73rd International Astronautical Congress (IAC), Paris, France, 18-22 September 2022.

IAC-22-B4.9-GTS.5.5,x70823

QUBE-II – Quantum Key Distribution with a CubeSat

Martin Hutterer [a], Michael Auer [b*], Adomas Baliuka [b*], Ömer Bayraktar [c*], Peter Freiwang [b*], Marcell Gall [a*], Kevin Günthner [c*], Roland Haber [e*], Janko Janusch[a*], Lukas Knips [b*], Pascal Kobel [a*], Markus Krauss [e*], Norbert M.K. Lemke [a*], Christoph Marquardt [c*], Florian Moll [d*], Christos Papadopoulos [d*], Jonas Pudelko [c*], Benjamin Rödiger [d*], Christian Roubal [d*], Julian Scharnagl [e*], Klaus Schilling [e*], Christopher Schmidt [d*], Harald Weinfurter [b*]

[a] *OHB System AG, Manfred-Fuchs-Straße 1, 82234 Weßling / Oberpfaffenhofen (OHB)*
(Munich Metropolitan Area), Germany
[b] *Ludwig-Maximilians-Universität, Munich, Germany (LMU)*
[c] *Friedrich-Alexander-Universität Erlangen-Nürnberg, Germany (FAU)*
[d] *German Aerospace Center (DLR), Institute of Communications and Navigation,*
Weßling / Oberpfaffenhofen, Germany (DLR)
[e] *Zentrum für Telematik, Würzburg, Germany (ZfT)*
[*] By alphabetical order

Abstract

The digitization of our everyday lives is omnipresent. Secure data transmission is therefore of enormous importance in almost all areas of our society. An important part of the established cryptographic processes used for securing transmitted data today relies on assumptions about available computational power and algorithms. Although these assumptions seem to be securely fulfilled for now, there is already a real threat that intercepted data can be stored and decrypted in the future with more powerful or even quantum computers, which are currently under development. In contrast, instead of relying on these assumptions one can use the fundamental laws of quantum mechanics to generate secret keys between two parties. This so-called Quantum Key Distribution (QKD) enables a solution to the key distribution problem and the consecutive transmission of data where the underlying physical principle can guarantee long-term security of keys, which is impossible to achieve with current technology. However, due to losses fiber-based systems are currently limited to a few hundreds of kilometers. One approach to overcome this limit and enable global distribution of quantum keys is routing via satellite. Scalable exchange of secret keys between several ground stations via satellite can benefit from the standardized and scalable CubeSat platform to support global, secure communication. This paper provides insight into the structure of the ongoing QUBE-II project and lays out the challenges of a successful key exchange between a CubeSat and a ground station. In this context, also the future innovations compared to the predecessor project QUBE are discussed.

Keywords: QUBE, CubeSat, QKD, QRNG, Quantum Mechanics, Quantum Payload

1. Motivation

With SpaceX, Kuiper and OneWeb at the latest, the idea of scalable and low-cost satellite constellations has achieved visible success. In particular, extensive European or global coverage of communication infrastructures with the ability to perform quantum key distribution requires scalable solutions. Due to their small and standardized size, CubeSats are promising in this direction, as they offer a rapid and cost-effective development option as well as excellent scalability [1]. As a first phase the QUBE consortium developed important core technologies for satellite-based quantum communication and a satellite has been built, which will now allow a first evaluation of the quantum modules based on a CubeSat [2, 3]. This satellite is completed, waiting for a planned launch at begin of 2023. In QUBE-II, further developments are now performed subsequently to fully integrate all functional elements to build and launch a CubeSat, able to perform quantum key distribution. The demonstration of secure quantum key distribution between the QUBE-II satellite and a ground station on earth is expected to lay the foundation for global, secure communications with in particular, low resource requirements.

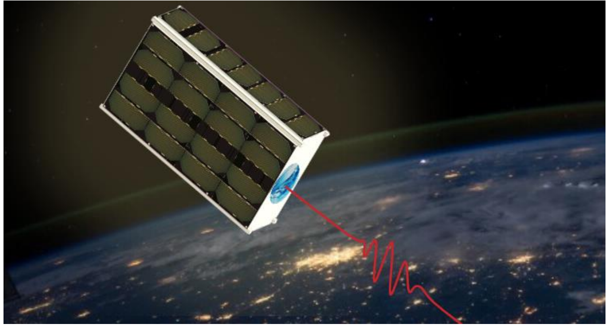

Fig. 1: QUBE-II (Artist's Impression by ZfT)

The first demonstration of satellite QKD was done by the Chinese mission Micius [5] in 2017 and currently, a number of projects aim for an implementation of satellite-based QKD [4]. However, up to today no system is known that can perform quantum key exchange via the much more affordable CubeSat-platform. The planned system which is presented here should show the route towards a favourable price-performance ratio. This then opens up exciting prospects for future satellite networks, where 100-200 QKD Microsatellites could be launched in place of a typical satellite, with the same rocket capacity - and similar costs.

2. QUBE-II Overview

The QUBE-II consortium plans to combine the agile CubeSat technology with the research in the field of quantum key distribution (QKD). In a close cooperation between universities, research institutes and industry, the consortium aims at demonstrating a CubeSat-based secure key exchange with a ground station for the first time. In the mission, we will develop fully functional hardware for low-cost and secure communication using small satellites. The CubeSat economic platform is to be expanded for this purpose by the necessary technology components, some of which have already been developed in the previous QUBE mission [6]. These developments have the ability to create the basis for powerful but economical satellite systems for secure global communication.

In the first round of experiments for the QUBE-II mission, we plan to test the payloads and various components individually before advanced tests are performed in the interaction of multiple payloads. This will involve testing the optical transmission of the laser terminal and its interface with the QKD transmission modules, and characterizing the classical communication bandwidth. Subsequently, a first quantum key distribution will be demonstrated between the satellite and an optical ground station in Oberpfaffenhofen, Germany.

3. Mission Architecture

The QUBE-II mission architecture envisages a single satellite space segment, i.e. a CubeSat, which accommodates the payloads to perform the mission objectives. Besides the space segment, several ground segments and the launch segment complete the mission architecture. A detailed system analysis will determine the final functional and logical architecture. The ground segment is split into two parts. First, for receiving the optical signals and for processing the payload data, an optical communication segment will be used. Second, a radio frequency ground station will handle controlling and commanding of the satellite by establishing a RF link with the space segment.

Fig. 2: Optical Ground Station (DLR-IKN)

Based on the realization of a compact space-qualified QKD transmitter unit within the QUBE consortium, QUBE-II aims to develop an overall QKD system. This includes the full implementation of QKD communication protocols including two different sender payloads with corresponding receivers at different wavelengths, a quantum random number generator, a laser terminal with high antenna gain and powerful classical communication channels.

Requirements arise from this, which demand novel technical solutions. The implementation of full key processing requires the selection of suitable protocols, compatible with a small and economical platform and limited classical bandwidth. For the generation of the quantum signals and the quantum random numbers, modules are required which are compliant with the limited resources on a CubeSat. Furthermore, a post-processing module must be developed allowing to perform several complex processing steps to actually generate a key from the transmitted data on the spacecraft. The highly efficient optics of the laser terminal require precise control of the laser beam as well as very accurate attitude control of the satellite. The necessary communication capacity shall be available optically during the overflight as well as in the RF range.

3.1 CubeSat Platform

While QUBE-I was based on a 3U-CubeSat with a total mass of 3.5 kg [3], the more powerful payload of QUBE-II requires an increase to a 6U-CubeSat with the dimension 10x23x35 cm³, despite it is to be built as compact as possible. Specific challenges concern the high precision pointing requirements of the optical link to ensure efficient key transfer. Position determination employs a GNSS in combination with laser reflectors. To achieve the pointing requirements, the attitude control system utilizes a multi layered control approach of coarse- and fine pointing control routines. Coarse pointing control relies on attitude information gathered by fusing multiple redundant attitude sensors, among others star sensors, with adaptive filters. Once a laser beacon is received fine pointing control relies on the highly precise measured beacon direction for attitude information. Both control routines appropriately coordinate the redundant 6 miniature reaction wheels for precise 3-axes pointing. Desaturation is handled by magnetorquers integrated in all side panels.

Trade-offs concern the power generation and distribution system for dimensioning solar arrays and battery storage appropriately for the planned operations during eclipse.

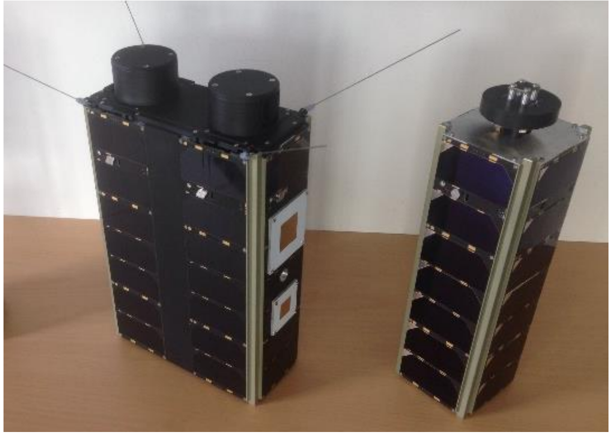

Fig. 3: Flight model of QUBE-I (right) and mechanical engineering model of QUBE-II (left) realized by a ZfT/S^4-Standard CubeSat

3.2. Quantum Payloads

Within QUBE-II two discrete variable (DV) quantum key payloads with wavelength at 850nm and 1550nm will be built. With the available power both modules plan to achieve a symbol rate of at least 100 MHz (for comparison, other QKD demonstrator missions plan for a symbol rate of 2 GHz). For QUBE-II this results in a key rate that is about a factor of 20 smaller, but at a dramatically lower system cost. The QKD analysis in the ground station will use extremely low-noise superconducting detectors to still obtain secure keys even at low count rates.

The DV-QKD transmitter at telecom wavelengths will be developed by FAU and consists of a laser, a fast I/Q-modulator and an attenuator. With this setup, amplitude and phase modulation of very weak coherent pulses can be achieved. With this setup, not only the DV protocol can be implemented, but also further experiments can be conducted, e.g. performing a continuous variable (CV) channel characterization or testing additional protocols. By using a photonic-integrated circuit (PIC) and a custom electronic design a reasonable small setup compatible with the CubeSat-standard can be achieved.

Additionally, LMU develops a QKD sender module at 850 nm for polarization encoding DV-QKD. Here, VCSEL diodes together with integrated optics and photonic waveguides will be employed to generate the required quantum signals.

For the post-processing of the QKD data, a module with processor and large memory as well as communication within the satellite and to the ground station will be developed. It will allow to efficiently perform the required tasks to generate a key from the measurement data.

The random numbers will be generated by a quantum random number generator (QRNG) built by the FAU. It is based on a homodyne measurement of the quantum mechanical vacuum state. An additional PIC will be employed, with all required optical components (e.g. Laser, beam splitter and photodiodes) on a single chip. Combined with external electronics for control and fast AD conversion plus a FPGA for real time post-processing, high data rates can be achieved.

3.3 Laser Communication Terminal

The basis of QUBE-II's terminal is a modified OSIRIS4CubeSat (O4C) module which allows the installation of a powerful optical system with an aperture of more than 80mm.

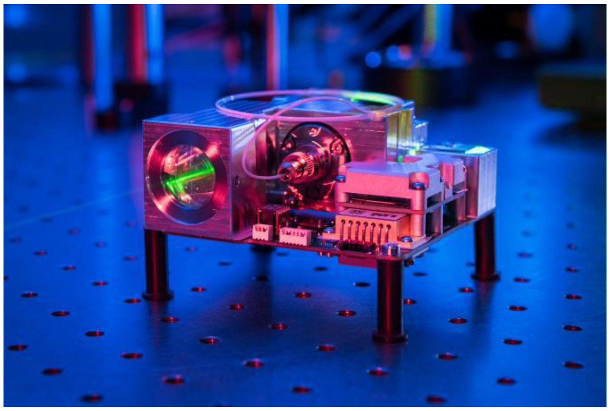

Fig. 4: Osiris4CubeSat [7]

Thus, QUBE-II will achieve a link efficiency comparable to missions with larger satellites but with terminals of similar size. The larger aperture places higher requirements on the alignment accuracy of the satellite; due to the lower divergence of the laser beam, an alignment accuracy of 0.1° is required. This must go hand in hand with the extension of the optical system to two-wavelength operation at 1550nm and 850nm. In addition, this terminal will enable high-rate optical uplinks for the post-processing step.

3.4 Interfaces

With several subsystems developed by different partners and the required close interaction, an early determination of the necessary interfaces between all subsystems is important for guaranteeing the success of the project.

The required interfaces are identified and defined taking into account the initial satellite design and the requirements profiles created. This ranges from the electrical and optical interfaces of the satellite down to the subsystem level, to the software interfaces of the microprocessors and FPGAs of the different modules. In the further design process, they are then specified and defined using the performance requirements before they are fixed for the final design.

4. Outlook

The presented QUBE-II mission aims to demonstrate the first quantum key exchange between a CubeSat and ground. In the long term, the project could be an essential building block towards the development of quantum communication infrastructures and a tap-proof transmission of data, based on a constellation of 10 to 20 QKD-microsatellites compatible to a large number of ground stations.

Acknowledgements

The work on QUBE-II is funded by the Federal Ministry of Education and Research (BMBF) in the field of Networking and Security of digital Systems under contract number 16KISQ047K.

References

[1] H. Heidt et al., “CubeSat: A New Generation of Picosatellite for Education and Industry Low-Cost Space Experimentation.” (2000)

[2] R. Haber et al., “QUBE – A CubeSat for Quantum Key Distribution Experiments”, Proceedings *32nd Annual AIAA/USU Conference on Small Satellites*, Logan, USA, 2018, paper SSC18-III-05

[3] I. Mammadov et al., „Quantum Key Distribution for Secure Communication by Nano-Satellites”, Proceedings IAC 2022 Paris, IAC-22-B2.2.7

[4] I. Khan et al., “Space-based QKD”, OPN 2 (2018), https://www.osa-opn.org/home/articles/volume_29/february_2018/features/satellite-based_qkd/

[5] S.-K. Liao et al., Satellite-to-ground quantum key distribution. Nature 549, 43-47 (2017)

[6] L. Knips et al., "QUBE – Towards Quantum Key Distribution with Small Satellites," in Quantum 2.0 Conference and Exhibition, Technical Digest Series (Optica Publishing Group, 2022), paper QTh3A.6.

[7] C. Schmidt et al., "DLR's Optical Communication Terminals for CubeSats," 2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS), 2022, pp. 175-180, doi: 10.1109/ICSOS53063.2022.9749735.