SSC21-IX-04

Payload Testing of a Weak Coherent Pulse Quantum Key Distribution Module for the Responsive Operations on Key Services (ROKS) Mission

Cassandra Mercury, Sonali Mohapatra, Craig Colquhoun, Steve Greenland, Mikulas Cebecauer, Philippos Karagiannakis, Ahren McTaggart
Craft Prospect Ltd
Suite 4A Fairfield, 1048 Govan Road, Glasgow, G51 4XS; +44(0)7562596023
cassandra@craftprospect.com

David Lowndes, Milan Stefko, John Rarity
Quantum Engineering Technology Labs, University of Bristol
H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB

ABSTRACT

Quantum Key Distribution (QKD) missions currently in development for space are expanding in number due to the increasing need for more secure means of encryption combined with the range limitations of terrestrial QKD. Most of these new missions are using smaller satellites to test their payloads. The ROKS (Responsive Operations for Key Services) mission is one such mission. It will utilize a 6U CubeSat bus and is set to launch in Q4 2022. A breadboard model of a 785 nm weak coherent pulse quantum source module designed for ROKS, named JADE, was tested within a lab testbench environment with the mission's systems represented by breadboard models with equivalent components. JADE's optical module was miniaturized to be compatible with the limited payload volumes of these small classes of satellites. Lab-based testbench characterization of JADE's ability to emit quantum pulses with four polarization states that propagate through the beamsteering system for analysis by a receiver box was demonstrated. Future work will focus on further shrinking the JADE module down to less than 1/3U size, increasing the interoperability of the module with standard interfaces for both CubeSats and SmallSats, and adding further capabilities and full environmental testing qualification to JADE.

BACKGROUND

Ensuring forward security for data, quantum key distribution (QKD) remains the only theoretically provable secure encryption method against future attacks[1,2]. It uses the principles of quantum mechanics to securely create a private key through the use of encoded photons. This private key is shared by two parties and can then be used with a one-time pad to send encrypted information.

BB84[2,3] and its iterations are the most common protocols for non-entanglement QKD[3]. Using a weak coherent pulse (WCP) transmitter (normally referred to as Alice), photons prepared in one of four polarization states (horizontal, vertical, diagonal, and anti-diagonal) are sent to a receiver (referred to in literature as Bob) where the decision to measure the photon is randomly selected to be either in the + (for horizontal and vertical) or × (for diagonal and anti-diagonal) polarization basis. This random selection means that half of the received photons will be measured in the incorrect basis choice on chance alone, leading to the recording of an incorrect bit by the receiver. A reconciliation process is then performed over classical communication channels wherein the recorded transmitted and received photons are transformed into a shared private key. Attempts to eavesdrop on the sent photons will leave a fingerprint in the form of increased quantum bit error rates (QBER)[3,4]. Once the QBER rises above a certain threshold, any key generated from it would be considered insecure and would not be used. In this case the exchange of photons and the following reconciliation process would need to start over again. This protects against any data being compromised since insecure keys will not finish the reconciliation process and thus no decryptable information will ever be shared.

To prevent any successful eavesdropping attacks, it is necessary to ensure that the average number of photons emitted is less than one per pulse. This will stop photon number splitting attacks where one photon of a multi-photon pulse is siphoned off by an eavesdropper (usually designated Eve) to gather information without the ability of the communicating parties to detect it in the QBER[4].

The transmission of those encoded photons can be done over three paths – fiber optic cable, terrestrial free space, or free space between space and ground. Transmission over any medium will introduce losses due to attenuation

of the signal. After sufficient distances (depending on the medium) this will lead to QBERs that rise above the security threshold. Fiber optic networks for QKD remain limited in range due to degradation of the signal through the fiber leading to high QBERs and unsustainably low key generation rates after 50–100 km[5,6]. Terrestrial distribution through free space networks is similarly limited to a range of a couple of hundred kilometers due to atmospheric attenuation[7].

QKD in Space

To obtain a fully connected and scalable global network, space-based QKD where satellite relays can act as trusted nodes will be an essential component[8]. This should allow keys between any two places to be exchanged without regard to the distances between them. While there are atmospheric attenuation effects that lead to channel losses, these are less than those of terrestrial free space channels due to the significantly reduced atmosphere at the satellite side[9]. For space to ground QKD, the distance travelled by the photons through atmosphere is far less than in terrestrial free space, and for much of that distance the atmosphere is less dense, leading to lower attenuation.

The only full quantum key distribution demonstration mission to date is the Micius satellite[10], a satellite built by the Chinese Academy of Sciences and the University of Science and Technology of China and launched in 2016. The approximately 600 kg satellite hosted an encrypted video conference between Vienna, Austria and Beijing, China secured by quantum keys.

Several QKD missions are in development around the world currently[11], many of them using considerably smaller satellites. QEYSSat[12] from Canada will be under 100 kg and the joint effort mission between the UK and Singapore will be a 12U CubeSat[13]. A U is a standard unit of measurement for a CubeSat representing a 10 cm x 10 cm x 10 cm cube. Multiple cube spaces may be combined such that some multiple of the volume of a standard U is used for the CubeSat. A 12U CubeSat therefore represents twelve 10 cm x 10 cm x 10 cm cube equivalents of volume, with 4 columns stacked 3U high and arranged in a square with a maximum payload mass of 20 kg.

The Responsive Operation on Key Services (ROKS) satellite, led by Craft Prospect Ltd (CPL) and partnered with the University of Bristol (UoB) and the University of Strathclyde (UoS), will be a 6U CubeSat. This mission is scheduled for launch late 2022 and is intended to demonstrate night-time QKD as well as cloud detection capabilities to intelligently select ground stations free from cloud cover for efficient key delivery. Operating in a sun-synchronous orbit at an altitude of 500 km, the ROKS orbit is optimized for maximum eclipse period to allow for the greatest number of opportunities to perform QKD.

CubeSats offer a unique opportunity to demonstrate hardware with faster turnaround and much lower capital outlay. Being so small, they can be built and deployed quickly, allowing a network of CubeSats to augment the space QKD network and allow for a rapid response to demand. With the standardization of size, parts, and deployers for CubeSats, a CubeSat-ready WCP module can allow for greater availability of QKD services in space at reduced overall mission cost and risk, in addition to allowing greater ease of lab-based hardware demonstrations.

WCP QKD MODULE

A breadboard model of the WCP transmitter was created to demonstrate the functionality of the transmitter in a lab-based end-to-end QKD demonstration. The Joint Alignment, Diode, and Emitter (JADE) module consists of an optical module to combine the 785 nm polarization states of the four quantum sources into one fiber-coupled pathway, a monitoring system to calibrate the intensities of the emitted states, an alignment laser for use in aligning the quantum signals through the optical pathways of the ROKS satellite, and an electronic board that controls all the systems in JADE. The breadboard model is shown in Figure 1.

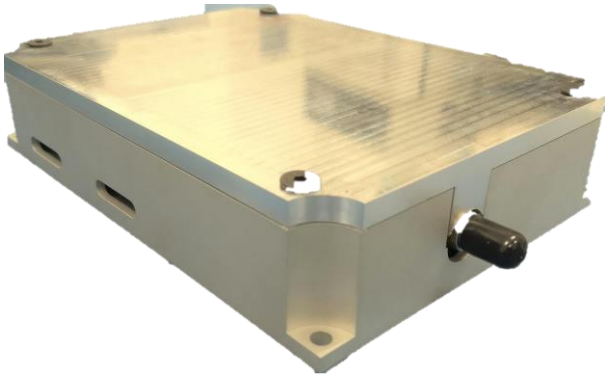

Figure 1: JADE Breadboard Model

A nominal pulse frequency of 100 MHz was selected with a pulse width of 2.5 ns. Depending on the dead time of the instruments used to measure the signal, some high frequency pulses may not be detected. Hence, the module has the built-in capability to run at reduced frequencies which was used during testing.

The primary consideration for the module was lowering the overall SWAP (size, weight, and power) of the transmitter, while increasing its robustness. The optical

module – named the GNEISS for Generating New and Extended Independent Signal States – was designed in an iterative process between CPL and UoB. Initial models were tested in space qualifying vibration and thermal environments with results showing no change in nominal performance either during (for thermal) or after being in those environments (for thermal and vibration). However, these optical modules were only tested for emissions of photons and were tested neither with the JADE electronics nor as part of a testbench with the full QKD payload combined with receiver optics that had the capability to analyze those pulses. The vibration test setup of the initial design can be seen in Figure 2 where the optics module is centered on the vibration test platform at the Higgs Centre for Innovation in Edinburgh, Scotland.

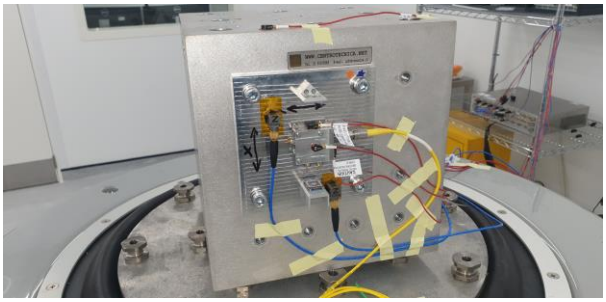

Figure 2: First Generation Optics Module Under Vibration Testing

The current model tested in-house at CPL and described in this paper uses four laser diodes and several optical elements to create the four needed polarization states for WCP QKD. The module also includes the alignment laser and a photodiode to monitor the optical output power of each laser. There is only one optical output to serve all the laser diodes, aiding indistinguishability of polarization states since all laser beams share a single spatial mode. This model, however, did not incorporate full indistinguishability into its design in order to better understand the effects operation and the thermal environment would have on the wavelengths of individual diodes. This breadboard model uses a standard FC/PC optical fiber interface, as seen in Figure 3.

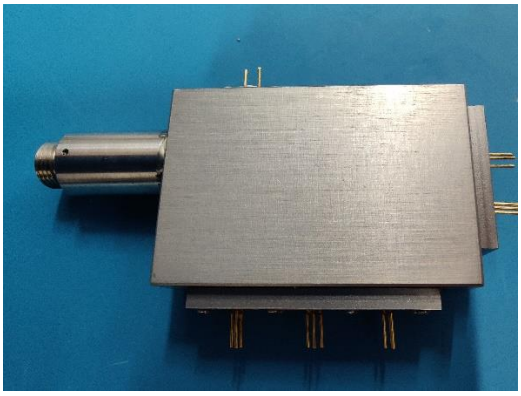

Figure 3: The GNEISS Module

A power monitoring capability is included to provide feedback to the laser drivers, ensuring that the average number of photons emitted per pulse is both consistent and at the output needed.

The electronics subsystem consists of a custom daughterboard with an FPGA-based motherboard. Two electrical outputs are used – one to produce the LVDS signals for quantum signal selection and an RS422 interface for telemetry and general commanding.

Size wise, the aim was to create an optics module suitable for incorporation into a 1/3U-sized JADE flight model (FM). This is the volume allocated for the module in the ROKS configuration as indicated in Figure 4. Electronic development was aimed at selecting commercial off-the-shelf (COTS) components with low power consumption and robust safety margins. Size optimization for the electronic boards in order to fit the CubeSat footprint was not a concern for the breadboard development and was not attempted in this iteration. The breadboard model itself has a footprint of approximately 185 mm x 136 mm.

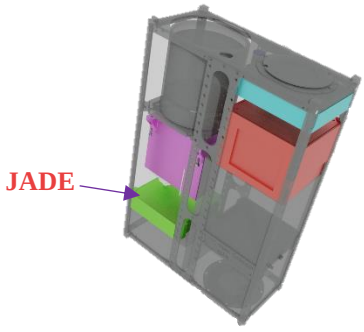

Figure 4: ROKS CubeSat Configuration

TESTING AIMS

The GNEISS was tested throughout the assembly process and characterized for standard measures of performance after full assembly in an ambient environment. The aim of the initial testing was to ensure the highest quality coupling of the quantum sources and to confirm optimal orientation of the polarization states.

The JADE module was tested as an isolated module and as part of a testbench for the ROKS mission.

As an isolated module, the purpose of the testing was to confirm the ability to command on four polarized quantum states separated by 45 degrees, the ability to equalize the output power levels of all diodes, and to obtain 2.5 ns wide pulses at 100 MHz.

The tests performed on the ROKS QKD payload were designed to verify that it can be used to transmit quantum signals through the optical beam steering system to an optical ground station (OGS) reliably and produce the required signals and data to create quantum keys.

TEST SETUP

The ROKS testbench is a breadboard model of the ROKS satellite QKD payload and the receiver optics module which will be ground based. Here, Alice was represented by the JADE module fiber-coupled to the representative ROKS optical beam steering components and Bob was represented by a receiver designed to emulate the signal state detection feature of an OGS. The payload computer was included and drove the JADE module. The full setup was staged inside an optical enclosure to lower background counts, as seen in Figure 6.

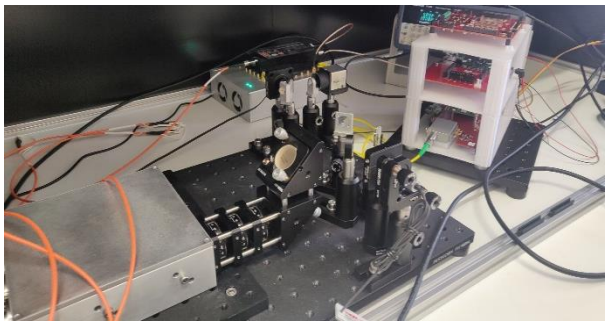

Figure 6: ROKS Breadboard Testbench Setup

Bob the BOULDER, the name given to the receiver box, is of custom design, containing COTS optics for alignment and polarization state separation. There are six fiber output ports - one for each linear polarization state, and one for each handedness of circular polarization for calibration purposes - to which detectors can be coupled. The detector used to detect photons is an Excelitas SPCM-AQRH-12-FC single photon counting module

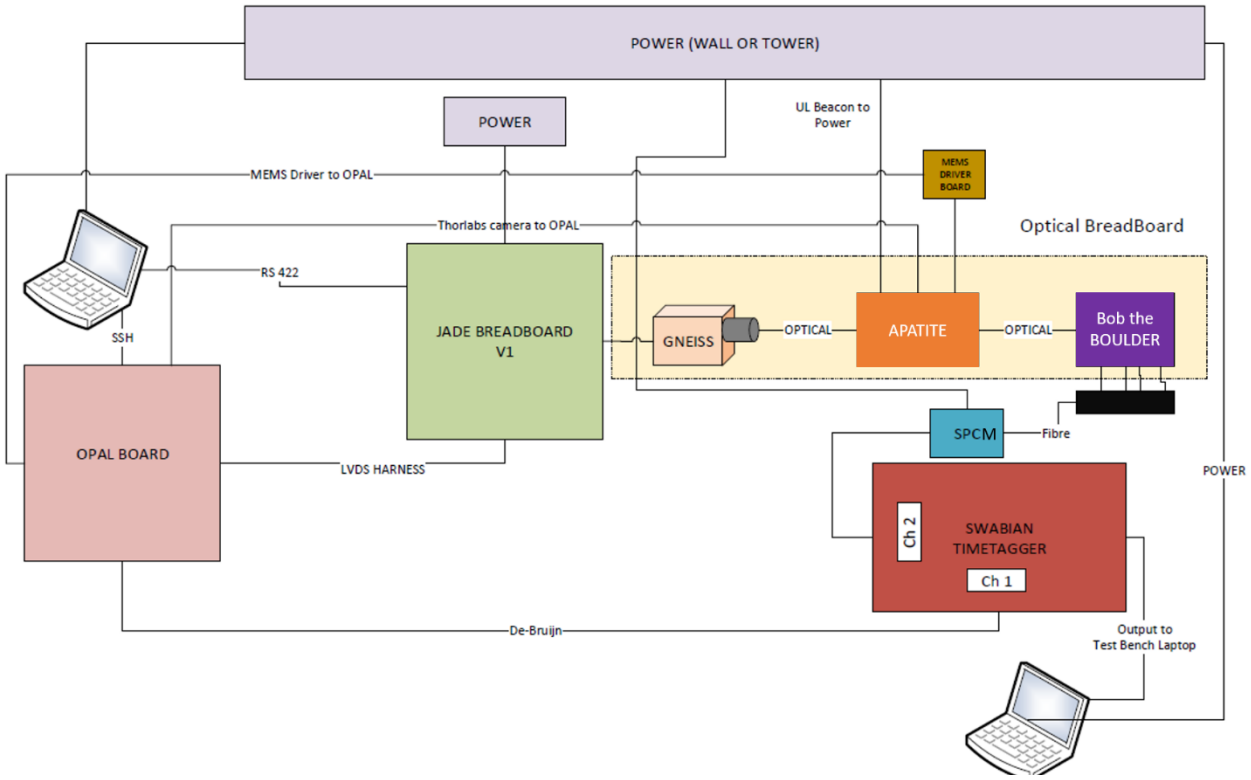

Figure 5: ROKS Testbench Setup Block Diagram

(SPCM) connected to a Swabian TimeTagger Ultra for timing the arrival of pulses. A block diagram of the apparatus can be seen in Figure 5.

The optical beam steering module called the APATITE (Acquisition, Pointing, And Tracking In Tiny Environments) was tested on an optical bench using components that will be used inside the ROKS payload. An FPGA is used to control a MEMS mirror to overlap an alignment laser beam generated by the GNEISS with a laser beam representing an OGS uplink beacon. A CMOS camera is used for feedback to the FPGA which adjusts the MEMS mirror until both beams are incident at the same position on the camera sensor.

During an OGS pass in LEO, the overlap between the uplink beacon and the alignment laser beam would indicate that any QKD light pulses generated by JADE would be aligned with detectors present in the OGS. The MEMS steering and camera feedback features are controlled by a Xilinx Zynq based FPGA development board. Meanwhile, the JADE board (also powered by a Zynq FPGA) is used to generate 2.5 ns QKD pulses from the GNEISS module at 100 MHz. For the purpose of the testbench, each of the four possible signal states of the GNEISS is pulsed consecutively in a repeated test pattern. These pulses are guided into Bob the BOULDER, which contains a series of optics designed to split the polarization states for detection via its numerous output fiber ports. Fibers are connected to these outputs, at the other end of which are SPCMs to detect the pulses. These SPCMs are connected to a single time tagger which generates histograms of the photon transit duration from the time photon count events occur after each pulse has been generated. This setup is shown below in Figure 7.

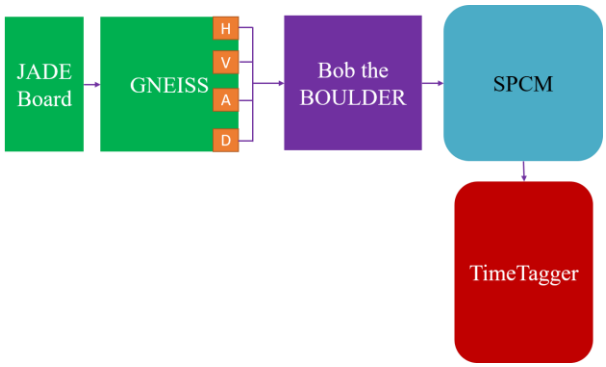

Figure 7: JADE Functional Testing Setup

TEST RESULTS

The GNEISS optical module's assembly was guided by the dual requirements to maximize the outputs while maintaining a relatively even output between the four diodes, with the result shown in Figure 8 for the coupling with the same source driver parameters. The smaller differences in coupling were then controlled by changing the parameters in each source's laser driver.

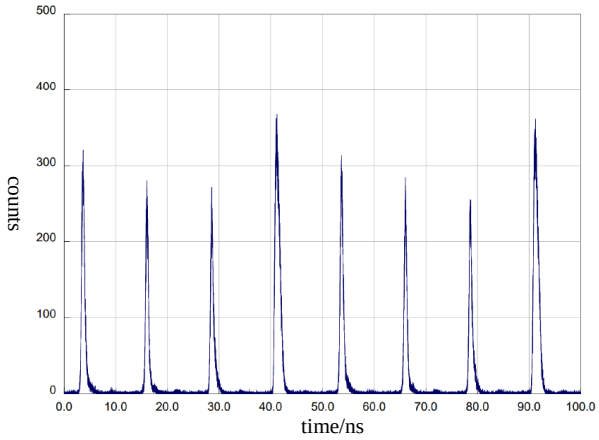

Figure 8: Optical Output of GNEISS

The polarization orientations of the four quantum source diodes were measured by adjusting the rotation of a half wave plate through which all the polarization states propagated, monitoring the transmission through the output ports in Bob the BOULDER. The results for this measurement are shown in Figure 9 as a plot of normalized transmission vs the rotation angle of the half wave plate. The vertical dashed lines are each separated by 22.5 degree half wave plate rotation, corresponding to separations of 45 degrees for each polarization state.

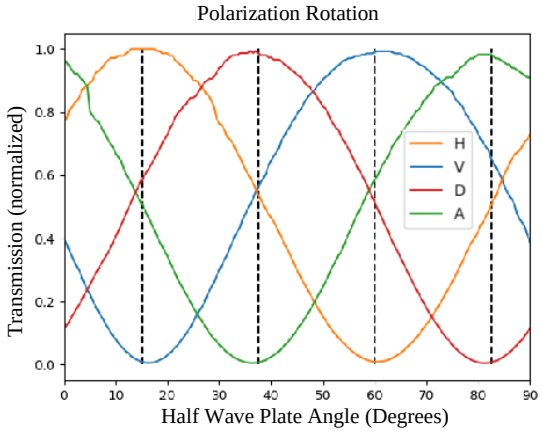

Figure 9: Polarization Analysis

The polarization rotation data from Figure 9 is used to generate an extinction matrix for the four quantum sources of the GNEISS module shown in Figure 10. To obtain this matrix the best extinction ratio for the transmission of orthogonal polarization states between 0

and 22.5 degree half wave plate rotation is obtained, giving the rotation where either the H/V or D/A polarization basis is measured most accurately. In the case shown in Figure 9, the best extinction ratio is measured in the H/V basis, indicated by the leftmost dashed line. From that rotation, the transmission values are extracted for 22.5 degree increments of further half wave plate rotation. The extinction values for horizontal, vertical, diagonal, and anti-diagonal polarizations are 1.03%, 0.54%, 1.15%, 0.45% respectively, resulting in an average of 0.79%.

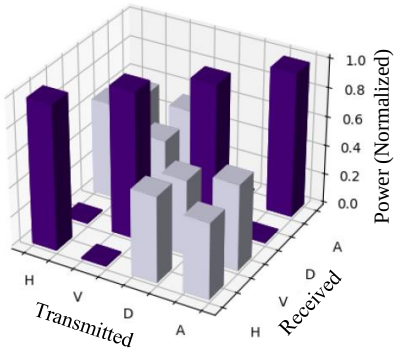

Figure 10: Extinction Matrix

After the optical module was fully assembled and characterized, GNEISS was soldered onto the JADE electronics module for pulsed control of the laser sources. Confirmation of the JADE signaling via the LVDS lines showed the driver's ability to output the desired 2.5 ns pulse widths at 100 MHz, seen in Figure 11.

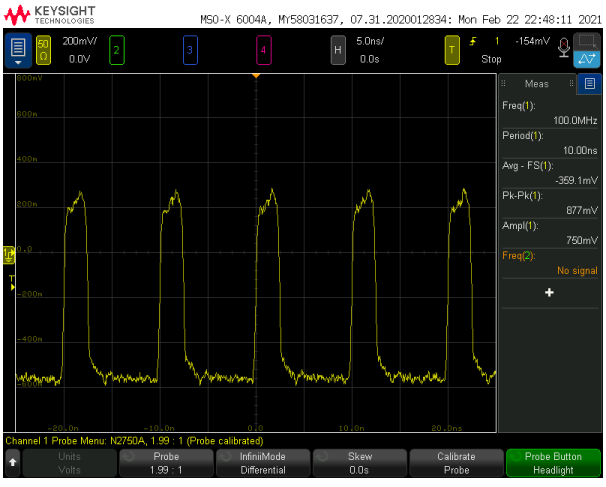

Figure 11: Electrical Pulses to Command 2.5 ns Pulse Widths at 100 MHz

A free space biased detector was used to confirm the optical pulsing (see Figure 12). The signals were detected at the frequency commanded, confirming the ability to emit pulses at the desired inputs. Testing then was able to proceed to the testbench.

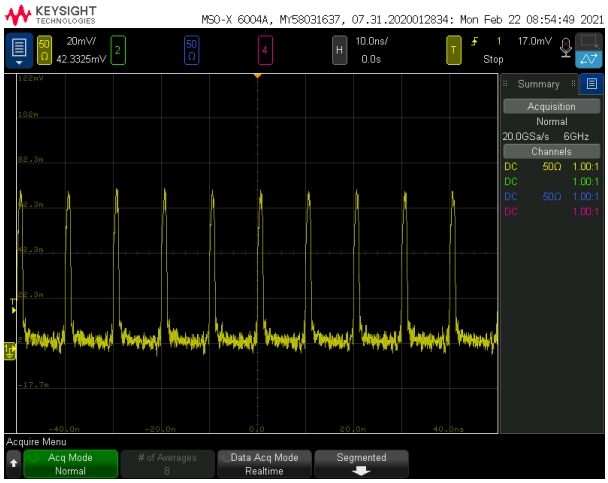

Figure 12: Optical Output Signals at 100 MHz

Once attached to the JADE electronics, the GNEISS optical module was tested as shown in Figure 7. The diodes were pulsed in sequence at 100 MHz, in a repeated pattern of horizontal → vertical → diagonal → anti-diagonal, with 10 ns between the rising edge of each new pulse. Due to the dead time of the SPCM used, if the same diode were to be pulsed at a rate greater than 45 MHz, consecutive pulses would not be detected. The periodic repeating pattern described above was selected for testing, as it results in an effective pulse frequency of 25 MHz for each individual diode, avoiding undetected pulses due to detector dead time.

The BOULDER received transmissions from the JADE module as sent. With transmit and receive of photons confirmed, testing proceeded with the full testbench as seen in Figure 5. The payload computer commanded JADE, and the BOULDER received the photons successfully. Reconciliation with a BB84 protocol without any decoy state was implemented. This involved the sharing of data over the "classical communication channel" which was simulated over USB for testbench purposes. A key was generated from the process, though Alice and Bob had perfect knowledge of what was sent with neither WCP nor channel losses due to atmospheric attenuation modeled in.

CONCLUSION

The JADE breadboard model demonstrates that a CubeSat suitable WCP transmitter is feasible and can reliably generate the needed quantum signal states. Four

polarization states generated at 45 degree increments were achieved and the coupling efficiency was sufficient even using COTS components and with a rapid build process of the optics module. The extinction ratios were higher than what would be desired in a final model and requires attention in the next iterations to lower them.

The receiver optics box was demonstrated to be sufficient in testing out a WCP transmitter payload. The delicate nature of the alignment of the box necessitates more durable builds in future iterations for use in field trials. Attention was given mainly to ensure that the payload was robust such that the receiver optics remained the only weak link requiring care while moving the test setup around the lab. However, the breadboard approach allowed for overall rapid prototyping and testing. This work demonstrates the viability of the approach and is an important step forward in building standardized, modular quantum sources for space.

Future Work

While the GNEISS allows for greater control of the quantum source signals and much lower polarization extinctions than previous iterations, more work is needed to lower the average to below 0.5% which the next iteration is on course to achieve.

Concurrently with the testing of the breadboard model, work has continued on upgrades to be used in the next version. Firstly, new laser drivers have been selected and tested, and are being incorporated into the follow-on version. These new laser drivers will allow for better control of the current output for greater precision of the photon number emitted as well as to enable decoy state capabilities. Decoy states are essential to performing secure BB84 QKD[4]. The new drivers also allow the pulse width to be reduced to 1 ns. Their lower power requirements in comparison to the current laser drivers also make them more suitable for the low SWAP parameters of the ROKS mission.

The next generation of the board will also include a quantum random number generator[15,16] on the electronics board, with the intention of configuring JADE to be a full quantum source solution. These combined changes will allow for full implementation of the BB84 protocol within JADE.

The current breadboard model's electronics were not optimized for size. Future work will focus on optimization so that the final size of the full module is equivalent to 1/3U, with a footprint of 10 cm x 10 cm. This will allow for JADE to be incorporated into standard CubeSat buses as well as onto small satellites.

It is worth mentioning that one key environmental test not completed as part of this work is vacuum testing. While care was applied to the selection of materials to have low outgassing and be compatible with a vacuum environment, performance measurements of the JADE under thermal vacuum conditions is required for the next iteration. Results from the thermal and vibration testing on the latest updates to JADE are ongoing at the time of writing this paper. Testing is continuously performed with each iteration to ensure changes do not affect performance or survivability at the extreme environmental bounds.

ACKNOWLEDGEMENTS

The authors of this paper would like to thank Fraunhofer CAP for their generosity in allowing for the use of some of their equipment during initial checkout testing of the breadboard PCBs.

We also would like to thank Dr. Daniel Oi and his team at the Computational Nonlinear and Quantum Optics group at the University of Strathclyde for their invaluable inputs to the design theory of the JADE module.

Special thanks to the UKSA for their backing and financial support of the ROKS project development that enabled design of the mission to get to testbench level.

REFERENCES

1. Lo HK, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. Science. 283, 2050 (1999)
2. D. Deutsch, et al., "Quantum privacy amplification and the security of quantum cryptography over noisy channels" Phys. Rev. Lett.77, 2818(1996)
3. Bennett, C. H. Quantum cryptography: public key distribution and coin tossing. Int. Conf. Comput. Syst. Signal Process. IEEE 1984, 175–179 (1984).
4. H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution" Phys. Rev. Lett. 94, 230504 (2005).
5. Tamura, Y. et al. Lowest-ever 0.1419-db/km loss optical fiber. Optical Fiber Communication Conference Postdeadline Papers, Th5D.1 (Optical Society of America, 2017)
6. Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys. Rev. Lett.117, 190501 (2016).
7. Schmitt-Manderbach, T. et al. Experimental demonstration of free-space decoy-state

quantum key distribution over 144 km. Phys. Rev. Lett. 98, 010504 (2007).
8. J. Sidhu, et al. “Advances in Space Quantum Communications.” (2021).
9. J G Rarity et al “Ground to satellite secure key exchange using quantum cryptography” 2002 New J. Phys.4 82
10. Juan Yin, et al. Satellite-to-Ground Entanglement-Based Quantum Key Distribution, Phys. Rev. Lett. 119, 200501 (2017).
11. O. Lee, T. Vergoossen, “An updated analysis of satellite quantum-key distribution missions” (2019)
12. A. Scott, T. Jennewein, J. Cain, I. D'Souza, B. Higgins, D. Hudson, H. Podmore, W. Soh, "The QEYSSAT mission: on-orbit demonstration of secure optical communications network technologies," Proc. SPIE 11532, Environmental Effects on Light Propagation and Adaptive Systems III, 115320H (20 September 2020)
13. C. Dalibot, S. Tustain, “The Preliminary Thermal Design for the SPEQTRE CubeSat”, 2020 International Conference on Environmental Systems (2020)
14. UK National Quantum Technologies Programme. Space-based quantum security. 2019. Available online: http://uknqt.epsrc.ac.uk/files/spacebasedquantumsecurity/ (accessed on 20th May 2021)
15. Ma, X., Yuan, X., Cao, Z. et al. Quantum random number generation. npj Quantum Inf 2, 16021 (2016).
16. R. Bedington, J. Arrazola, A. Ling, “Progress in satellite quantum key distribution” npj Quantum Information (2017) 3:3