Quantum Science and Technology

RECEIVED
15 December 2016

REVISED
13 April 2017

ACCEPTED FOR PUBLICATION
28 April 2017

PUBLISHED
6 June 2017

PAPER

Airborne demonstration of a quantum key distribution receiver payload

Christopher J Pugh[1,2], **Sarah Kaiser**[1,2,4], **Jean-Philippe Bourgoin**[1,2], **Jeongwan Jin**[1,2], **Nigar Sultana**[1,3], **Sascha Agne**[1,2], **Elena Anisimova**[1,2], **Vadim Makarov**[1,2,3], **Eric Choi**[1,5], **Brendon L Higgins**[1,2] and **Thomas Jennewein**[1,2,6]

[1] Institute for Quantum Computing, University of Waterloo, 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada
[2] Department of Physics and Astronomy, University of Waterloo, 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada
[3] Department of Electrical and Computer Engineering, University of Waterloo, 200 University Avenue West, Waterloo, Ontario N2L 3G1, Canada
[4] Present Address: Department of Physics and Astronomy, Macquarie University, Balaclava Road, North Ryde, NSW, 2109, Australia.
[5] Present Address: Magellan Aerospace, 3701 Carling Avenue, Ottawa, Ontario K2H 8S2, Canada.
[6] Author to whom any correspondence should be addressed.

E-mail: thomas.jennewein@uwaterloo.ca

Keywords: quantum key distribution, quantum communication, quantum cryptography, quantum optics, photon detection, quantum satellite payload

Abstract

Satellite-based quantum terminals are a feasible way to extend the reach of quantum communication protocols such as quantum key distribution (QKD) to the global scale. To that end, prior demonstrations have shown QKD transmissions from airborne platforms to receivers on ground, but none have shown QKD transmissions from ground to a moving aircraft, the latter scenario having simplicity and flexibility advantages for a hypothetical satellite. Here, we demonstrate QKD from a ground transmitter to a receiver prototype mounted on an airplane in flight. We have specifically designed our receiver prototype to consist of many components that are compatible with the environment and resource constraints of a satellite. Coupled with our relocatable ground station system, optical links with distances of 3–10 km were maintained and quantum signals transmitted while traversing angular rates similar to those observed of low-Earth-orbit satellites. For some passes of the aircraft over the ground station, links were established within 10 s of position data transmission, and with link times of a few minutes and received quantum bit error rates typically ≈3%–5% , we generated secure keys up to 868 kb in length. By successfully generating secure keys over several different pass configurations, we demonstrate the viability of technology that constitutes a quantum receiver satellite payload and provide a blueprint for future satellite missions to build upon.

1. Introduction

Quantum key distribution (QKD) [1, 2] establishes cryptographic keys between two distant parties in a way that is cryptanalytically unbreakable. Ground-based implementations of QKD using optical fibre links are limited to distances of a few hundred kilometres due to absorption losses, which scale exponentially with distance, leading to insufficient signal-to-noise [3–5]. Alternatively, free-space links have been demonstrated over ground with varying distances, both in stationary [6–10] and moving [11–13] configurations. But despite losses due to geometric effects scaling quadratically with distance, the addition of atmospheric absorption and turbulence, and the necessity of having clear line of sight, limit terrestrial free-space transmissions to also a few hundred kilometres.

Much greater distances could be spanned in free-space transmissions outside Earth's atmosphere. Utilising orbiting satellites, therefore, has potential to allow the establishment of global QKD networks, with 'quantum' satellites acting as intermediaries. Such satellites could operate as untrusted nodes linking two ground stations

simultaneously [14, 15], or trusted nodes connecting any two ground stations on Earth at different times [16–22]. The majority of such analyses propose a quantum downlink, where photons are generated at the satellite and transmitted to receivers on the ground. Since 2010, the Canadian Space Agency (CSA) has studied the proposed Quantum Encryption and Science Satellite (QEYSSat) [23] where a mission concept was developed in partnership with COM DEV (now Honeywell Aerospace). This concept, in contrast to many other missions, proposes a quantum uplink, placing the receiver on the satellite while keeping the quantum source at the ground station.

Under similar conditions, the uplink configuration has a lower key generation rate than the downlink, owing to atmospheric turbulence affecting the beam path earlier in the propagation. Nevertheless, comprehensive theoretical comparative study of QKD under uplink and downlink conditions—which included the effects of atmospheric turbulence, absorption, beam propagation, optical component losses, detector characteristics, noise contributions, and representative pointing and collection capabilities at a hypothetical satellite—concluded that an uplink approach is viable, with the reduction in generated key bits (compared with downlink) being less than one order of magnitude [24]. Importantly, an uplink also possesses a number of advantages over a downlink, including relative simplicity of the satellite design, not requiring high-rate true random number generators, relaxed requirements on data processing and storage (only the photon reception events need be considered, which are many orders of magnitude fewer than the source events), and the flexibility of being able to incorporate and explore various different quantum source types with the same receiver apparatus (which would have major associated costs were the source located on the satellite, as for downlink). Recently, China launched a quantum science satellite that aims to perform many quantum experiments with optical links between space and ground [25, 26]. However its exact capabilities are unverified as no details or results have been published at this time.

Demonstrations of QKD with moving and airborne platforms take important steps to verifying the readiness of quantum technology, and the supporting classical technology, for deployment within a satellite payload. To date, however, reported demonstrations of QKD with aircraft have operated exclusively in the downlink configuration [11, 12], where the quantum states are generated and transmitted from the aircraft to a receiver at a stationary ground location. Here, we demonstrate QKD uplink to a receiver on a moving aircraft. Our apparatuses incorporate coarse- and fine-pointing systems necessary to establish and maintain optical link, quantum source and measurement components that conduct polarisation-encoded QKD, and suitable post-processing algorithms to extract secure key. The results show good performance at the same angular rates exhibited by low-Earth-orbit (LEO) satellites.

Our QKD receiver makes extensive use of components custom-designed according to the mass, volume, power, thermal and vacuum operating environment requirements of systems to be embedded in a satellite payload: many components are already space suitable, and others have a clear path to flight. In a recent study conducted with the University of Toronto Institute for Aerospace Studies Space Flight Laboratory (UTIAS SFL), a realistic satellite concept was developed, incorporating the space-ready receiver apparatus demonstrated here and integrated into the flight-proven NEMO-150 [27] micro-satellite bus (see below). This, together with our airborne operational demonstration, illustrates the technological advancements made towards the development of a space-suitable QKD receiver, and highlights the feasibility and technological readiness of an uplink QKD satellite.

2. Apparatuses and methods

2.1. Concept

The apparatuses for our demonstration consist of a QKD source and transmitter, located at a ground station near the airstrip of Smiths Falls–Montague Airport, and a QKD receiver, located on a Twin Otter research aircraft from the National Research Council of Canada. Optical links were only attempted at night so as to limit optical noise. One systems-test daytime flight was conducted (where the optical links were not attempted), followed by nighttime flights.

Two nighttime flights were conducted, each of two-hour duration and consisting of several passes of varying trajectories. Optical links were established using tracking feedback to two-axis motors, guided by strong beacon lasers (at a wavelength different from the quantum signal) and an imaging camera, at each of the two sites. The QKD signals produced by the source were guided through a telescope on the ground and pointed to the receiver on the aircraft. There, the QKD signal polarisations and times of arrival were recorded for later correlation and processing to complete the QKD protocol and extract the key.

We focused on two path types: arcs with (approximately) constant radius around the ground station and straight lines past the ground station. For straight line paths, the distance we quote is the minimum. Over the two nights, we performed 14 passes with nominal distances of 3 km, 5 km, 7 km and 10 km, in both line and arc configurations at an altitude of ≈1.6 km above sea level; see, for example, figure 1 for the flight path of an arc at

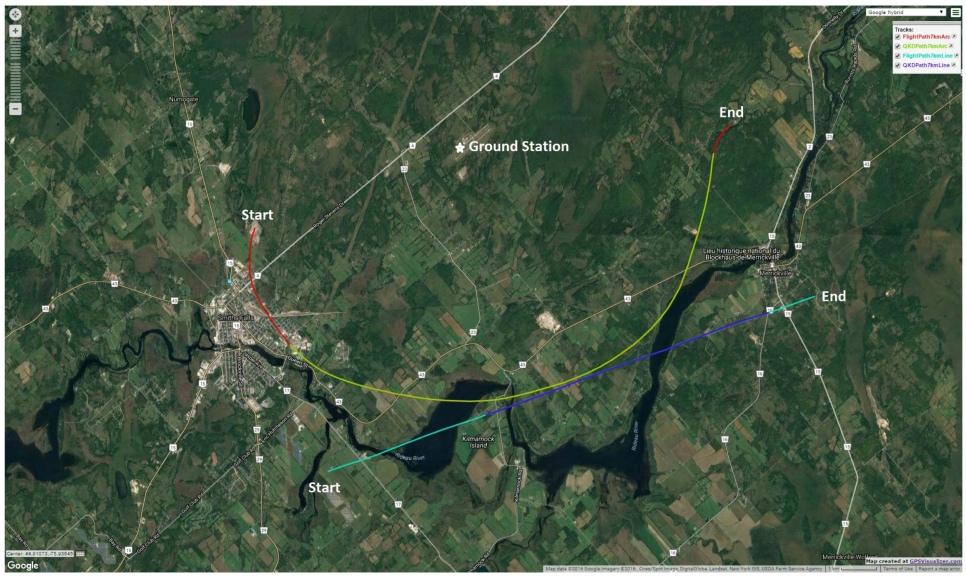

Figure 1. Flight paths for the 7 km arc and line, followed from left to right. The star indicates the location of the ground station at Smith Falls–Montague Airport. The inner portions represent where the quantum link was active. Photo produced using GPSVisualizer.com, map data © 2016 Google, imagery © 2016 Cnes/Spot Image, DigitalGlobe, Landsat, New York GIS, USDA Farm Service Agency.

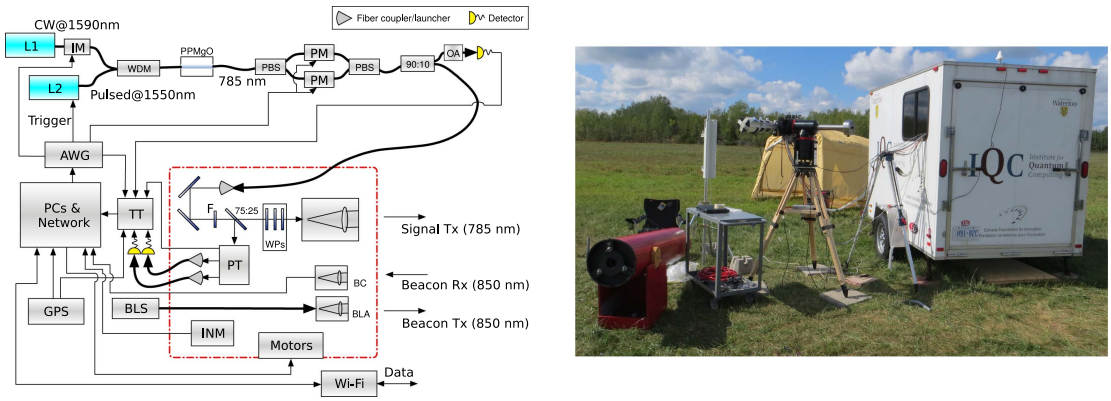

Figure 2. Left, schematic diagram of the quantum source and transmitter apparatus. Acronyms are as follows: arbitrary waveform generator (AWG), wavelength division multiplexer (WDM), polarising beam splitter (PBS), optical attenuator (OA), band-pass filter (F), polarisation tomography (PT) and time tagger (TT). Other acronyms and details given in the text. The red border indicates components that are mounted on the motors. Right pane: ground station located at Smiths Falls–Montague airport, showing (right to left) the trailer where the source is located, motor mount with transmitter telescope attached, Wi-Fi antenna and calibration telescope.

7 km radius. For this flight mission concept, a sequence of GPS coordinates was calculated for each flight, with the start angle relative to the ground station and the distance were used as input. These coordinates were transferred to the flight software of the aircraft by the pilots. We developed a decision tree such that, based on the observed performance of each pass, we could immediately select an appropriate course of action (e.g. to perform troubleshooting or collect data under different conditions). That a mission concept such as this is viable shows that a similar mission concept, appropriate for an orbiting satellite receiver, can realistically be achieved.

2.2. Source and transmitter

Our QKD source is a significantly improved version of a previous-generation apparatus [28], implementing BB84 with decoy states [29] at 400 MHz. Weak coherent pulses at 785 nm wavelength are generated by combining a narrowband 1590 nm continuous-wave (CW) laser (L1) with 1550 nm triggered-pulsing laser (L2) through sum frequency generation in a periodically poled magnesium oxide (PPMgO) waveguide (see figure 2). For each pulse, one of three intensity levels is chosen: signal, decoy or vacuum, with probabilities of 80%, 14% and 6%, respectively. Signal and decoy levels are generated using a fast electro-optical intensity modulator (IM)

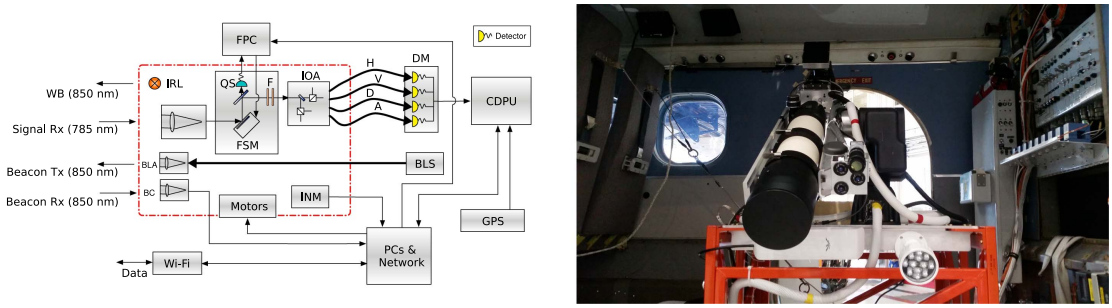

Figure 3. Left: schematic diagram of the receiver apparatus. Acronyms are as follows: band-pass filters (F) and wide-field beacon (WB; produced by the IRL). Other acronyms and details given in the text. The red border indicates components that are mounted on the motors. Right, receiver apparatus facing out the port-side door of the NRC Twin Otter research aircraft, showing (clockwise) the telescope, beacon assembly, motor mount, IRL, Wi-Fi antenna and FPC (behind). Other components not visible (primarily electronics) are mounted in front of the seats seen at the left of the picture.

calibrated to emit $\mu \approx 0.5$ and $\nu \approx 0.1$ mean photon number at the entrance of the transmitter telescope, respectively. The vacuum state is made by suppressing the laser trigger.

Each of the four BB84 polarisations—horizontal (H), vertical (V), diagonal (D) and anti-diagonal (A)—are imposed using two electro-optical phase modulators (PMs), each in one arm of a balanced Mach-Zehnder polarisation interferometer. With a balanced input (D), the PMs can address any point on the circle through D, right-circular (R), A and left-circular (L). A subsequent unitary rotation takes these to D, H, A and V, respectively. The intensity and polarisation states are generated according to a randomised sequence that repeats every 1000 pulses. Although this is insecure, it is sufficient for our demonstration, while upgrading to a fully random sequence (e.g., given by a quantum random number generator) is straightforward and a suitable system has been identified.

Pulse intensities are measured locally through the weak output of an optical fibre splitter (90:10) connected to a silicon avalanche photodiode (Si-APD) operating in Geiger mode with active quenching. The bulk of the pulse power is guided from the source to the transmitter through single-mode optical fibre. The beam passes through a 785 nm band-pass (3 nm bandwidth) filter (to impede Trojan-horse attacks [30]) and then a 75:25 beam splitter. We employ a polarisation correction system to undo the unknown unitary rotation applied by the single-mode fibre—the reflected 25% of pulses undergo characterisation, while the remaining 75% of pulses pass through a triplet of wave plates (WPs) in motorised rotation stages that apply a compensation operation to the states, and are finally transmitted through a 12 cm diameter Sky-Watcher BK 1206AZ3 refractive telescope.

The polarisation characterisation subsystem consists of two beam paths, where each path passes through a port of a rotating chopper wheel that contains linear polarisers. The linear polarisers are each calibrated to project onto the H, V, D or A state; however, one of the two beam paths contains a quarter-wave plate just prior to the chopper wheel, thereby facilitating projections onto a tomographically complete set of three polarisation bases: H/V, D/A and R/L. The actual state any given photon is projected to depends on which blade of the wheel is open at the time the photon passes through (the rotation of the wheel is also recorded).

The two beams are each coupled into fibre and directed to Si-APDs. With near real-time analysis of source and detection data (performed on per-second integrated counts), we obtain tomographic reconstructions, for each of the generated polarisation states, of the states at the transmitter after the rotation applied by the fibre. We then optimise the compensating wave plate triplet (a sequence of quarter-, half-, and quarter-wave plate) to maximise the fidelity of the states expected after compensation with the nominally generated states. The optimal positions are given to the motorised stages, applying the (rotated) wave plates to pulses that are then transmitted through the telescope towards the receiver.

During our airborne trials, the QKD source optics and electronics, as well as computers for data recording and pointing feedback, were located inside of a trailer to maintain thermal and humidity stability. The transmitter pointing stages, polarisation characterisation optics, and telescope were located just outside the trailer, with cabling running through a small window. Equipped with an electric generator, our ground station is relocatable and self-sufficient.

2.3. Receiver

At the receiver (figure 3) the signal is collected by a Tele Vue NP101is refractive telescope with a 10 cm aperture, and coupled into a sequence of custom components developed under contract with the Canadian Space Agency [31]. First of these is a fine-pointing unit (FPU), developed with Institut National d'Optique (INO) and Neptec Design Group, which guides both the quantum and beacon signals with a fast-steering mirror (FSM). Inside the

FPU, a dichroic mirror separates the quantum and beacon signals: the beacon is reflected towards a quad cell photo-sensor (QS), providing position feedback to a fine-pointing controller (FPC) that guides the fast-steering mirror in a closed loop [32]. The FPU, measuring 330 × 240 × 95 mm and 2.61 kg, has a ±0.3° field of view.

The collected quantum beam is guided through a 50 μm pinhole, acting as a spatial-mode filter [33], followed by a pair of 785 nm (3 nm bandwidth) spectral filters. It then passes into a custom integrated optical assembly (IOA) developed with INO, containing a passive-basis-choice polarisation analysis module with a 50:50 beam splitter and polarising beam splitters. The IOA, measuring 48.2 × 56.8 × 120 mm and 129 g, produces four beams coupled into multimode fibres, corresponding to the four BB84 measurement states (H, V, D, and A) with state contrasts between 532:1 and 2577:1.

The four IOA output fibres are guided to a detector module (DM) containing four Excelitas Technologies SLiK Si-APD detectors operating in Geiger mode with passive quenching. The DM measures 30 × 127 × 143 mm and 516 g, and operates at 2.3 W steady state (including thermoelectric cooling of detector active areas to −20 C) to give a detection efficiency of ≈45% , biased 28 V above breakdown.

The detectors trigger low-voltage differential signalling pulses which are measured at a control and data processing unit (CDPU) based on Xiphos Systems Corporation's Q7 processor card (recently flown on GHGSat [34]) with a custom daughterboard. The CDPU utilises an ARM Cortex-A9 processor and measures 25 × 107 × 118 mm, 129 g, drawing 4.5 W while operating. A field-programmable gate array embedded in the CDPU is programmed to implement time tagging of detection pulses with a resolution of 78 ps, while data storage, communication and processing software running in the Linux operating system implement the receiver-side QKD protocol.

The receiver telescope was mounted facing out the cabin door on the port side of the aircraft and flown with the door removed. The electronics and computers were located six feet forward in the aircraft cabin, and optical fibres and cables conducted signals between the electronics and the receiver telescope and pointing equipment.

2.4. Acquisition and calibration

The transmitter and receiver each have a beacon laser assembly (BLA) consisting of three fibre launchers with fixed divergence angles of 0.74° and individual tip/tilt control. These are mounted on each telescope and fed strong (≈40 mW) 850 nm laser light from fibre-coupled beacon laser source (BLS) arrays located away from the telescopes. A beacon camera (BC)—a 50 frame-per-second, 2 megapixel imaging camera with an 850 nm band-pass filter (10 nm bandwidth)—is also mounted to each telescope.

Each telescope is attached to a commercial two-axis motor system (transmitter: ASA DDM85 standard, receiver: FLIR PTU-D300E), providing first-stage 'coarse' pointing. When light at the beacon wavelength is visible as a bright spot on the camera image, our custom pointing software (running on PCs at each site) controls the angular speeds of the motors to minimise the deviation of the spot's position from a calibrated reference position. The control feedback loop incorporates the estimated angular speed of the spot (based on position differences between recent images, taking into account previous motor motions), a factor proportional to the spot's current deviation, and a factor proportional to the accumulated (integrated) spot deviations. The pointing software operates as a state machine and also includes a 'coasting' state to handle short drop-outs of the beacon signal, and 'acquiring' and 'searching' states to support the initial acquisition of the beacon.

To achieve initial acquisition, we employ inertial navigation modules (INMs), containing GPS receivers and attitude sensors, mounted to the telescopes. Each site transmits their GPS location to the other site via a classical RF (Wi-Fi) link and then calculates the other site's orientation relative to its own based on its local attitude data. During initial testing, the INMs exhibited an attitude uncertainty of about ±2.5°—significantly larger than the 0.74° divergence of the beacon lasers. To mitigate this, we turn on a bright infrared light-emitting diode array (IRL) at the receiver with much greater divergence (of order 80°), allowing the transmitter to find and point towards the receiver. Once the receiver sees the transmitter's beacon spot in its camera image and has moved to position, the IRL is switched off and two-way beacon tracking continues for the remainder of the pass.

A necessary practical feature of our transmitter and receiver apparatuses is that they can be independently calibrated, as they would not be co-located prior to establishing a link (much like for a satellite mission). To align each of the beacon lasers with the quantum signal beam path, we first inject alignment laser power into each telescope, and point the telescope towards a separate larger-diameter (≈20 cm) telescope, located ≈20 m away, equipped with a camera imaging the far field. We then observe the position of the beacon beams on the camera image, and adjust the tip and tilt of each beacon fibre launcher to centre its output over the signal spot. To calibrate the reference position of the beacon camera at the transmitter and the collimation of the transmitted quantum beam, we optimise the power received (using the alignment laser injected into the transmitter telescope) at another telescope located at a sufficient distance ≈850 m down the runway. The receiver beacon camera, which has greater tolerance due to the receiver's fine-pointing unit, is calibrated using a corner cube located ≈50 m away in the NRC hangar. These alignments were done prior to each flight. These independent

Table 1. Summary of data from passes where a quantum link was established. All times are UTC. Except where indicated (*), secure key lengths incorporate finite-size effects.

Pass	5 km arc 1	7 km line	5 km arc 2	3 km line	3 km arc	7 km arc	10 km arc
	2016-09-21	2016-09-21	2016-09-22	2016-09-22	2016-09-22	2016-09-22	2016-09-22
Parameter	2:57:45	3:30:45	1:15:23	2:19:33	2:24:45	2:42:16	2:57:42
Classical link duration [s]	288	172	352	34	170	210	289
Quantum link duration [s]	235	158	250	33	158	206	269
Mean speed [km h^{-1}]	208	200	198	236	216	259	212
Maximum angular speed [°]	0.76	0.45	0.75	1.0	1.28	0.60	0.37
Transmitter pointing error (10^{-3})[°]	22.0	4.85	1.33	3.42	2.91	1.58	2.82
Receiver pointing error (10^{-3})[°]	125	126	63.0	86.5	89.8	78.6	87.2
Receiver fine-pointing error (10^{-3})[°]	2.73	9.98	No data	2.62	2.39	3.01	12.7
Source QBER [%]	5.08	3.58	3.32	2.66	4.37	2.80	3.39
Signal QBER [%]	13.13	5.24	3.42	2.96	5.20	2.96	3.30
Decoy QBER [%]	19.54	11.1	6.13	6.35	7.93	5.97	8.46
Theoretical loss [dB]	52.1	41.6–44.8	28.1	33.3–35.1	30.9	32.1	39.9
Mean measured loss [dB]	48.0	51.1	34.5	39.5	34.4	39.4	42.6
Error correction efficiency	1.4	1.16	1.33	1.4	1.18	1.46	1.27
Signal-to-noise threshold	0	1500	2000	1000	1000	2000	2500
Sifted key length [bits]	152508	95710	5212446	853066	5102122	2348086	1175317
Secure key length [bits]	None	9566*	867771	71648	44244	200297	70947

calibrations allowed link acquisition to begin immediately upon the arrival of the airplane in the vicinity of the ground station.

3. Results

In total, seven of the 14 airplane passes over the ground station successfully established a quantum signal link. Issues, including minor equipment failures (e.g., a loose beacon camera lens) and accidental controller misconfigurations, particularly hampered link establishment during the first night: two of the seven attempts were successful. These issues were addressed during the intervening day, and the second night had considerably better link establishment rate: five of seven attempts. (We attribute the two failures on the second night—both attempted straight-line paths—to the fixed orientation of the Wi-Fi transceiver at the aircraft being poor for this geometry, particularly at the beginning of a pass.)

Secret key was extracted out of six of the seven successful passes. From data collected during these passes, we observe the performance of the system at various distances and with angular speeds. Circular-arc passes allowed us to demonstrate longer duration of key exchange, compared with straight-line passes, as the receiver telescope held a relatively constant position during the pass, making link establishment and pointing easier. Straight line passes, however, are much more representative of a satellite passing over a ground station, as they simulate the change in angular speed that would be experienced during such a pass. The maximum angular rate is reached when the airplane is closest to the ground station for that pass: the greatest maximum angular rate we measured for our passes was 1.28°/s at a distance of 3 km (arc). This angular rate is consistent with overflying LEO spacecraft such as 0.72°/s for a 600 km orbit, as baselined for QEYSSat, or 1.2°/s for the International Space Station (ISS).

Table 1 summarises the seven passes where quantum signal was successfully transmitted to the receiver aboard the aircraft. Passes typically lasted a few minutes, with the aircraft travelling at 198–259 km/h. To quantify pointing performance, we define the typical pointing error as the measured distance of the beacon spot from the calibrated reference point on the camera image, discarding times when the motors had just begun tracking. The mean typical pointing error at the transmitter varied from 0.00133° to 0.0220° over the passes; at the receiver, it was 0.0630° to 0.126°. The receiver's fine-pointing unit measured pointing errors similar to the pointing error of the transmitter, between 0.00239° to 0.0127°, where the deviation was measured from the centre of the quad cell sensor. (These values are used in the link analysis model, below.)

Figure 4 shows observed results for two representative passes, including the motor speed of the transmitter in the horizontal axis and link acquisition stages, the coarse- and fine-pointing errors at the receiver, the calculated time of flight of the quantum signal from the transmitter to the receiver, the rate of detections of all

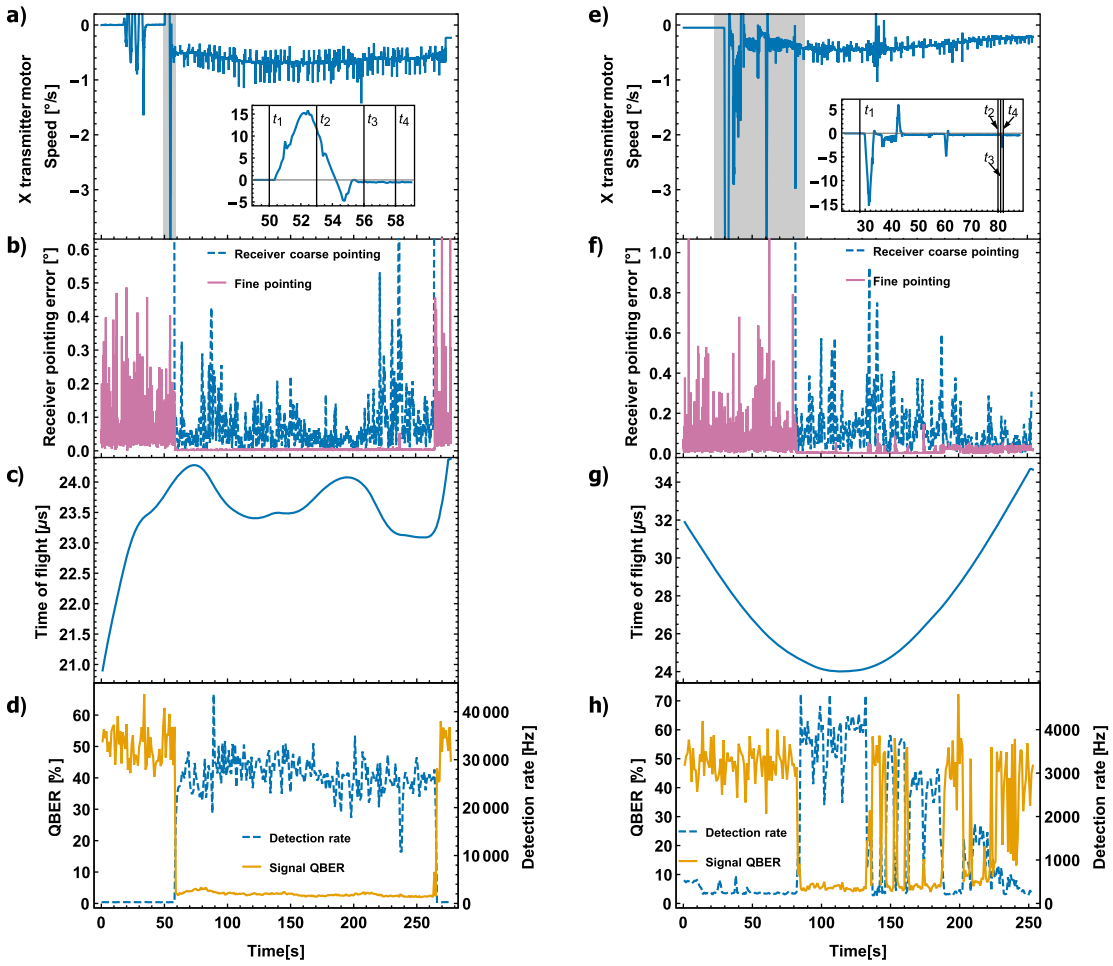

Figure 4. Results for the 7 km arc pass (left) and the 7 km straight-line pass (right). (a) and (e) show the speeds of the azimuthal (coarse) motor at the transmitter. The insets, corresponding to the shaded portions, show the motor speed during initial acquisition, with times t_1 through t_4 identifying establishment of the Wi-Fi link, identification of the beacon spot, lock to the beacon spot and first counts received, respectively. The oscillation prior to this in (a) is from a spiralling search state of the pointing software. (b) and (f) show coarse- and fine-pointing performance at the receiver. Where there are no coarse pointing data (e.g., at the beginning of a pass), no beacon spot was found in the camera image. This corresponds with large fluctuations in the fine-pointing deviation: in the absence of beacon light, the unit operates on electrical noise generated at the quad cell. (c) and (g) show the estimated time of flight of the photons from the transmitter to the receiver (used in event time-correlation), calculated from per-second GPS coordinates at each site. The smooth curve in (g) is particularly characteristic of the straight-line pass, with a similar shape to that of a satellite pass. (d) and (e) show the total detection rates at the receiver and the QBER of the signal.

four DM channels combined and the quantum bit error rate (QBER) of the signal. There, the maximal angular speed was about 0.5° to 0.7°/s during beacon pointing lock, after initial acquisition.

The mean measured loss of the quantum link during the flights varied from 34.4–51.1 dB. Our theoretical loss model [24] assumes a mid-latitude, rural atmospheric model in summer with the ground station located 128 m above sea level and 5 km visibility. Other model parameters include 43% detector efficiency and receiver optical transmittance of 59.7% (determined from the measured properties of the receiver prototype). We simulate the effect of atmospheric turbulence at our location using Hufnagel–Valley parameterisation of atmospheric conditions [35, 36], with a sea-level turbulence strength of 1.7×10^{-14} m$^{-2/3}$ and high-altitude wind-speed of 21 m s^{-1}. The measured pointing accuracy, aircraft altitude and ground distance for each pass was also used. The divergence angle of the quantum beam could not be measured during the flight campaign. For the model, we assume diffraction-limited divergence, resulting in lower bound theoretical loss estimates. Indeed, in the experiment a number of passes were conducted with the transmitter intentionally slightly defocussed so as to avoid saturating the detectors. Consequently, the experimental losses we observed are generally higher than the theoretical losses. The difference between the theoretical loss of an arc pass and the minimum theoretical loss of a line pass at the same nominal distance is due to varying pointing accuracy experienced for each pass, as well as the actual ground distance and altitude deviating from nominal.

For QKD analysis we utilise a signal-to-noise (SNR) filter [37], which assesses the total counts in each 1 s frame of data and discards any frame with counts less than a threshold, prior to distiling key bits. We choose thresholds between 1000 and 2500, depending on the pass. Background detection rates at the beginning and end

of the pass are sufficiently low that those frames are discarded by the SNR filter. Some drop-outs can be seen in figure 4(h)—these frames are also discarded by the SNR filter.

The source's intrinsic QBER, as predicted by the polarisation correction system, varied between 2.66%–5.08% for each pass. At the receiver, the FPU, IOA, and fibres leading to the detectors were shielded with black cloth to minimise stray light entering the detectors, leading to typical total background detection rates of ≈285 Hz.

The QBER measured at the receiver drops to a few percent upon optical link lock, and rests at ≈50% due to the random noise of background detections at all other times. For passes where secure key was generated, the QBER measured at the receiver, after the SNR filter, varied from 2.96%–5.24% . The received QBER during the first night flight was observed to be higher than for the second night, possibly due to an issue with the wave plate motorised stage controller.

We generate secure key bits from the data collected during each pass using algorithms tailored for the asymmetric processing resources that would be available with a satellite platform [38]. These algorithms consist of source and receiver event time-correlation (performed at the ground station), error correction utilising low-density parity check codes and privacy amplification via reduced-Toeplitz-matrix two-universal hashes. To ensure security, the uncertainty due to the finite number of samples used to estimate link parameters must be taken into account. Of the six passes from which key could be extracted, five yielded secure key including these finite-size effects (where we use the common ten-standard-deviation heuristic to bound parameter estimates [39]). The remaining pass had too few counts and could only generate secure key assuming no finite-size effects.

4. Discussion and conclusion

We have successfully demonstrated quantum key distribution to a satellite receiver payload prototype on an aircraft moving at up to 259 km h^{-1}. Our pointing and tracking system was able to establish and maintain an optical link with milli-degree precision over 3–10 km distances while BB84 decoy-state signals were sent across the channel to the aircraft moving at the angular speeds of a LEO satellite. Our custom fine-pointing system, IOA, DM and CDPU, along with the other commercial components, all performed in concert on the aircraft to generate secure keys, of tens to hundreds of kilobits in length in various flight scenarios, including the straight-line paths approximating the apparent trajectory a LEO satellite. With source intrinsic QBER typically 2%–4% and post-processing algorithms representative of what would be achievable with a satellite platform, we extracted finite-size secure key for many of the tested passes.

The details of path-to-flight modifications necessary to construct space-suitable versions of our receiver components varies. Some elements present on the CDPU daughterboard, for example, will need to be replaced with radiation-hard equivalent versions or, for the IOA, glues designed for low out-gassing must be used. Sensitivity of the Si-APDs in the DM to proton radiation in orbit is of particular note, as such radiation can significantly increase dark counts. However, strategies including cooling and thermal annealing [40], as well as laser annealing [41], are capable of mitigating these effects and a space-suitable prototype DM implementing these strategies is being developed.

For pointing to a satellite from the ground, initial acquisition will likely not have a real-time classical communication link to exchange position data. In this case, however, predictions of the satellite position at the time when a link is to be established can be used, as the orbital trajectory of a satellite is predictable with far greater accuracy than the flight path of an airplane. In this context, point-ahead may be necessary (depending on the transmitter's divergence) to ensure that the quantum beam is coincident with the satellite when it arrives, owing to the satellite's motion during the time of flight of the optical signals. A fine-pointing system would likely also be required to achieve sufficient accuracy over the significantly larger transmission distance. For the aircraft, this was not necessary.

One advantage of the uplink approach is source flexibility. While we have demonstrated only operation with a weak coherent pulse source here, we fully expect that QKD using entangled photon pairs generated at the appropriate wavelength by, for example, spontaneous parametric down-conversion will produce equivalent results under a BBM92-style protocol [42], with one photon of each pair measured on the ground. To support this, no aspect of the receiver prototype need be modified.

Our system demonstrates the viability of an uplink QKD satellite mission. The core quantum components of a QKD satellite receiver have been demonstrated and have clear path to inclusion in space-faring system. In particular, see figure 5 from a recent study conducted with UTIAS SFL, which shows our receiver hardware—FPU, FPC, IOA, DM and CDPU—with minor modifications, cohesively integrated onto the flight-proven NEMO-150 micro-satellite bus. With the feasibility of performing uplink QKD with moving platforms well supported with satellite-ready hardware, QKD at the global scale utilising satellite uplinks is within reach.

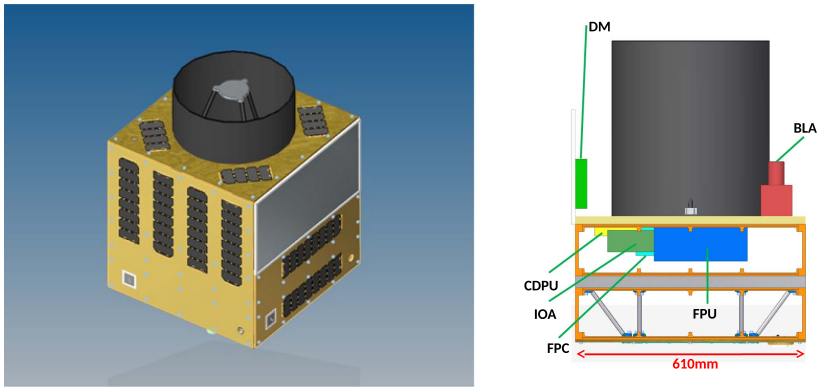

Figure 5. UTIAS SFL NEMO-150 micro-satellite bus housing the quantum receiver payload. Left: external view showing extended telescope and baffle. Right: cross-section showing the possible placement of the main receiver payload components demonstrated during this airborne QKD campaign. Images provided by UTIAS SFL.

Acknowledgements

The authors acknowledge funding from the Canadian Space Agency Flights and Fieldwork for the Advancement of Science and Technology (FAST) programme as well as the Space Technology Development Program (STDP), Ontario Research Fund, the National Sciences and Engineering Research Council, the Canadian Institute for Advanced Research and the Canada Foundation for Innovation. CJP acknowledges support from the Natural Sciences and Engineering Research Council Canadian Graduate Scholarship–Doctoral Program and the Ontario Government Ontario Graduate Scholarship Program. JJ acknowledges support from the Korean Institute for Science and Technology. SK acknowledges support from the Mike and Ophelia Lazaridis Fellowship Program.

The authors thank Jeremy Dillon and the Flight Research Laboratory team at the National Research Council of Canada for their expertise in integrating and flying scientific aircraft payloads, training and assistance during the flights. We thank the members of the Smiths Falls Flying Club, especially Peter Campbell, for access to their airfield and facilities, Phil Kaye for providing hangar space and assistance and Ramy Tannous for assistance at the ground station. We thank Ian D'Souza and Jeff Kehoe for assistance with preliminary equipment test flights and Rolf Horn for allowing us to set up a temporary ground station on his property. We also thank Dotfast-Consulting, Excelitas Technologies, Institut National d'Optique, Neptec Design Group and Xiphos Systems Corporation for the development and support of the custom components.

CJP, EC and TJ managed the project and planned and executed logistics. SK, CJP and TJ conducted feasibility and aircraft flight-path studies, with link analysis conducted by CJP and JPB. CJP, SK, JPB, BLH and TJ designed and tested system components with industry partners. SK, EA, VM and TJ designed and built the receiver detector module. CJP and SK designed and assembled the receiver payload. BLH developed the coarse pointing system, data acquisition, data processing and polarisation compensation system software, supervised by TJ. JPB, NS and TJ designed and built the quantum source. CJP, SK, JPB, JJ, SA, BLH and TJ conducted outdoor full-system calibration and tests. CJP and JJ integrated the receiver payload into the aircraft, assisted by BLH. CJP, JPB, BLH and TJ developed and managed flight operations and mission tasking. CJP operated the receiver in flight, assisted by JJ. BLH conducted data acquisition and pointing at the ground station. JPB operated the quantum source, assisted by BLH. NS, SA and TJ supported ground station operations. CJP analysed the data, supervised by BLH and TJ. TJ conceived and supervised the project. CJP and BLH wrote the manuscript with contributions from all authors.

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *In Proc. of the IEEE International Conf. on Computers, Systems and Signal Processing* (New York: IEEE Press) pp 175–9

[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution *Rev. Mod. Phys.* **81** 1301–50

[3] Stucki D, Walenta N, Vannel F, Thew R T, Gisin N, Zbinden H, Gray S, Towery C R and Ten S 2009 High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres *New J. Phys.* **11** 075003

[4] Liu Y *et al* 2010 Decoy-state quantum key distribution with polarized photons over 200 km *Opt. Express* **18** 8587–94

[5] Korzh B, Lim C C W, Houlmann R, Gisin N, Li M J, Nolan D, Sanguinetti B, Thew R and Zbinden H 2015 Provably secure and practical quantum key distribution over 307 km of optical fibre *Nat. Phot.* **9** 163–8

[6] Buttler W T, Hughes R J, Kwiat P G, Lamoreaux S K, Luther G G, Morgan G L, Nordholt J E, Peterson C G and Simmons C M 1998 Practical free-space quantum key distribution over 1 km *Phys. Rev. Lett.* **81** 3283–6

[7] Hughes R J, Nordholt J E, Derkacs D and Peterson C G 2002 Practical free-space quantum key distribution over 10 km in daylight and at night *New J. Phys.* **4** 43

[8] Ursin R *et al* 2007 Entanglement-based quantum communication over 144 km *Nat. Phys.* **3** 481–6

[9] Schmitt-Manderbach T *et al* 2007 Experimental demonstration of free-space decoy-state quantum key distribution over 144 km *Phys. Rev. Lett.* **98** 010504

[10] Vallone G, D'Ambrosio V, Sponselli A, Slussarenko S, Marrucci L, Sciarrino F and Villoresi P 2014 Free-space quantum key distribution by rotation-invariant twisted photons *Phys. Rev. Lett.* **113** 060503

[11] Nauerth S, Moll F, Rau M, Fuchs C, Horwath J, Frick S and Weinfurter H 2013 Air-to-ground quantum communication *Nat. Phot.* **7** 382–6

[12] Wang J-Y *et al* 2013 Direct and full-scale experimental verifications towards ground-satellite quantum key distribution *Nat. Phot.* **7** 387–93

[13] Bourgoin J-P, Higgins B L, Gigov N, Holloway C, Pugh C J, Kaiser S, Cranmer M and Jennewein T 2015 Free-space quantum key distribution to a moving receiver *Opt. Express* **23** 33437–47

[14] Hughes R J, Buttler W T, Kwiat P G, Lamoreuax S K, Morgan G L, Nordholt J E and Peterson C G 2000 Quantum cryptography for secure satellite communications *In 2000 IEEE Aerospace Conf. Proc. (Cat. No. 00TH8484)* **1** 191–200

[15] Tang Z, Chandrasekara R, Sean Y Y, Cheng C, Wildfeuer C and Ling A 2014 Near-space flight of a correlated photon system *Sci. Rep.* **4** 6366

[16] Rarity J G, Tapster P R, Gorman P M and Knight P 2002 Ground to satellite secure key exchange using quantum cryptography *New J. Phys.* **4** 82

[17] Ursin R *et al* 2009 Space-quest, experiments with quantum entanglement in space *Europhys. News* **40** 26–9

[18] Villoresi P *et al* 2008 Experimental verification of the feasibility of a quantum channel between space and Earth *New J. Phys.* **10** 033038

[19] Etengu R, Abbou F M, Wong H Y, Abid A, Nortiza N and Setharaman A 2011 Performance comparison of BB84 and B92 satellite-based free space quantum optical communication systems in the presence of channel effects *J. Opt. Comm.* **32** 37–47

[20] Meyer-Scott E, Yan Z, MacDonald A, Bourgoin J-P, Hübel H and Jennewein T 2011 How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss *Phys. Rev.* A **84** 062326

[21] Yin J *et al* 2013 Experimental quasi-single-photon transmission from satellite to earth *Opt. Express* **21** 20032–40

[22] Vallone G, Dequal D, Tomasin M, Schiavon M, Vedovato F, Bacco D, Gaiarin S, Bianco G, Luceri V and Villoresi P 2016 Satellite quantum communication towards GEO distances *Proc. SPIE* **9900** 99000J–99000J–8

[23] Jennewein T *et al* 2014 QEYSSAT: a mission proposal for a quantum receiver in space *Proc. SPIE* **8997** 89970A–89970A–7

[24] Bourgoin J-P *et al* 2013 A comprehensive design and performance analysis of low Earth orbit satellite quantum communication *New J. Phys.* **15** 023006

[25] Gibney E 2016 Chinese satellite is one giant step for the quantum internet *Nature* **535** 478–9

[26] 2016 Quantum optics lifts off *Nat. Phot.* **10** 689

[27] UTIAS SFL. Products & services: satellite platforms http://utias-sfl.net/?page_id=89

[28] Yan Z, Meyer-Scott E, Bourgoin J-P, Higgins B L, Gigov N, MacDonald A, Hübel H and Jennewein T 2013 Novel high-speed polarization source for decoy-state BB84 quantum key distribution over free space and satellite links *J. Lightwave Technol.* **31** 1399–408

[29] Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 230504

[30] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C and Leuchs G 2014 Trojan-horse attacks threaten the security of practical quantum cryptography *New J. Phys.* **16** 123030

[31] Canadian Space Agency. Quantum key distribution receiver.contract no. 9F063-120711/002/MTB

[32] Pugh C J *et al* A fine pointing system suitable for quantum communications on a satellite In preparation

[33] Sajeed S, Chaiwongkhot P, Bourgoin J-P, Jennewein T, Lütkenhaus N and Makarov V 2015 Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch *Phys. Rev.* A **91** 062301

[34] GHGSat Inc. GHGSat. http://www.ghgsat.com/

[35] Hufnagel R E 1974 Variations of Atomspheric Turbulence *In Digest of Topical Meeting on Optical Propagation Through Turbulence, OSA Technical Digest Series (Optical Society of America, Washinton, D.C.)* p WA1–1–WA1–4 http://www.ast.cam.ac.uk/sites/default/files/Hufnagel_Var_251109.pdf

[36] Hardy J W 1998 *Adaptive Optics for Astronomical Telescopes* (*Oxford series in optical and imaging sciences*) (Oxford: Oxford University Press)

[37] Erven C, Heim B, Meyer-Scott E, Bourgoin J P, Laflamme R, Weihs G and Jennewein T 2012 Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere *New J. Phys.* **14** 123018

[38] Bourgoin J-P, Gigov N, Higgins B L, Yan Z, Meyer-Scott E, Khandani A K, Lütkenhaus N and Jennewein T 2015 Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations *Phys. Rev.* A **92** 052339

[39] Sun S-H, Liang L-M and Li C-Z 2009 Decoy state quantum key distribution with finite resources *Phys. Lett.* A **373** 2533–6

[40] Anisimova E, Higgins B L, Bourgoin J-P, Cranmer M, Choi E, Hudson D, Piche L P, Scott A, Makarov V and Jennewein T Mitigation of radiation damage of single photon detectors for space applications EPJ Quantum Technol. in press (arXiv:1702.01186)

[41] Lim J G, Anisimova E, Higgins B L, Bourgoin J-P, Jennewein T and Makarov V Laser annealing heals radiation damage in avalanche photodiodes *EPJ Quantum Technol.* in press (arXiv:1701.08907)

[42] Bennet C H, Brassard G and Mermin N D 1992 Quantum cryptography without Bell's theorem *Phys. Rev. Lett.* **68** 557–9