IAC-19-B4.2.14.x48880

Fundamentally Secure Data with the Help of Quantum Key Distribution on CubeSats

Roland Haber[a]*, Julian Scharnagl[a], Klaus Schilling[b], Harald Weinfurter[c], Christoph Marquardt[d], Florian Moll[e], Matthias Grünefeld[f], Peter Freiwang[c], Wenjamin Rosenfeld[c], Ömer Bayraktar[d], Benjamin Rödiger[e], Christopher Schmidt[e]

[a] *Zentrum für Telematik, Magdalene-Schoch-Str. 5, 97074 Wuerzburg, Germany, roland.haber@telematik-zentrum.de*
[b] *Informatics VII: Robotics and Telematics, Julius-Maximilians-University Wuerzburg, Am Hubland, 97074 Würzburg, Germany, schi@informatik.uni-wuerzburg.de*
[c] *Ludwig-Maximilians-Universität, Munich, Germany*
[d] *Max-Planck Institute for the Science of Light, Erlangen, Germany*
[e] *German Aereospace Center (DLR), Institute of Communications and Navigation, Weßling / Oberpfaffenhofen, Germany*
[f] *OHB System AG, Manfred-Fuchs-Straße 1, 82234 Weßling / Oberpfaffenhofen (Munich Metropolitan Area), Germany*
* Corresponding Author

Abstract

With the uprise of worldwide satellite communication networks, data security is a critical issue. This issue is being addressed in the QUBE project, which proposes a CubeSat for quantum cryptography experiments. The satellite and its subsystems are currently being developed and will be used for the downlink of individual photons, or strongly attenuated light pulses, containing encoded quantum information, which can then be employed for the exchange of encryption keys. The launch of the 3U Nanosatellite is planned for early 2020. It will be built using the UNISEC-Europe standard, which has demonstrated to be able to provide a robust structure for increased reliability in CubeSat missions. In addition to state-of-the-art reaction wheels for precision pointing, the satellite will be bringing the OSIRIS optical downlink system from DLR as well as two dedicated payloads for testing components required for quantum key distribution. A sequence of numbers will be created by a miniaturized quantum random number generator (QRNG), which will be used to set the quantum states of the light pulses. These pulses will then be downlinked to the optical ground station (OGS) at DLR in Oberpfaffenhofen, Germany. The ground station is also equipped with the corresponding components for receiving individual quantum states. In addition, the random numbers will be made available via an RF downlink. The photon states received by the optical ground station will then be compared to the previously generated numbers. Due to the underlying quantum mechanics, any attempt of reading the quantum states will alter them, which makes interceptions easily detectable. These quantum key distribution experiments will evaluate whether secure communication links are possible even on a CubeSat scale. A major challenge for building the proposed CubeSat is the attitude determination and control system that will provide precise pointing. This work will outline detailed mission requirements as well as the chosen subsystems for tackling these challenges in order to achieve a successful mission and prepare for future data security.
Keywords: CubeSat, QKD, QRNG, Quantum Encryption

1. Introduction

When using encryption for the exchange of sensitive information, two major problem areas have to be considered. First, the method by which encryption keys are generated, and second, the approach for exchanging these keys between the communication partners.
While encryption keys with extensive lengths can be generated, the underlying algorithms are still prone to reverse engineering. Additionally, even if secure keys can be generated, the manner in which these keys are shared between the participating parties has to be thoroughly designed, in order to minimize potential interceptions. Both of these problem areas are addressed by quantum key distribution (QKD). This paper will explain how QKD can provide a fundamentally secure alternative to current encryptions and explain how it is employed in the QUBE CubeSat.

2. Quantum Key Distribution

QKD encompasses the generation and distribution of quantum keys for the encryption and decryption of existing communication channels. Two or more parties can share this truly random key and apply it to their communications with provable security. [1]

2.2 QKD Technology

While most encryptions rely on asymmetric cryptography, QKD is based on a quantum random number generator (QRNG) for the generation of a number sequence, which is used to set the quantum states of photons. Then these photons are transmitted using optical channels, such as fiber or laser.

Interceptions on this transmission channel will be easily detectable due to the underlying quantum mechanics, which dictate that any observation of quantum states also causes these states to be altered [2]. Using this principle in combination with a one-time pad implementation, fundamentally secure keys can be sent to multiple communication partners, and then be applied to traditional communication channels. Distributing the keys to distant locations is however limited by the transmission range of the optical fibers or the visible range of the lasers involved. To alleviate this issue, satellites can be used to distribute keys from orbit. [3]

2.2 QKD from Space

Using a satellite to distribute encryption keys has the advantage of being able to cover a broad area at once. Especially low Earth orbit (LEO) satellites are able to reach multiple targets on the ground with a much smaller attenuation compared to geostationary satellites. The basic QKD principle is depicted in Fig. 1. Conservative communication channels already exist between Alice and Bob, however unsecure.

Using traditional encryption methods, such as Elliptic-curve cryptography (ECC) [4], Alice and BOB are able to safely communicate in most scenarios. Since these traditional encryption methods are based on mathematical algorithms though, given sufficient computing power they can potentially be cracked. Therefore the original communication channel can be secured by a quantum key, which is distributed from a satellite to each participant. The evesdropper, Eve, is now unable to decipher the communication between Alice and Bob, and also unable to reverse engineer the encryption method. In case Eve tries to intercept the quantum channel between each partner and the satellite, the underlying quantum physics ensure that any interception is easily detectable on ground by measuring the quantum bit error rate (QBER). Therefore, if either Alice or Bob discover that Eve has succesfully intercepted the quantum key exchange, then the key can be discarded and a new one can be generated [5].

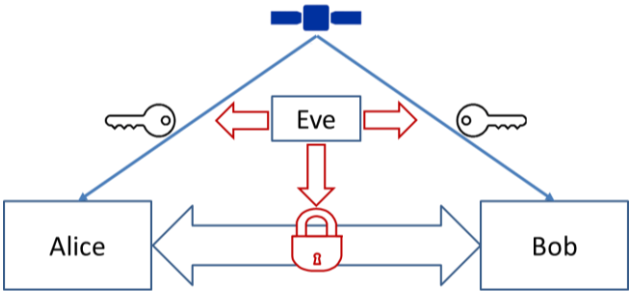

Fig. 1. QKD from Space [3]

In order to maximize QKD coverage, the spatial and temporal resolution of the satellites can be increased by employing a network of multiple satellites in a constellation or formation.

2.3 QKD on CubeSats

The first successful QKD demonstration mission in space was the Chinese MICIUS satellite, which is a 631 kg space craft [6]. In order to make QKD feasible on a global scale, many satellites have to be launched and flown in a constellation. By employing CubeSats, a large constellation can be placed in orbit much more rapidly and cost-effectively than by using traditional larger satellites [7]. However, the process of miniaturizing all the components for QKD is challenging. Implementing QKD protocols requires preparation and measurement of states at the quantum limit, such as detection of single photons or small phase variations comparable to vacuum fluctuations. With recent advancements of integrated photonics technologies, as well as of detectors, the required components can in principle be miniaturized to fit even into very small satellites, such as CubeSats [8, 9].

In addition to the necessary miniaturization of the QKD components, satellite components, such as the attitude determination and control system (ADCS) also have to made small enough to fit into the limited mass, volume, and power budget of a CubeSat, while still meeting the pointing precision required by the laser module. The integration and operation of additional modules, such as the communication laser and more precise attitude sensors and actuators, represents another challenge.

3. The QUBE CubeSat

QUBE is being developed as a 3U+ satellite, as determined by the CubeSat Design Specifications (CDS) [10]. The satellite houses its main subsystems in the bottom unit. This includes the on-board computer (OBC), ADCS including the six reaction wheels, communication module (COMM), and the electronic power system (EPS). All of these subsystems are connected to a common backplane, which provides

access to the UNISEC-Europe system bus [11]. The UNISEC-Europe bus has been used is multiple past missions and has proven to be a reliable and almost entirely cable-free solution for connecting the CubeSat subsystems. The UWE-3 satellite has been operational in LEO since 2013, exclusively using COTS components on the UNISEC architecture. Using a modular backplane scheme, the satellite design is optimized towards size, mass, and energy efficiency. Due to redundant power and data paths as well as a software-based radiation shielding, the UNISEC-Europe system bus is providing a very robust and reliable alternative to traditional CubeSat designs.

Fig. 2. QUBE CubeSat Design [3]

Extending up from the backplane, the fron access board (FAB) features the UNISEC connections along the z-axis towards the top of the satellite. This allows for the same plug & play connectivity as the lower backplane. The middle unit of the satellite houses the two quantum payloads by the Ludwig Maximilian University in Munich (LMU) [12] and the Max Planck Institute for the Science of Light (MPL) [13] for the generation of quantum signals and of quantum random numbers respectively, as well as a triplexer for the connection of the quantum payloads to the optical downlink system. Aside from the UNISEC bus, the quantum payloads are also connected to the DLR [14] Optical Space Infrared Downlink System (OSIRIS), which is located in the top unit. Using multiple optical fibres and the triplexer, OSIRIS is able to have inputs from both quantum signal sources. Additionally in the top unit is a star tracker that will provide precise attitude information for space craft pointing during overpaths. The proximity of the star camera to OSIRIS is crucial for ensuring the validity of the attitude data with regard to the laser module. Ultimately, the achievable limit for the transmission of a secure key is determined by the signal-to-noise ratio of the quantum signal compared to the detector noise and scattered light noise. Therfore, any light scattering from the satellite or other sources has to be minized in order to conform to the extremely low light requirements for QKD. Additonally, night time overpasses are preferred for the same reason. In order to achieve recurring experiment times, a sun-synchronous orbit (SSO) would be ideal. An SSO has the advantage of a point on Earth passing the orbital plane at the same local time each day. It is created by choosing the right inclination for the corresponding altitude, so that the change of the longitude of the ascending node rotates around Earth in exactly one year. By selecting a suitable launch window for this SSO, the required Local Time of Ascending Node (LTAN) can be chosen in order to achieve an orbit, where flyovers at the optical ground station repeat at the same time of night.

Since the limited power budget does not allow for full-scale temperature stabilization of critical components, large temperature drifts of several 10° C have to be considered. This impacts their mechanical stability as well as possible wavelength drifts and drifts of the birefringence, influencing the polarization [15]. Hermetical packages are employed in order to assure the required dry gas atmosphere for the operation of certain components, such as vertical cavity surface emitting lasers (VCSEL). This also helps reducing problems with outgassing and contamination of optical surfaces.

Communication between all subsystems and payloads is handled by the COMPASS protocol, which provides a multi-level structure for turning every component into a globally accessible node, while also offering a wide range of common services to share the available functionalities throughout the satellite. COMPASS includes various functions to effectively tackle typical challenges faced with in subsystem communications, such as delay, real-time requirements, and dynamic and manual routing options inside a network. In-orbit software updates for each subsystem will also be tremendously smoother with the combination of the UNISEC bus and the COMPASS protocol [16].

During this mission, tests of the functionality of individual components as well as of their interactions, are being performed. This includes tests of the satellite attitude determination and control system as well as the optical communication system. Therefore, special measurements of the performance of the optical channel and the optical terminal are planned. Additionally, the

performance of the QRNG will be measured. An on-board payload controller (PCON) is used for payload operations and will also be employed for analyzing the random bits on the satellite. For this first testing phase, the BB84 scheme will be employed as quantum cryptography protocol by the LMU using a wavelength of 850 nm. The MPL with support by the OHB System AG will be testing the performance of a QRNG and experiment with the detection of weak phase modulated signals in the 1550 nm range.

The OSIRIS payload is a modified version of the original module, which was designed for high data rate laser communication from space. The earlier iterations have already been successfully operated on the BIROS and Flying Laptop satellites [17]. These satellites had a much bigger mass, volume, and power budget available though, so DLR has since developed the OSIRIS4CubeSat (O4C) version, which can fit in 0.3 units and weighs around 300g. The downlink data rate is still above 100 Mbit at a power level of 8 W. This version will also be flying on the Telematics Earth Observation (TOM) mission. For QUBE, the focus lies on the transmission of unmodulated light signals, thus the OSIRIS4QUBE (O4Q) version will be slightly extended in order to house the two input wavelengths from the quantum payloads. The goal is to send light pulses to the optical ground station (OGS) in Oberpfaffenhofen, Germany. Additionally, DLR will be performing multiple in-orbit experiments regarding signal acquisition and tracking, channel measurements, and performance analyses of the OSIRIS payload as well as the optical ground station.

DLR-IKN operates a fixed rooftop OGS, which has previously been used for airborne QKD experiments [17]. It also operates a mobile system, which can be transported and deployed at remote locations. Either option can theoretically be used with the OSIRIS payload on the QUBE satellite. However, due to the complex nature of the components involved in photon reception, an additional installation of adaptive optics and receivers is being implemented in a coudé room close to the rooftop OGS [18].

7. Conclusions

This work has covered the various challenges of building a CubeSat for quantum key distribution (QKD) experiments. In the QUBE project, the CubeSat form factor as major design driver is met by high demands in attitude control and pointing accuracy as well as pointing stability for the optical downlink system. The goal of this first phase of the project is to test the components and the viability of performing QKD between a single CubeSat in low Earth orbit (LEO) and an optical ground station (OGS) in Germany. Two payloads for quantum communication tests are being developed in addition to the main satellite components and the optical terminal. After the challenging task of integration, QUBE is planned to launch in 2020. In a potential second phase, the complete QKD systems will be integrated and extended to enable the generation and distribution of actually useable keys. In the future, it will possibly be implemented on additional satellites or networks for the distribution of encryption keys to multiple ground stations around the globe.

Acknowledgements

QUBE is funded by the German Federal Ministry of Education and Research (BMBF) within the IKT 2020 program. Project partners in QUBE are LMU Munich, MPL Erlangen, DLR-IKN, OHB System AG, and ZfT.

References

[1] C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, IEEE International Conference on Computers, Systems and Signal Processing, volume 175, page 8.

[2] M. Tomamichel, A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, Quantum. 1: 14, 2017.

[3] R. Haber, D. Garbe, K. Schilling, QUBE - A CubeSat for Quantum Key Distribution Experiments, SSC18-III-05, 32nd Annual AIAA/USU Conference on Small Satellites, Logan, USA, 2018, 04 – 09 August.

[4] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, 48 (177): 203–209.

[5] I. Khan, B. Heim, A. Neuzner, C. Marquardt, Space-based QKD, OPN 2, 2018, https://www.osa-opn.org/home/articles/volume_29/february_2018/features/satellite-based_qkd/ (accessed 02.10.19).

[6] R. Bedington, J. M. Arrazola, A. Ling, Progress in satellite quantum key distribution, npj Quantum Information, 2017

[7] K. Schilling, Perspectives for Miniaturized, Distributed, Networked Systems for Space Exploration, Robotics and Autonomous Systems Vol. 90 (2017), p. 118–124.

[8] I. Khan et al., Satellite-Based QKD, Optics and Photonics News, February 2018.

[9] D. Oi et al., Nanosatellites for quantum science and technology, Contemporary Physics, 58:1, 25-52, 2017.

[10] CubeSat Design Specifications Rev.13, The CubeSat Program, Cal Poly SLO, http://www.cubesat.org/resources, (accessed 02.10.2019).

[11] UNISEC Europe, http://www.unisecglobal.org/pdf/uniglo3/day3_09100920.pdf, (accessed 02.10.2019).

[12] LMU Munich, https://www.uni-muenchen.de, (accessed 02.10.2019).

[13] Max Planck Institute for the Science of Light, https://www.mpl.mpg.de, (accessed 02.10.2019).

[14] Deutsches Zentrum für Luft- und Raumfahrt e.V., Institute of Communications and Navigation, www.dlr.de/kn, (accessed 02.10.2019).

[15] G. B. Xavier et al., Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation, New Journal of Physics, Volume 11, April 2009.

[16] S. Dombrovski et al., Uniform, Multi-Level protocol for Ground and Space Segment Operations and Testing, 4S Symposium, Sorrento, Italy, 2018.

[17] C. Schmidt et al., OSIRIS Payload for DLR's BiROS Satellite, International Conference on Space Optical Systems and Applications (ICSOS), Kobe, Japan, May 2014.

[18] F. Moll et al., Aerospace laser communications technology as enabler for worldwide quantum key distribution, SPIE Photonics Europe, Brussels, Belgium, 2016.