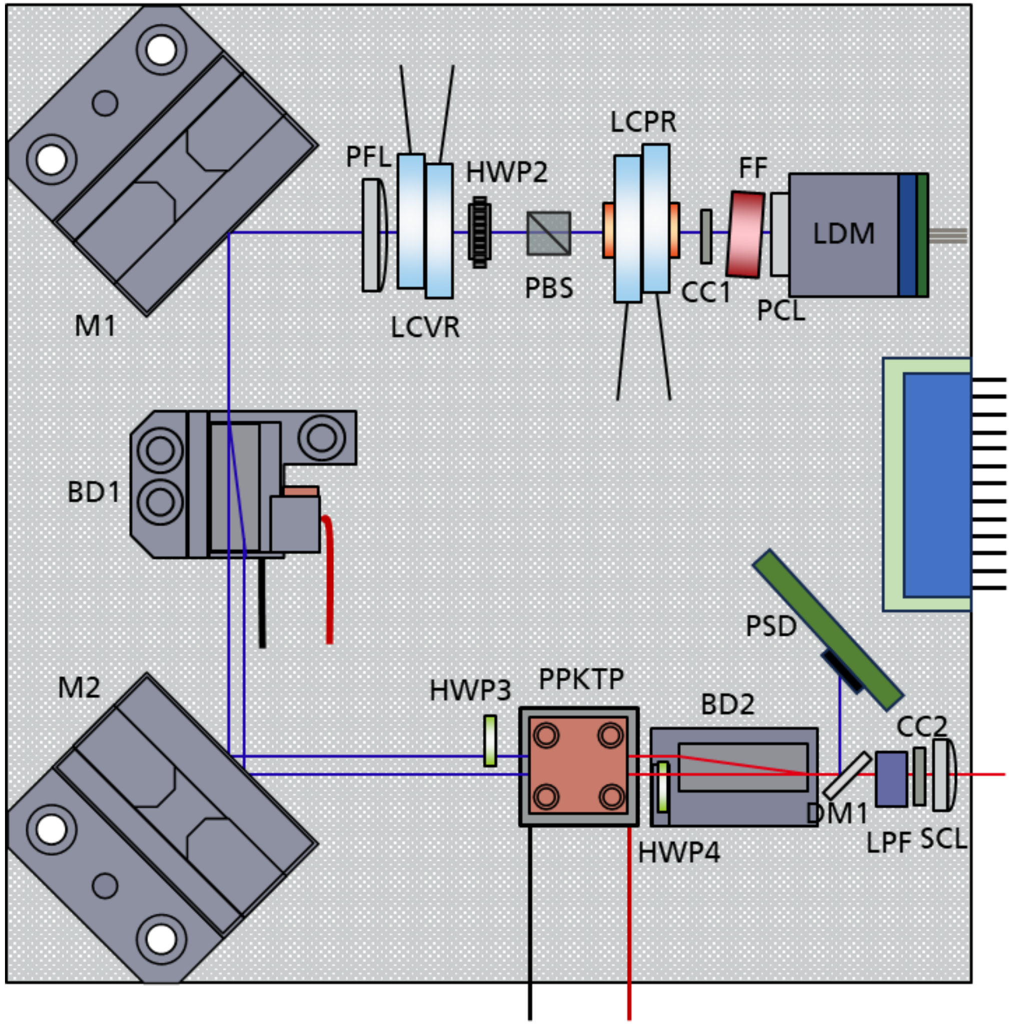


[1] A. Lohrmann, et. al.,. "Broadband pumped polarization entangled photon-pair source in a linear beam displacement interferometer." *Applied Physics Letters* 116, no. 2 (2020): 021101

Breadboard prototype design iteration

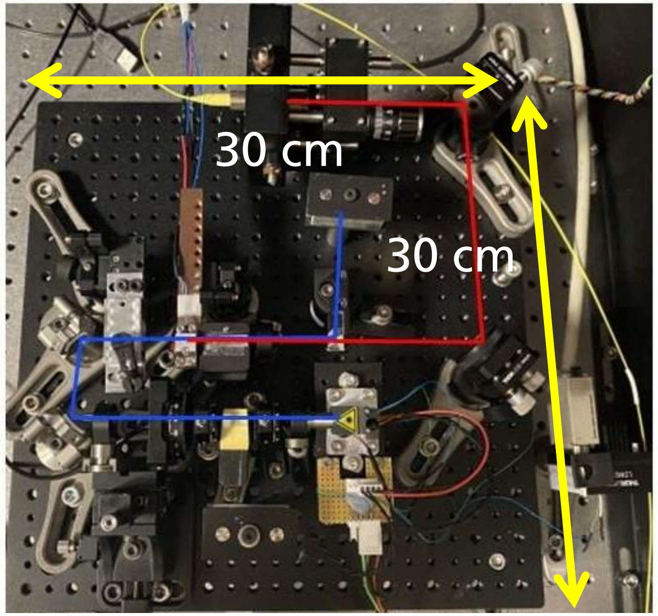
- Compatibility with 1U form factor
- Liquid crystal polarisation controllers



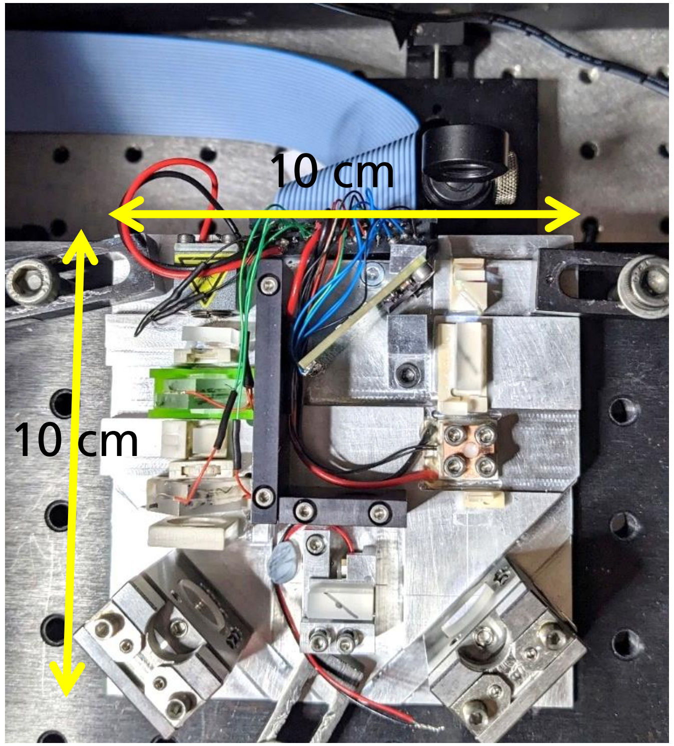


Breadboard and prototype build

- Development of a polarisation entangled photon source (EPS) with lower SWaP requirements.
- Successfully developed three similar working prototypes of the EPS with CubeSat Standards (1U size).
- Developed an FPGA based software for remote control of the source during flight.

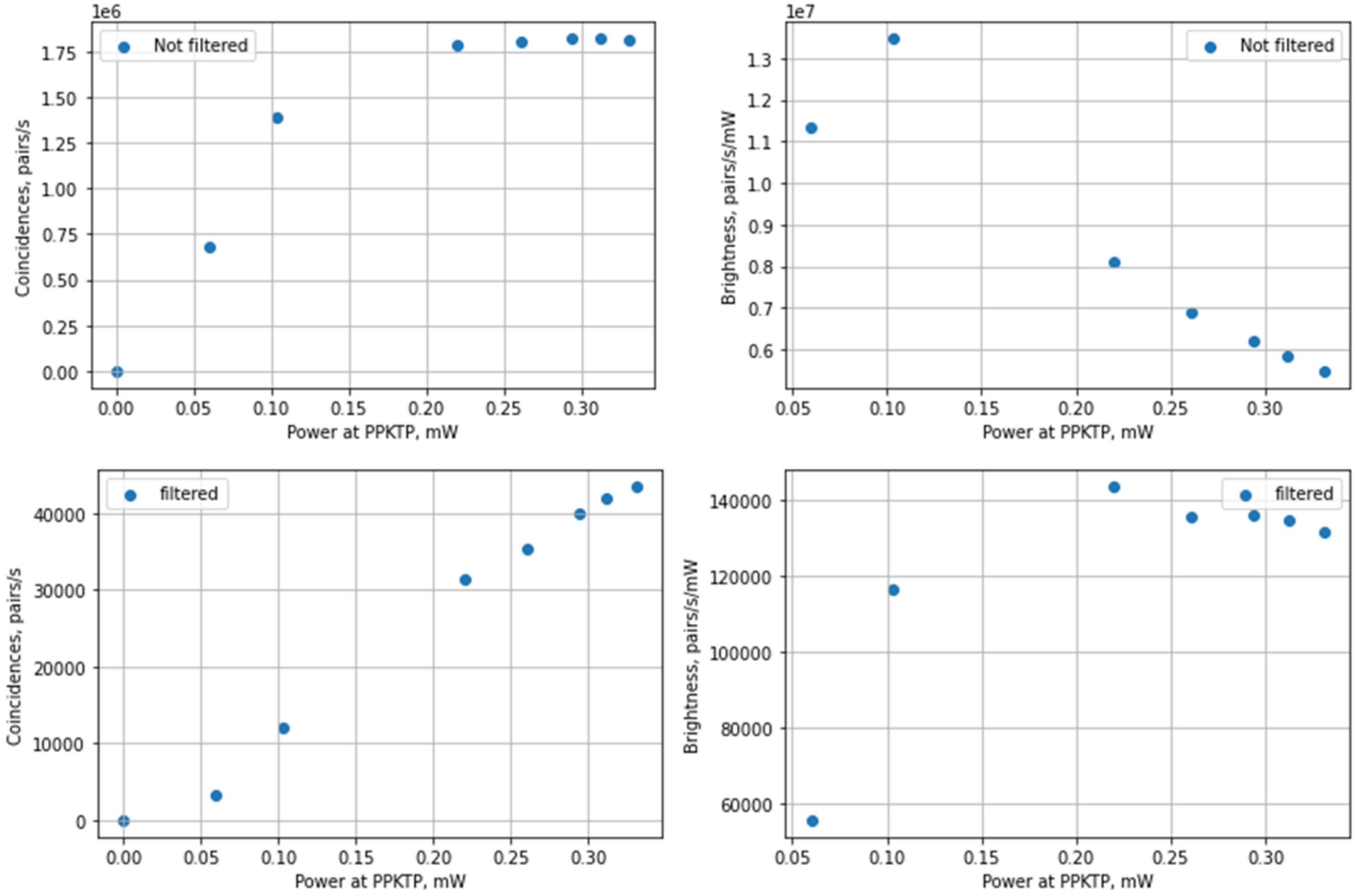


Lab setup



Packaged unit

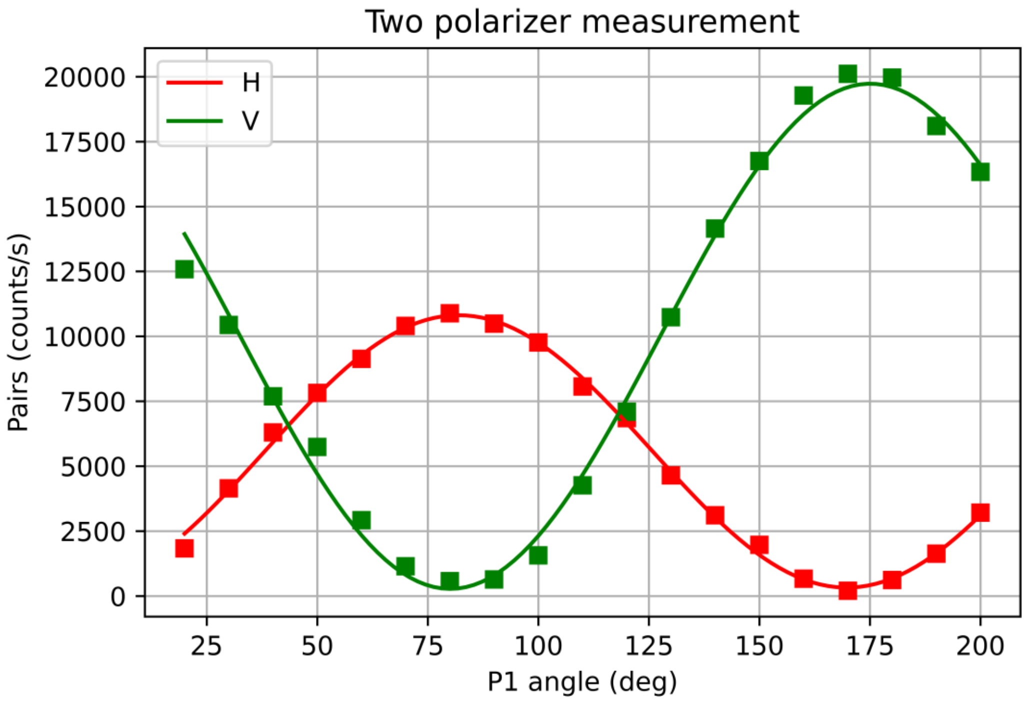
Protype unit preliminary tests

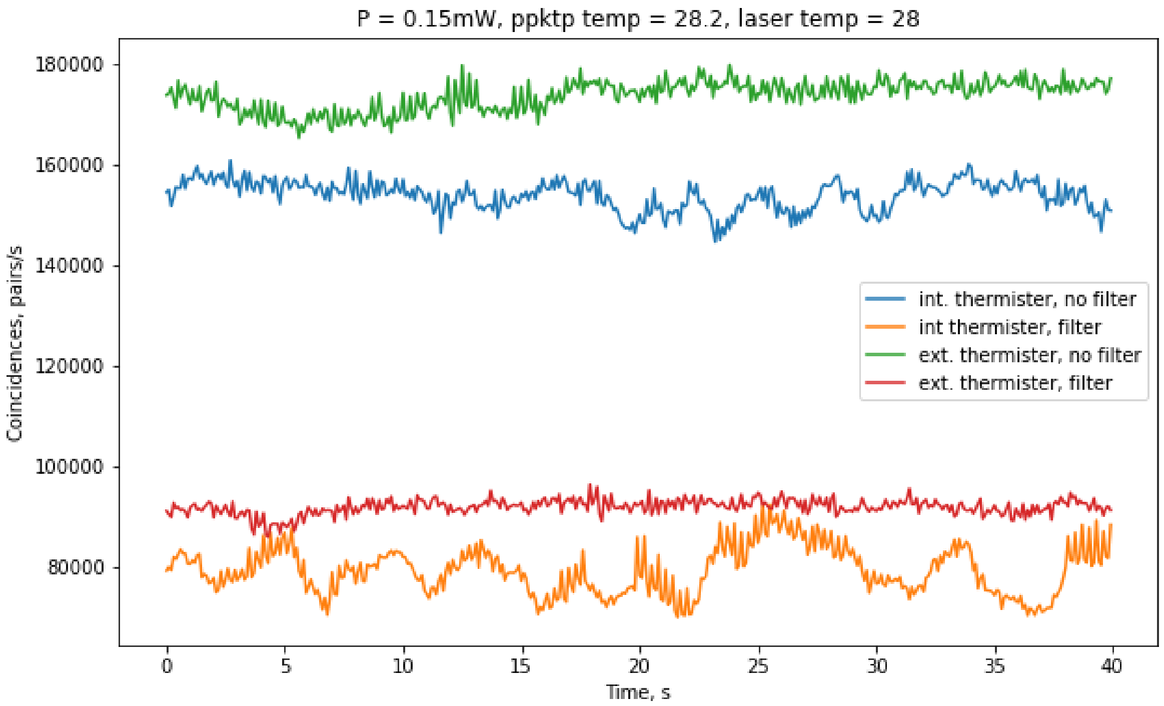


- Measured coincidences and brightness
- Shown with and without spectral filter 780+/-10 nm
- Without the filter (for a broadband source), the brightness decreases at higher pump powers.
- With the aid of filters, the brightness is constant with pump power.

Protype unit preliminary tests

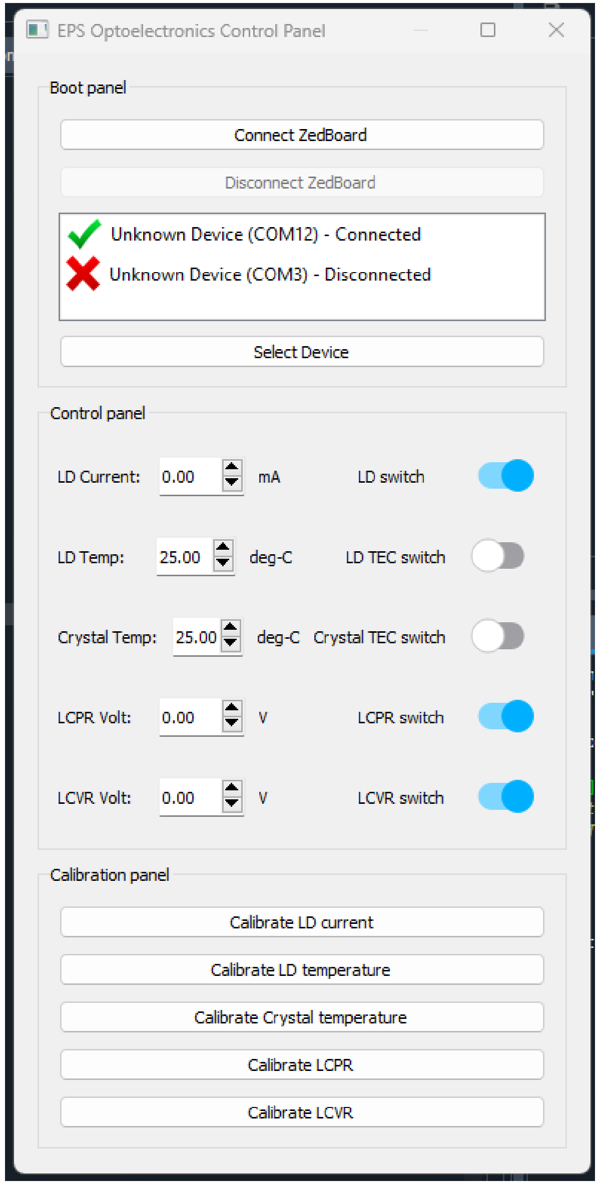
- Entanglement tests of the source
- Long term tests on the source are ongoing.
- Temperature fluctuation identified as the parameter
  - Explore more robust mounting designs, inspect the quality of the TECs





Summary of features.

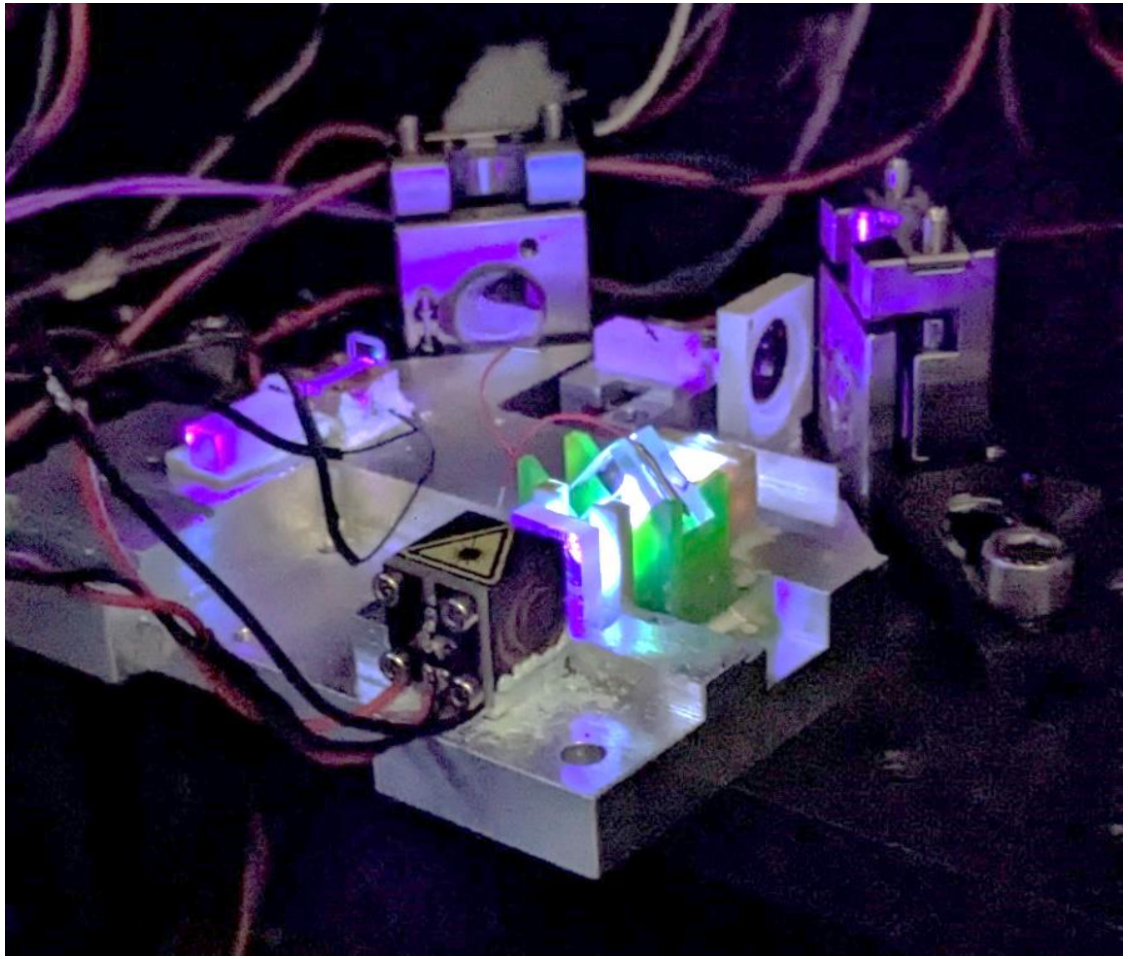
- A source based on linear displacement interferometer.
- Source developed mostly with COTS components.
- Generates entangled photon-pairs at broadband NIR wavelengths around 810 nm, at a rate of approx. 10 million pairs per second with 1 mW of the pump power.
- Customizable to a fibre coupled unit based on user requirements.
- Good functional stability with less critical elements.
- Use of liquid crystal devices for power and polarization controls, which allow fast switching between different entangled states (Phi+ to Phi-).
- Can be used for different applications such as quantum communication, quantum computing and quantum sensing.



ALTER TECHNOLOGY CRAFT PROSPECT Fraunhofer UK

Future activities

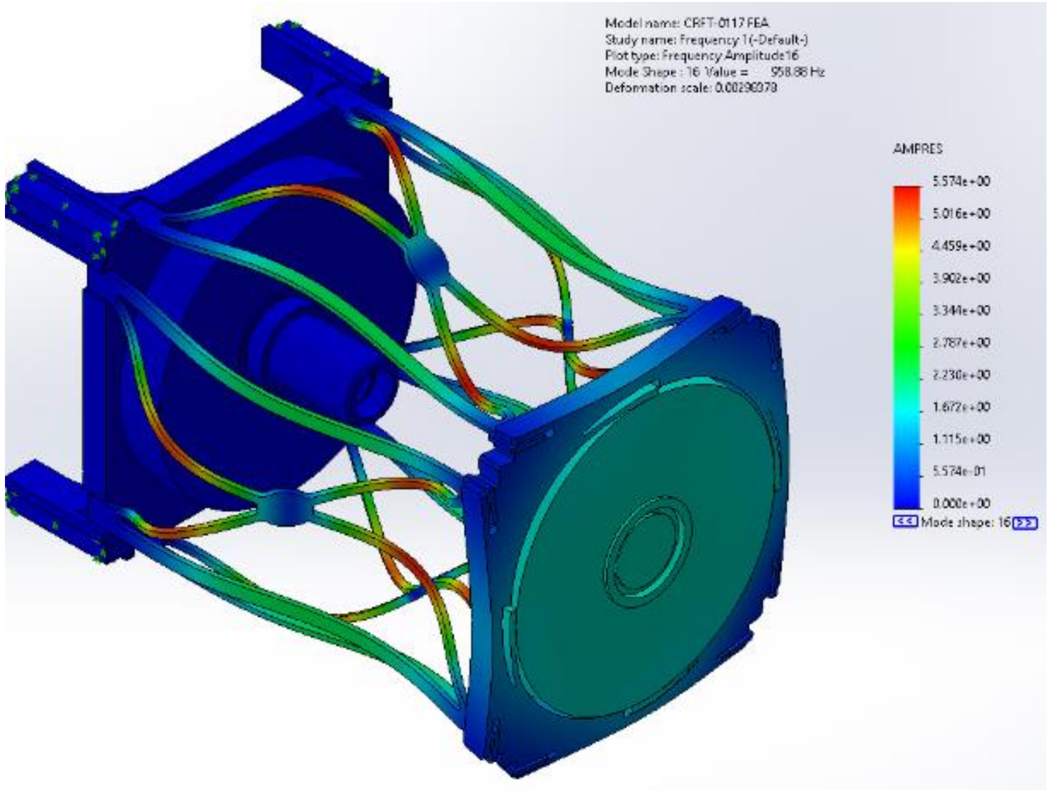
- Development of a real-time quantum key generator based on the unit.
- Development liquid-crystal based high-speed entanglement analyser module and integration to the unit.
- Verification of environmental stability of the source unit.
- Integration with classical comms systems

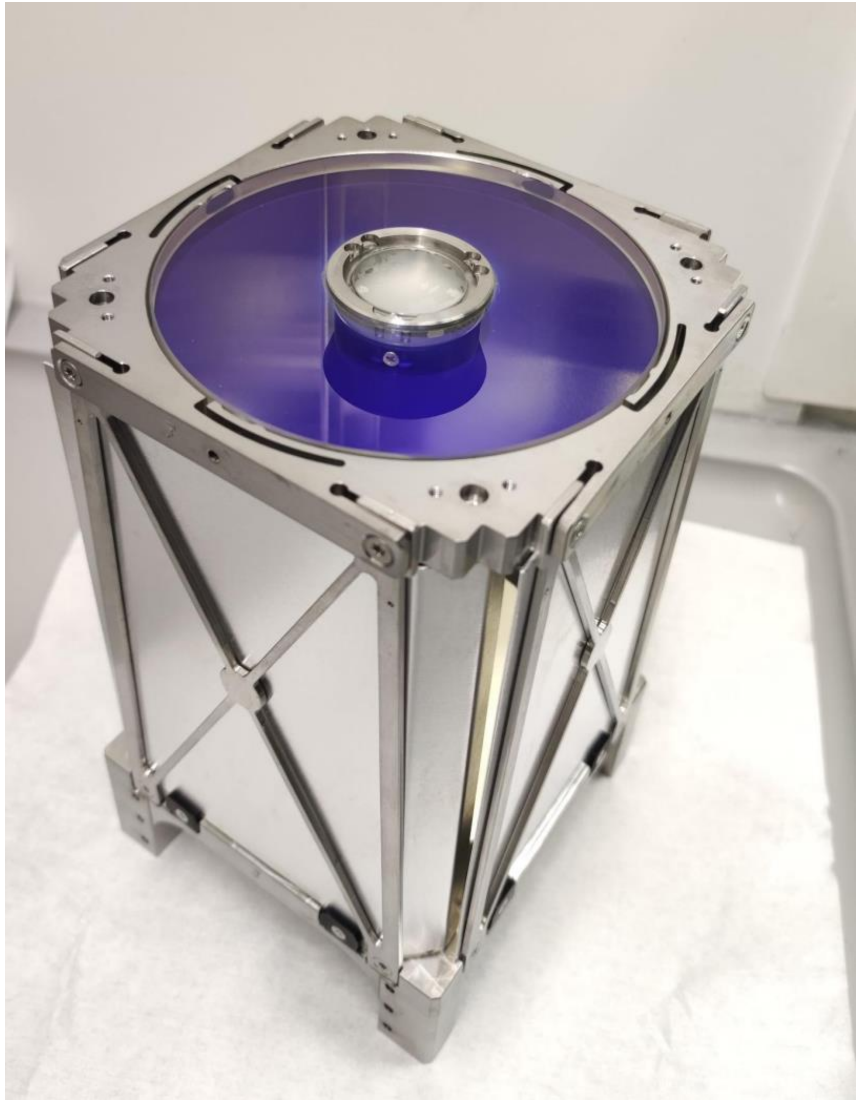


Other ongoing activities

Quantum key distribution components for space

- Space compact telescope development
  - Operation at near infrared wavelengths
  - Size less than 10 cm x 10 cm x 20 cm
  - Interfaces with beamsteering, transmitter and beacon source

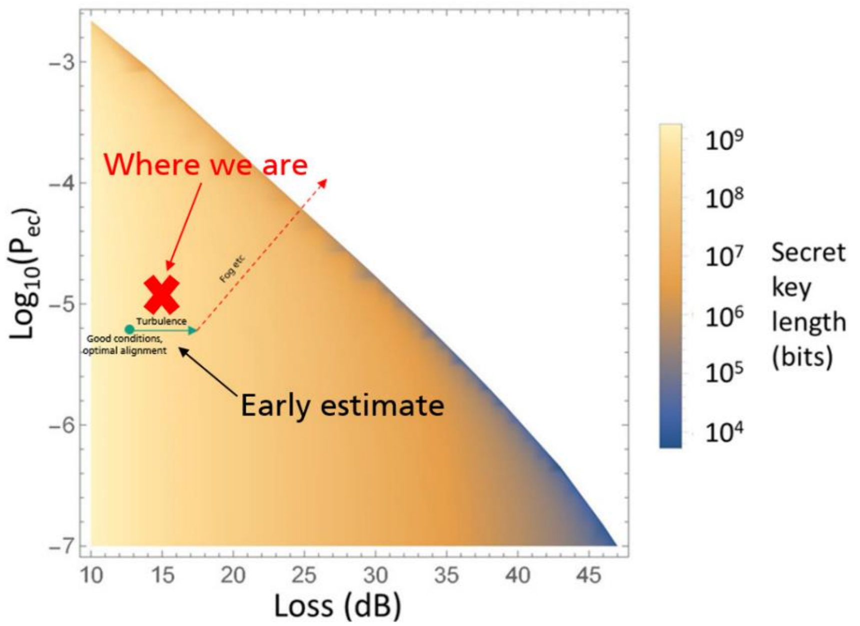




CRAFT PROSPECT Fraunhofer UK

Building-building free-space optics QKD Links

- 200m range rooftop building links across the city of Glasgow.
- Gbit secret key lengths achievable.
- Beam steering and lock technology.
- Components for space-QKD



BT AIRQKD University of Strathclyde Fraunhofer UK

Thank you!