A Compact and Robust Sender for Polarization-Encoded Satellite-to-Ground Quantum Key Distribution

Moritz Birkhold[1,2], Adomas Baliuka[1,2], Michael Steinberger[1,2], Michael Auer[1,2], Harald Weinfurter[1,2,3], Lukas Knips[1,2,3]

[1] *Ludwig Maximilian University (LMU), Faculty for Physics, Munich, Germany*

[2] *Munich Center for Quantum Science and Technology (MCQST), Munich, Germany*

[3] *Max Planck Institute of Quantum Optics (MPQ), Garching, Germany*

Quantum key distribution (QKD) enables the secure exchange of secret keys by bounding information leakage during transmission. While fiber-based QKD is effective over short and medium distances, global-scale key distribution requires satellite links. For this purpose we present QSS-8, a compact 10x10x3 cm module for polarization-encoded satellite-to-ground quantum key distribution on the QUBE-II [1-3] small satellite mission. QSS-8 (Fig. 1) generates weak coherent pulses for BB84 with decoy states and supports the full protocol chain, including synchronization, sifting, LDPC-based error correction [4], and privacy amplification. The system uses four VCSELs in combination with polarizers to prepare the required polarization states and micro lenses to couple into a single mode fiber. It also includes onboard monitoring as well as sufficient memory and processing capacity for complete key-generation workflows during low-Earth-orbit overpasses. Environmental tests confirmed robustness of our new micro optics assembly against launch vibration and thermal-vacuum conditions from -30°C to +40°C. State-analysis yields an intrinsic QBER below 0.5%. These results show that QSS-8 combines compactness, flexibility, and resilience, making it a scalable solution for CubeSat-based BB84 QKD missions.

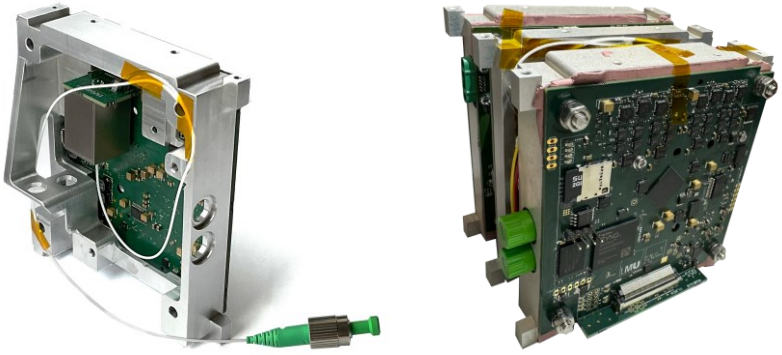

Fig. 1: *Left: QSS-8 subsystem top view. Right: QSS-8 (back view) integrated into quantum payload stack of QUBE-II mission featuring two identical copies of QSS-8 as well as the payload controller PCON with a quantum random number generator and QSS-C, a quantum state source in the telecom-C band, both developed by Friedrich-Alexander University of Erlangen-Nuremberg, all connected by a connection board for fast data and clock signals.*

References

[1] L. Knips et al., “QUBE – Towards Quantum Key Distribution with Small Satellites”, In Proc. Quantum 2.0 Conference and Exhibition, Optica Publishing Group (2022).

[2] L. Knips et al., “Prospects of scalable quantum key distribution using nano satellites”, in Proc. SPIE 13148, Quantum Communications and Quantum Imaging XXII, 1314808 (2024).

[3] M. Hutterer et al., “QUBE-II – Quantum Key Distribution with a CubeSat”, in Proc. IAC (2022).

[4] A. Baliuka et al., “Open-Source LDPC Error Correction for QKD, Qcrypt Conference”, in Proc. QCrypt, HAL open science (2021)