69th International Astronautical Congress (IAC), Bremen, Germany, 1-5 October 2018.

IAC-18-B4.2, x47743

25th IAA SYMPOSIUM ON SMALL SATELLITE MISSIONS (B4)
Small Space Science Missions (2)

QUBE – Quantum Key Distribution with CubeSat

Norbert M.K. Lemke [a]*, Harald Weinfurter [b], Christoph Marquardt [c], Florian Moll [d], Roland Haber [e], Matthias Grünefeld [a], Stephan T. Seidel [a], Peter Freiwang [b], Wenjamin Rosenfeld [b], Ömer Bayraktar [c], Benjamin Rödiger [d], Christopher Schmidt [d], Klaus Schilling [e]

[a] *OHB System AG, Manfred-Fuchs-Straße 1, 82234 Weßling / Oberpfaffenhofen (Munich Metropolitan Area), Germany*
[b] *Ludwig-Maximilians-Universität, Munich, Germany*
[c] *Max-Planck Institute for the Science of Light, Erlangen, Germany*
[d] *German Aereospace Center (DLR), Institute of Communications and Navigation, Weßling / Oberpfaffenhofen, Germany*
[e] *Zentrum für Telematik, Würzburg, Germany*

* Corresponding Author

Abstract

QUBE (Quantum Key Distribution with CubeSat) is one out of three pilot projects in the frame of the national German initiative QUTEGA to promote quantum technologies. The project is funded by the German Federal Ministry of Education and Research (BMBF) with co-funding of industry as preparation for the European flagship on Quantum Technology. With the current development pace in quantum computation, it has been predicted that in less than two decades quantum computers will be able to break encryption codes deployed today, which are currently based on mathematical problems difficult to solve with classical computation. This shows the urgent need for quantum-safe encryption that is resistant to attacks of both, quantum and classical, computers. A long term solution for quantum-safe encryption is the use of a completely random, so-called One-Time-Pad generated with true Random Number Generation (RNG) and distributed via Quantum Key Distribution (QKD). The QKD in fiber networks is limited to approx. 100 km due to damping within the carrier medium. For longer distances so far only satellite based techniques are able to transmit the keys. As a pathfinder, QUBE plans perform an in-orbit demonstration of the core technologies on a CubeSat platform.

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

1. Motivation

Currently a large part of secure communication is based on asymmetric cryptography schemes such as Elliptic-curve cryptography (ECC) [1, 2] or Rivest-Shamir-Adleman (RSA) System [3]. The security of these systems is threatened by the emergence of quantum computers that will be able solve the underlying mathematical problems significantly faster or to be more specific in polynomial time instead of exponential time. With quantum computing it will therefore be able to break the cryptographic systems our secure communication ecosystem is based on.

Quantum computers are expected to be available in the next decades and therefore a replacement of the existing encryption systems is of immediate need. QKD in combination with truly random One Time Pad offers an information-theoretically proven secure alternative. In contrast to Post-Quantum Cryptography (focusing on development of quantum computer resistant algorithm), QKD can provide provable long-term security already today.

Due to this development there is large interest in the implementation of QKD as a service worldwide. These efforts can be divided in two approaches: terrestrial, fiber-based and satellite-based.

While fiber-based systems are well suited for QKD on a local or regional level it cannot be used for a global implementation. This is due to the damping of the signal in the fibers that limits the range of fiber-based QKD effectively to the range of 100 km. Even though this range can be extended using node stations, this creates the need to trust these stations and therefore undermines the advantage of provable end-to-end security. Quantum repeaters as an alternative solution are still at the stage of fundamental research.

The QUBE consortium consists of the Ludwig-Maximilians-Universität (LMU, faculty of physics) in Munich, the Max Planck Institute for the Science of Light (MPL) in Erlangen, the Institute of Communications and Navigation of DLR in Oberpfaffenhofen, OHB System in Oberpfaffenhofen, (Munich Metropolitan Area), the Zentrum für Telematik (ZfT) in Würzburg, and Tesat as associated partner.

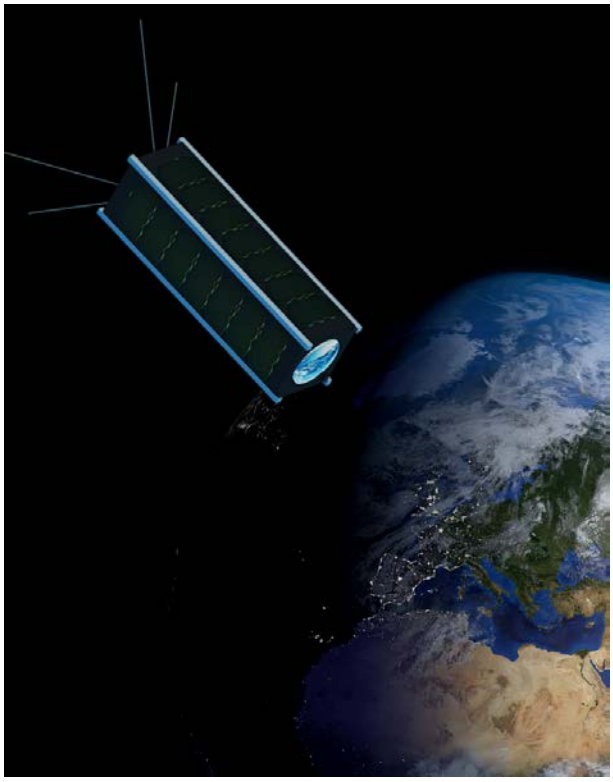

Fig. 1. QUBE (Artist's Impression).
(created with data from Visible Earth, NASA)

For QKD on a global scale a space-based implementations is currently the only technically feasible way forward. A constellation of QKD-equipped satellites would allow for a simultaneous global coverage. Its application include securing critical infrastructure for example energy, transport, and navigation and guaranteeing long term confidentiality of classified information. An overview of Satellite-based QKD is provided in [4].

2. QUBE Overview

The QUBE project has the goal of developing and testing key hardware necessary to establish global secure communication via a satellite-based QKD. CubeSats have been selected as platform in order to allow for a fast and economic realization.

The current project will develop the technological basics based on photonic integrated circuits for a quantum random number generator (QRNG) and QKD transmission. These modules can be installed on printed circuit boards and allow for a high degree of miniaturization.

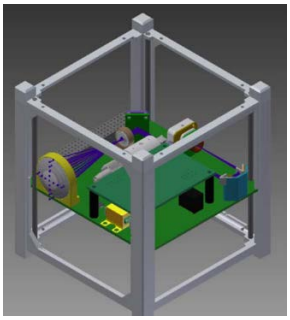

Fig. 2. Optical Terminal fitting in one cubesat unit
(DLR-IKN)

The random numbers are generated by a homodyne measurement of the quantum mechanical vacuum state. For this purpose MPL develops a PIC where the beam of a laser is brought to interference with the dark input of a beam splitter and the outputs are then detected on two photodiodes. Laser, beam splitter and photodiodes are integrated on the PIC and only external read-out and processing electronics are needed.

The QKD transmitter for CV-QKD at telecom wavelengths consists of a laser, a fast I/Q-modulator and an attenuator. The laser is operated in continuous wave mode and the I/Q-modulator is used for amplitude and phase modulation of the light. The modulated light can then be used to transmit the quantum states.

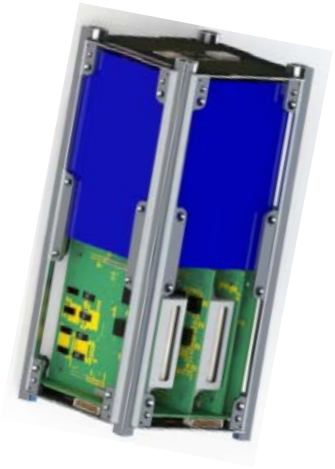

Fig. 3. Cubesat (2U, w/o optical terminal) (ZfT)

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.

A laser communication terminal based on the OSIRIS4CubeSat system with an aperture of 20 mm will be developed by DLR-IKN. In parallel, DLR's ground station OGSOP NG at Oberpfaffenhofen will be equipped with special receivers for the QKD signal. This will allow for the demonstration of a satellite to ground link.

The three unit (3U) cubesat including an improved attitude determination and control system is developed by ZfT. OHB is responsible for the industrialization of the quantum light sources as well as the QRNG.

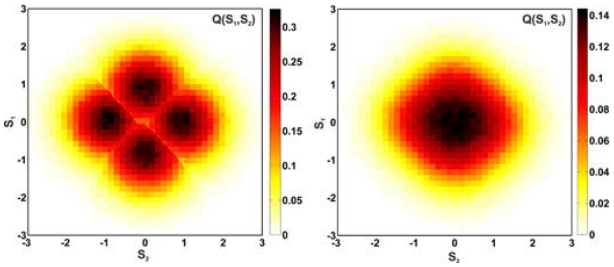

Fig. 4. Continuous-variable Encoding: Q-function of four states [5]

Fig. 5. Optical ground Station (DLR-IKN)

3. Outlook

Based on the experiences gained in this mission (launch planned for 2020) in a further phase a second, fully functional CubeSat could demonstrate with simple, cost-effective means secure key exchange between remote ground stations on a global scale.

Acknowledgements

Thanks to all the LMU, MPL, OHB, DLR-IKN and ZfT colleagues for the professional cooperation in the QUBE program. The work described has been funded under contract no. 16K1S0769 a.o. in the frame of the QUTEGA initiative by the Federal Ministry of Education and Research (BMBF).

References

[1] Koblitz, N. (1987). "Elliptic curve cryptosystems". Mathematics of Computation. 48 (177): 203–209.

[2] Miller, V. (1985). "Use of elliptic curves in cryptography". CRYPTO. Lecture Notes in Computer Science. 85: 417–426

[3] Rivest, R.; Shamir, A.; Adleman, L. (February 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" (PDF). Communications of the ACM. 21 (2): 120–126.

[4] Imran Khan, Bettina Heim, Andreas Neuzner and Christoph Marquardt, "Space-based QKD", OPN 2 (2018), https://www.osa-opn.org/home/articles/volume_29/february_2018/features/satellite-based_qkd/

[5] B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, Ch. Marquardt, G. Leuchs (2014). "Atmospheric continuous-variable quantum communication". New Journal of Physics, Vol 16, Nov 2014