Invited Paper

QEYSSAT: a mission proposal for a quantum receiver in space

T. Jennewein *[a], J. P. Bourgoin[b], B. Higgins[a], C. Holloway[a], E. Meyer-Scott[a], C. Erven[a,c], B. Heim[a,d], Z. Yan[a,e], H. Hübel[a,f], G. Weihs[a,g], E. Choi[a], I. d'Souza[b], D. Hudson[b], R. Laflamme[a]

[a] Institute for Quantum Computing, Department of Physics and Astronomy, University of Waterloo, 200 University Ave West, Ontario, Canada

[b] COMDEV Canada, Cambridge Ontario, Canada

[c] Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol, BS8 1UB, UK

[d] Max Planck Institute for the Science of Light, Guenther-Scharowsky-Str. 1/Bldg 24, 91058 Erlangen; Institute of Optics, Information and Photonics, Friedrich-Alexander University of Erlangen-Nuremberg (FAU),Staudtstr.7/B2, 91058 Erlangen; Erlangen Graduate School in Advanced Optical Technologies (SAOT),FAU, Paul-Gordan-Str.6, 91052 Erlangen, Germany

[e] Centre for Ultrahigh bandwidth Devices for Optical Systems (CUDOS), and MQ Photonics Research Centre, Department of Physics and Astronomy, Macquarie University, Sydney, NSW 2109, Australia

[f] Department of Physics, Stockholm University, Roslagstullsbacken 21, 10691 Stockholm, Sweden

[g] Institut für Experimentalphysik, Universität Innsbruck, Technikerstr. 25, 6020 Innsbruck, Austria

ABSTRACT

Satellites offer the means to extend quantum communication and quantum key distribution towards global distances. We will outline the proposed QEYSSat mission proposal, which involves a quantum receiver onboard a satellite that measures quantum signals sent up from the ground. We present recent studies on the expected performance for quantum links from ground to space. Further studies include the demonstration of high-loss quantum transmission, and analyzing the effects of a fluctuating optical link on quantum signals and how these fluctuations can actually be exploited to improve the link performance.

Keywords: Quantum cryptography, quantum key distribution, quantum communication, single photons, satellite quantum receiver, quantum entanglement, fluctuating and turbulent quantum channel

1. QUANTUM COMMUNICATION ON A GLOBAL SCALE

1.1 Encryption in the 21st Century

The secure distribution of cryptographic keys has always been a crucial element for the task of protecting and sharing important secrets. Today's algorithmic key distribution makes assumptions on the computing power of a possible hacker, which leads to fundamental problems for long-term security. Quantum key distribution (QKD) establishes highly secure keys between distant parties by using single photons to transmit each bit of the key [1]. Since single photons behave according the laws of quantum mechanics they cannot be tapped, copied or directly measured without disturbance. In this way, QKD solves the long-standing problem of securely transporting cryptographic keys between distant locations. Even if they were to be transmitted across hostile territory, their integrity could be unambiguously verified upon receipt. The huge benefit for users of such systems is the peace of mind of knowing that any attack, manipulation or copying of the photons can be immediately detected and overcome.

Ground-based QKD systems are commercially available today. However, current systems can only cover distances of up to 200 km due to photon absorption in fibre optic cables. Quantum repeaters in principle allow safely concatenating

Advances in Photonics of Quantum Computing, Memory, and Communication VII, edited by Zameer U. Hasan, Philip R. Hemmer, Hwang Lee, Charles M. Santori, Proc. of SPIE Vol. 8997, 89970A © 2014 SPIE · CCC code: 0277-786X/14/$18 · doi: 10.1117/12.2041693

several shorter quantum links and overcoming the limitations of direct long-distance quantum transmissions, and much research is devoted to solving technical hurdles that prevent deployment of these devices outside laboratory settings [2].

Satellite-based quantum communication systems offer an approach for surpassing distance limitations even with today's technology: and a truly global network for quantum communication is feasible (**Figure 1**).

1.2 The international quantum space race

The potential for satellite-based quantum communication has been noticed almost two decades ago, most notably by the group of Hughes and Nordholt, [1] at Los Alamos, USA, which led the development of a prototype system and several field tests. Other research groups around the world, including in Europe, China, Japan, Singapore, and Canada, are pursuing satellite based quantum optics or quantum communication experiments, with launches planned within a few years [4][5][6].

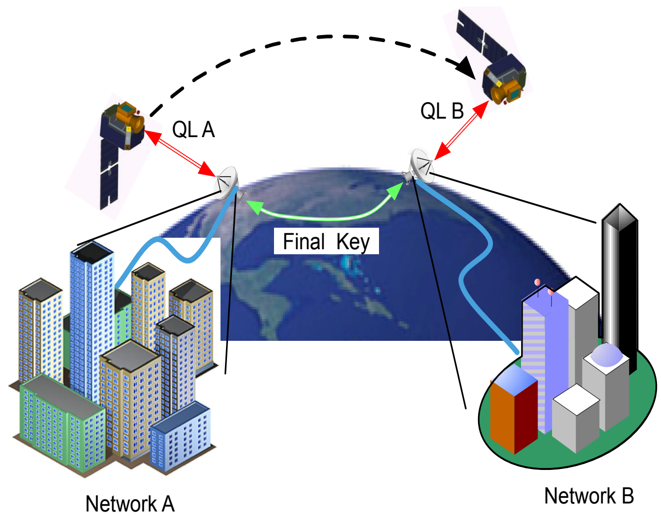

Figure 1: A satellite can be used as a trusted node to bridge the large distance gap between two city-wide networks.

2. QEYSSAT MISSION CONCEPT FOR SPACE QUANTUM SCIENCE

Over the past three years, our group has been working with industry partners to advance a proposed microsatellite mission called Quantum EncrYption and Science Satellite (QEYSSat) through a series of conceptual and technical studies funded primarily by the Canadian Space Agency (CSA). QEYSSat's mission objectives are to demonstrate the generation of cryptographic keys through the creation of quantum links between ground and space, and also to conduct fundamental science tests of long-distance quantum entanglement [7].

2.1 Proposed Technology

The main challenge is to advance existing quantum devices to make them suitable for the space environment. The QEYSSat payload will include the capability to analyze and detect single optical photons with high efficiency and accuracy. Each arriving photon will be analyzed in a polarization analyzer, and detected in single-photon detectors. Onboard data acquisition will register all detection events and record their time-stamps to sub-nanosecond precision, which will be processed at a later time on the ground.

The quantum signals will be generated in photon sources located on the ground. An optical transmitter on the ground will point the beam of photons towards the satellite. An important aspect of this mission concept in particular is to keep the complex source technologies on the ground and ensure the satellite is simple and cost-effective. It also allows implementing the quantum link using various different types of quantum sources, including entangled photons and weak coherent pulses. It should be noted that placing the quantum receiver in space does pose additional technical challenges:

firstly that the expected link losses are higher for the uplink than for a downlink [9], and secondly that the dark counts of single-photon detectors will rise due to radiation exposure in orbit [8].

The current platform for the QYESSat mission proposal is based on a microsatellite, to be located in a Low Earth Orbit (LEO) at about 600 km altitude; see Figure 2. The payload will have an optical receiver with 40 cm aperture as the main optics. Currently we are working with a team of industry partners and the CSA to build and test a compact prototype for the main elements of the quantum key distribution receiver (QKDR) compatible with the performance for QEYSSat, and the form-fit-function compatible with the satellite bus.

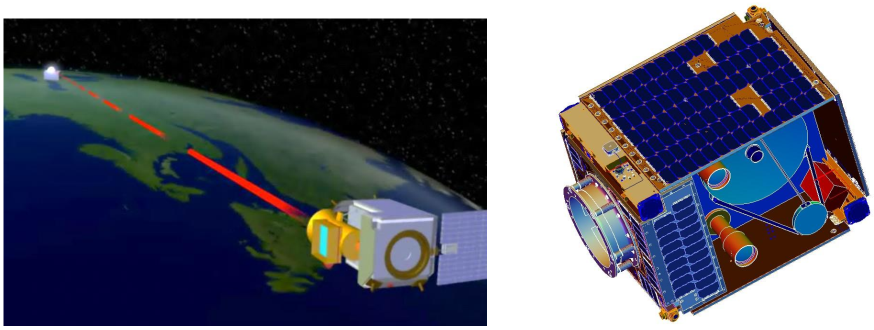

Figure 2: Left: Artist's depiction of a quantum communications link between a ground station and the satellite. Right: CAD drawing of the proposed QEYSSat spacecraft.

3. QUANTUM LINK PERFORMANCE MODELLING

The quantum signals travelling from the transmitter to the receiver will inevitably be affected by Earth's atmosphere. In order to perform a detailed analysis of the quantum link [9], we calculated the expected atmospheric absorbance under various conditions and elevation angles (see Figure 3). In addition, the beam spreading due to diffraction as well as atmospheric turbulence is modelled; background counts from city lights, moon and the sky, as well as single-photon detector performance are taken into account, and incorporated in a full quantum optical simulation of the QKD system. Satellite passes were simulated based on expected orbit parameters, and the performance for each satellite trajectory as a function of time allows calculating an average QKD key rate and QBER per month. Roughly, the upper quartile of satellite passes offer about 100 kbit of secure key – of course, the results vary with parameters and assumptions. A comparison of the results for some different wavelengths and types of quantum sources is shown in Table 1.

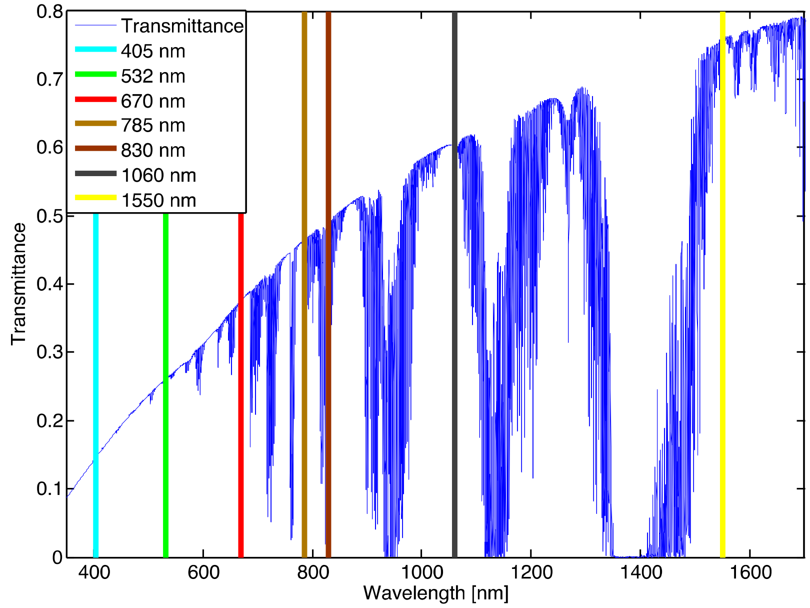

Figure 3: Modeled atmospheric transmittance at a typical rural location, for propagation at zenith. The vertical lines represent wavelengths of commercially available laser systems we considered for the optical quantum link. See [9] for full details.

Table 1: Simulated performance computed for satellite to ground QKD, based on an altitude of 600 km. WCP means a Weak Coherent Pulse source of photons based on an attenuated laser. See [9] for details.

Wavelength (nm)	Secure key length obtained for the upper quartile satellite pass (kbit)			
	Downlink, WCP source	Uplink, WCP source	Downlink, entangled photon source	Uplink, entangled photon source
405	68.5	3.5	6.2	0
532	264.5	33.1	119.3	12.1
670	465.6	87.7	324.7	67.4
785	458.3	111.3	272.9	75.7
830	317.3	82.1	136.1	39.7
1060	175.4	67.6	21.8	8.1
1550	123.9	94.8	12.8	14.4

4. EXPERIMENTAL VERIFICATION OF CONCEPTS

First, we will present an experimental study implementing quantum transmission under very high losses. Our system achieves quantum transmission above 50 dB channel loss, almost two orders of magnitude above the level of many reported systems. We used an advanced quantum source to create photons with very precise timing and high quality in the visible optical spectrum, allowing us to suppress background noise through careful timing analysis. Secondly, we will present our study on quantum transmissions over fluctuating quantum channels. We performed an extensive experimental and numerical study on the fluctuation statistics measured in free-space quantum links on the ground, as well as laser transmission with satellites.

4.1 Quantum Key distribution over a channel with 57dB transmission loss

We implemented a laboratory-based experiment in order to demonstrate the design and viability of a QKD system capable of operation under the high channel losses of up to 57 dB expected for a ground to satellite uplink. Our setup satisfies the challenging requirements for an uplink of quantum keys for QEYSSat, whose attenuation is expected to be 40dB or higher.

The experimental setup, as shown in full detail in [10], included a high-speed source of weak coherent pulses operating at a rate of 76 MHz, each pulse with about 10 picoseconds pulse duration. In order to implement decoy-state QKD, each individual pulse was attenuated to about 0.5 photon/pulse for signal states, and 0.1 photon/pulse for decoy states, modulated in polarization and intensity using fast electro-optical switches. The QKD receiver system that represents the satellite based QKD payload was a polarization analyzer with a passive basis choice, and utilized ultra-low-noise silicon photon detectors, with only about 50 dark-counts per second. An elaborate algorithm achieved synchronization between source and receiver, in order to minimize the coincidence-timing window and thereby suppress background signals. The main experimental results are shown in Figure 4, and demonstrate a quantum transmission up to channel losses of 57 dB, hence validating the basic concept of a quantum uplink to a satellite.

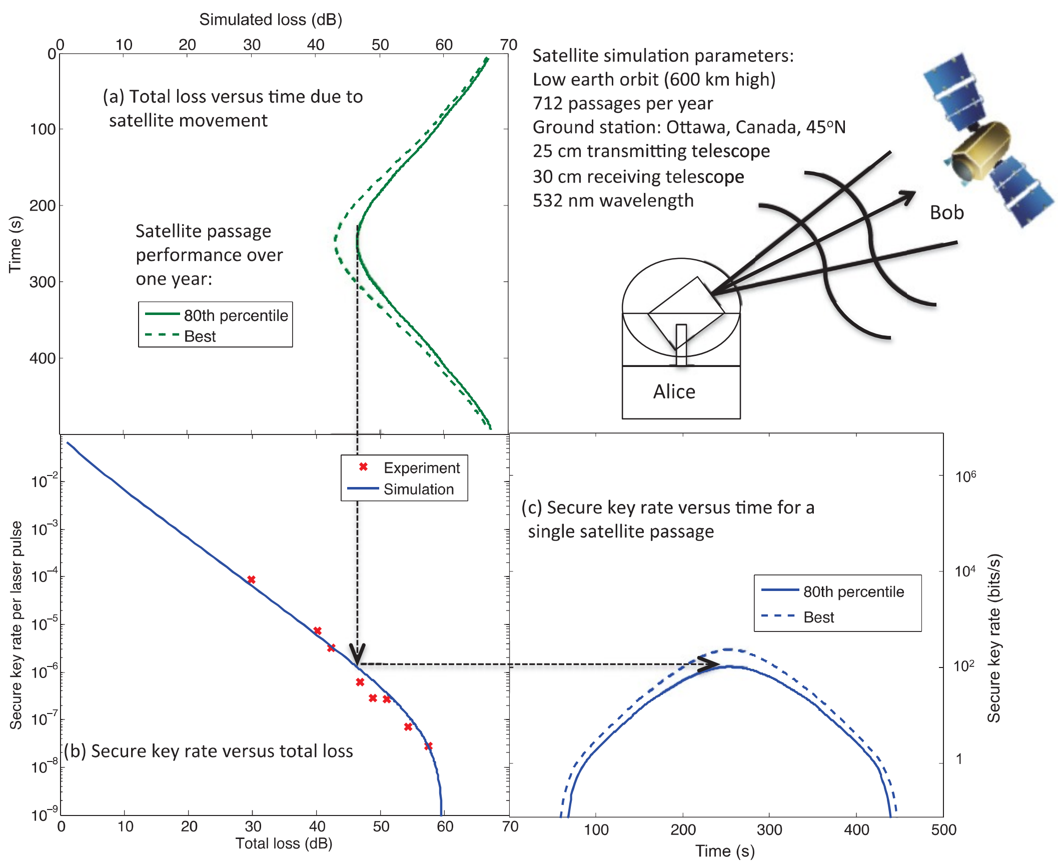

Figure 4: Experimental test of a high-loss quantum channel, emulating the performance of a quantum-uplink to a satellite based receiver in low-earth orbit (LEO). (See [10] for details.)

4.2 Improving the quantum transmission over a fluctuating free-space link

Due to atmospheric turbulence and other beam instabilities such as pointing accuracy, the quantum channel will fluctuate inherently when crossing considerable distances in free space. We studied the effects of beam fluctuations in a quantum channel both in simulation as well as experiment, in order to verify how the fluctuations over time may affect the QKD performance. We analyzed both weak coherent pulsed sources (WCP), and entangled photons sources. The experimental data for a typical transmission of one photon from an entangled pair, after travelling a horizontal distance of about 1 km, is shown in Figure 5. We conducted a careful analysis of the fluctuation statistics, and were able to show that for weaker turbulence, in good approximation the beam follows the expected log-normal distribution [11]. However, at stronger, artificially induced atmospheric turbulence, the distribution became more erratic and deviated from the log-normal distribution.

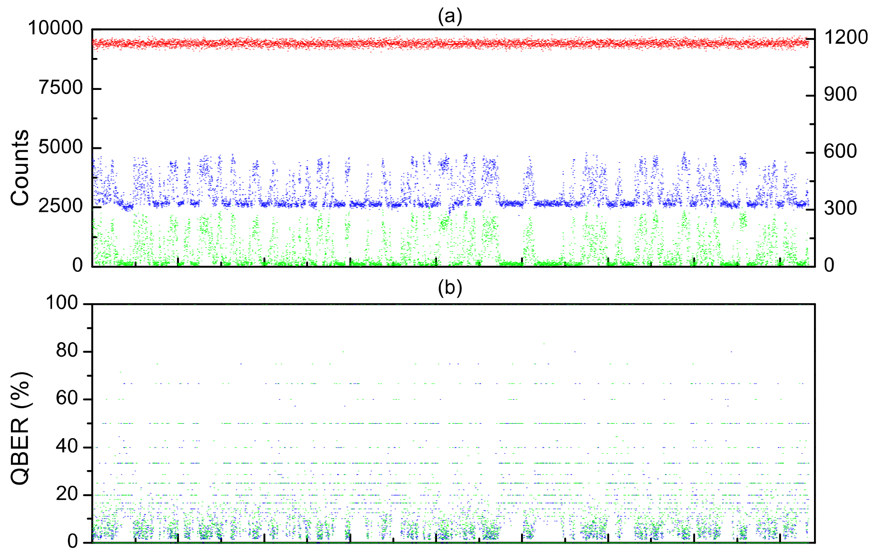

Figure 5: Fluctuations of count rates (a) and the QBER (b) for transmission of entangled photons over a 1 km free-space channel. Red: single counts in Alice; Blue: Single counts in Bob; Green: coincidences. (See [11] for more details.).

4.2.1 Suitability of decoy state QKD for a fluctuating channel

From our results we were able to show that the decoy state method in QKD [12] may break down at low average channel losses, because the basic assumption that the channel is linear and constant does not apply, and there are different effective transfer probabilities for the stronger signal pulses than for the weaker decoy pulse. The decoy state protocol may therefore require some adaptation. However, at higher channels losses (> 20dB), we found that this effect is neglibile, as the overall very low transmission probability provides sufficiently scarce sampling of the photons in the different pulse intensities, that the average transmission model applies. Therefore, in the situation of a satellite link, where transmissions losses are expected to be 30dB and higher, decoy state QKD can be used directly.

4.2.2 Improving a quantum link using a data filter in post processing

In a further, more detailed analysis we established that at very high transmission losses the link fluctuation could even be exploited in order to improve quantum transmission quality, during post processing of the data. As outlined in Table 2, by applying a transmission threshold-filter to the data measured using an entangled photon link, we are able to improve the number of secure key bits by almost 25%. We performed additional simulations that indicate that using this threshold-filter may even generate a secure key for satellite passes at high loss (or with high background noise), which may have been useless otherwise. While it is not obvious that applying such a filter would affect the security of a QKD system, it is still under investigation if, and how, the security proofs for QKD may need to be adapted.

Table 2: Observed QKD analysis for the data from the transmission experiment of Figure 4. No SNR filter: all signals used. Above SNR filter: only signals are considered which come with signal strengths above the optimal threshold value. Below SNR filter: the (expectedly low) quality of the counts that were rejected by the filter. (See [11] for full details.)

Scenario	raw key	sifted key	secret key	f	qber
No SNR filter	535,530	259,855	78,009	1.2697	5.51%
Above SNR filter	466,441	226,279	97,678	1.2202	4.30%
Below SNR filter	69,089	33,576	-	-	13.77%

5. SUMMARY

To summarize, we have presented the proposed QEYSSat mission, which aims to test quantum key distribution and quantum entanglement sciences using a quantum receiver in space. In order to show the viability of this mission concept, we have outlined the results from several recent theoretical and experimental studies, including a comprehensive link performance analysis, QKD experiments over high transmission losses and over a rapidly fluctuating channel. The proposed QEYSSat mission continues to be advanced, with a CSA funded project to build and test a compact prototype for the main elements of a microsatellite-compatible QKD receiver currently in progress.

ACKNOWLDEGEMENTS

This work is currently supported by the Canadian Space Agency, FedDev Ontario, NSERC, CIFAR, CFI Innovation Fund, Ontario Government MEDI ORF and ERA,. An initial quantum microsatellite mission feasibility study had been funded by Defence Research and Development Canada.

REFERENCES

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. "Quantum cryptography." Rev. Mod. Phys., 74(1):145, (2002).

[2] N. Sangouard, C. Simon, H. Riedmatten, and N. Gisin. "Quantum repeaters based on atomic ensembles and linear optics." Rev. Mod. Phys., 83:33–80, (2011).

[3] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. "Practical free-space quantum key distribution over 1 km." Phys. Rev. Lett., 81(15):3283–3286, (1998).

[4] R. Hughes and J. Nordholt. "Refining quantum cryptography." Science, 333(6049):1584–1586, (2011).

[5] T. Jennewein and B. Higgins. The quantum space race. PHYSICS WORLD, 26(3):52–56, (2013).

[6] "The solace of quantum", The Economist, May 25, (2013).

[7] D. Rideout, T. Jennewein, et al. "Fundamental quantum optics experiments conceivable with satellites-reaching relativistic distances and velocities." CLASSICAL AND QUANTUM GRAVITY, 29(22):224011, (2012).

[8] M. A. Krainak, A. W. Yu, G. Yang, S. X. Li, and X. Sun. "Photon-counting detectors for space-based laser receivers." SPIE Proceedings, 7608(760827):1, (2010).

[9] J. P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Huebel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein. "A comprehensive design and performance analysis of low earth orbit satellite quantum communication." NEW JOURNAL OF PHYSICS, 15:023006, (2013).

[10] E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Huebel, and T. Jennewein. "How to implement decoy-state quantum key distribution for a satellite uplink with 50-db channel loss." PHYSICAL REVIEW A, 84(6):062326, (2011).

[11] C. Erven, B. Heim, E. Meyer-Scott, J. P. Bourgoin, R. Laflamme, G. Weihs, and T. Jennewein. "Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere." NEW JOURNAL OF PHYSICS, 14:123018, (2012).

[12] H.-K. Lo, X. Ma, and K. Chen. "Decoy state quantum key distribution." Phys. Rev. Lett., 94:230504, (2005).