Satellite QKD developments for secure communications

Agnes Ferenczi, Stefanie Häusler, Davide Orsucci, Innocenzo De Marco, and Florian Moll

Institute of Communications and Navigation, German Aerospace Center (DLR), Münchener Str. 20, 82234 Weßling, Germany

2025-09-10

ABSTRACT

Quantum key distribution (QKD), the technology to generate distant secure keys for later usage in secure communication, has become a mature topic since the 1980s. While terrestrial QKD over fiber networks is suitable for short-distance urban networks, QKD via satellites promises to gap the distance requirement on a global scale that limits terrestrial QKD. Satellite QKD requires the exchange of quantum states between a satellite and multiple ground stations. The goal is then to facilitate shared secret keys between the ground stations, which can then be relayed to users near the ground stations. The satellite usually carries the quantum sources as its payload and sends them to the ground station via a downlink. The QKD protocol is heavily influenced by the choice of the quantum source, with typically one of two types: approximate single photon source (such as a weak laser) or an entangled source. Similarly, the ground station must be equipped to receive, measure and process the quantum signals sent by the satellite. Although there are also reverse schemes, where the satellite acts as the receiver and the ground station as the sender, these schemes are less explored due to higher noise in the uplink and less engineering experience. As with any system containing a high heterogeneity, many different implementation schemes lead to a variety of optimized use cases based on different criteria. Satellite QKD carries the further complication that it must be adapted to international standards. In this paper we present different satellite and ground station architectures that lean on the developments in the projects EAGLE-1, QUBE, QuNET, RoGloQuaN, addressing different protocols, sources, satellite sizes and telescope sizes. We also discuss the need for agility and configuration of components in a heterogeneous environment.

1. INTRODUCTION

In a QKD protocol, a sender and a receiver agree on a protocol to exchange quantum and classical signals, which allows them, in theory, to extract via classical communication a secret key with unconditional information-theoretic security guarantees. This key can then be used for cryptographic primitives later on.

Photons have been considered the best (and basically only) carriers of the quantum signals in a QKD protocol. Ideally, the photon source produces single photons deterministically on demand and with an high repetition rate. In practice, though, due to lack of availability and technological maturity of such a perfect single photon source, a weak coherent laser with a Poissonian photon

Further author information:
Agnes Ferenczi: E-mail: agnes.ferenczi@dlr.de

Quantum Technologies for Defence and Security II, edited by Giacomo Sorelli, Veronica Fernandez
Sylvain Schwartz, Proc. of SPIE Vol. 13676, 136760I · 2025 Published by SPIE
0277-786X · doi: 10.1117/12.3072107

number distribution attenuated to less than one photon per pulse is used. In order to protect the protocol against eavesdropping attacks on the multi-photon states such as the photon number splitting attack, decoy states are mixed into the signal states.

Protocols can be grouped into three main schemes, depending on the direction of the quantum signal flow and the number of senders and receivers. In the prepare-and-measure (PM) scheme the sender prepares quantum states and sends them to the receiver. In the entanglement-based (EB) scheme the sender prepares an entangled state and sends each half of the pair to two receivers. In the measurement-device-independent (MDI) scheme two senders prepare entangled states and send each half of the pair to one receiver.

In satellite-based QKD[1] the sender is typically located on the satellite and the receiver on the ground implementing a PM scheme with a weak coherent laser source.

2. EAGLE-1

EAGLE-1[2–6] is the first quantum key distribution (QKD) satellite mission funded by ESA under the ARTES ScyLight (SeCure and Laser communication Technology) program. The system is developed by a consortium of European space companies, research institutes and universities led by the satellite company SES. The goal of the mission is to provide semi-commercial QKD services from a sun-synchronous low earth orbit (LEO) satellite for European users, thereby boosting European sovereignty and cybersecurity needs. As part of the the space segment of European Quantum Communication Infrastructure (EuroQCI), EAGLE-1 will provide mission data during its validation and in-orbit testing phase. The launch date of the satellite is planned for 2026.

EAGLE-1 implements a phase-encoded PM version of the Bennett and Brassard (BB84) protocol[7] with a weak coherent laser source, decoy states and bright reference pulses on the satellite. The signal states encode the 4 BB84 states in the phases of consecutive double pulses. At an altitude baseline of 500 km (454 km - 600 km), a high-performance repetition rate of 12.5 GHz aims to reach a maximum secret key rate of about kbit/s at estimated losses of 40 dB - 60 dB. For compatibility reasons with existing telecommunication wavelengths, the down-link quantum channel (1565.5 nm) and the bidirectional classical channel for down-link (1553.3 nm) and uplink (1536.6 nm) are chosen in the C-Band.

2.1 QKD Transmitter

At the heart of the payload is the QKD Transmitter,[3] a component developed by DLR-KN, that generates the quantum pulses and provides the control, monitoring and operations as well as a hacking protection unit.

The hardware of the QKD Transmitter consists of electronics, optics and a field programmable gate array (FPGA). In order to generate the signals states, a cascade of lasers, modulators, amplifiers, attenuators and PIN diodes are mounted on a main board. All hardware components are chosen such that they are robust against the harsh environment in space. A calibration unit implemented in hardware serves to ensure the quality of the signals to the standards required by the QKD security proof. The control of all hardware elements is shared by the FPGA and a soft-core embedded microcontroller unit. In this way, weak and bright laser pulses can be generated on demand according to the QKD protocol specifications with the desired signal quality.

DLR-KN develops the software package running on the microcontroller unit. It contains all code for the calibration algorithms, monitoring, control flow logic, software updates and maintenance, command and control (telemetry and telecommand), data storage (volatile and non-volatile) and data processing. Information about the hardware system is collected in control loops that continuously evaluates the optics, electronics and the PIN diodes to counteract and monitor any deviations. Analog-to-digital converters (ADCs) convert the analog signals from the hardware back into digital form for the microcontroller to use in monitoring and calibration. A telecommand and telemetry interface provides communication to the ground.

Due to the extremely high signal repetition repetition rate of EAGLE-1, the high-speed data processing for the signal generation must be outsourced to an FPGA. The FPGA generates the digital signals that drive the fast optical hardware components. Conversion from digital to analog signals is realized by high-speed digital-to-analog converters (DACs). In this way, the desired signal patterns are imprinted into laser light to produce the signal.

For the development of the hardware and software of the QKD Transmitter, a parallel development scheme has been employed to keep in line with the stringent timeline until the launch. As the QKD transmitter hardware evolves over the development time, the software is bound to keep track with the major hardware versions evolving from the first prototype to the electric and functional model (EFM) and all intermediate minor versions. Keeping up with the hardware is achieved with a modular software design principle, such that that it allows to swap the underlying hardware models with minimal changes and adaptations in the software necessary. The software is separated into hardware-dependent and hardware-independent layers to reflect the changing and static parts with respect to hardware evolution. The hardware-dependent section is modifiable and must be versioned with each hardware model. The hardware-independent section abstracts general high-level application logic. This allows the software of the EAGLE-1 payload to react quickly to hardware developments without losing sight of the general features that shall be valid for the mission overall.

2.2 Optical Ground Station

Besides the QKD Transmitter on the satellite, DLR-KN develops the optical ground station (OGS) in Oberpfaffenhofen.[3] The first in-orbit tests in the initial 6 months period after the satellite launch will be conducted by the OGS. The OGS consists of a telescope with a main aperture of 80cm. The OGS is equipped with the ability to perform pointing, tracking and acquisition (PAT), reception and measurement of the quantum signal, and an adaptive optics (AO) system to mitigate atmospheric turbulence. The telescope is mounted on top of the DLR-KN building with a Coudé path leading to a laboratory below hosting the measurement and AO equipment.

3. QUBE

The CubeSat trilogy of the missions PIXL-1, QUBE and QUBE-II is a series of three projects funded by the German BMFTR.[8–11] The three missions build on each other, with increasing QKD capabilities integrated into cost-efficient CubeSat platforms. The trilogy features miniaturized, space-qualified QKD components that shall enable a full stack QKD exchange between CubeSat and an optical ground station. The modular approach and the reuse of the laser communication terminal (LCT) highlights the fast adaptations in the mission trilogy.

3.1 PIXL-1

The PIXL-1 mission carries the CubeL CubeSat satellite[8] and targets compact and energy-efficient classical high-data transfers. The satellite carries the OSIRIS4CubeSat LCT build by DLR-KN. The mission was launched on 2021-01-21 and has successfully demonstrated a high-data download rate of 100 Mbits/s.[12]

The miniaturised LCT of CubeL measures 0.3U with an aperture of 20mm. The system is designed to receive optical signals at a wavelength of 1590 nm, and transmit optical signals at a wavelength of 1550 nm.[13]

3.2 QUBE

The subsequent mission, QUBE,[14] is equipped with quantum technologies components and tested for scientific measurements. The goal of QUBE is to transmit quantum signals (phase and polarisation) from the satellite to ground.

QUBE is a demonstration mission carrying two quantum sources with two wavelengths. It is a 3U-CubeSat weighing 3.5 kg. The quantum sources are 1) a discrete-variable BB84 polarisation-encoded source at 100MHz repetition rate using 4 VCSELs with a wavelength of 850 nm in the L-Band, and (2) a quadrature modulated weak coherent laser source at wavelenght of 1569 nm - 1571 nm in the telecommunication C-Band for time-bin or continuous-variable QKD. Both quantum sources couple into the LCT built by DLR-KN.

The challenge in QUBE was to adapt the OSIRIS4CubeSat LCT to transmit the two wavelengths in the C-band and L-Band simultaneously. This modular adaptation created the successor LCT, OSIRIS4CUBE, that incorporates capabilities to transmit different wavelength for QKD purposes without having to redesign the entire system.

QUBE was successfully launched on 2024-08-16. First in-orbit results measurements highlighting the achievements of the attitude determination and control of the high-precision pointing mechanism.[15]

3.3 QUBE II

The final mission, QUBE II, will implement a full stack QKD protocol from space to ground. The goal is the complete generation of a quantum key.[16]

With respect to QUBE, QUBE II is a larger: a 6U-CubeSat weighing approximately 10 kg. It will portray a larger aperture of 80mm, upgrades to reduce the channel loss and a laser terminal with high antenna gain, while retaining a low-cost hardware development. QUBE II will features integrated optics, photonic waveguides, real-time processing with fast ADCs and an FPGA.

The expected repetition rate in QUBE II aims at 100 MHz, which is about 20 times lower compared to a large satellite system like EAGLE-1. Thus, the key rate in QUBE II is also expected lower than EAGLE-1. Nevertheless, this drawback is compensated by cost-efficiency and a faster production and deployment cycle.

4. QUNET

QuNET is a national initiative,[17] funded by the German BMFTR, which aims to develop the foundation for secure and robust communication networks using quantum technologies. The initiative is part of the EuroQCI framework on the German national level.

4.1 Multi-Encoding Transmitter

QKD being a cybersecurity resource, it is not unreasonable to assume that different countries or organisations will want to develop their own technology, to avoid depending on a foreign entity for their own data protection. It follows that the QKD landscape is very heterogeneous, as different players have different QKD implementation requirements; this could lead to potential issues with international communication if using incompatible hardware. The topic of interoperability has fueled the development of solutions within DLR-KN and the QuNET project.

The multi-encoding transmitter[18,19] is able to transmit time-bin and polarization encoded quantum signals so that it can cater to several different QKD ground stations. The transmitter contains a module for time-bin encoding and a module for polarisation encoding, mounted in series in such a way that, they don't interfere with each other, if one of them is not in use. The time-bin encoding module is realized by a sequence of a phase modulator and two intensity modulators. The polarisation-encoded module uses a POGNAC encoder[20] for self-compensation.

Such a setup is preferable to a "universal" receiver, as the receiving side of a QKD system is arguably its most expensive part, especially when considering free-space nodes for satellite communications, as it involves a telescope, adaptive optics and several single photon detectors, all of which can significantly increase space resources and costs if they have to be adapted to different transmitter layouts. On the other hand, the multi-encoding transmitter has a much lower SWAP, making it more suitable to be the section of the system that adapts to the different receivers.

Tests for the multi-protocol transmitter are foreseen in the upcoming key experiment 3 (SE3) of the QuNET project, for which the transmitter is integrated into the DLR-built FELT-II terminal.[21] The terminal and the transmitter will be then integrated in an aircraft and will communicate with a ground station to perform the exchange of quantum states encoded in either the polarisation or the time-bin degree of freedom.

4.2 QuNET+SKALE

The QuNET+SKALE project focuses on the development of a scalable and modular quantum ground station (QGS) architecture intended for use in satellite-based quantum key distribution (QKD) networks. The project addresses current limitations in ground station deployment by introducing a design that supports off-the-shelf supply and modularity.

A central aspect of the OGS is its modular QKD subsystem, which allows for the integration and interchange of various QKD receiver modules. These include free-space continuous-variable QKD receivers operating at around 800 nm, multimode fiber-coupled QKD receivers, and single-mode fiber coupling modules in the C-band. This modular design enables the exchange of QKD subsystems without requiring a complete redesign of the OGS hardware.

The ground station developed in the QuNET+SKALE project contributes to the broader QuNET initiative, which aims to establish a secure quantum communication network in Germany. The modular and scalable design aligns with the initiative's objectives by providing a flexible platform for both satellite-based and terrestrial QKD. It also supports interoperability across different quantum communication technologies and encourages collaboration between academic institutions and industrial partners.

5. ROGLOQUAN

The project Robust Global Quantum Networks (RoGloQuaN) focuses on future quantum communication networks, which leverage advanced technologies for quantum information processing to allow the distribution of entanglement on a global scale. In particular, the project envisions the use of quantum repeaters on board of satellites, leveraging the use of inter-satellite free-space optical links to bridge global distances using very few intermediate nodes. This would enable performing QKD between end-users located at arbitrary distances on the Earth without the need to trust any of the intermediate nodes. Beyond that, the generation of long-distance entanglement could enable a broad family of application scenarios, such as distributed quantum computation, distributed quantum sensing, as well as many cryptographic primitives beyond QKD.

The goal of the project is the development of some of the fundamental network components enabling the realisation of satellite-based quantum repeater links. A crucial technology that needs further development are portable, resilient and high-performance quantum memories. They are needed to perform entanglement swapping on pairs of photons that have arrived asynchronously at the satellite. Several technologies could be employed to this end and are being experimentally developed within the project, including a portable trap for cooling and storage of an Yitterbium cold quantum gas. Another promising candidate are Atomic Frequency Combs realised with Rare-Earth Ion Doped crystals, as they feature long coherence time, multi-mode storage capacity and controllable delay time between photon write-in and photon read-out. A second fundamental technology for quantum repeater networks are entanglement photon sources. Here, the project has focused on the development of sources meeting the stringent photon bandwidth requirements imposed by most quantum memory technologies. Finally, the project has contributed to the operation and further development of the OSIRIS laser communication terminal. This is required, as very high efficiency links, supporting the transmission of single photons over distances of several thousand kilometers with efficiencies that are as high as possible.

Furthermore, in order to support the development of quantum communication networks from a holistic perspective, end-to-end simulations of quantum repeater links has been performed.[22] The focus of the simulations carried out so far has been on quantum repeater links featuring a single entanglement swap. This is implemented with three low Earth orbit satellites flying in formation, with only the central ones hosting quantum memories to actively perform the asynchronous entanglement swap and the later ones carrying either entanglement sources (in a downlink architecture) or setups to perform synchronous two-photon Bell state measurements (in an uplink). In the work, a comprehensive model has been developed, which integrates analytical expressions for entanglement swapping rate and the associated error rate, realistic satellite orbit dynamics for a three-satellite constellation with a realistic model of the optical links, accounting for beam geometry, atmospheric effects, and adaptive optics. Several trade-offs have been carried out: the confguration works best for intercontinental distance, while for continental distances a simple entanglement distribution from a single satellite would be favourable; it is highlighted that different technological hurdles affect uplink and downlink architectures, with the former requiring the use of guide star systems for high performance beam forming in uplink, while the latter requires technologies to herald the arrival of a photon without absorbing it; finally, the comparison between the use of three satellite in the same orbital plane or in three distinct Sun-synchronous orbits shows that the former performs better than the latter, but only if the links can be established also during the day, rather than only by night.

6. CONCLUSION

In conclusion, this paper summarizes the projects EAGLE-1, QUBE, QuNET, and RoGloQuaN at DLR-KN on quantum technologies. Modularity of various subcompontents of the projects is key for fast and efficient development: modularity of LCTs for reusability in subsequent missions, modularity in payload software architecture for fast development during hardware evolution, modularity of QKD transmitter implementations for international compatibility, modularity in QKD OGS to enable compatibility with different senders. Furthermore, DLR-KN focuses on future quantum network components, simulations for holistic QKD networks to realize quantum repeater networks that can link users at arbitrary distances.

REFERENCES

1. Davide Orsucci, Philipp Kleinpaß, Jaspar Meister, Innocenzo De Marco, Stefanie Häusler, Thomas Strang, Nino Walenta, and Florian Moll. Assessment of practical satellite quantum key distribution architectures for current and near-future missions. *International Journal of Satellite Communications and Networking*, 43(3):164–192, 2025.
2. European Space Agency. Eagle-1. https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1.
3. Gabriela Calistro-Rivera, Oliver Heirich, Amita Shrestha, Agnes Ferenczi, Alexandru Duliu, Jakob Eppinger, Bruno Femenia Castella, Christian Fuchs, Elisa Garbagnati, Douglas Laidlaw, et al. Building europe's first space-based quantum key distribution system–the german aerospace center's role in the eagle-1 mission. *arXiv preprint arXiv:2412.03222*, 2024.
4. Thomas Hiemstra, David Hasler, Domenico Paone, Fabian Reichert, Frank Heine, and Julian Struck. The european satellite-based qkd system eagle-1. In *Free-Space Laser Communications XXXVII*, volume 13355, pages 216–222. SPIE, 2025.
5. SES Techcom SA. Eagle-1 documents. https://ses-techcom.com/download-category/eagle-1-documents/, 2024.
6. Kevin Günthner, Conrad Rößler, Bastian Hacker, Ivan Derkach, Vladyslav Usenko, and Christoph Marquardt. The eagle-1 qkd protocol - phase encoded bb84 decoy in a practical satellite qkd application. https://www.ses.com/sites/default/files/2024-11/2024-11-11_The-Eagle-1_QKD_protocol.pdf, 2024.
7. Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984. IEEE Press.
8. Deutsches Zentrum für Luft-und Raumfahrt. Osiris4cubesat / cubelct. https://www.dlr.de/de/kn/forschung-transfer/projekte/osiris-programm/cube4cubesat.
9. Technologie und Raumfahrt Bundesministerium für Forschung. Qube. https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qube, 2020.
10. Technologie und Raumfahrt Bundesministerium für Forschung. Qube ii. https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/qube-2, 2025.
11. Christos Papadopoulos, Christian Roubal, Benjamin Rödiger, Florian Moll, and Christopher Schmidt. Development of laser terminals for satellite-based qkd on cubesat platforms. 2023.
12. Benjamin Rödiger, Marie-Theres Hahn, Christian Fuchs, and Christopher Schmidt. Osiris4cubesat-system engineering with new space approach from the development of a high data-rate optical communication payload to the demonstrator in a quasi-operational mission. In *SECESA, the 9th International Systems & Concurrent Engineering for Space Applications Conference.*, 2020.
13. René Rüddenklau, Fabian Rein, Christian Roubal, Benjamin Rödiger, and Christopher Schmidt. In-orbit optical calibration for acquisition and tracking on osiris4cubesat. In *Free-Space Laser Communications XXXVII*, volume 13355, pages 274–284. SPIE, 2025.
14. Lukas Knips, Michael Auer, Adomas Baliuka, Ömer Bayraktar, Peter Freiwang, Matthias Grünefeld, Roland Haber, Norbert Lemke, Christoph Marquardt, Florian Moll, et al. Qube–towards quantum key distribution with small satellites. In *Quantum 2.0*, pages QTh3A–6. Optica Publishing Group, 2022.
15. Benjamin Rödiger, René Rüddenklau, Lisa Elsner, Timon Petermann, and Philip Bangert. First in-orbit results of the qube mission hosting a laser communication terminal for experiments towards quantum key distribution from cubesats. *SmallSat Europe 2025*, 2025.

16. Martin Hutterer, Michael Auer, Adomas Baliuka, Oemer Bayraktar, Peter Freiwang, Marcell Gall, Kevin Günther, Roland Haber, Janko Janusch, Lukas Knips, et al. Qube-ii-quantum key distribution with a cubesat. In *73rd International Astronautical Congress, IAC 2022*, 2022.

17. Bundesministerium für Forschung Technologie und Raumfahrt BMFTR. The qunet initiative. https://qunet-initiative.de/.

18. Innocenzo De Marco, Robert I Woodward, George L Roberts, Taofiq K Paraïso, Thomas Roger, Mirko Sanzaro, Marco Lucamarini, Zhiliang Yuan, and Andrew J Shields. Real-time operation of a multi-rate, multi-protocol quantum key distribution transmitter. *Optica*, 8(6):911–915, 2021.

19. Innocenzo De Marco, Eltimir Peev, Till Dolejsky, Javier Garcia Olmedo, Davide Orsucci, Carlo Riester, and Florian Moll. A multi-encoding, multi-protocol quantum key distribution transmitter. 2024.

20. Costantino Agnesi, Marco Avesani, Andrea Stanco, Paolo Villoresi, and Giuseppe Vallone. All-fiber self-compensating polarization encoder for quantum key distribution. *Optics Letters*, 44(10):2398–2401, 2019.

21. Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter. Air-to-ground quantum communication. *Nature Photonics*, 7(5):382–386, 2013.

22. Jaspar Meister, Philipp Kleinpaß, and Davide Orsucci. Simulation of satellite and optical link dynamics in a quantum repeater constellation. *EPJ Quantum Technology*, 12(1):5, 2025.