*SPIE Quantum-Physics-Based Information Security Conference*
*22-25 September 2014*

# The NanoQEY Mission: Ground to Space Quantum Key and Entanglement Distribution Using a Nanosatellite

T. Jennewein[1*], C. Grant[2], E. Choi[1], C. Pugh[1], C. Holloway[1], JP. Bourgoin[1], H. Hakima[2], B. Higgins[1], R. Zee[2]

[1] *Institute for Quantum Computing, and Department of Physics and Astronomy, University of Waterloo*
[2] *Space Flight Laboratory, University of Toronto Institute for Aerospace Studies*
** Corresponding Author: thomas.jennewein@uwaterloo.ca, 519-888-4567 x37485*

## Abstract

The NanoQEY (Nano Quantum Encryption) Satellite is a proposed nanosatellite mission concept developed by the Institute for Quantum Computing (IQC) at the University of Waterloo and the Space Flight Laboratory (SFL) at the University of Toronto Institute for Aerospace Studies (UTIAS) that would demonstrate long-distance quantum key distribution (QKD) between two distant ground stations on Earth using an optical uplink. SFL's existing and proven NEMO (Nanosatellite for Earth Monitoring and Observation) bus forms the baseline spacecraft for NanoQEY, with a QKD receiver payload designed by IQC. The primary objective of the NanoQEY mission would be to successfully distribute at least 10 kbit of secure key between two optical ground stations, where the satellite acts as a trusted node. The secondary mission objective would be to perform Bell tests for entangled photons between ground and space. We designed a compact QKD receiver payload that would be compatible with the mass, volume, power and performance constraints of a low-cost nanosatellite platform. The low-cost rapid schedule "microspace" approach of UTIAS/SFL would allow for the proposed NanoQEY mission to be developed in 2.5 years from project kick-off to launch of the spacecraft, followed by a one-year on-orbit mission.

## Introduction

Quantum key distribution (QKD) establishes highly secure keys between distant parties by using single photons to transmit each bit of the key. According to the laws of quantum mechanics the photons cannot be tapped, copied or measured without leaving tell-tale signs of observation. Such systems provide the peace-of-mind knowledge that any eavesdropping can be immediately detected and addressed.

Terrestrial QKD networks using fiber optic cables or free-space atmospheric transmission are in operation today for both research and niche commercial applications such as secure bank transactions and data transfers. There are, however, some fundamental physical constraints that would require the implementation of a complementary solution for distances beyond a few hundred kilometers. Even with the best-case ultra-low attenuation fiber optic cables, light will suffer exponential signal losses as well as polarization and chromatic dispersion as it is transmitted through the material. Conventional signal amplifiers cannot be used because doing so would effectively constitute an observation of the quantum state of the single photons, thereby invalidating the very quantum mechanical techniques upon which QKD depends for the detection of attack or manipulation. While transmission losses for free-space QKD within the atmosphere can be lower than in optical fiber, such links are limited to line-of-sight and are therefore subject to geographical constraints such as local landscape and ultimately the curvature of the Earth.


**Figure 1: A Satellite Based Trusted Node Would Enable a Bridge between Two Terrestrial Quantum Communications Networks over Long Distances**

Satellites in Earth orbit represent the only way using currently feasible technology to provide global-distance QKD services, and several approaches are studied internationally [1]. In the simplest configuration, satellites could be used as complementary trusted nodes to bridge the distance between geographically dispersed QKD ground networks, for example, between cities or continents as shown in Figure 1. In the future, quantum repeaters may be developed which could establish long range quantum entanglement, however, there will still be a role for satellites, as the currently most optimistic quantum repeater protocols may still only facilitate distances up to about 1,000 km [2] on terrestrial links, while very recent results show that a quantum receiver based on satellite links and quantum memories on ground are able to reach 10,000 km and beyond [3].

## Objectives of the Mission

The NanoQEY (Nano Quantum Encryption) Satellite is a proposed nanosatellite mission concept developed by the Institute for Quantum Computing (IQC) at the University of Waterloo and the Space Flight Laboratory (SFL) at the University of Toronto Institute for Aerospace Studies (UTIAS) that would demonstrate long-distance quantum key distribution (QKD) between two distant ground stations on Earth using an optical uplink. For a successful QKD demonstration, quantum signals must be received with a low enough error rate to exclude an eavesdropper while having sufficiently large photon numbers to account for statistical fluctuations [4]. Success for a single key generation requires a full QKD protocol that includes timing analysis, basis reconciliation, error correction and privacy amplification. The primary objective of the NanoQEY mission is to successfully distribute at least 10 kbit of secure key between two optical ground stations separated by at least 400 km during the lifetime of the mission.

Since the quantum link itself would be fully characterized it could 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 it can only be tested at over relatively short (<300 km) distances terrestrially. The secondary objective of the NanoQEY mission is to perform a Bell test for entangled photons separated by at least 400km, where one photon shall be measured on ground, the other on the satellite.

## Mission Architecture

The existing and proven NEMO (Nanosatellite for Earth Monitoring and Observation) bus developed by SFL would be the baseline spacecraft for NanoQEY, with a QKD receiver payload designed by IQC. As shown in Figure 2, the satellite would have a volume of approximately 40×26×20 $cm^3$ and, through the use of a lightweight magnesium alloy structure, would have a total mass of only 15 kg, of which 7.5 kg would be occupied by the QKD payload. Onboard computers and radios, like most units onboard, would use designs with significant flight and design heritage to minimize technical, financial and schedule risk. Peak power generation would be 24 W with a battery capable of providing up to 20 W to the payload in eclipse.

NanoQEY would be launched into an orbit with an initial altitude between 400 km and 600 km and a mean LTAN (local time of the ascending node) of noon ± 2.5 hours, the latter being driven by the need for regular eclipses as the key transfers can only be done at night. The mission would employ the existing ground station at SFL for TT&C (telemetry, tracking and control) and at least two optical ground stations separated by a minimum distance of 400 km for demonstrating the establishment of a secure key between them via QKD. Depending on the locations of the optical ground stations two or three dark passes should be possible per night, however, only passes with clear skies can be used.

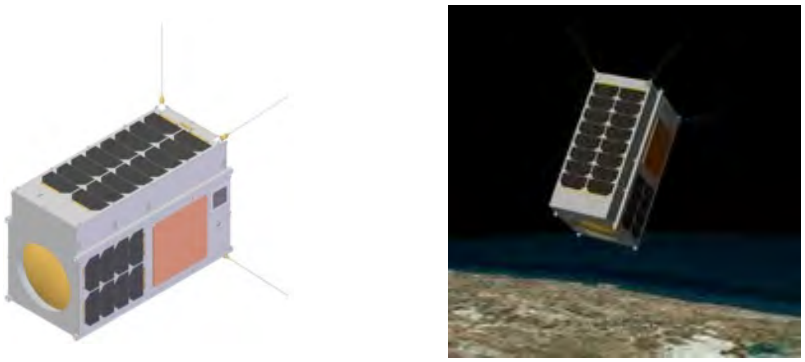

**Figure 2: Exterior View of NanoQEY (Left) and Spacecraft in Orbit (Right)**

## Concept of Operations

The minimum mission duration would be one year from launch. This is based on the design lifetime of the SFL NEMO bus while providing sufficient time for commissioning and achieving both the primary mission – demonstrating long-distance secure key distribution – as well as the secondary mission – performing Bell tests for entangled photons. During nominal operations, when the NanoQEY satellite is in daylight it would be oriented for optimal power generation and thermal control while protecting the quantum receiver payload optics from the Sun. As the satellite approaches an optical ground station, it will slew to point the tracking beacon towards where the station will appear on the horizon. The single photon quantum link would be acquired and the initiation of the quantum protocol would begin, during which the resulting data would be stored for later downlink to the SFL TT&C ground station.

In order to securely distribute encryption keys, the NanoQEY satellite will act as a "trusted node" in which the keys would be held during operations. The satellite would create a secure key between itself and Ground Station A during one or more passes, and then create another secure key between itself and Ground Station B during one or more passes. 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 themselves.

The proposed NanoQEY mission architecture is based on a quantum photon uplink from the ground to the satellite in order to minimize the complexity of the spacecraft and payload. Having the photon source at the ground stations would also allow for flexibility and future upgrades. The NanoQEY satellite would carry the photon polarization detectors and the encryption key management software. Crucial systems for the mission include laser beacon sources and receivers (at both ends) for link acquisition and tracking, polarization monitoring and compensation, and clock alignment for the precise time-tagging of the photons is also essential. In addition to the quantum channel, a non-secure classical RF communications link is also required for the key exchange.

## QKD Payload Design

For the proposed NanoQEY mission, IQC has designed an innovative compact QKD payload that would be compatible with the mass, volume, power and performance constraints of a low-cost nanosatellite platform. One of the major simplifications of the payload was to remove the necessity for a fine pointing system. By using large collection optics and narrowband filters, it is possible to increase the field-of-view (FOV) so as to collect the quantum signal within the nominal attitude determination and control performance capabilities of the SFL NEMO spacecraft bus. Figure 3 provides a block diagram and solid model of the NanoQEY payload, and Figure 4 shows an initial setup at IQC of a functional prototype representative of the NanoQEY payload.

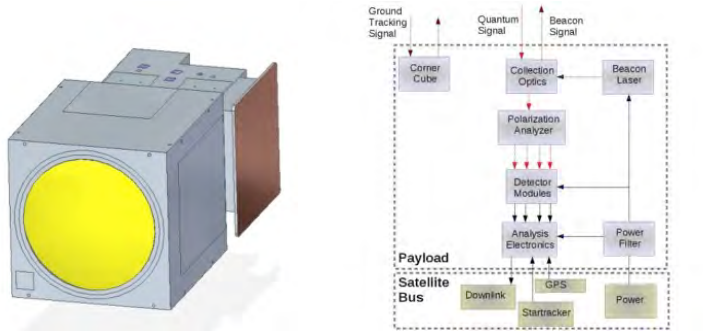


**Figure 3: Payload Solid Model (Left) and Block Diagram (Right). Solid model shows outer casing (grey), collection lens (yellow) and radiator (brown).**

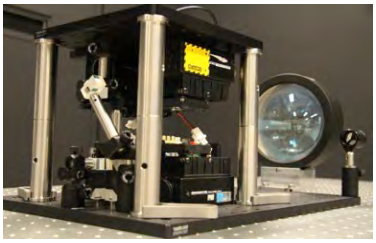

**Figure 4: Functional Test Setup Representative of NanoQEY Payload**

## Attitude Determination and Control

The attitude determination and control needed to accurately point the payload (±0.4° with 95% confidence) would be provided by a star tracker and a set of three reaction wheels, all of which have significant heritage. SFL has performed analyses that demonstrate the feasibility of the NEMO star tracker system to perform the required tracking of an optical ground station. Optional upgrades to the ADCS algorithms, sensors and actuators could be considered to further improve the fine pointing mode performance of the NanoQEY satellite.

## Estimated Performance of the Mission

Using our developed approach and methods to estimate the performance for a ground to space quantum link [4], we studied the amount of quantum key that could be transferred in the case of NanoQEY. In particular, because the NanoQEY payload would have a large field of view, the quality of the ground station site is crucial and is ideally located far from light pollution, and has very clear air. Furthermore, the operation of NanoQEY would be restricted to nights without Moon. Assuming the satellite receiver has an aperture of 150 mm, operates at the optimal wavelength of 639nm, and the ground transmitter has 500 mm aperture, is located at sea level altitude, operates a weak-coherent pulse source with a rate of 300 MHz, the system is expected to have an average of 3 usable passes per month, which combined would generate about 10 kbit of secure key. These key rates as well as the number of successful passes can be improved by elevating the transmitter to higher altitudes, for example at 2400m altitude the system is expected to have up to 12 successful passes per month.

## Launch Opportunities

To date, SFL has arranged the launches of dozens of nanosatellites and microsatellites and has an excellent business relationship with many launch providers worldwide, all of whom routinely launch into the type of orbit required by the proposed NanoQEY mission. As a result, finding a suitable launch opportunity for NanoQEY is not expected to be a significant issue. Furthermore, since these launch providers have all worked with SFL's launch separation systems (XPOD Duo) in the past, the integration of the NanoQEY satellite onto their launch vehicles and into their manifests is expected to be straightforward.

## Programmatics

The low-cost rapid schedule "microspace" approach of UTIAS/SFL would allow to develop the proposed NanoQEY mission in 2.5 years from project kick-off to launch of the spacecraft, followed by a one-year on-orbit mission. Figure 5 shows a notional project schedule for NanoQEY.

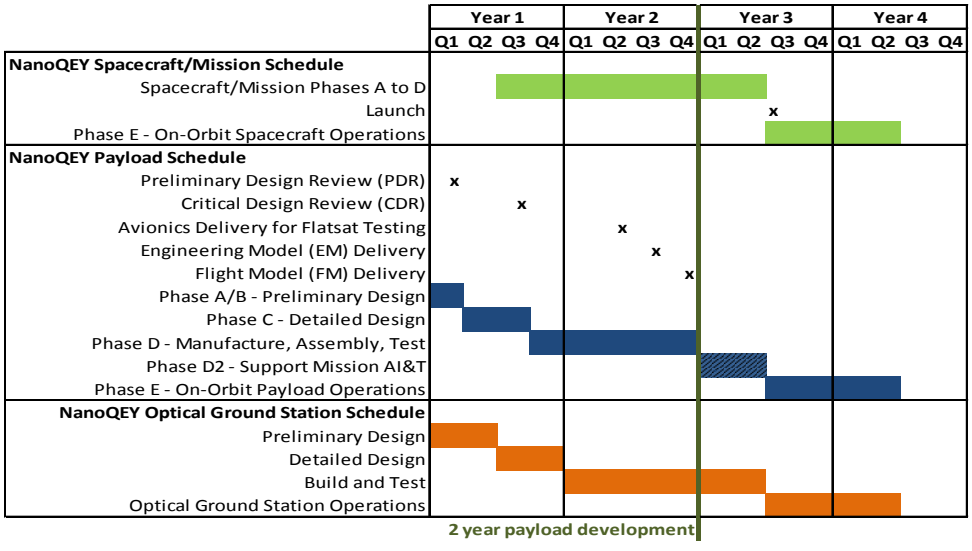


**Figure 5: Notional NanoQEY Mission Project Schedule**

## Conclusion

A feasibility study performed by IQC and SFL has shown that a nanosatellite mission to demonstrate long-distance QKD is feasible and practical with current technology. NanoQEY would employ SFL's existing and proven NEMO

bus with an innovative compact QKD receiver payload designed by IQC that would be compatible with the mass, volume, power and performance constraints of a low-cost nanosatellite platform. If executed using the low-cost rapid schedule "microspace" approach of UTIAS/SFL, the proposed NanoQEY mission could be developed in 2.5 years from project kick-off to launch of the spacecraft, followed by a one-year on-orbit mission.

## Acknowledgements

The authors gratefully acknowledge the financial support of the Federal Economic Development Agency for Southern Ontario (FedDev Ontario) administered by Communitech, NSERC, MEDI Ontario, CIFAR.

[1] T. Jennewein, B. Higgins, "The quantum space race." PHYSICSWORLD, 26(3):52–56 (2013).
[2] Neil Sinclair, Erhan Saglamyurek, Hassan Mallahzadeh, Joshua A. Slater, Mathew George, Raimund Ricken, Morgan P. Hedges, Daniel Oblak, Christoph Simon, Wolfgang Sohler, and Wolfgang Tittel, "Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control" Phys. Rev. Lett. 113, 053603 (2014).
[3] K. Boone, J.-P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon, "Global quantum communication with satellites and quantum repeaters" in preparation, (2014).
[4] J-P Bourgoin, E. Meyer-Scott, Brendon L. Higgins, B. Helou, Chris Erven, Hannes Huebel, B. Kumar, D Hudson, Ian DSouza, Ralph Girard, Raymond Laflamme, Thomas D. Jennewein, "A comprehensive design and performance analysis of low earth orbit satellite quantum communication." New Journal of Physics 15(2), 023006 (2013).