Quantum Key Distribution from CubeSats (SSC20-P2-16)

CRAFT PROSPECT

With partners

Cassandra Mercury, Doug McNeil, Steve Greenland, Colin Aitken, Sonali Mohapatra
Craft Prospect Ltd
cassandra@craftprospect.com

Daniel Oi
University of Strathclyde
daniel.oi@strath.ac.uk

Siddarth Joshi, David Lowndes, Elliott Hastings
University of Bristol
sk.joshi@bristol.ac.uk

Peter Mendham, Marta Przyszlak
Bright Ascension
peter@brightascension.com

A need for post-quantum computing encryption methods

Popular modern encryption methods are at threat by quantum computing, where quantum algorithms have already been developed that can crack popular encryption methods.

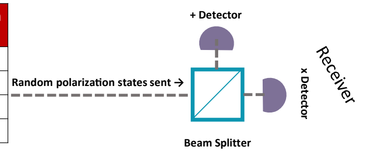
Quantum Key Distribution (QKD) can future proof our communication systems by using quantum principles to create a new encryption method. Using satellites to provide key delivery to future QKD secured networks and systems, the approach of key delivery from space as a service will provide a fundamental tool within modern cybersecurity systems for authentication and encryption.

How does QKD work?

A transmitter sends a series of encoded photons to a receiver. Each photon can be either a 0 or a 1 and will be sent in one of two polarizations, + or x.

Transmitter

Basis	Bit	Polarization States
+	0	→
+	1	↑
x	0	↗
x	1	↘

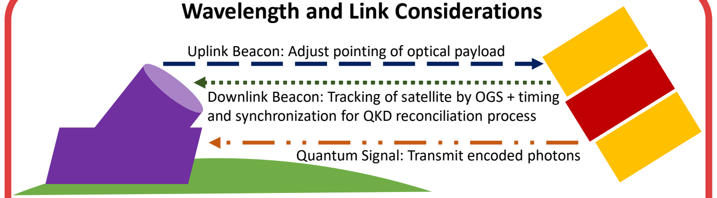


The polarization state is sent over the optical channel and is randomized. The receiver's beam splitter will randomize which basis the photon will be measured in, which then limits the theoretical maximum of correctly measured photons to 50%. This is because a truly random process will choose the incorrect basis 50% of the time.

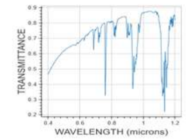
These raw bits then go through a reconciliation process over classical communication channels to arrive at a shared, secret key.

These secret keys are then used in symmetric key encryption algorithms to encrypt data between any two actors without the possibility of decryption by a bad actor.

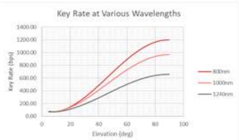
Wavelength and Link Considerations



Three optical signals are transmitted along the ground to space optical path. The uplink beacon is transmitted from the ground to the satellite, while the downlink beacon and quantum signal are transmitted from the satellite to the OGS.



Transmittance through the atmosphere must be considered. Higher wavelengths have better transmittance, but increases in diffraction. That will lead to lowered received intensity and reduced key rates.



Atmospheric turbulence leads to higher beam wander and spread; the transmitter is put on board the satellite to reduce total optical losses during transmission as compared to ground-to-space transmission.

ROKS (Responsive Operations for Key Services)

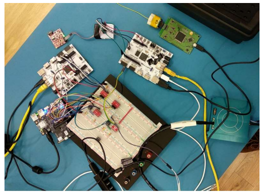
The first scheduled UK mission to deploy QKD from space. Will use the small form factor of a CubeSat to put a quantum source transmitter and full optical payload into orbit.

All optical systems including the pointing, tracking, and time synchronization systems have been condensed in order to fit the allotted payload capacity of the CubeSat. An optical ground station provided by our partners at the University of Bristol will receive the keys and showcase the ability to conduct efficient key transfer methods.

Satellite

CubeSat Size: 6U
QKD Payload Size: 2.5U
Orbit: LEO (600km)
Launch: Summer 2022

Transmitter
Quantum Source: Weak coherent pulse
Protocol: Decoy state

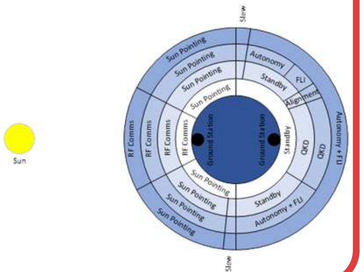


Payload computer systems for the PIU, Quantum Payload, CASSA, and FLI interfaced and under test in lab

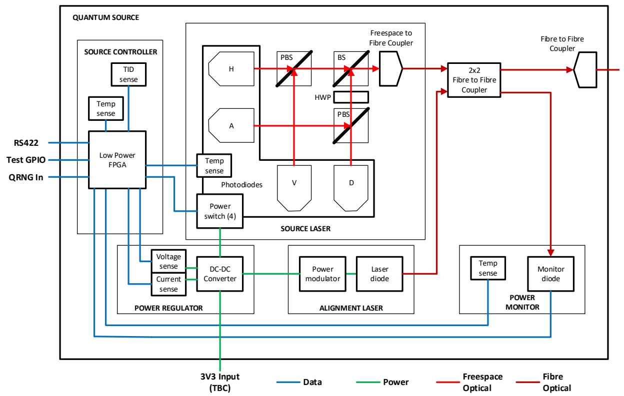
Onboard Autonomy

Also onboard will be a Forwards Looking Imager (FLI) that will scout targets ahead of the flight path for obstruction and/or suitability. An autonomous onboard computer (CASSA) will self-select targets during orbital passes to produce efficiency savings in operations.

Operational modes will vary depending on position of satellite relative to day/night side of Earth, as shown in diagram to the right.

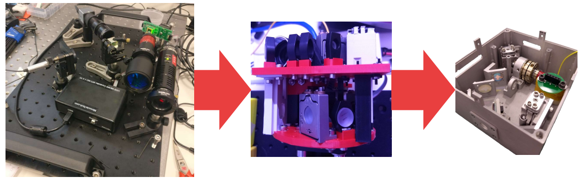


JADE (Joint Alignment, Diode, and Emitter) which will combine the quantum source with a monitor to evaluate the emitted number of photons and an alignment system to correct for in-orbit optical path changes.

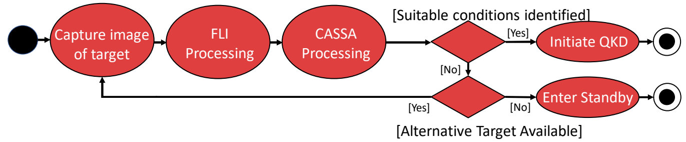


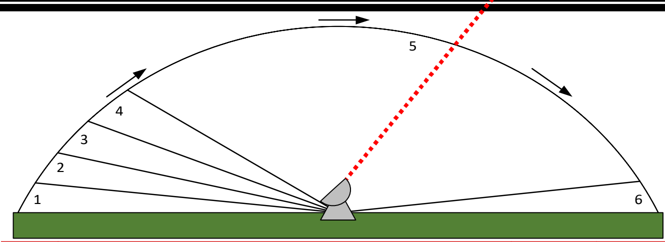
Miniaturization Effort

The quantum payload efforts began at the University of Bristol and has progressed at Craft Prospect Ltd. The aim has been to miniaturize the components to a CubeSat form factor. Development is currently at an engineering model, shortly to progress to a proto-flight model. Environmental testing of the payload will commence shortly.



Concept of Operations





Phase	Description	Minimum Elevation	Maximum Elevation
1	CubeSat above horizon but not in view of ground station.	0°	10°
2	Platform pointing to target ground station.	10°	20°
3	Authenticate ground station.	20°	30°
4	OGS alignment.	30°	40°
5	QKD transmission to OGS. Possibly followed by reconciliation with RF ground station.	40°	170°
6	CubeSat out of view of ground station but above horizon.	170°	180°

CubeSat operations by elevation above horizon