The QEYSSat Mission:
Demonstrating Global Quantum Key Distribution Using a Microsatellite

I. D'Souza, D. Hudson, C. Evans, E. Choi
COM DEV Canada
60 Struck Ct, Cambridge, ON, Canada; +1.519.622.2300
ian.dsouza@comdev.ca

T. Jennewein
Institute for Quantum Computing, University of Waterloo
200 University Ave. W., Waterloo, ON, Canada; +1.519.888.4567 Ext 37485
tjennewe@iqc.ca

K. Sarda
Space Flight Laboratory, University of Toronto
4925 Dufferin Street, Toronto, ON, Canada; +1.416.667.7864
ksarda@utias-sfl.net

ABSTRACT

QEYSSat (Quantum EncrYption and Science Satellite) is a proposed microsatellite mission concept under development for the Canadian Space Agency (CSA) that will demonstrate long-distance quantum key distribution (QKD) from space. Under the leadership of principal investigator Dr. Thomas Jennewein of the University of Waterloo's Institute for Quantum Computing (IQC) and in partnership with the Institut National d'Optique (INO), the University of Toronto Space Flight Laboratory (UTIAS/SFL) and the Neptec Design Group, COM DEV has advanced the QEYSSat mission concept over the last two years through a series of technical studies funded initially by Defense Research and Development Canada (DRDC) and subsequently by the CSA.

QKD is a highly secure method of creating an encryption key between two remote parties using the exchange of individual photons. Current terrestrial quantum key networks employ optical fiber links for the photon exchange. The most important attribute of keys generated and distributed in this manner is the security of the method. In theory, QKD is impervious to eavesdropping because under the laws of quantum mechanics the properties of an individual photon cannot be measured without impacting its state. Any eavesdropping can therefore be detected, allowing a quantitative measurement of the security of the generated key.

The principal shortcoming of this method is that single-photon exchange processes are necessary for the implementation of a QKD network, which requires either line-of-sight between the network nodes or the use of low-loss optical fiber. This line-of-sight requirement restricts distances due to the curvature of the Earth, and optical fiber is limited to distances of about 200 km due to losses. There is no way to implement a "repeater" or amplifier in the link because this would impact the state of the photon and essentially defeat the inherent anti-eavesdropping characteristics of the technique.

Using satellites as nodes in the QKD network would overcome this distance limitation and allow keys to be distributed over much larger distances. QEYSSat will demonstrate QKD from space, providing insight into single-photon link behavior and also serving as a platform for fundamental quantum physics experimentation. The proposed mission is currently baselined to use the AIM (Advanced Integrated Microsatellite) bus developed by COM DEV for M3MSat (Maritime Monitoring and Messaging Micro-Satellite). AIM is a responsive, flexible and cost-effective platform that meets or exceeds the CSA's Multi-Mission Microsatellite Bus (MMMB) specification. The proposed QEYSSat spacecraft would carry a quantum payload designed to measure the polarization of individual photons. It would operate in conjunction with dedicated ground stations that will transmit the polarized photons. The payload is expected to have the capability to generate the quantum keys and manage their distribution between distant ground stations.

This paper will describe the proposed QEYSSat mission concept and summarize the development work to date. A successful demonstration of QKD from space could pave the way for the future development of secure global quantum networks for users in both government and the private sector.

INTRODUCTION

Quantum mechanics offers communication with an unprecedented level of security based on entangled photon states or on other signals exhibiting quantum mechanical properties, as in the polarization states of single photons. The security originates in the fact that, in contrast to classical information, quantum information cannot be copied without disturbing the quantum state. Any attempt to obtain knowledge about the information content of a signal will perturb the quantum state carrying the information. One application of these principles is the secure distribution of data encryption keys using individual photons. Such transmission methods are impervious to eavesdropping, and this is ensured by the laws of quantum mechanics – there is no way to circumvent this principle. Encryption keys can be securely distributed to individual users using quantum methods and the end user can then make use of their unique keys to communicate via standard methods (cipher encryption).

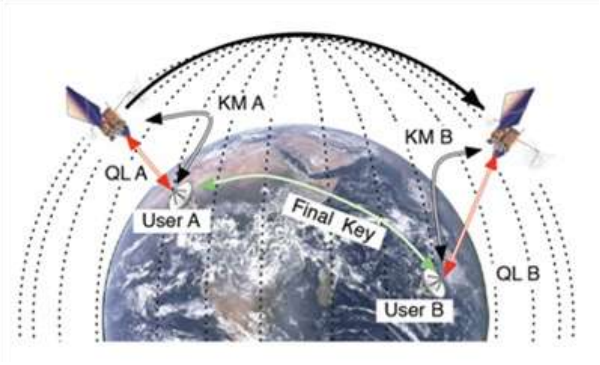

Figure 1: Key exchange

While terrestrial quantum networks exist to distribute keys, the distance over which one can successfully perform quantum key distribution (QKD) is currently limited because of the exponential transmission losses experienced in optical fiber, and because a quantum signal cannot be amplified without disturbing the quantum state (no-cloning theorem [1]). Future prospects for low-loss fiber are also not likely to yield significant improvement over the next several decades. One way to overcome this barrier is through the use of trusted nodes at intermediate points between users: a key is exchanged between a user A and the trusted node, and user B and the trusted node. The trusted node then connects the two users, using its full knowledge of both keys. Using trusted nodes in ground systems is possible but requires a very large number of nodes to connect two distant users. Using satellites as trusted nodes will enable arbitrarily large separation of QKD, which is virtually impossible on ground.

A system designed to demonstrate space-based quantum key distribution is fundamentally a quantum link that can be used for a variety of purposes. The link itself will be fully characterized and optimized, and thus can also be used for other science experiments, in particular, the verification of the non-locality of quantum mechanics by demonstration of quantum entanglement over large distances. Quantum entanglement is of fundamental relevance to quantum physics, yet can only be tested at relatively short (< 200 km) distances terrestrially. The satellite mission proposed here will provide the world's first long distance entanglement test, with entangled particles separated by over 600 km. While the scientific opportunities in this QKD mission are somewhat more limited than in other missions that have been considered specifically for science-only applications, the simplicity of this mission allows aspects of these science experiments to be achieved much sooner and at a lower cost, while at the same time providing a demonstration mission of space based QKD. This mission will also lower the risk for future bigger, more complex, science missions that could follow, and will provide a sufficiently long mission life so that QKD can be operationally demonstrated. The satellite can potentially be used to distribute keys in an operational service, providing a degree of utility as well as a long term test bed for future scientific investigations and collaborations.

The development of this quantum key distribution demonstration mission follows a nine month feasibility study, during which a long list of potential quantum space missions was evaluated and down selected to two potential mission proposals. These two proposals, a double-entangled link science experiment and this QKD demonstration mission, were developed in more detail in order to demonstrate the concept feasibility and evaluate their relative merits. The current QKD mission was therefore selected after significant consideration of the possible applications of quantum mechanics that could be served only with a space segment. Specific reasons for the development of this

QKD mission included the multiuse aspect – this mission demonstrates the application of QKD, but can also be used for science experiments – and the relative simplicity of the proposed microsatellite concept. An important quality is also the shorter development timeline for quantum physics experiments in space.

The configuration for this mission is to create a single quantum link from a photon source on the ground to polarization detectors on a satellite in low Earth orbit. This was selected during the feasibility study as the best configuration to achieve a quantum key exchange between space and ground, after careful consideration of uplinks, downlinks, and alternate orbit altitudes. In addition to the simplification of the required payload, this configuration has the advantage of allowing various photon sources to be used/tested on the ground. A recommended weak coherent laser pulse source can also be added to the satellite, to allow studies of both the uplink and downlink transmission directions (the atmospheric interaction of the link is different for up and down links), and to provide space heritage for a photon source.

MISSION OVERVIEW

Mission Objectives

The objective of the proposed mission is to create a quantum link between ground and space using polarized photons and to generate encryption keys for ground based users using this link. These keys can be used to re-key the satellite itself, or distributed to one or more ground stations, with the QKD satellite acting as the trusted node as described in the previous section. In achieving this goal, the quantum link will be measured and tested to gain insights into such things as the applicability of different types of photon sources and transmission schemes. The satellite will be used for concurrent scientific experiments with the long distance quantum link. Of particular interest are tests of the quantum mechanics of pairs of entangled photons, with one photon remaining on ground and one being sent to the satellite. The insights that may be gained from this demonstration mission will provide information and risk mitigation strategies relevant to future missions, both application and science oriented.

For successful quantum key distribution, quantum signals must be received with a low enough error rate to exclude an eavesdropper, and with large enough photon numbers to account for statistical fluctuations. Success for a single key generation requires a full QKD protocol which includes timing analysis, basis reconciliation, error correction, and privacy amplification. The application of the protocol must return a nonzero key transfer rate over a single satellite passage using the best security bounds available. This key must also be exchanged with a second ground station in order to demonstrate the global key distribution concept required of this mission. To achieve the science goals, sufficient link quality and timing alignment is crucial.

A Core Users Team has been formed to formally define the mission objectives and the mission success criteria have been identified. This team currently consists of Science Users, and representatives from Defense Research and Development Canada, and the Communications Security Establishment Canada. These users and representatives have guided the development and scope of this mission.

It is clear that countries worldwide are ramping up to perform their own QKD space experiments and Canada is interested especially due to the world leading research currently underway in Canada in the area of Quantum Communications and Quantum Computing.

System Overview

To securely distribute encryption keys anywhere on the globe, the satellite will act as a 'trusted node,' meaning that the keys will be held/stored on the satellite during operations, and that the security of the satellite is assumed. The satellite will create a secure key between itself and ground station A during one or more passes. It will also create a secure key between itself and ground station B during one or more passes. Then to create a secure key between station A and station B, a Boolean combination of the two keys is calculated on the satellite. The result is transmitted (classically and in the open) to one of the two ground stations. Using the combined key and the knowledge of its own key, a station can then calculate the other station's key, and use it for secure communications between station A and B.

A single ground station is sufficient to demonstrate the quantum link and the key creation process; however, two ground stations are proposed in order to have a realistic demonstration of key distribution between distant locations. Using multiple ground stations also extends the opportunities available to experimentalists, with respect to measurement opportunities, quantum sources, and environmental (clear sky) conditions, and invites global collaboration.

The proposed system is based on a quantum photon uplink from ground to the satellite, in order to minimize the complexity of the spacecraft. The quantum source will be at the ground station, which will allow for flexibility and future upgrades. This source is expected to be either a weak coherent pulse (WCP) laser source or an entangled photon source which generates entangled photon pairs from a laser. Different types of sources can be used at different ground stations, but having at least one entangled photon source is important for scientific experiments. The satellite will carry the photon polarization detectors, and encryption key management software. Additionally, a weak coherent pulse source is proposed to be carried on board the satellite. It would not be used for QKD, but would maximize the scientific benefit of the mission by providing vital information on the quantum optical down-link path, as well as providing flight heritage for the hardware.

Crucial systems for this mission include laser beacon sources and receivers, at both ends, for link acquisition and tracking, polarization monitoring and compensation, and fine pointing for the quantum link. A clock alignment process for the precise time tagging of photons is also essential. In addition to quantum communication, classical communication of non-secure information is required for the key exchange; this will be performed using standard RF links.

Key Exchange

Since the satellite is purely a quantum receiver, the protocol used to realize the QKD mission depends on the quantum source: BB84[2] for a WCP and decoy states, or BBM92[3] for an entangled photon source. The following descriptions of each protocol use the names Alice and Bob for the source and receiver, as is common in physics and cryptography. For this mission, Alice is the source on ground and Bob is the receiver on the spacecraft.

BB84 was the original QKD protocol developed which later was augmented with the idea of decoy states in order to assure security for longer transmission distances. It has the following steps:

1. Alice randomly chooses three parameters for each quantum: a basis to encode in (H/V or +45°/-45°), a bit value (0/1), and a laser intensity (μ/μdecoy).

2. Using the selected laser intensity Alice encodes her photon with the chosen basis and bit value and sends it over the free-space channel to Bob; at the same time Alice saves a list of all of the parameters for each photon sent.

3. Bob receives the photon and randomly chooses one of the two bases (H/V or +45°/-45°) to measure the photon in. He records the basis, the result of the measurement, and the arrival time of the photon (time-tag list).

4. Alice and Bob perform many rounds of this distribution until enough raw signals have been detected by Bob to meet the necessary security conditions (usually around 106 photons).

5. Bob then sends Alice his list of time-tags so that she can filter her list down to only those events which Bob received. This is called the Raw Key.

6. Each laser intensity, μ and μdecoy, have certain photon number statistics. Alice checks to make sure that the measured statistics match the theoretical ones closely enough to assure security.

7. Bob sends Alice a list of the bases he used for each of his measurements. Alice sifts her list down to only those results where she encoded her bit in the same basis that Bob measured. She also sends this index list to Bob so that he can also sift his results. This is called the Sifted Key.

8. Since the channel and QKD system itself will likely have errors, Alice and Bob perform error reconciliation on their sifted keys to correct these errors. The most efficient algorithm is for them to use a one-way low density parity check (LDPC) error correction algorithm. Here Bob calculates syndrome information on his key and sends this to Alice. Alice then performs a maximum likelihood routine in order to correct her key given the syndrome information. This is called the Error Corrected Key.

9. The error correction algorithm also gives Alice and Bob the exact quantum bit error rate (QBER) experienced during their quantum transmission. Using the secure key generation formula from the proof of security for QKD, they calculate how much final secure key that they can generate.

10. Alice and Bob each perform privacy amplification on their error corrected keys which reduces their key size to that calculated in the previous step and ensures security. This is called the Final Secure Key.

11. Alice and Bob can now use this secure key to encrypt their communications between each other. Or Alice can wait until the satellite establishes a key with a second ground station, for example Charlie. Once Bob and Charlie

share a secure key, Bob on the satellite can compute the XOR of the two keys and provide it (non-securely) to Charlie. Charlie can then recover the key shared by the satellite and Alice and use it to securely communicate with Alice, thus accomplishing secure global QKD. This scenario is called the trusted node scenario since the satellite must be a trusted node because it holds a copy of each key.

The other possibility to perform QKD is to use a source of entangled photons in order to distribute the secure key. The BBM92 protocol essentially symmetrizes the BB84 protocol. Security in the entangled scheme relies on the fact that correlations in two bases are only possible with a particular quantum mechanical correlation and any eavesdropper would ruin that correlation. So Alice and Bob in this case do not need a decoy step.

Payload Data

Raw data acquired from the quantum link consists of time tagged polarization measurements. The polarization and measurement basis bit are arbitrarily defined, but Table 1 provides an example for clarity. For a secure key exchange, only the times and the measurement bases can be communicated to ground, along with the information from key processing steps as described above. However, the demonstration/science aspect of this mission implies more data will be available on ground than would normally be collected in an operational QKD scenario. For science experiments the detected polarizations will be included in the raw data transferred to ground for analysis.

Table 1: Example of Raw Data Definitions

Measurement	Basis Bit	Polarization Bit
→	0	0
↑	0	1
↘	1	0
↗	1	1

The amount of data generated on board is slightly different depending on the source type. The amount of raw data required to generate a secure key is slightly different as well, due to the differences in the key exchange protocols.

The data stored on ground depends on the source type. For an entangled source, it is time tagged photon detections, similar to what is recorded on the satellite. For a WCP, the data consists of time tags and bits of data. The data consists of bits to indicate the pulse intensity and polarization.

Nominally, the payload data will be transferred to ground during the pass used for the quantum link. A ground station used for the key exchange is expected to have the classical communications equipment on site. If the processing is not completed during a single pass, or an RF link is not available on site, key creation is still possible but additional delays will occur. In particular, ground stations without RF links can be used for science objectives, with the payload data downlinked to an alternative location. If the time tags need to be stored for later download, sufficient storage space is required on board. If they are transmitted to ground in real time during the key exchange, a sufficient buffer is required but only the bits (polarizations) need to be stored in memory.

In an operational system, the data from intermediate steps can be deleted once the Final Secure Key is created. However, multiple passes may be needed to collect a sufficient number of photons for the final key, in which case intermediate storage is still required. In this mission all data will be optionally stored for later downlink.

The final destination of the secure encryption key is local to the ground station. Once received on ground, the key is considered delivered. Local operators are responsible for encrypting and de-encrypting communication using the secure key.

Concept of Operations

The satellite will be placed in a sun-synchronous orbit, at approximately 600 km altitude. This is the nominal orbit used for all the mission analysis, but a link analysis can be calculated for other similar orbits, once launch opportunities are identified. However, the payload can only function when both the satellite and ground station are dark. Depending on the ground station location, two to three dark passes will be possible per night, but only passes with clear skies can be used. The satellite will be designed for a two year lifetime with no propulsion capabilities. The two year lifetime is selected somewhat arbitrarily, as a reasonable design lifetime for a microsatellite class bus. This also provides sufficient time for in-orbit debugging, science testing various sources, and analyzing and optimizing the quantum link.

Planning will be done at COM DEV, interacting with each optical ground station to determine weather and conditions for seeing. Planning initially will consist of trial transmissions during a commissioning phase to allow for calibration and performance characterization of the various signal detection systems, including pointing and tracking.

After commissioning and satellite characterization, the main QKD and science activity can take place. In normal operations, when the satellite is in daylight, it can be oriented to maximize power generation, while protecting its optical systems from the sun. As it approaches a ground station, it will slew to point the tracking beacon towards where the ground station will appear on the horizon. The beacon from ground will be detected by the on-board tracking system in order to maintain the optical link with the ground station throughout the pass. The single photon quantum link will be acquired and the initiation of the quantum protocol will begin. The resulting data will nominally be downlinked to a collocated RF station, or alternatively be stored for later downlink to an offsite station. The pass will automatically terminate if the ground beacon is lost and not reacquired after a set delay.

Potential Launcher

Using the COM DEV AIM class microsatellite bus as an example, it is designed to be compatible with Delta IV, Rockot, Dnepr, Falcon 1e, Taurus, Vega, and PSLV launchers. However, the secondary mirror of the receiver telescope may extend outside of the AIM bus target volume envelope. This means that Delta IV and Vega launchers will need to be considered on a case by case basis. The other launchers listed provide a larger volume envelope, so should accept the extension without issue. Further constraints may be identified in the next phase of this project, in particular for the shock and vibration of the telescope and optical path.

MISSION SPECIFIC OPERATIONS

Acquisition Pointing and Tracking (APT)

Figure 2 shows the sequence required for transferring quantum information between the satellite and the groundstation. In anticipation of the pass, the satellite slews to point towards the ground station. When it comes into view, the satellite transmits its beacon and tracks the ground station accurately enough to maintain the beacon target on the fine pointing detector. The ground station also illuminates its beacon, and tracks the satellite. At the end of the pass, the payload powers down, and the ADCS returns to a stand-by mode.

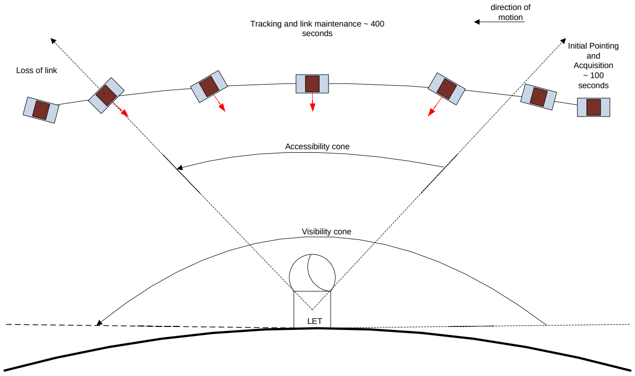
direction of motion
Tracking and link maintenance ~ 400 seconds
Initial Pointing and Acquisition ~ 100 seconds
Loss of link
Accessibility cone
Visibility cone
LET

Figure 2: Target acquisition, pointing and tracking

The ADCS will utilise star trackers for high accuracy and high bandwidth attitude pointing knowledge and reaction wheels for quick slewing and high bandwidth control. Other hardware includes sun sensors, magnetometer and GPS receiver for attitude determination and autonomous spacecraft position estimation, and torquers for satellite momentum dumping and crude control. The beacon receiver on the telescope, though decoupled from the ADCS, is an integral part of the APT concept as it dictates the pointing accuracy requirements for the ADCS.

The following baseline parameters are assumed for the definition of the system:

1. Circular, Sun synchronous orbit with an altitude of 600 km.
2. Average effective pass duration: 400 s
3. Satellite moment of inertia of 15 kg•m2 (AIM Class bus)
4. Beacon receiver FOV of ±0.3°
5. Spacecraft beacon transmitter FOV of ±0.3 °

Fine Beam Steering Optics

The main function of the fine steering system is to provide the final fine correction of the quantum signal focusing onto the quantum detectors to correct for the following factors:
(a) Limitations in the satellite attitude control system to provide precise pointing of the optical systems.
(b) Correct any misalignment between the payload and the spacecraft (isolation mounts).

One of the principal requirements of any fine steering optics is that it maintains the integrity of the quantum signal. Since polarization of the photons must be accounted for, any optical design must be constrained to either maintain polarization, or accurately account for any potential changes. The current design proposed by COM DEV will ensure this requirement. The APT subsystem on the satellite tracks the ground station optical transmitters with sufficient accuracy, precision, and speed to accumulate enough single photons for a credible demonstration of QKD. As such, an apportionment of the pointing and tracking tasks is allocated between the ground station, the spacecraft bus, and the APT fine tracking control. Each of these plays a role to ensure the maximum successful photon exchange.

Initial studies have provided the analysis to size the APT subsystem to meet the user requirements. With the requirements met, the pointing and tracking optical subsystem is expected to have a mass just over 3 kg, power requirements under 12 W average and about 20 W peak, and fit in a volume of 28x20x11 cm^3.

In the current design, the APT subsystem is not coupled to the attitude determination and control system. They operate independently, and so the QKD payload is transferable to other platforms, as long as the spacecraft bus meets the required pointing and station tracking accuracy.

ADCS Requirements

The ADCS requirements imposed by the QKD mission requirements (amount of quantum key transferred per unit time) have been shown to be feasible, even in a microsatellite bus. In particular the University of Toronto's Space Flight Lab (UTIAS/SFL) has performed analysis that demonstrates the feasibility of a star tracker system to perform the coarse targeting and tracking of a ground station

The ADCS system of QEYSSat should be able to meet a pointing accuracy of ±0.3°. Further, simulations performed by UTIAS/SFL has shown the angular error jitter to be small (less than a tenth of the overall error), and has frequency components which are much smaller (< 1Hz) than the control bandwidth of the APT fine target tracking controller. Figure 3 shows the expected tracking jitter from the ADCS.

This implies that the acquisition tracking and lock can be accomplished by the APT to maximize the quantum link efficiency, using only conventional ADCS pointing and tracking mechanisms, only with special attention provided to the optics to maintain the quantum signal.

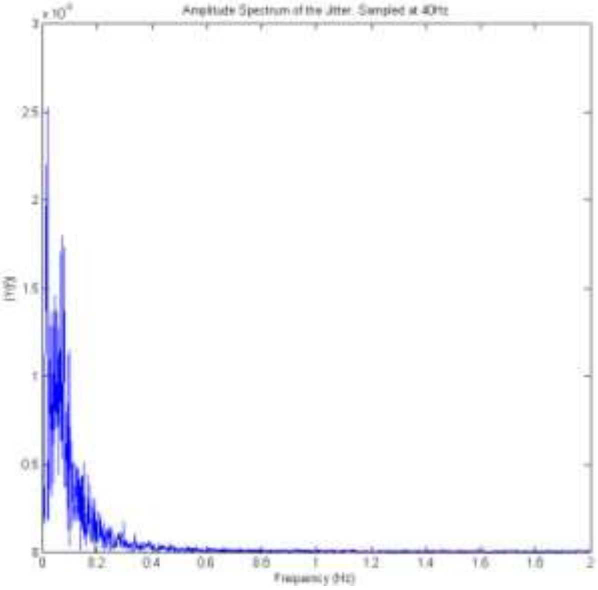

Figure 3: Spectrum of expected jitter from ADCS ground station tracking manoeuver

Conclusions

The detailed feasibility study performed by COM DEV in partnership with the Institute of Quantum Computing and in consultation with theInstitut National d'Optique (INO), UTIAS/SFL, and Neptec have shown that a microsatellite mission to demonstrate long range QKD is feasible and practical with current technology. The implementation of QKD from a satellite would open up the possibility of long range (global) secure encryption key distribution that makes use of the fundamental laws of quantum mechanics rather than relying on the impracticality of implementating mathematical algorithms (even on fast computers) to break a key. Physics prohibits interception of the key without destroying the information, providing an unprecedented level of security.

Acknowledgments

The authors would like to gratefully acknowledge the financial and technical support from the Canadian Space Agency, and scientific consultations and recommendations from the Perimeter Institute for Theoretical Physics, Waterloo, ON

References

1. W. K. Wootters and W. H. Zurek. "A single quantum cannot be cloned", Nature, 299:802–803, 1982.
2. C.R. Benn and S.L. Ellison. "La Palma night-sky brightness", New Astron. Rev., 42:503–507, 1998

3. C. Bonato, A. Tomaello, V Da Deppo, G Naletto, and P. Villoresi. "Feasibility of satellite quantum key distribution". New J. Phys., 11:045017:1–25, 2009.