CRAFT PROSPECT

Responsive Operations for Key Services

1. Abstract

The ROKS IOD mission will showcase the technology required for a responsive quantum key distribution (QKD) service. The ROKS CubeSat will both demonstrate space based QKD and the use of advanced AI/ML onboard sensing and processing to make best use of limited resources within the platform. The payload uses modular building blocks for quantum and AI technology components that can be applied to other missions. The CubeSat will rely on the BB84 protocol to generate secure keys with target ground stations. This paper will highlight the key details of this mission including the concept of operations, design, and behaviour.

2. Introduction

Current cryptography methods, including RSA and AES, rely on algorithms to generate keys used in encryption. These algorithms are easy to create but exceptionally hard for conventional computers to crack. However, with the increased development of quantum computers and the immense processing power they can achieve, these algorithm-based methods of encryption are now at risk.

Quantum key distribution (QKD) relies on the properties of quantum mechanics to generate secure keys used in encryption. ROKS will be employing the BB84 protocol to generate quantum keys. In the BB84 protocol randomly polarized photons are generated onboard, single photons are then transmitted to the receiver. A quantum random number generator (QRNG) is used to randomly select the polarization used. The QRNG generates a superposition which, when measured, collapses into one of two states at random, this provides a truly random bit stream. The receiver will randomly select a polarization basis when detecting a photon. In ROKS case there are four polarizations that can be separated into two basis, vertical and horizontal (V/H) known as the plus basis, and diagonal and antidiagonal (D/A) known as the cross basis. When the receiver selects the same basis as the transmitter, the receiver will measure the correct polarization. If the receiver does not select the same basis as the transmitter, the receiver will get a random result. Once this transmission phase has been completed the results are subjected to a process known as reconciliation. This is used to refine the data into the usable quantum key and ensures that the key is protected from a potential eavesdropper. Keys produced in this way are truly random and therefore protected against quantum computer technology.

Currently QKD technology does exist in ground-based forms, however, it suffers from large losses in optical fibres and experiences line of sight issues (when transmitting through free space). This inhibits ground based QKD services from operating over large distances.

Space based QKD can provide keys to ground terminals throughout an orbit, enabling long range communication between terminals with quantum keys.

3. Mission Overview

The ROKS IOD mission will combine responsive operations with QKD to provide an automated, efficient, and secure QKD service. The 6U CubeSat will be able to identify the presence of clouds and other environmental factors that can inhibit the delivery and constraints of QKD services, and respond accordingly to ensure efficient use of the onboard and ground infrastructure resources.

ROKS will employ neural networks to identify cloud cover over target areas, visualised in Figure 1. The results, along with telemetry data, will be processed using geolocation algorithms to determine the identified cloud cover's location relative to target ground terminals. ROKS can then use this information to determine the best course of action and update the platform schedule through a process known as platform commanding. For example, if the conditions are acceptable the payload will inform the platform that it is to proceed, the platform will align with the target ground station and activate the quantum payload. If the conditions are not acceptable the payload can inform the platform to abandon the pass attempt and save onboard resources for a future QKD opportunity.

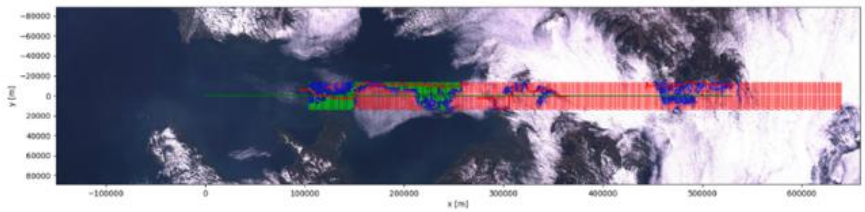

Figure 1 ROKS Cloud Detection

ROKS will rely on the BB84 protocol to generate quantum keys with target ground terminals. ROKS will be capable of generating randomly polarized photons and transmit them to the target optical ground station. The ground segment and ROKS will then communicate over RF to refine the key, as per the BB84 protocol requirements.

QKD operations are optimal in dark environments and therefore the CubeSat is preferred to be launched in late summer, to maximise the night duration over the initial period of the mission. A sun synchronous orbit, with a fixed altitude of 500km, that maximises the eclipse period has been baselined to ensure QKD availability. The selected orbit will allow for at least one pass per day of the UK during the night that exceeds 40 degrees elevation, when viewed from any stationary point on mainland UK.

4. CubeSat Design

The 6U CubeSat consist of a 2.5U platform and 3.5U payload. The platform will provide S-band communication, ADCS, and power systems required for the mission. The payload can be separated into three distinct subsystems. The quantum payload (QPL), forward looking imager (FLI), and payload computer (PLC).

The QPL is responsible for the QKD process, generating and refining quantum keys. The FLI will image target locations and identify cloud cover using neural networks. The PLC will be responsible for controlling payload operations, ensuring the security of the payload subsystems, and responsive operation activities including geolocation and platform commanding. Figure 2 shows an initial design of the payload configuration.

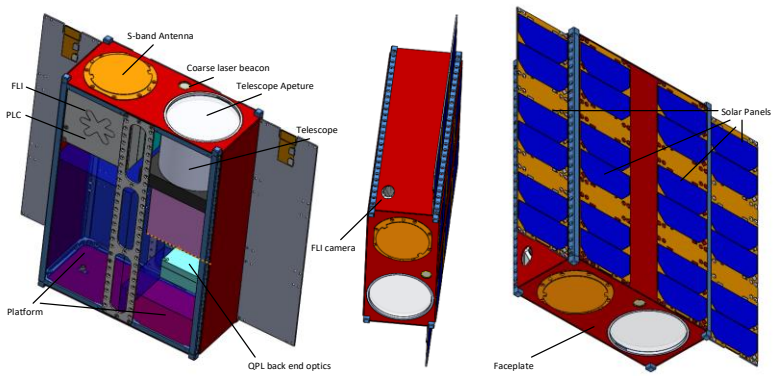

Figure 2 ROKS CubeSat Configuration

5. Concept of Operations

To prepare for a QKD pass, ROKS will image the target location with the FLI and determine cloud cover. The PLC will determine the location of the cloud by running the FLI's results through a geolocation algorithm. In a future service where multiple ground targets exist the PLC will determine the optimal target for QKD operations. The PLC will have the ability to perform platform commanding, updating the platforms schedule to point at the desired target. The process is shown in Figure 3.

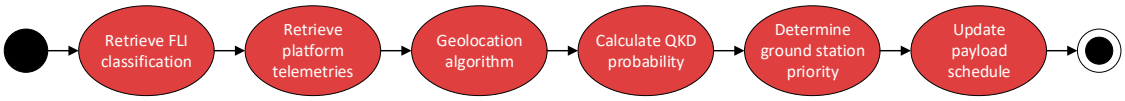

Figure 3 PLC Optimisation of Schedule

At the start of a pass, the platform will align the QPL with the optical ground station (OGS). To achieve the high pointing accuracy required for QKD activities, the QPL and OGS will utilise lasers and MEMS mirrors to ensure the internal optics are correctly aligned.

Once aligned, the QPL will transmit a weak coherent pulse of randomly polarized photons to the OGS. Once complete, the QPL will utilise the platforms S-band antenna to perform reconciliation with the OGS. This will generate a secure key shared between ROKS and the OGS.

Figure 4 provides a visualisation of the concept of key delivery with cloud detection.

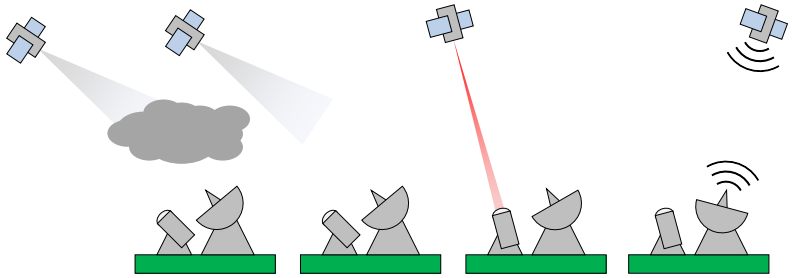

Figure 4 Concept of Cloud Detection and Key Delivery

This process is repeated for a secondary ground terminal to generate a new unique key. The QPL will then combine the two keys using an XOR function and deliver the result to either ground terminal. The terminal can then use the key it already has to solve the XOR and obtain the other terminals key. The terminal may then use this key to encrypt data and communicate securely with the other terminal.

6. Conclusion

The ROKS mission will provide an important demonstration of QKD technology, preparing for a time when classical encryption methods are no longer reliable for security. The ROKS mission provides a unique solution by combining the QKD service with responsive operation techniques. By utilising AI, the limited resources available to the CubeSat form will be used efficiently to achieve mission objectives. Platform commanding techniques will also reduce the requirement of operator intervention and therefore reduce operating costs of future services.