QKD Hardware on Small Satellites

Peter Freiwang

München 2023

QKD Hardware on Small Satellites

Peter Freiwang

Dissertation
an der Fakultät für Physik
der Ludwig–Maximilians–Universität
München

vorgelegt von
Peter Freiwang
aus Seeon-Seebruck

München, den 31.01.2023

Erstgutachter: Prof. Dr. Harald Weinfurter
Zweitgutachter: Prof. Dr. Alexander Högele
Tag der mündlichen Prüfung: 28.04.2023

Zusammenfassung

Quantenschlüsselverteilung (Engl. quantum key distribution, QKD) ermöglicht den Austausch von geheimen Schlüsseln, bei denen, basierend auf den Gesetzen der Quantenphysik, Abhörversuche erkannt und deren maximale Information bestimmt werden kann. Durch die Nutzung von Satelliten, ausgestattet mit QKD-Hardware und einem optischen Kommunikationsterminal, können fundamentale Limitierungen von faserbasierten QKD-Netzwerken hinsichtlich der Entfernung zwischen den Kommunikationspartnern überwunden werden. In dieser Arbeit wird ein kompaktes und robustes QKD-Sendermodul, welches für die Integration in den 3-unit ($30 \times 10 \times 10\,\mathrm{cm}^3$) Cube-Satelliten QUBE konzipiert, gebaut und qualifiziert wurde, präsentiert. Das Ziel von QUBE ist der Test und die Verifizierung der Tauglichkeit von, zwei auf unterschiedlichen Technologien basierenden QKD-Sendern unter realen Weltraumbedingungen. Unser Sender implementiert das BB84-QKD-Protokoll mit der Polarisationskodierung von schwachen kohärenten Pulsen (Engl. weak coherent pulses (WCPs)). Die Kompaktheit und der geringe Stromverbrauch werden durch den Einsatz hauptsächlich passiver mikrooptischer Komponenten erreicht. Kollegen des MPL in Erlangen stellen eine weitere Nutzlast zur Verfügung, welche die Phasenkodierung von WCPs basierend auf photonisch integrierten Schaltungen implementiert. Die harten Umwelteinflüsse im All (Strahlung, thermische Zyklen, Vakuum) und die mechanischen Vibrationslasten beim Raketenstart erfordern umfangreiche Tests der Hardware die auf baugleichen Geräten durchgeführt wurden. Es wurden vielversprechende Ergebnisse mit dem fertig integrierten Satelliten erhalten, beispielsweise eine gute Qualität der präparierten Polarisationszustände und ein niedriges Quantenbitfehlerverhältnis (Engl. quantum bit error ratio, QBER) von nur 2,2%.

Abstract

Quantum Key Distribution (QKD) enables the exchange of secret keys by which, based on the laws of quantum physics, eavesdropping attempts can be detected and their maximum information can be determined. By using satellites equipped with QKD hardware and an optical communication terminal, fundamental limitations for fiber based QKD networks regarding the distance between the communicating parties can be overcome. In this thesis, a compact and robust QKD sender module, which has been designed, built, and qualified for the integration into the 3-unit ($30 \times 10 \times 10\,\mathrm{cm}^3$) Cube-Satellite QUBE, is presented. The goal of QUBE is to test and verify the suitability of QKD senders based on two different technologies under real space conditions. Our sender implements the BB84 QKD protocol with polarization encoding of weak coherent pulses (WCPs). Its compactness and its low power consumption is reached by the usage of mostly passive micro-optical components. Colleagues of the MPL in Erlangen provide a further payload which features the phase encoding of WCPs based on photonic integrated circuits. The harsh environmental influences in space (radiation, thermal cycles, vacuum) and the mechanical vibration loads during the rocket launch require considerable tests of the hardware, which were performed on devices identical to the ones later integrated as flight models in the satellite. Promising results were achieved, which for example show a good quality of the prepared polarization states and a low quantum bit error ratio (QBER) of only 2.2% of the light emitted by the fully integrated satellite.

Contents

Zusammenfassung **v**

Abstract **vi**

Table of Contents **x**

1 Introduction **1**

2 The QUBE Mission **5**
2.1 Mission Description 5
2.2 Design of the Satellite 6
2.2.1 Overall Structure 6
2.2.2 Quantum Payloads 6
2.2.3 Optical Terminal OSIRIS 7
2.2.4 Interfaces 8
2.3 Optical Ground Station and QKD Receiver 11
2.4 QKD Feasibility Analysis 13
2.4.1 Fundamentals to QKD 13
2.4.2 QUBE QKD Link Simulation 16

3 Polarization Encoding QKD Sender Module **21**
3.1 Sender Design and Components 21
3.1.1 Microoptics 21
3.1.2 QKD Sender PCB 25
3.2 Assembly of the Microoptics and Overall Module 28
3.2.1 Setup for the Assembly 28
3.2.2 Assembly of the Microoptics Part 29
3.2.3 Assembly of the Sender Module Unit 33

4 Qualification of the QKD Sender **35**
4.1 Radiation Tests 35
4.1.1 Space Radiation Effects and Radiation Sources in Space 35
4.1.2 Total Ionizing Dose Tests 39
4.1.3 Proton Radiation Tests 45

4.1.4 Conclusion . . . 46
4.2 Vibration Tests . . . 47
4.2.1 Mechanical Simulations . . . 47
4.2.2 Test Facility and Methods . . . 48
4.2.3 Vibration Tests Results and Conclusion . . . 49
4.3 Thermal Cycles under Vacuum Condition . . . 52
4.3.1 Thermal Vacuum Chamber (TVC) Setup . . . 52
4.3.2 EQM Long-term TVC Tests . . . 53
4.3.3 TVC Tests Conclusion . . . 59

5 Characterization of the QKD Sender Flight Model 61
5.1 Optical Characteristics . . . 61
5.1.1 Timing Characteristics . . . 61
5.1.2 Spectral Characteristics . . . 62
5.1.3 VCSEL Response Curves . . . 63
5.1.4 Preparation Quality of the Polarization States . . . 66
5.2 Determination of Driving Parameter . . . 67

6 Integration and Characterization of the Satellite 71
6.1 Satellite Flight Model Integration . . . 71
6.2 Satellite Optical Characteristics . . . 73
6.2.1 Synchronization Channel . . . 73
6.2.2 Quantum Signal Output . . . 75

7 Conclusion and Outlook 77

Bibliography 79

List of Abbreviations 92

Acknowledgments 95

Chapter 1

Introduction

The first methods of cryptography were developed already thousands of years ago in Egypt, Mesopotamia, India, Greek, and the Roman Empire, with the Caesar cipher being one of the best-known ones [1, 2]. Yet, until the 20th century, the cryptography schemes were often based on the encryption of written characters using simple mechanical devices. The upcoming potential for sophisticated fine mechanical constructions and electromechanical machines marked a turning point in the reachable number of combinations by that information can be encrypted. For example, the encryption device Enigma, commercially built starting in 1932, allowed up to 10^{23} possibilities, which corresponds to a key length of about 76 bit [3]. Especially because of the digitization and globalization, the worldwide information flow increased drastically over the last decades. Thus the demand regarding the security of the used cryptography schemes again reached a turning point. With the ongoing development of quantum technologies, the moment where the security of the widely used asymmetrical (also called public and private key) schemes such as RSA [4] can be attacked by the Shor algorithm [5] on a quantum computer, seems to come closer. But also in the absence of a fully functional quantum computer, there is so far no proof that for example RSA can not be broken also by classical algorithms. Here, the recent example of breaking one of the intended candidates for Post-Quantum Cryptography algorithms [6, 7] on a standard laptop [8] shows the urgent need of cryptographic methods based on a drastically reduced number of mathematical assumptions. Provable security against eavesdropping can be achieved using symmetrical encryption methods, i.e., schemes which use the same key for encryption and decryption, such as the One-Time-Pad (OTP). Their disadvantage is that a secret key must be exchanged beforehand, which up to now has mostly been done using asymmetric schemes such as Diffie-Hellman key exchange [9], which in turn could be broken using a quantum computer.

Here, Quantum Key Distribution (QKD) [10–13] provides a powerful solution for the problem of the key exchange since its theoretical framework is only based on quantum mechanics laws. Inspired by the ideas of Stephen Wiesner regarding quantum coding in 1983 [14], Charles H. Bennett and Gilles Brassard proposed the first QKD protocol in 1984, called the BB84 protocol [15]. It uses orthogonal polarization states from two conjugated bases, which are exchanged between a sender (Alice) and a receiver (Bob) over a quantum

channel, in practice an optical fiber or a free-space link. Since 1984 numerous protocols have been emerged—often classifiable as extensions or modifications of the initial BB84 protocol [16, 17], or using different degrees of freedom of photons, e.g., by phase [18] or time-bin encoding [19], entanglement based schemes [20, 21], or continuous variable (CV) QKD protocols [22–24]. Great effort has been put on theory and experimental side to harden the QKD implementations against all kinds of attacks, like trojan horse [25], detector control [26], or other side-channel attacks [27–29]. Revealing weak points of QKD implementations and the aspired independence of trust in the QKD hardware gave rise to the so-called device independent (DI) QKD [30, 31], where recently the results of first implementations could be reported [32, 33]. However, the experimental complexity of DI QKD limits its suitability in former and present QKD networks [34–38] so far.

Independent from the implemented QKD protocol, the intensity of the QKD signals can not be chosen arbitrarily high with the consequence that the optical losses in the quantum channel limit the reachable distance. Despite that the current record for fiber based QKD systems accounts to 833.8 km [39], application-oriented QKD fiber-links can currently be operated up to a distance of the order of about 100 km. This is mainly because of the absorption losses in optical fibers, which are exponentially increasing with the distance. Optical free-space links only show a quadratic dependence with the distance—satellite-based QKD benefits from this and therefore enables the interconnection of QKD nodes even on a global scale. Statical long-distance QKD free-space links [40, 41] or links between a static ground station and moving platforms, such as an airplane [42] or a balloon [43], substantiated the feasibility of satellite-based QKD. The Chinese satellite mission *Micius* marked the beginning of a new era with outstanding experimental results including satellite-to-ground QKD based on the BB84 protocol [44], entanglement-based QKD [45], as well as an intercontinental QKD demonstration [46]. Other QKD space missions have been reported [47–50], however, the results obtained from *Micius* are unrivaled so far. A crucial factor in this is the cost of such a mission. *Micius* is assumed to cost far beyond 100 Mio $, which is possibly record-breaking for a technology demonstration in space, at least outside China. Ongoing progress in the miniaturization of QKD hardware either based on micro-optics [51–55] or on photonic integrated circuits [56–60] have opened the door that such hardware can be combined with small and therefore cost-efficient satellites. The Cube-satellite standard [61, 62] provides here an ideal platform as it allows, depending on the mission and system requirements, the modular combination of $10 \times 10 \times 10\,\mathrm{cm}^3$ (1U) elements.

This thesis deals with the development, construction, and qualification of a small QKD payload within the 3U-Cube-Satellite mission QUBE (chapter 2). Based on former works within our group on miniaturizing a QKD sender [55, 63, 64], further progress in the hardware development could be achieved, which allowed to build a QKD sender unit including optics and driver hardware on a $9 \times 9\,\mathrm{cm}^2$ printed circuit board (chapter 3). An engineering qualification model of the QKD sender was tested for its sensitivity to radiation and vibration loads as well as its behavior under thermal fluctuations in vacuum (chapter 4). Finally, a flight model of the QKD sender has been built, characterized, and integrated into the satellite (chapter 5 and chapter 6). The QUBE-consortium, consisting of scien-

tists and engineers from the DLR IKN in Oberpfaffenhofen, the MPL in Erlangen, the ZfT in Würzburg, and OHB in Munich under the lead of the LMU Munich, has the goal to test and verify the suitability of the sophisticated QKD hardware in space. With the outcomes of QUBE, a great step in the development of low-SWaP but high-performance QKD hardware can be made, which shows that satellite-based QKD is no longer only a scientific topic but can also become a commercially attractive part of future, global QKD networks.

Chapter 2

The QUBE Mission

The low-Earth orbit (LEO) mission QUBE pursues to test and to verify highly integrated QKD-hardware on-board of a Cube-satellite. This hardware generates QKD signals based on weak coherent pulses, which are then transmitted via a downlink to an optical ground station (OGS) on Earth. This chapter gives an overview about the mission, the design of the satellite, the OGS, and the QKD receiver. Furthermore, QKD fundamentals are discussed and a QKD feasibility analysis based on the presented hardware is made.

2.1 Mission Description

The QUBE mission is planned for a minimum operation duration in space of one year. Within this time, we plan to perform several experiments, ranging from rudimentary status requests and internal subsystem tests over the generation of quantum random numbers (QRNGs) all the way to the establishment of an optical downlink including QKD test sequences. To reduce the influence of stray and backscattered light on the detection recordings of the weak QKD signals, we plan to perform the optical experiments during night and, if possible, during eclipse, i.e., while the satellite is not illuminated by the sun. At the time of writing this thesis, the final orbit characteristics were still unknown, however, we plan with a sun-synchronous orbit with a local time of ascending node (LTAN) between 22:00 and 01:00. One orbit around the Earth takes about 90 min. A typical overflight scenario starts with turning on the required subsystems approximately minutes before the satellite appears on the horizon. Depending on the elevation angle of the corresponding overflight, the usable link duration varies between a few minutes up to about ten minutes. The schedule after the pass depends on the tasks to be performed after the experiment (data processing or data downlink over UHF), but as the available electrical energy is very limited, not required subsystems get directly shut down or set to idle mode again.

2.2 Design of the Satellite

The design of QUBE has been developed in close collaboration between all consortium partners. In this section the general structure of the QUBE satellite is presented and a detailed description of the quantum payloads and the optical terminal is given. In addition, the electrical, mechanical, and optical interfaces are specified.

2.2.1 Overall Structure

All operational and payload subsystems of QUBE fit into a 3U Cube-Satellite construction with outer dimensions of $10 \times 10 \times 30\,\mathrm{cm}^3$ (see figure 2.1). The optical terminal OSIRIS features a fast controllable mirror for beam steering with an operating range of one degree (full angle). Therefore, in preparation of and also during an optical downlink, the attitude determination and control system (ADCS) must align the satellite towards the OGS and stabilize it within this angular range. When the satellite is in eclipse, the sun sensors cannot supply the ADCS with telemetry data. To still obtain attitude data, QUBE is equipped with a star tracking sensor. The communication module enables a bidirectional UHF link for, e.g., telemetry and telecommand (TMTC) or software updates, with a data rate of up to 9.6 kbit/s. In addition to the on-board computer (OBC), which serves for the operational tasks of the satellite, the payload by the MPL comprises a payload controller (PCON) for the management of the experimental sequences. The electric power system provides an electrical energy of 30 Wh and must deliver a peak output power of approximately 20 W during a downlink sequence when all required systems are turned on. Based on simulations and empirical studies we expect that, depending on the orbit characteristics, the solar panels produce an electrical energy of 3 to 10 Wh per orbit.

2.2.2 Quantum Payloads

The QUBE satellite contains two QKD sender payloads based on different technologies, allowing to test various QKD protocols and encoding schemes. The hardware built by the LMU implements the BB84 protocol [15] with polarization encoding at a wavelength of 850 nm. This payload in described in great detail in chapter 3 (design and assembly), chapter 4 (tests and qualification), and chapter 5 (characterization of the final flight hardware).

The payload built by the MPL in Erlangen features two photonic integrated circuits (PICs) on indium phosphide (InP) basis [65], together with all electronics parts for its interfacing to the satellite bus as well as for its operation, and the payload controller. The QKD sender PIC is based on a distributed Bragg reflector laser emitting at about 1571 nm, which gets modulated by nested Mach-Zehnder interferometers. By this, continuous-variable protocols [22] and distributed-phase-reference protocols as the differential phase-shift protocol [18] and the coherent one-way protocol [19], can be tested. The second InP PIC, which implements a QRNG scheme based on the optical homodyne measurement of the vacuum

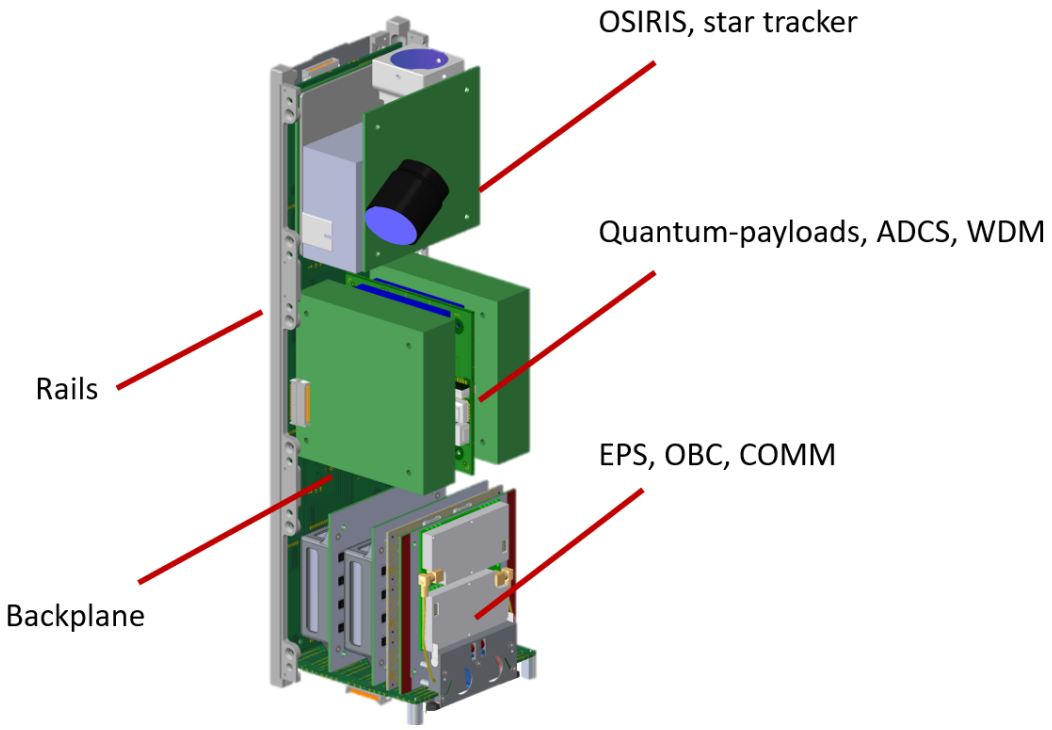


Figure 2.1: Overall structure of the QUBE satellite. Rails and backplane build the basic structure. At the top part are the optical terminal OSIRIS built by the DLR IKN and the star tracking sensor. The middle part contains the quantum payloads from LMU and MPL, the attitude determination and control system (ADCS), and the wavelength division multiplexer (WDM) unit. The actuating parts of the ADCS are magnetotorquers and reaction wheels. The bottom part comprises the electric power system (EPS) including batteries, the on-board controller (OBC), and the communication module (COMM). Not shown are the UHF antennas and the solar panels.

state [66], can provide random numbers for the payload-internal QKD sender as well as for the LMU payload. For a picture of the MPL unit, please see figure 4.5.

The optical signals of both, the sender units from MPL and from LMU, are coupled into two separate single mode fibers, which are interfaced to a wavelength division multiplexer unit (see section 2.2.3 and section 2.2.4).

2.2.3 Optical Terminal OSIRIS

The optical link between the satellite and the optical ground station (OGS) (see section 2.3) is provided by the optical terminal OSIRIS (optical space infrared downlink system, see figure 2.2), built by the DLR IKN in Oberpfaffenhofen. It features a clear aperture of 22 mm and is equipped with a 1540 nm laser with an optical peak output power of 100 mW, which is required for the pointing, acquisition, and tracking (PAT) routine for the optical link. Here, in the first phase, the OGS points towards the satellite, which is supported by the

GPS coordinates received from the satellite. In the second phase, the OGS sends a beacon, which is detected by the four-quadrant photodetector of OSIRIS. This finally allows a closed-loop tracking control towards the OGS via the fast steering mirror of OSIRIS within an angular range of one degree. Furthermore, the tracking laser of OSIRIS can be modulated with the clocks of the QKD senders to enable the synchronization of the satellite and the OGS (see section 6.2.1).

The optical fiber from the tracking laser is, similarly as the two fibers from the QKD sender modules, plugged into a wavelength division multiplexer (WDM) unit (see section 2.2.4). The output of the WDM unit is connected to the optical input port of OSIRIS. The optics design of OSIRIS, the used materials for the lenses, and the surface coatings are optimized for bichromatic operation. The divergence for both QKD signals accounts to about 135 μrad full angle compared to 27 μrad for diffraction limited operation. Thus, the link efficiency is further reduced due to the larger illuminated spot on Earth.

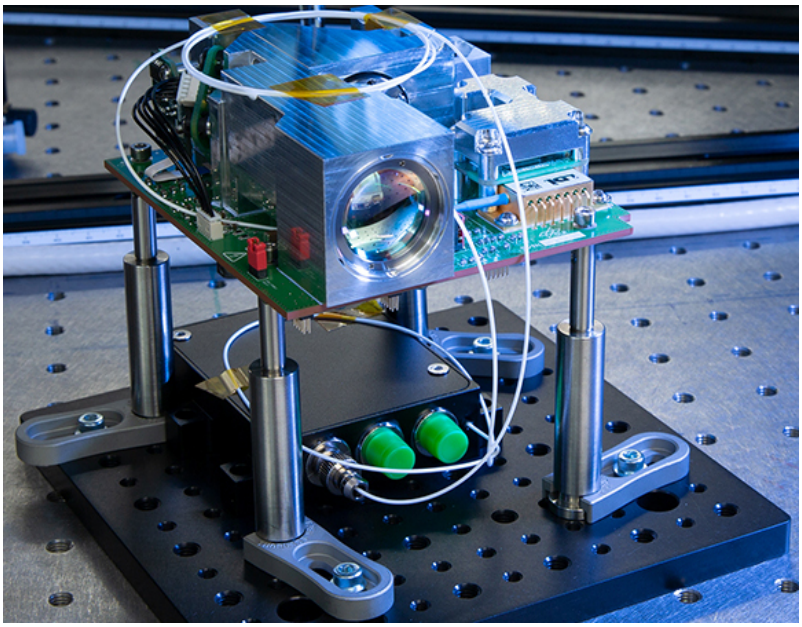


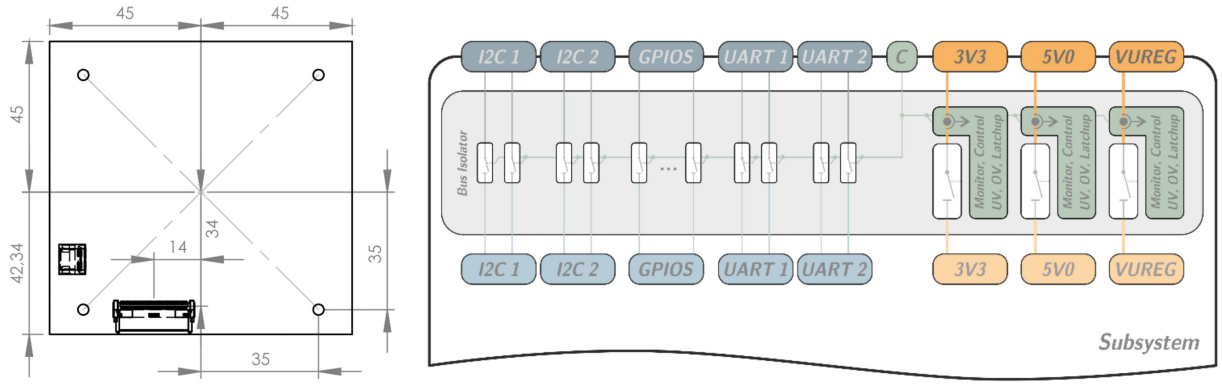
Figure 2.2: The OSIRIS terminal, with a clear aperture of 22 mm supports bichromatic operation. The black box under OSIRIS contains the wavelength division multiplexer (WDM) parts. On the most left port the fiber coming from the OSIRIS tracking laser is plugged in. For more details regarding the WDM unit, please see section 2.2.4. The picture is shown with kind permission of the DLR IKN.

2.2.4 Interfaces

The payloads described in the last section must be mechanically integrated into the satellite and need to be interfaced electrically and optically.

UNISEC Standard for the Mechanical and Electrical Interface

The university space engineering consortium (UNISEC) [67] provides standards for the geometrical and the electrical interfaces of a Cube-satellite, which we implemented in QUBE. The dimensions of the standard printed circuit board (PCB) are defined with 90 mm × 87.35 mm (see figure 2.3 (a)). All data and power supply lines are provided by a compact 50-pin connector and must be able to be controlled and isolated for every subsystem which is connected on the bus (see figure 2.3 (b)).



(a) (b)

Figure 2.3: The mechanical (a) and electrical (b) UNISEC interface [67] used in QUBE. Except for the bus isolation parts (see figure 3.2 (e)), front and back part of the PCB can be freely fit with electronics components. Resulting hardware is shown in figure 3.2 and figure 3.6.

Synchronization Interface

To establish the synchronization of the QKD payloads on the satellite and the optical ground station, we modulate the tracking laser of the optical terminal OSIRIS with the QKD sender clocks, which then can be detected and fed into a clock recovery circuit on ground. The UNISEC bus does not provide high bandwidth data lines capable to transmit a clock signal with a low jitter of maximally a few hundred picoseconds. For this reason we implemented a dedicated twisted pair cable, allowing for the transmission of low voltage differential signals between the LMU and MPL payloads and between the MPL payload and OSIRIS. On the MPL board it can be switched which of the two clocks, either the LMU input clock or the one generated on-board, becomes fed into OSIRIS. The finally achieved characteristics of the implementation of this scheme can be found in section 6.2.1.

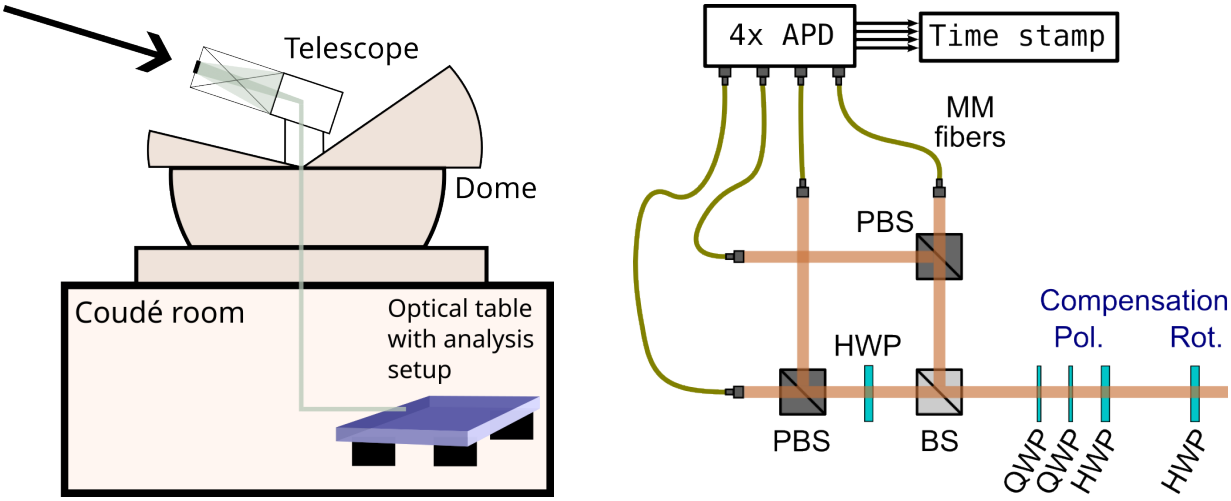
Optical Interface

The optical terminal OSIRIS (see section 2.2.3) comprises one optical input. For this reason the three laser sources in QUBE, i.e., the tracking laser of OSIRIS emitting at a

wavelength of 1540 nm, the MPL QKD sender at 1571 nm, and the LMU QKD sender at 850 nm, must be combined into one single mode fiber. This is achieved by the usage of a wavelength division multiplexer (WDM) unit (see figure 2.2) based on thin-film filters [68], which has been built by the company Bitline Systems Pty. Ltd. The cascading is designed such that at a first WDM the fibers coming from MPL and OSIRIS, and at a second WDM the output of the first WDM and the fiber coming from LMU, are combined. The insertion loss of the three inputs of the WDM unit is specified to below 1 dB each and the polarization-dependent loss of each path to below 0.2 dB. For the WDM unit output fiber, which is connected to the OSIRIS input port, we have chosen a HI980 fiber produced by Corning. This fiber provides sufficiently low attenuation for both wavelength divisions and still shows adequate single-mode characteristics at a wavelength of 850 nm.

2.3 Optical Ground Station and QKD Receiver

The optical ground station (OGS) is located at the DLR IKN in Oberpfaffenhofen nearby Munich. The OGS features a Cassegrain telescope with a diameter of the primary mirror of 80 cm and is designed for a wide spectral working range from 598 nm to around 1550 nm. The optical elements (lenses and mirrors with corresponding coatings) along the optical path into the Coudé room are optimized to provide low polarization-dependent losses of below 1 dB in total. An optical link between the OSIRIS terminal on the satellite and the OGS can be established by performing a pointing, acquisition, and tracking (PAT) scheme (see section 2.2.3) using a 1590 nm uplink beacon, which gets detected on the satellite. A dichroic mirror in front of the QKD analysis setup serves for the separation of the weak QKD signals and the downlink tracking laser of OSIRIS. Telemetry and telecommand (TMTC) of the satellite over the UHV connection is planed to be made from the ZfT in Würzburg.



(a) (b)

Figure 2.4: (a) Schematics of the optical ground station (OGS). The 80 cm Cassegrain telescope collects the incoming light and guides it to the Coudé room under the dome construction. (b) Schematics of the polarization analysis unit consisting of a beam splitter (BS), two polarizing beam splitters (PBSs), and a half wave plate (HWP). The reflected path of the BS corresponds to a measurement in the B_Z basis, while the transmitted light gets analyzed in the B_X basis due to the HWP behind the BS. The analysis part and the avalanche photo diodes (APDs) are interfaced via multimode mode (MM) fibers. Further waveplates serve for the compensation of the rotated polarization states and the rotation of the satellite around the Z-axis.

The QKD analysis setup for the QKD signal at 850 nm consists of a standard BB84 receiver with a passive basis choice as shown in figure 2.4 (b). The detection events of the four APDs are fed into a timestamp unit, which runs synchronously to the QKD

sender. The synchronization scheme, here based on the clock recovery from the modulated downlink tracking laser of OSIRIS (see section 2.2.4 and section 6.2.1), has been already shown in a comparable scenario also using an additional laser, please see Refs. [55, 69, 70]. The polarization of the incoming QKD signals is on the one hand initially rotated due to the optical fiber used in the satellite and, on the other hand, gets further rotated in the OGS because of the optical elements along the optical path towards the analysis setup. Both rotations can be compensated by an unitary transformation using three waveplates. The compensation scheme requires that bright calibration pulses are sent by the QKD sender before a QKD sequence in order to optimize the setting of the waveplates. The final procedure has not been tested yet but is also based on former works within our group, please see Refs. [55, 69, 71, 72]. A question to be investigated is the influence on the incoming polarization states depending on the orientation of the telescope. If necessary the telescope must be characterized at different positions such that a look-up table for compensation settings can be made. Using a motorized HWP in front of the polarization compensation unit and the known rotation speed of the satellite around the Z-axis, which is assumed to be a few degrees per second at most, the rotation of the satellite can be compensated.

2.4 QKD Feasibility Analysis

2.4.1 Fundamentals to QKD

The basic concept of QKD can be introduced best by discussing the first QKD protocol, proposed in 1984 by Charles H. Bennett and Gilles Brassard, called the BB84 protocol [15]. The protocol encodes information in *qubits*, which can be seen as the quantum mechanical analogon to the smallest classical information unit *bit*. A qubit is represented by a quantum mechanical two-level system, which can be implemented for example using the polarization degree of freedom of a photon. A quantum mechanical two-level system spans a two-dimensional Hilbert space providing three maximally conjugated pairs of basis states. By staying in the picture of the polarization of a photon, this can be for example the horizontally and vertically polarized states in the basis B_Z, the $+45°$ and $-45°$ polarized states in B_X, and the circularly left and right polarized states in B_Y, corresponding to the eigenstates of the respective Pauli spin operators σ_x, σ_y, and σ_z. The BB84 protocol utilizes that a measurement of a certain state out of these bases leads to uncorrelated results if the measurement is performed in an other basis. The presented bases are even a special case as for a measurement in the wrong basis the uncertainty is maximal, for which they are called mutually conjugated bases. In the case of a measurement in the eigenbasis of the state, the results are, by ignoring the imperfections in real implementations here, perfectly correlated. While the last point is used in order to generate the key material, the first point provides the security against eavesdropping. Another important fact is that quantum states can not be copied or cloned, which is shown by the non-cloning theorem [73].

The sequences of the BB84 protocol require a sender (Alice) which can prepare the eigenstates of two of the three possible bases, a receiver (Bob) capable to analyze the states in the same two bases, a quantum channel (freespace link or optical fiber) which connects the sender and the receiver, and an authenticated classical channel over which post-processing tasks can be performed. Then the procedure works as follows:

- Alice sends a stream of single photons, each randomly prepared in one of the four possible polarization states. By considering the potentially simplest implementation in practice, we choose an equal proportion of the states from the bases containing linearly polarized states, namely $B_Z = \{|H\rangle, |V\rangle\}$ and $B_X = \{|+45\rangle, |-45\rangle\}$.

- Bob measures the incoming photons with 50% probability in either the B_Z or the B_X basis respectively, such generating a string of detection results, called the raw key, with a length of N_{raw}.

- Alice and Bob perform the so called sifting, i.e., Bob communicates in which basis the measurement was performed for each detected photon. Only the events with matching bases are kept and stored in the so called sifted key of the length N_{sifted}.

- Unavoidable imperfections in the hardware implementation and also a possible intervention by an attacker will lead to errors in the sifted key, which must be corrected us-

ing error correction schemes as Cascade [74, 75], Winnow [76], or low-density parity-codes [77–79] over the classical channel. The ratio of the false to the total number of events in the sifted key defines the so called quantum bit error ratio (QBER). Here, a comment to point out the unique property of QKD regarding the scope of Alice and Bob, even if an eavesdropping attempt has been recognized, should be made. Based on the QBER, not only the presence of an eavesdropper (Eve) can be detected but even the amount of information which maximally could have been leaked can be determined. Also important is that the protocol treats all errors equally, independently whether they occurred due to hardware imperfections, e.g., detector dark counts, or due to an attack.

- In the so-called privacy amplification, the error-corrected sifted key gets shortened, typically performed by using universal hash functions [80], by the amount of information resulting from the measured QBER. The key is shrunk further by the amount of information which is unavoidably leaked because of the communication between Alice and Bob to perform the error correction. From these two contributions, the upper bound for the resulting secure key length N_{sec} results to

$$N_{\text{sec}} = N_{\text{sifted}} \times (1 - 2H_2(\text{QBER})), \tag{2.1}$$

  where $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the Shanon entropy.

Let us consider the most obvious and simple attack, namely that an attacker intercepts the photon stream and resends newly prepared photons to Bob. Here, Eve is forced to analyze each incoming photon in one of the two bases and then resends a photon, which is prepared in the same polarization state as the measured one. In the case of matching bases between Alice, Eve, and Bob, Eve's intervention cannot be detected. However, in the case when the bases between Alice and Bob match but Eve has chosen the wrong one, Alice and Bob will observe uncorrelated results in the sifted key, which results in an increased QBER.

So far we assumed an ideal implementation of the protocol, however, weaknesses of real QKD devices, which allow Eve a multitude of possibilities to attack the system, must be considered. At Bobs side for example the detection efficiency mismatch [27], the dead time of detectors [28], the blinding of the detectors [26], or the spatial mode mismatch [29] can be exploited as side channels by Eve. The security of the system can be reestablished by counter measures often realizable by appropriate temporal, spatial, or wavelength filtering. The particular vulnerability of the detection part of the QKD systems gave rise to the measurement-device-independent QKD protocols [81, 82]. For the hardware implementation at the sender side, the non-perfect preparation of the polarization states must be taken into account by the preparation quality q:

$$q = -\log_2 \max |\langle \Psi_{B_Z} | \Psi_{B_X} \rangle|^2. \tag{2.2}$$

Here, the largest overlap between the states of the two bases quantifies how well the

settings are conjugated indeed. Because of the steep characteristics of the log-function for values < 1, even slight preparation imperfections will lead to significant deviations to the ideal value of mutually conjugated bases with $q = 1$.

Furthermore, the usage of lasers for generating weak coherent pulses instead of a real single photon source [83–85] has opened the door for the so-called photon number splitting attack [86–88]. Here, Eve utilizes that weak coherent pulses can contain more than one photon per pulse, from which theoretically one photon could be split of and stored for later analysis. Gottesmann et al. [89] provided a theory to encounter this by introducing the *tagging* probability $\Delta = p_M/p_D$, where p_M and p_D denotes the probability for a multi-photon pulse and that an emitted photon is detected, respectively. By also taking the preparation quality of equation (2.2) into account [55], the achievable secure key length is

$$N_{\text{sec}} = N_{\text{sift}} \times \left((1-\Delta) - f_{\text{err}}(\text{QBER}) H_2(\text{QBER}) - (q-\Delta) H_2\left(\frac{\text{QBER}}{1-\Delta}\right) \right), \tag{2.3}$$

where $f_{\text{err}}(\text{QBER})$ denotes the efficiency of the error correction. As already discussed in [72], the key generation capabilities scale with $e^{-2\eta}$, where η is the overall transmittance between Alice and Bob, including detector efficiency. While this is manageable for moderate losses of up to approximately $-15\,\text{dB}$, it does not work for higher losses as it is the case for example in satellite-to-ground links, which exceed $-30\,\text{dB}$.

W.-Y. Hwang and H.-K. Lo et al. [90–92] proposed a concept to extend the BB84 protocol by so called *decoy* states, i.e., using not only one pulse intensity, which, in the quantum mechanical picture, are non-orthogonal states. The idea behind is that an eavesdropper is forced to treat the incoming pulses similarly as the attacker cannot distinguish them with certainty, when perfoming a PNS attack. By this, the photon statistics of the corresponding pulse intensities get changed differently, which can be detected by Alice and Bob. A further development of this method by Ma et al. [93], which uses a hardware model of the QKD devices by N. Lütkenhaus [94], provided a theory by which all needed parameters are experimentally accessible. Here, the sender generates phase-randomized weak coherent pulses each containing an i-photon state $|i\rangle$ with $i = 1, 2, ...$, which can be described by a density matrix following a Poisson distribution with a mean photon number μ:

$$\sum_{i=0}^{\infty} \frac{\mu^i}{i!} e^{-\mu} |i\rangle \langle i| . \tag{2.4}$$

The transmittance of an i-photon state sent by Alice through the quantum channel can be expressed by

$$\eta_i = 1 - (1-\eta)^i. \tag{2.5}$$

The so called *yield* of an i-photon state Y_i represents the conditional probability that an i-photon state sent by Alice leads to a detection event at Bob's side:

$$Y_i = Y_0 + (1-Y_0)\eta_i = Y_0 + \eta_i - Y_0\eta_i \cong Y_0 + \eta_i, \tag{2.6}$$

where Y_0 is the probability for a background detection event caused by stray light and detector darkcounts. Further, we introduce the *gain* of an i-photon state Q_i,

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu}, \tag{2.7}$$

which is the product of the i-photon yield and the probability that Alice sends an i-photon state. By summing over all values of i the overall gain Q_μ is given by

$$Q_\mu = \sum_{i=0}^{\infty} Q_i = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} = Y_0 + 1 - e^{-\eta\mu}. \tag{2.8}$$

With the given hardware model, Ma et al. [93] expressed the achievable secure key rate for the so called *vacuum + weak decoy state protocol*. Here, besides the signal pulses with a mean photon number of μ, empty pulses and weak decoy pulses with $\nu < \mu$ are sent.

$$R_{\text{sec}}^{\text{decoy}} \geq B \mathrm{f}_{\text{rep}}(-Q_\mu f_{\text{err}}(\text{QBER}_\mu) H_2(\text{QBER}_\mu) + Q_1(1 - H_2(\text{QBER}_1))), \tag{2.9}$$

where B denotes the basis choice ratio[1], f_{rep} is the repetition rate of the sender, QBER_μ and QBER_1 are the QBERs of the signal and 1-photon pulses and Q_1 is the 1-photon gain. Ma et al. gave lower and upper bounds for the 1-photon gain Y_1, Q_1, and $QBER_1$, which are solely dependent on experimentally accessible protocol parameter:

$$Y_1^L = \frac{\mu}{\mu\nu - \nu^2}\Big(Q_\nu \mathrm{e}^\nu - Q_\mu \mathrm{e}^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\Big) \leq Y_1, \tag{2.10}$$

$$Q_1^L = \mu \mathrm{e}^{-\mu} Y_1^L \leq Q_1, \tag{2.11}$$

$$\text{QBER}_1^U = \frac{\text{QBER}_\nu Q_\nu \mathrm{e}^\nu - \text{QBER}_0 Y_0}{Y_1^L \nu} \geq \text{QBER}_1. \tag{2.12}$$

The η-dependency regarding the key generation capabilities is, similar to the case when using a true single photon source, proportional to $\mathrm{e}^{-\eta}$. This again enables sender concepts based on weak coherent pulses to be securely used QKD applications with high channel losses.

2.4.2 QUBE QKD Link Simulation

In this section, the QKD feasibility of QUBE will be discussed. For this, a realistic mission scenario has to be investigated and merged with the model of the QKD hardware, detailed

[1] A typical value for B is $\frac{1}{2}$, which corresponds to a basis choice ratio of 50/50. Lo et al. [95] proposed an asymmetric basis choice scheme by which the key generation rate can be improved by almost a factor of two in the asymptotic limit. For real implementations a basis choice ratio of 70/30 or 90/10 seems realistic.

in the previous section.

Before going into detail, one must note that a full QKD procedure cannot be performed with the built system. On the one hand, our QKD sender is not equipped with sufficient post-processing capabilities and on the other hand, cannot run a decoy protocol, which is mandatory for scenarios with high channel loss, such as satellite links. In an ongoing project within our group, decoy state generation could already be demonstrated with an enhanced table-top electronics [70] and can also be straightforwardly implemented within future satellite hardware. Furthermore we discuss the QKD feasibility in the asymptotic limit, i.e., under the assumption that the determination of protocol parameters can be performed without uncertainties. Theories which also include finite statistics effects do exist [96–98], however, the influence for our mission QUBE is an ongoing subject to be investigated and beyond the scope of this work.

Based on the theory by Ma et al. (see section 2.4.1), we simulated the secure key rate dependent on the channel loss for different hardware scenarios. For this we modeled the overall transmission η, the background detection probability Y_0, and the expected QBER for the signal pulses QBER_μ close to a work by Gruneisen et al. [99]:

$$\eta = \eta_{\mathrm{channel}} \times \eta_{\mathrm{receiver}} \times \eta_{\mathrm{spectral}} \times \eta_{\mathrm{detector}}, \tag{2.13}$$

with η_{channel} being the transmission of the channel[2], η_{receiver} the transmission of the analyzer setup, η_{spectral} the transmission of the spectral filter before the analyzer setup, and η_{detector} the efficiency of the detector.

$$Y_0 = (R_i \times \eta_{\mathrm{receiver}} \times \eta_{\mathrm{spectral}} \times \eta_{\mathrm{detector}} \times 4R_{dc}) \times t_{dw}, \tag{2.14}$$

with R_i being the rate of the background photons collected by the receiver telescope, R_{dc} the detector dark count rate of one of the four detectors used in the receiver setup, and t_{dw} the detection window for time filtering.

$$\mathrm{QBER}_\mu = \mathrm{QBER}_0 Y_0 + \mathrm{QBER}_{\mathrm{intr}}(1 - \mathrm{e}^{\eta\mu}), \tag{2.15}$$

where QBER_0 denotes the error probability caused by background noise and $\mathrm{QBER}_{\mathrm{intr}}$ the QBER due to preparation and detection imperfections.

The performance of two different detector systems has been investigated for this work: Silicon avalanche photo diodes (Si-APDs) and superconducting nanowire single photon detectors (SNSPDs). Besides differing in their detection efficiency and dark count rate, SNSPD systems require single mode (SM) coupling, which is only optional for Si-APDs. Latter ones can also be directly freespace coupled or used with multi mode fibers. On the one hand, SM coupling enables a highly effective background photon filtering, as the receiver system field of view can be designed extremely small, however, due to atmospheric turbulences, adaptive optics is needed to improve the SM coupling or enable it at all (ex-

[2]From ex-aperture satellite over the hundreds of km freespace-distance including losses at the receiver telescope up to the entrance of the BB84-polarization analyzer.

pressed by $\eta_{\text{coupling-SM}}$, see table 2.1). For the key rate simulation, a background photon contribution similar to the one of the QKD experiment by Nauerth et al. [42] is assumed. There, after $-2\,\text{dB}$ losses on the telescope mirrors and $-4\,\text{dB}$ losses due to the detector efficiency, about 500 clicks on each of the four detectors have been measured. This corresponds to about 8000 photons per second which are collected by the receiver telescope. As we plan to use a narrower interference filter (3 nm FWHM instead of 10 nm), this number can be reduced by the filter ratio, leading to 2400 photons per second. These and the remaining simulation parameters are shown in table 2.1. They are based on specifications of commercially available hardware (filters, detectors) as well as reasonable values for protocol and performance parameters as the basis choice ratio, QBER, time as well as spatial filtering and the efficiency of the error correction code. This allows in the following to give a realistic picture of the key rate generation capabilities, despite most of the receiver hardware at the optical ground station is not set up and tested so far.

f_{err}	Efficiency of the error correction	1.2
f_{rep}	Repetition rate	100 MHz
B	Basis choice ratio	70/30
μ	Mean photon number signal pulses	0.5
ν	Mean photon number weak decoy pulses	0.15
QBER_0	QBER caused by background detections	50%
$\text{QBER}_{\text{intr}}$	QBER due to preparation and detection imperfections	2.50%
η_{receiver}	Transmission through polarization analysis unit	80%
η_{spectral}	Transmission through spectral filter (3 nm FWHM)	80%
t_{dw}	Time filtering window	0.5 ns
$R_{dc(\text{SNSPD})}$	Dark count rate for SNSPDs per detector	$25\,\text{s}^{-1}$
$\eta_{\text{detector(SNSPD)}}$	Efficiency of the SNSPDs	90%
$R_{dc(\text{Si-APD})}$	Dark count rate for Si-APDs per detector	$100\,\text{s}^{-1}$
$\eta_{\text{detector(Si-APD)}}$	Efficiency of the Si-APDs	60%
$\eta_{\text{coupling-SM}}$	Efficiency single mode coupling (adaptive optics)*	90%
R_i	Background photons**	$2400\,\text{s}^{-1}$
δ_{R_i}	Background reduction by strong spatial filtering	$-10\,\text{dB}$

Table 2.1: Parameters used for the QKD key rate simulation. *For the simulation of the corresponding scenario, this value gets multiplied with the detector efficiency. **The number of photons collected by receiver telescope and detected after an interference filter with a center wavelength of 850 nm and a FWHM 3 nm.

For the secure key rate simulation, three combinations of detector and filter systems have been investigated: An SNSPD configuration, strong spatially filtered (SM coupled) as well as two Si-APD configurations, with either strong (SM coupled) or moderate (freespace or multi-mode coupled) spatial filtering (see figure 2.5).

Up to a channel attenuation of about $-40\,\text{dB}$, the three configurations show the identically decreasing trend of the secure key rate over the channel loss. However, within this attenuation regime, the SNSPD system enables higher key rates due to their higher

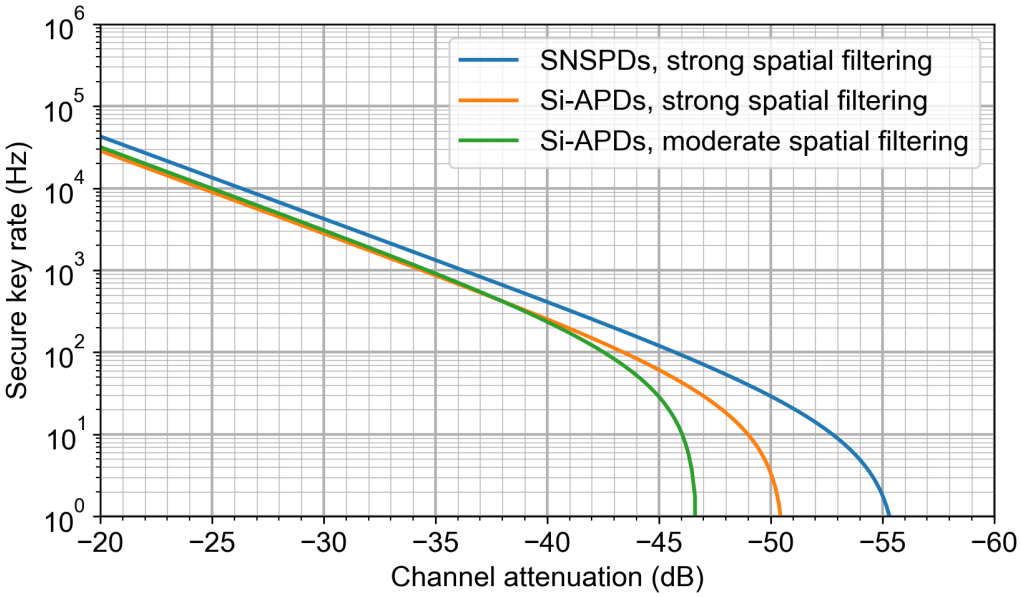


Figure 2.5: The simulation of the secure key rate, based on the theory provided by Ma et al. [93] (see section 2.4.1), over the channel attenuation, i.e., freespace- and collecting-losses, excluding losses due to analysis and detection. The simulation parameter are given in table 2.1. Three hardware configurations regarding used detectors and background filtering are plotted: Superconducting nanowire single photon detectors (SNSPDs) strongly filtered and silicon avalanche photo diodes (Si-APDs) with strong and moderate filtering.

detection efficiency, despite the additional losses due to the required SM-coupling. By comparing the two Si-APD configurations in this regime, the system with moderate filtering performs slightly better because of the higher coupling efficiency. For channel losses greater than about −40 dB, the key generation performance starts to differ significantly. The deviation from the, in the log-log representation, linearly decreasing key rate starts at first at the moderately spatially filtered Si-APD system. This is because with increasing losses, the background photon contribution becomes relevant compared to the already strongly attenuated QKD signal pulses, leading to a rapidly rising QBER. The point of vanishing key generation capabilities is at around −46 dB. This point can be pushed to above −50 dB with the same Si-APDs by a reduction of the background photons by one order of magnitude with strong spatial filtering. By comparing the two strongly filtered systems, the SNSPD configuration in general allows higher key rates but also a higher channel attenuation up to −55 dB. The higher key rate generation performance is because of the better detection efficiency and the increased loss tolerance is because of the lower dark count rate of this detector type.

The discussion so far within this section allows for the general valuation of the QKD capabilities with the built QKD sender for QUBE. An important point to note is that the presented results are only valid for night-time operation (both satellite and optical ground

station are in the Earth's shadow and thus the relatively low contribution of background photons) and also do not account for finite-statistics effects. Already at a very early stage of this project it was foreseeable that, mainly because of the small sender telescope aperture ($\varnothing = 22\,\mathrm{mm}$), the channel losses will most probably exceed $-50\,\mathrm{dB}$. Later performed optics simulations by the colleagues of the DLR IKN confirmed this, estimating a channel attenuation between about $-47\,\mathrm{dB}$ and almost $-60\,\mathrm{dB}$ dependent on the link distance and reachable optical beam quality. In other words, that a secure key can be generated at all is very at the edge or actually beyond the tolerable loss limits even for the most performant and expensive receiver systems featuring adaptive optics and SNSPDs.

Chapter 3

Polarization Encoding QKD Sender Module

Our contribution to the satellite project QUBE is a QKD sender using BB84 polarization encoding, which fulfills the requirements regarding its size, weight, and power consumption to fit into a CubeSat as well as regarding its resilience against the harsh environmental conditions in space. This chapter details the design of this sender unit, followed by an overview of the assembly procedure of the microoptical part and the overall sender module.

3.1 Sender Design and Components

The design specifications for this QKD sender have been worked out in close coordination with our consortium partners. The dimensions of the sender unit were defined by the UNISEC standard [67] and its peak power consumption must be on the order of only a few Watts. The materials used and the mechanical construction must withstand a rocket launch, thermal cycles under vacuum conditions and the radiative environment in space. In this section, the resulting design of the microoptics part and the driver electronics are presented.

3.1.1 Microoptics

The design of the sender optics for QUBE is based on works by former colleagues within our group, mainly by Gwenaelle Vest [63, 64]. The goal there was to build a compact and robust QKD sender for handheld applications. This was achieved by using vertical-cavity surface-emitting lasers (VCSELs) together with passive microoptics components. Due to changed requirements for QUBE regarding the harsh environmental influences during a space mission, the need of higher optical output power, and the reproducibility of the assembly process, modifications of the underlying design had to be made, which are also discussed in this section. Furthermore, the main components of the QKD optics are described in more detail.

Optics Design

The true-to-scale representation of the QKD sender optics is shown in figure 3.1. A microlens array focuses the light emitted by four VCSELs into four waveguides embedded in a waveguide glass chip (WGC), which combines the four optical paths into one waveguide output. A single-mode fiber, which is attached to this waveguide output, interfaces the sender unit and the optical terminal OSIRIS in the satellite. The four BB84 polarization states are set by four polymer polarizer stripes. All components of the optics are assembled on a staircase-shaped holding structure made out of Kovar. Because of its low thermal expansion coefficient (TEC) of 5 ppm/K, which is close to that of many types of glass, Kovar is commonly used for submounts and fiber feedthroughs in optical packages. In our case, the TEC of the boro aluminosilicate glass from which the WGC is made amounts to 3 ppm/K, which acceptably agrees. For comparison, the TEC of aluminum or titan is 23 ppm/K and 9 ppm/K, respectively. Except for the VCSEL array, which is fixated via a silver epoxy adhesive (H20E by Epoxy), all components are fixated using an UV curing adhesive (OP-67-LS by Dymax). The procedure of the whole assembly is detailed in section 3.2.

Regarding the vulnerability of the microoptics components and adhesives to radiation damages or degradation, a first design review of the components together with experts of the consortium partner OHB in Munich did not identify potentially hazardous components in our design. To reinforce this, radiation tests have been performed during the project (see section 4.1).

Concerning vacuum, we identified the operation of the VCSELs in vacuum as the most critical one. Because of the lack of literature and studies regarding this issue, we decided to perform an in-house long-term study in a thermal vacuum chamber (see section 4.3). In the case of identifying the incompatibility of any of the optics components against vacuum, a possible remedy would have been to hermetically package the whole optics part.

Modifications of the Underlying Design for a Handheld QKD Sender

- The maximally reachable mean photon number per pulse (μ) of the handheld device was less than 1 [72], directly measured at the output of the waveguide. For QUBE, additional losses occur due to a fiber coupling after the waveguide chip (in the worst-case about -10 dB) and the transition through the wavelength-division multiplexing unit (-2 dB) as well as through the optical terminal (-13 dB). Furthermore, for testing purposes within the QUBE mission, it is beneficial to send brighter pulses with, e.g., $\mu = 10$. Altogether, these requirements made an increase of the optical output power of about three orders of magnitude necessary. We identified three points to improve the optical output power:

  1. Omitting the neutral density filter used in the handhald device (-10 dB).
  2. The usage of a polymer polarizer foil, which features less optical losses (-4 dB) compared to the wire-grid polarizers used so far (-11 dB) [100].

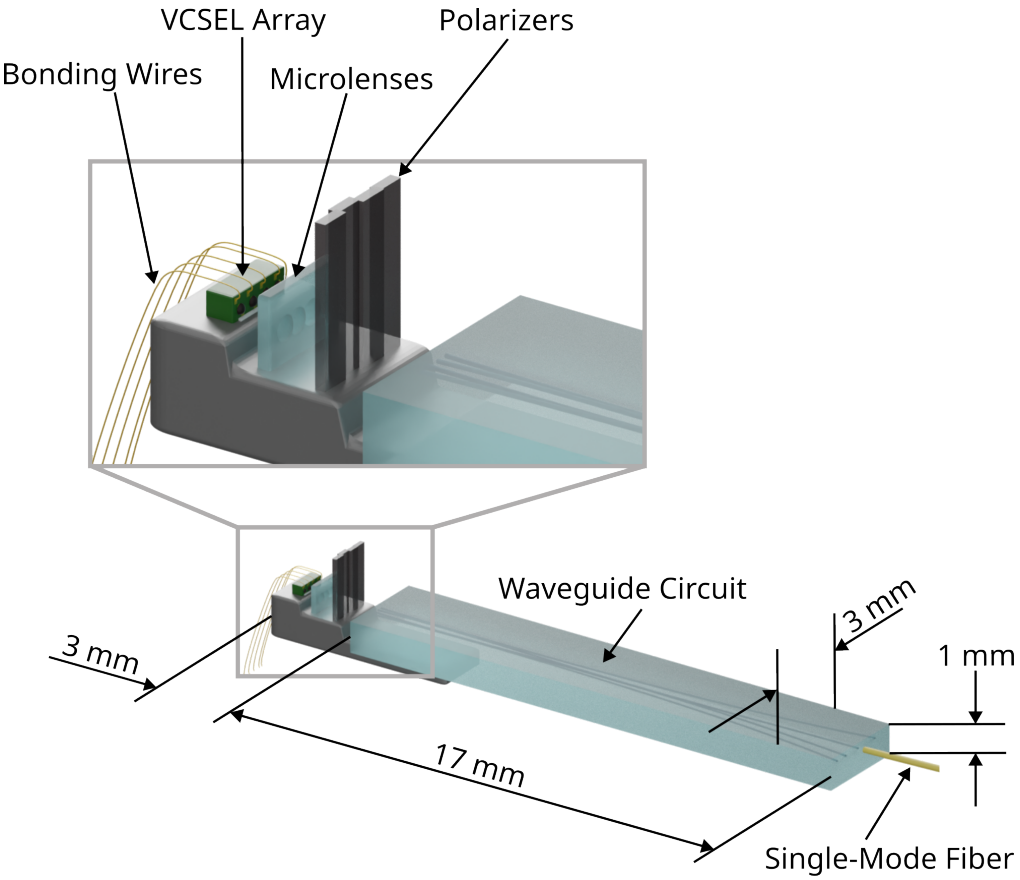


Figure 3.1: The design of the QKD optics comprising the waveguide glass chip (WGC) as well as all active and passive components for the preparation of BB84 polarization states. The VCSEL array, microlens array, and the polarizer stripes are attached to the WGC with a Kovar holding structure. Height and distances between the components are optimized for simultaneous and efficient coupling into the four waveguide inputs. A single-mode fiber is attached onto the defined output port.

3. An improved assembly procedure to optimize the coupling from the VCSELs into the waveguides. Here, the main factor is to assemble the optics without glass spacers. These are intended to provide the correct distances between the microoptics components, however, we believe that the lack of degrees of freedom to position the components can hinder an optimal coupling.

At the time of reviewing the optics design, the unknown losses at the fiber coupling as well as whether a new assembly procedure really can improve the coupling efficiency, made it difficult to estimate the final performance. However, an improvement in the required order of magnitude seemed feasible.

- For the QUBE mission, two identical sender optics must be assembled - one for testing

and qualification purposes (radiation, vibration, thermal-vacuum) and, in the case of passing all tests, one acting as flight model. The crucial task is the reproducibility of the microoptics assembly process, especially the gluing steps. By omitting all glass spacers, we can reduce the number of critical gluing steps to only two, namely fixing the microlens array and the waveguide chip onto a Kovar holding structure. Additionally, many UV curing processes, which can potentially harm already cured adhesive joints, are avoided.

- The already discussed modifications of the underlying design also have an impact on the operational stability. Due to the reduced number of components and adhesive joints, which goes hand in hand with a reduced number of mechanical interfaces and therefore potential mismatches of thermal expansion coefficients, the optical stability under thermal cycles (output power, polarization drifts) is improved. Another advantage is the reduced weight. This supports the mechanical robustness, which is important regarding the vibration loads during a rocket launch.

VCSEL Array

Vertical-cavity surface-emitting lasers (VCSELs) consist of distributed Bragg reflectors, which are built of a multitude of alternating layers of GaAs and AlGaAs, acting as a cavity. The active volume is placed in the cavity and comprises an InGaAS-GaAs[1] quantum well [101]. Due to their small size of only a few micrometer, they support high modulation speeds and feature single-mode operation.

The 4 x 1 array used in our QKD sender is manufactured by the company VI Systems in Berlin [102] (V50-850C product line, 250 µm diode pitch). The degree of polarization (DOP) of these VCSELs depends on the operation mode. While for continuous wave operation the DOP is close to 1, the DOP in pulsed mode is between 5% and 50% [63]. This enables to individually set the linear polarization directions using thin strips of foil polarizers.

Polarizers

The four polarization states required for the BB84 protocol are set via polymer based foil polarizers (XP-IR2 by Edmund Optics), also known as *Polaroid* polarizers [103–105]. By stretching a polyvinyl alcohol (PVA) foil, the PVA molecules become aligned in parallel. By doping the stretched foil with, e.g., iodine, a strongly polarization depending absorption characteristics for light transmitting through can be realized. The wavelength range can be modified by the insertion of dichroic dye molecules into the PVA foil.

Using a diamond saw, we cut off slim stripes with a width of 0.3 mm and a length of 4 mm[2]. The direction of polarization can be set with an accuracy of ±0.5°. An H, V,

[1] This hold for wavelengths between 650 nm and 1300 nm. For devices emitting between 1300 nm and 2000 nm, indium phosphide (InP) is used as laser active medium.

[2] The length of 4 mm is chosen for an easier handling of the fragile stripes. In a later step, the stripes are cut into two pieces with a length of 2 mm each.

+45°, and −45° oriented stripe become aligned along the long edges and fixated using UV curing adhesive. For more details to the production of the polarizer stripes please see Ref. [106].

Waveguide Circuit

The waveguide circuit utilized in the optics unit is used to overlap the four light sources into a single mode. Our device has been produced by the group of Prof. Roberto Osellame at the Politecnico di Milano. The waveguides are written into a boro aluminosilicate glass substrate using a femtosecond laser [63, 107, 108]. If the mutual distance of two waveguides is on the order of a few micrometers, evanescent coupling takes place forming a directional coupler. For our application, three balanced couplers are arranged in a 3D structure optimized for minimizing the path-dependent birefringence which causes a change of the orientation of polarization of the input states relative to each other. On the one hand this cannot be corrected later by an unitary transformation and on the other hand it leads to a worsening of the preparation quality q (see equation (2.2)). However, the path-dependent birefringence can be precompensated, i.e., the orientation of polarization before the waveguides can be chosen such that for the output states q is maximized. Note that with our scheme we only can prepare linearly polarized light as input states, which limits the capabilities for optimization.

We characterized four samples of waveguide circuits regarding the influence of each of the four waveguides embedded on the incoming directions of polarization. Please see Refs. [63, 72, 109] for details to the methods. We observed that the investigated samples show an almost negligible path-dependent influence. For this reason, we prepared the polarization foils oriented in H, V, +45°, and −45°, which is the easiest configuration in terms of their handling. Both optics units built with two of these waveguide circuits provide a high preparation quality of 0.98 each, which is close to the optimal value of 1 (see table 4.2 and table 5.1).

3.1.2 QKD Sender PCB

The printed circuit board (PCB) of our QKD sender unit comprises the electronic parts for the interfaces to the satellite, for controlling and operation, and moreover the area for the mounting of the optical bench.

A field programmable gate array (FPGA), with an emulated MSP430 microcontroller softcore, provides the software interface for telemetry and telecommand (TMTC) (see figure 3.2 a)). Furthermore, the FPGA controls the laser drivers (see figure 3.2b)) with a clock speed of 100 MHz. Here, one can choose between any predefined pattern or random numbers provided by the QRNG on the payload of the MPL. For tests with higher optical output power, the operation mode for the laser driver can be set to continuous wave (CW). The driving parameters and corresponding optical response of the final flight hardware can be found in table 5.2 and figure 5.3.

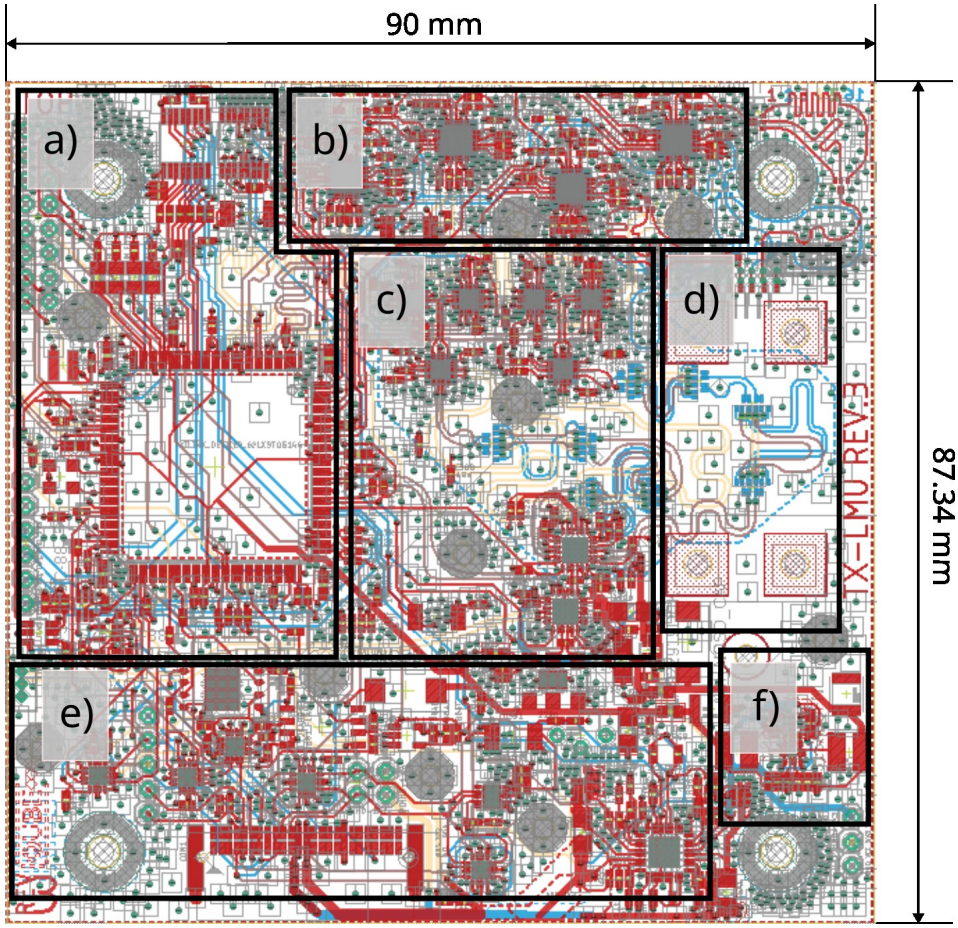


Figure 3.2: Schematics of the LMU QKD sender PCB with: a) FPGA and internal parts for operation, b) Laser drivers, c) Clock and pulse generation, d) Place for mounting and contacting the optics part, e) Interface to the satellite bus, (bottom center) 50-pin UNISEC [67], (top left corner) 3-pin connector for dedicated twisted pair cable for synchronization, f) Voltage conversion.

For the pulse generation (see figure 3.2 c)), hard-wired meander circuits for a passive clock delay between 20 ps and 160 ps in steps of 20 ps are used. Please see the Refs. [106, 109] for a detailed description of the pulsing scheme using these meander circuits as well as figure 4.3 and figure 5.1 which show the optical pulse timing characteristics of the built QKD senders.

The optical bench made of Kovar is mounted by four M2.5 screws from the bottom side of the PCB (see figure 3.2 d)). For contacting the VCSELs to the PCB we use holes at the contacts above the mounting area where the gold wires are put in and electrically contacted via a silver epoxy adhesive (H20E by Epoxy). In figure 3.6, the PCB together with the optical bench and the already contacted VCSELs is shown.

The electronics interface to the satellite is based on the definition of the UNISEC

bus [67] used in the QUBE satellite, comprising the power supply, I2C communication, and further data lines (see figure 3.2 e)). An additional dedicated twisted pair cable, which connects the MPL and DLR boards, serves for a low jitter transmission of the clock signal (see figure 6.1 and section 6.2.1). All lines coming from the UNISEC connector are controlled over isolation parts for protection purposes (see also section 2.2.4).

Besides 3.3 V, supplied by the UNISEC bus, two further voltage levels are required. Here, a step-down chip, which is connected to the unregulated voltage line on the bus, provides 1.2 V for the FPGA and 2.5 V for parts of the pulse generation (see figure 3.2 f)).

The mechanical fixation points of the PCB to the satellite structure using M3 threaded rods are provided by four holes at the corners of the PCB, which also serve for the thermal connection.

3.2 Assembly of the Microoptics and Overall Module

After the design phase of the QKD sender for QUBE, its components have been ordered, or built, respectively, and assembled. The PCB has been manufactured and assembled with the electronics components by the company Eurocircuits. Colleagues from the consortium partner OHB in Munich made an inspection of the PCB and performed minor adaptations. The assembly of the microoptics part and mounting it onto the electronics board were performed in our labs. The assembly setup and the various assembly steps are detailed in the following passages. At this point, two very important comments, which concern every single assembly step, should be made. First, at the workplace and during the transport or handling of the hardware, precautions against electrostatic discharges must be carefully considered. Second, all parts must be cleaned to be free of grease or other impurities, which especially holds for the surfaces where adhesive joints are made.

3.2.1 Setup for the Assembly

The setup for the assembly of the sender modules and its components consists of two manually operated 6-axis manipulation stages (I6000 by Luminos) for the translation of microgrippers (SG-1730 by SmarAct), a 3-axis basis stage as working area, and magnifying optics including lighting (Zoom 6000 by Navitar) (see figure 3.3).

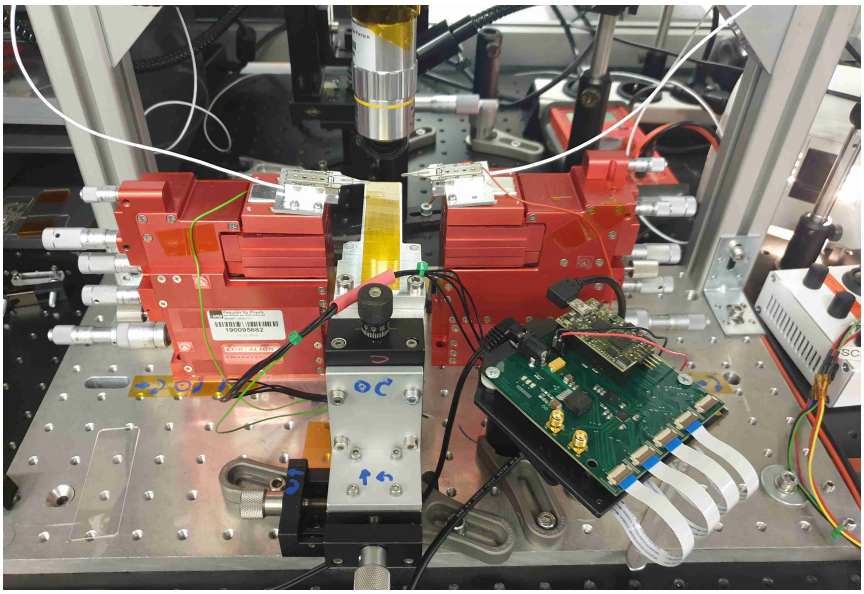
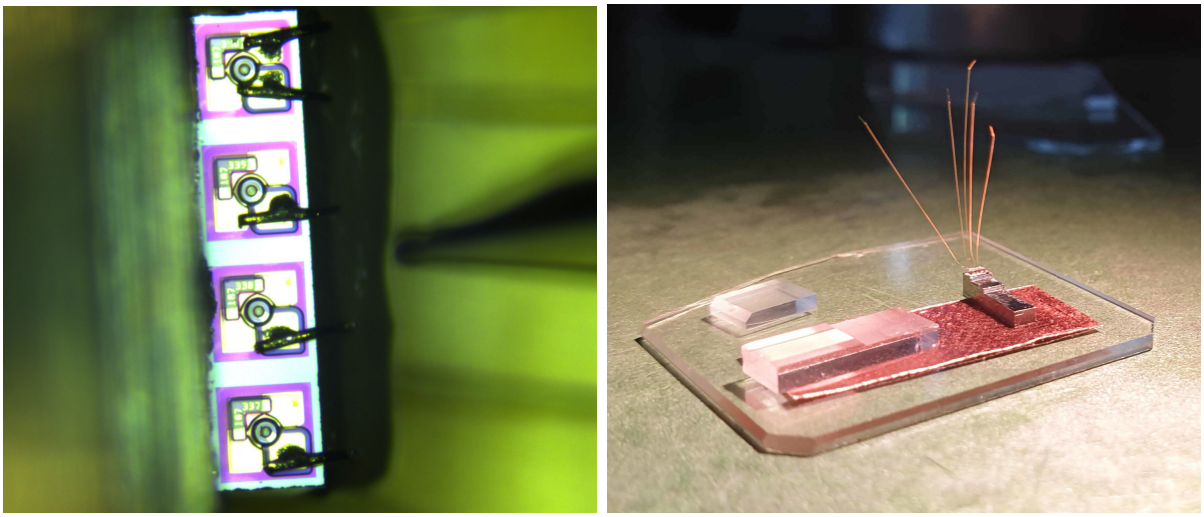


Figure 3.3: The manipulation setup for the integration of the sender modules. Two manual high precision 6-axis manipulation stages (red) equipped with microgrippers are placed left and right of a 3-axis movable aluminum base plate. Depending on the requirements different gripper tools as well as imaging optics can be used. A VCSEL driver electronics is used for the active alignment processes. Not shown are the UV curing components consisting of a light source and an optical fiber.

The combination of the high precision stages and the basis stage with large travel range of about 30 mm complement each other well as the former ones only provide a lateral travel coarse of 2 mm in all directions. For integration steps, which require direct optical feedback during the assembly, all four VCSELs can be driven using an appropriate driving electronics. The optical fiber which guides the UV light for the UV curing steps can be precisely aligned to the adhesive joints. The whole setup is placed under a filter flowbox providing a clean working environment corresponding to ISO class 5.

3.2.2 Assembly of the Microoptics Part

The first integration steps of the sender microoptics concern the preparation of the VCSEL array (see figure 3.4).



(a) (b)

Figure 3.4: (a) Topview on the VCSEL-array contacts with a standard bond wire fixed by silver epoxy adhesive. The VCSEL array has a common ground contacted via the topmost pad. For applying the epoxy a standard cannula is used. (b) Kovar staircase with fixed and contacted VCSEL array on the topmost step.

- Fixing of the VCSEL array with its side face onto the top step of the Kovar holding structure using silver epoxy adhesive.
- Adding a thin layer of UV adhesive, which acts as an isolation layer, on the other side of the VCSEL array where the gold bonding wires become placed with an excess length of about 0.1 mm.
- Fixing the loose wires via an second thin layer of UV adhesive. The short ends of the gold wires are bent over close to the contacts of the VCSELs.

- Applying a small amount of silver epoxy adhesive to every of the contacts using a hollow needle. The needle is not filled with the adhesive instead its tip gets only dipped into (see figure 3.4 (a)).

After the last of those steps, the VCSEL array and the Kovar holding structure are a unit that can nicely be handled (see figure 3.4 (b)) and temporarily mounted on a PCB where the loose wire ends are contacted. At this point, the optical response of the VCSELs can be tested. In some cases we observed that the contact between the bonding pad on a VCSEL and the gold wire has not been optimal, which leads to a strongly varying optical output power, zero output power, or a low frequent blinking in the order of some Hz of the corresponding VCSEL. This can be corrected by repeating the contacting procedure until a stable output power is measured. Thanks to the very long pot life time of the used silver epoxy adhesive of up to 3 days, multiple adhesive joints can be made without time pressure. The curing must be carried out between 80 °C and 100 °C for 3 h.

The next assembly steps comprise the alignment and fixation of the microlens array, the waveguide circuit, and the polarizer foils (see figure 3.5). For gripping the microlens array and the waveguide circuit, we use auxiliary metal wires which are glued on top of the devices (see figure 3.5 (a) and (b)). For holding the microoptical components also vacuum grippers could have been used, however, due to the extremely small size of especially the microlens array, the usage of the microgrippers seemed more feasible. The next steps are:

- Mounting of the PCB, where the Kovar staircase with the contacted VCSEL array is placed, onto the in 3-axis movable basis plate.

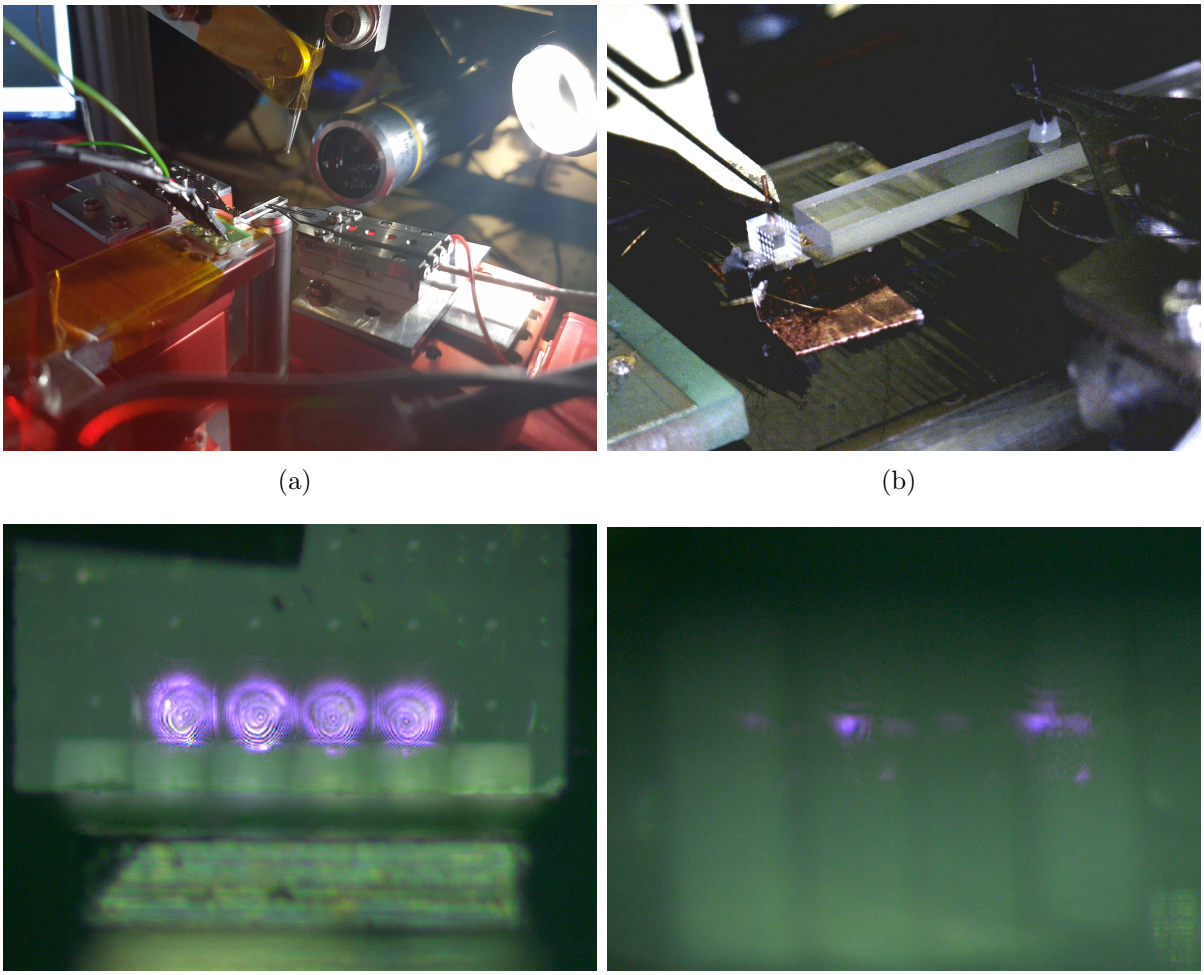
- Gripping and aligning of the microlens array and the waveguide circuit such that the coupling of the emitted light from the VCSELs into the four waveguides is maximized. The optical output power is monitored at the output of the WGC using a powermeter.

- Fixation of the microlens array: Lowering the 3-axis stage by about 1 cm enables to apply a small amount of UV adhesive by hand on the second highest plateau of the Kovar staircase. By returning to the initial position, the microlens array dips with its lower side into the applied adhesive. The coupling must be checked and, if necessary, corrected with the high precision stage. In the case of a satisfying position, the UV adhesive can be cured using the UV light source. Despite the very thin adhesive layer between the microlens array and the Kovar surface of about 100 µm (see figure 3.5 (c)), the shrink of the UV adhesive during the curing process must be considered. An empirical experience is to position the component before the curing slightly in front (sub-micrometer) of the maximum of the coupling in z-direction. The whole step of the fixation of the microlens array is impeded by the fast changing properties of the UV adhesive, even under strongly dimmed and filtered light conditions. Ideally, the whole process takes not longer than one minute. After the gluing process, the microlens array must be released by the gripper and the adhesive joint must be carefully examined under the microscope. Ideally, the whole area between the microlens array and the Kovar is filled with UV adhesive. To perform further

gluing steps to fill up missing areas is not recommended. Instead the microlens array must be carefully removed and the previous steps must be repeated.

- Fixation of the waveguide circuit: This integration step is performed similarly as the procedure of the microlens array, see above.
- Positioning and fixation of the polarizer foils: The polarizer foils are placed between the microlens array and the waveguide circuit. Their position can be monitored by observing them together with light from the VCSELs through the WGC (see figure 3.5 (d)). At an appropriate position, it can also be fixed by applying UV adhesive on its bottom side.

At this assembly stage, first tests of the polarization of the light at the output of the WGC can be performed. Then, the complete optics part can be removed from the auxiliary holding PCB and finally placed onto the driver electronics PCB, which is described in the following section.



(a) (b)

(c) (d)

Figure 3.5: (a) Setup with the microoptical components hold by the microgrippers. (b) Detailed view of the microlens array and waveguide circuit during their positioning. (c) Front view of the microlens array when all VCSELs are activated. The gap between the microlens array and the Kovar surface is about 100 µm. (d) Image through the waveguide circuit glass substrate showing the slim strips of polarizer foils with a width of approximately 0.3 mm.

3.2.3 Assembly of the Sender Module Unit

The steps for assembling the sender module are the following:

- Mounting the optical bench made of Kovar onto the driver electronics with four M2.5 screws from the bottom side of the PCB with a torque of 0.7 Nm.
- Fixation and contacting the microoptics unit. The adhesive gap between the waveguide circuit and the optical bench should be about 0.1 mm. The bonding wires are contacted to the PCB using silver epoxy adhesive.
- Attaching the optical fiber. This step is performed similarly as the procedure of the fixation of the microlens array and the waveguide circuit (see section 3.2.2). A strain relief of the optical fiber is realized via M2 screws which the fiber is fixed with UV adhesive.
- Fixation of the photodiode with UV ahesive. The electrical contacts are made with soldering joints.
- Fixation of the protective cover made of aluminum with three M2 screws from each of the two long sides with a torque of 0.35 Nm.
- Fixation of all screws on the module with UV adhesive.

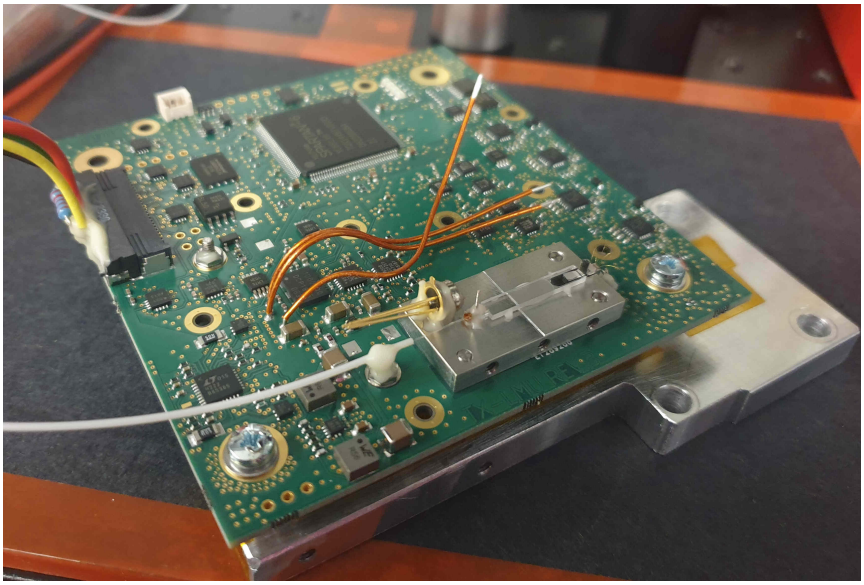


Figure 3.6: The sender flight model before the optical bench has been covered by an aluminum housing. The fully assembled flight model is shown in figure 6.1.

We have built two identical sender modules, namely the engineering qualification model (EQM) which serves for tests and the qualification for the mission (see chapter 4) and the

flight model (FM), which we have optically characterized (see chapter 5) and integrated into the satellite (see chapter 6).

Chapter 4

Qualification of the QKD Sender

Testing and qualification of satellite hardware is mandatory to ensure its functionality under space conditions, i.e., harsh radiation environment, vacuum, thermal cycles, and vibration loads during the satellite launch, but also its mechanical stability and therefore the safety for other space missions on the same launch vehicle. This chapter shows the methods and results of the performed radiation, vibration, and thermal-vacuum tests. All tests were performed with the engineering qualification model (EQM), which is an identical copy of the flight model (FM).

4.1 Radiation Tests

The following section discusses the radiation tests which were conducted to confirm the reliability of the LMU QKD sender under the space radiation environment in a low Earth orbit (LEO). At first, a short overview of space radiation effects and the radiation sources in space is given, followed by the methods and results of the total ionization dose (TID) tests of the EQM and proton radiation material tests of optics components.

4.1.1 Space Radiation Effects and Radiation Sources in Space

Due to their importance, radiation effects are already discussed in comprehensive reviews [110–112]. The content of this introduction into space radiation effects on electronics hardware follows the aforementioned references.

Particularly micro-electronic components are susceptible to damage under space conditions. An analytical analysis or simulation of the various radiation effects on every single component of a whole satellite in preparation of its design is basically impossible. Several electronics manufacturers offer an enhanced product line with radiation hardened components, however, mainly for cost reasons, CubeSat missions are often forced to also use customer-, industrial- or automotive-grade off-the-shelf components. Moreover, the *New Space* ansatz provides a fast-growing list of components with flight heritage due to the many small missions. Thereby, components which have initially not been designed to

be radiation hardened are yet shown to work under space radiation conditions. Besides electronics also other materials used, such as plastics or glass, can suffer from the space radiation environment. To reduce the chance for component failures or material degradation caused by radiation, critical structures can be shielded and tested by irradiating identical hardware during laboratory radiation tests. It should be also noted that failures occur not always because of an individual part or component, but can have their origin also in the electronics design as a whole, e.g., grounding or routing. To reveal and mitigate this type of problems, it is recommended to perform radiation tests on sub-system and system level.

In the following, a basic introduction into the main radiation effects, their sources (see table 4.1), and how laboratory radiation tests can support the space mission reliability is given.

	Trapped particles in Earth's magnetic field	Galactic cosmic rays	Solar events
Single event effects by direct ionization	No*	Yes	Yes
Single event effects by indirect ionization	Yes	No	Yes
Total ionizing dose	Yes	No**	Yes
Displacement damage	Yes	No	Yes

Table 4.1: Overview of space environment radiation sources and their effects
*exceptions by a few very susceptible devices, **excluding microdose effects, adapted from [110]

Radiation Damage Effects

In general, high energetic photons, electrons, protons and heavy ions can cause ionization by penetrating matter. The energy loss of an ionizing particle is due to its interaction with the electrons of an atom and/or the interaction with the atomic nucleus. In the context of radiation effects on spacecrafts, the main mechanism we consider is the electronic energy loss. Most of the electron-hole pairs, generated by incoming ionizing radiation, emerge in a two-step process. First, the incident particles transfer their energy onto primary knock-on electrons (delta rays). In a second step, these high-energetic electrons deposit their energy via further electron-hole pairs, excitation, but also phonon interaction causing the generation of heat [110].

Single Event Effects (SEEs) are a consequence of a single particle incident [113]. The initial ionization can be either direct, mostly over heavy ions, or indirect, i.e., the incident particles produce high energetic recoil particles, which is the dominant process for incident protons (min. required energy is about 10 MeV). For both mechanisms, the incident causes a high density of electron-hole pairs along the ion track followed by a phase of carrier recombination and/or carrier transport, i.e., carrier diffusion or, in presence of an electric field, carrier drift. The exact position of the particle incident in a device strongly

influences the impact by the single event transient (SET). Whereas deep in the silicon substrate the effect is typically small, the influence can become strong when happening near or inside of the active device volume, e.g., transition regions. There are two categories of SETs, namely nondestructive soft error effects and destructive hard error effects. Single- and multiple-bit upsets as well as single event functional interrupts account to the former, while single event latchups or single-event gate rupture/burnout belong to the latter [111].

Total Ionizing Dose (TID) Effects are considering cumulative effects due to the overall energy transfer of all incoming ionizing particles, which especially apply for insulators. In contrast to semiconductors, where the electron-hole pairs generated by the incoming ionizing radiation quickly dissipate, accumulating effects can appear, e.g., in the isolating gate oxide of a CMOS device [114] or in bipolar devices around the silicon-oxide region [115]. Due to electric fields, e.g., a bias potential, the liberated electrons move out of the oxide, while the number of the less mobile holes increases. The consequence is that a net positive charge in the oxide interior is accumulated, which can cause, for example, threshold voltage shifts in MOSFET devices. In contrast to CMOS devices, III-V material-based technology (GaAs devices, LEDs) is less susceptible because of a distinct electron-hole recombination. The electron-hole recombination condition can be differentiated between the cases when the generated electron-hole density is low (called "geminate") or high (called "columnar"). High energy electrons and protons lead to geminate recombination, while heavy ions cause columnar recombination. In the context of TID effects, geminate behavior is dominating and moreover the specific particle plays a secondary role if they belong to the same recombination type. For this reason TID effects can be also investigated via the geminate-type gamma radiation [110].

Displacement Damage (DD) is, similar to TID effects, an accumulated effect leading to a degradation especially of semiconductor devices. In this case, not the accumulated trapped charges but an increasing damage of the entire substrate or material volume harms the devices or components [116]. Semiconductor properties are defined by its crystal structure with the consequence that any crystal defect can lead to a at least local change in the electrical, thermal, and optical characteristics. While a single defect will not harm a device, at some point the accumulated defects will become important, for example in the switching speed of a MOSFET device. The underlying physical processes are non-ionizing interactions mainly from electrons, protons, and neutrons over Coulomb scattering liberating silicon atoms, elastic nuclear reactions producing silicon recoils, inelastic nuclear reactions causing excitation, and phonon processes leading to heating, up to local melting. For incident particle energies exceeding 10 MeV nuclear reactions are most relevant while for lower energies Coulomb scattering is dominant [111].

Radiation Sources in Space

In the following we describe effects relevant for the space mission QUBE. Other issues such as neutron influence [111], radiation effect mitigation by radiation hardening (by design

or hardening processes) [111, 117, 118] as well as spacecraft shielding [111, 119, 120] only play a minor role here.

Solar Particle Events (SPEs) can be categorized into two types: On the one hand solar flares, which are electron-rich energy bursts with a duration of typically hours, and on the other hand coronal mass ejections (CMEs) with a duration of typically days, which are large plasma eruptions containing all naturally occurring elements from protons to uranium [112], but mostly protons [121]. The solar protons, which can exceed 300 MeV [122], but also alpha particles are main contributors for TID and DD effects. Additionally to the protons and alpha particles, heavy ions account for SEEs, but with lower relative appearance.

Besides the particle flux, CMEs are also responsible for magnetic disturbances in the interplanetary space and the Earth magnetic field. The solar activity is varying in an eleven year cycle [123], with a tendency towards seven years with high activity and four years in a solar minimum[1]. The next solar maximum is predicted for July 2025. The chance for large particle events is highest during the declining solar maximum phase [124].

Galactic Cosmic Rays (GCRs) originate from outside of our solar system and consist of high energetic protons ($\sim 87\%$), alpha particles ($\sim 12\%$), and heavier nuclei ($\sim 1\%$) [125] covering a broad energy distribution, exceeding 10 GeV per nucleon. Despite their relatively low share, only the heavy ions do have a relevant impact on the SEE rate. In terms of TID and DD, GCR protons are nearly negligible in comparison to solar event or trapped protons in the Earth's radiation belt.

The solar cycle strongly influences the SEE rate caused by GCRs, as the resulting magnetic fields due to the solar winds in the heliosphere lead to deflecting effects preventing GCR particles entering the interplanetary space. The SEE rates related to GCRs decrease during the maximum solar activity [126]. This is because of the increased heliospheric shielding of the particles within the lower range of the energy spectra (below a few GeV), which however is the dominant part in terms of medium interaction. A further shielding is provided by the Earth's magnetic field, again, also mainly acting on the lower energy part of the spectra. Considering a spacecraft in a LEO, the GCR SEE rate is highest for a polar orbit but, due to the magnetic shielding, reduced by a factor three to five compared to the rate in an interplanetary scenario. For lower inclination orbits this shielding effect can rise by orders of magnitude [110].

Particles Trapped in the Earth's Magnetic Field form the so-called Earth's radiation belt and are a very relevant contributor to radiation induced failures especially for near Earth orbiting spacecrafts. The arrangement of the belt can be described with a magnetic dipole, fitting better for inner regions but failing for outer regions because of the

[1] Remarkably, the solar activity cycle can be reconstructed back to the 17th century from very early recordings of the number of sunspots. Today, the most established indicator for sun activity is the solar radio flux index F10.7, determined from radio emissions at 2800 MHz from the solar atmosphere. The number of sunspots and the radio flux index are in good correlation.

influence of the sun activity. The belt extension is about 10 times the Earth radius, mostly containing protons (1 keV - 300 MeV) and electrons (1 keV - 10 MeV) [112]. Sources of the high energy particles are the SPEs and GCRs but there also exist electron acceleration mechanisms within the radiation belt [127].

Considering a LEO, the particle exposure for a spacecraft is highest during the transition of the polar horns, below about 1000 km dominated by electrons, and of the South Atlantic Anomaly (protons and electrons) [128], but also strongly depends on the orbit inclination. During a solar minimum, the proton influence tends to get highest [129].

Laboratory Radiation Tests

To reduce the risk for a device or, in the worst case, an overall mission failure due to radiation damage, satellite hardware can be tested and qualified by laboratory radiation tests on Earth. Depending on the radiation source and energy as well as the radiation duration, TID effects, SEE, and DD can be investigated [111].

An often-used method for TID testing[2] is via gamma radiation from a Cobalt-60 source[3], emitting high energetic photons. By tuning the distance to the source and the radiation duration, the desired dose and dose rate can be applied. SEE testing[4] can be performed via heavy ions or protons at particle accelerator facilities. DD testing[5] is usually performed via neutrons as by testing with protons the effects between TID and DD cannot be distinguished well.

The decision about which tests and which specific procedures are performed for our space mission QUBE was also dependent on the project timeline, i.e., when appropriate hardware has been ready to test and on the accessibility of the radiation facility. The consortium decided to perform dedicated material tests with proton radiation at an early project phase. Here, we investigated the possible degradation or the change of physical properties of key components, which are used in the optical parts of the QKD payloads. At a later project phase, complete subsystems including electronics and optics were tested for TID effects. By this, we evaluated on the one hand the robustness and suitability of the chosen electronics components as well as the board design and on the other hand the fully assembled optics by analyzing the optical output before, during, and after irradiation.

4.1.2 Total Ionizing Dose Tests

Test Facility and Methods

The total ionizing dose (TID) test was performed at the Helmholtz Center for Materials and Energy in Berlin (see figure 4.1). The facility provides a Cobalt-60 source, which emits gamma radiation with energies between 1.17 MeV and 1.33 MeV. Based on the radiation

[2] TID test standards: ESA-ESCC-22900 [130], MIL-HDBK-883K [131]
[3] Alternatively cesium-137, X-rays and electrons or protons at particle accelerator facilities
[4] SEE test standards: MIL-STD-750, JESD57 [132], ASTM1192 [133]
[5] DD test standard: MIL-STD-883 TM1017 [131]

test standards ESA-ESCC-22900 [130] and MIL-HDBK-883K [131], colleagues from the QUBE-consortium partner OHB in Munich defined the test sequence and calculated the required radiation load of 25 krad TID. This load results from a worst-case environment estimation of 6 krad per year on a 800 km sun synchronous orbit, scaled by about a factor of four. The high extra charge accounts for a satellite lifetime of two years and a factor two as safety margin, which is recommended by ESA and NASA. In the joint measurement campaign, besides our QKD sender EQM, two further payload components from MPL have been irradiated. The test sequence for our QKD sender EQM was split into four sessions with a duration between 2 h and 15 h with applied dose rates between 0.5 krad/h and 3.3 krad/h. During the sessions of active radiation time the EQM was turned off. To monitor possible damages, the general functionality and laser response was tested between these sessions. More detailed investigations, including the spectral and timing characteristics of the VCSELs as well as the output polarization states, have been recorded and analyzed before and after the radiation test campaign.

Figure 4.1: The QKD sender EQM (left) in the TID test facility at the Helmholtz Center Berlin (right). The applied dose depends on the distance to the Cobalt-60 source as well as on the duration of irradiation. During a three-day campaign various dose rates were set with hardware switched-off during irradiation and intermediate short functional tests.

Results

Intermediate Functional Tests comprised the powering of the module, the configuration of the FPGA, reading of the temperature sensors and the photo diode, and a check of the VCSEL response. The EQM showed no notable change in functionality or behavior with exception of that an ID request of one memory chip failed. Further tests however showed that the ID is correctly replied but was wrongly interpreted by the software.

Spectral Characteristics of the LMU EQM have been measured in pulsed operation mode. During the recording, one of the four channels was turned on while the remaining three channels were turned off. The spectrometer used is self-built in our group by Martin Zeitlmair [134]. It is based on a 1200 lines/mm reflection grating and a highly sensitive CCD camera and features a spectral resolution of 0.1 nm.

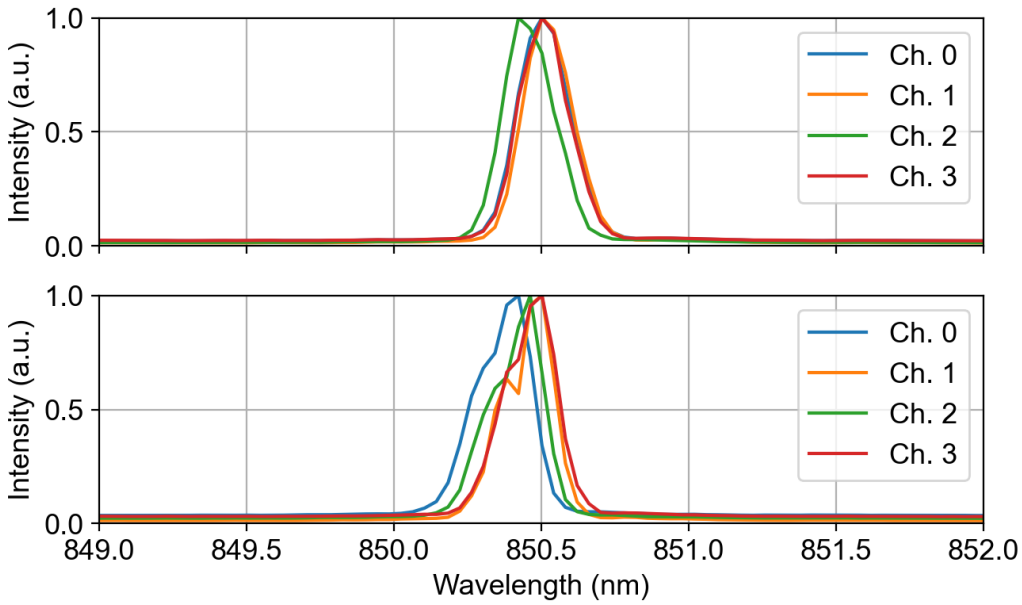


Figure 4.2: Spectra of the four VCSELs of the LMU EQM recorded before (top) and after (bottom) the TID radiation tests.

As a first observation it is remarkable that before the TID irradiation the spectra from VCSEL0, VCSEL1, and VCSEL3 show an almost perfect overlap while the center wavelength from VCSEL2 is shifted by about 0.05 nm (see figure 4.2). This is an important observation regarding a potential spectral side channel. It shows that in general, with exception of only one diode on this specific array, this type of VCSEL array is suited to provide a high spectral overlap. After the TID test, the channels 1 and 3 still show a high overlap and channel 2 is unchanged. Channel 0 is shifted towards lower wavelengths by about 0.1 nm. However, these results cannot be exclusively correlated with radiation effects as further sources for the slight wavelength change of channel 2 could be:

- Effects of settling in the VCSEL array fixation causing slightly changed stress conditions, which can occur simply over time and thermal cycles, but also during the transport or handling of the EQM.

- The wavelengths of the VCSELs show a slight temperature dependence (see section 4.3.2 and section 5.1.2) of 0.06 nm/K. However, the VCSELs on an array tend to behave similarly, i.e., if the temperature on the board or in the laboratory has been slightly different between the measurements, we would observe a common wavelength shift of all four VCSELs.

In conclusion, we state that the slight change of the spectra before and after the TID tests cannot be directly explained by radiation effects but they also cannot be fully excluded. The observed wavelength shift is in the order of the resolution of the spectrometer and do not affect the operation of the module in orbit. From a QKD security point of view it seems reasonable to test and analyze more samples. However, one also has to take into account that the discussed results represent the worst-case scenario, showing the spectral characteristics corresponding to only the beginning and the end of the mission. The shift during the mission is assumed, if at all, to be extremely slow over time by accounting for the order of magnitudes lower dose rate in space.

Timing Characteristics were recorded before and after the irradiation in pulsed mode, i.e., one channel was emitting short pulses while the remaining three channels were switched off. The optical pulse shape is reconstructed from the time difference between a reference clock signal generated on the EQM and the TTL signals from a fast silicon avalanche single photon detector (Micro Photon Devices, MPD-PD-050-CTE). As the rate of detections (approximately 1×10^5 counts/s) is significantly lower then the pulse rate of 100 MHz, the recorded time histogram is a faithful image of the optical pulse shape.

The optical pulse lengths before the TID tests are broader (FWHM 400 ps) compared to the optical pulse length after the TID tests (FWHM 200 ps), while the relative position between the four channels is nearly unchanged (see figure 4.3). We see that the recorded time histograms from before the TID tests are noisier, possibly caused by bad wiring or termination at the oscilloscope, which unfortunately cannot be reconstructed or affirmed. Among the various characterization measurements with the same type of VCSEL-arrays in the course of this work, including the diodes used in the LMU FM (see section 5.1.1), such a significantly increased width of the pulses has been only observed with the EQM before the radiation.

Essentially we state that, with high probability, the TID tests had no influence on the optical pulse characteristics of the four VCSELs and the driving electronics. There are hints for discrepancies in the data acquisition but we observed consistent pulsing behavior before and after the TID test. Hence, an additional, so called delta qualification seems not necessary.

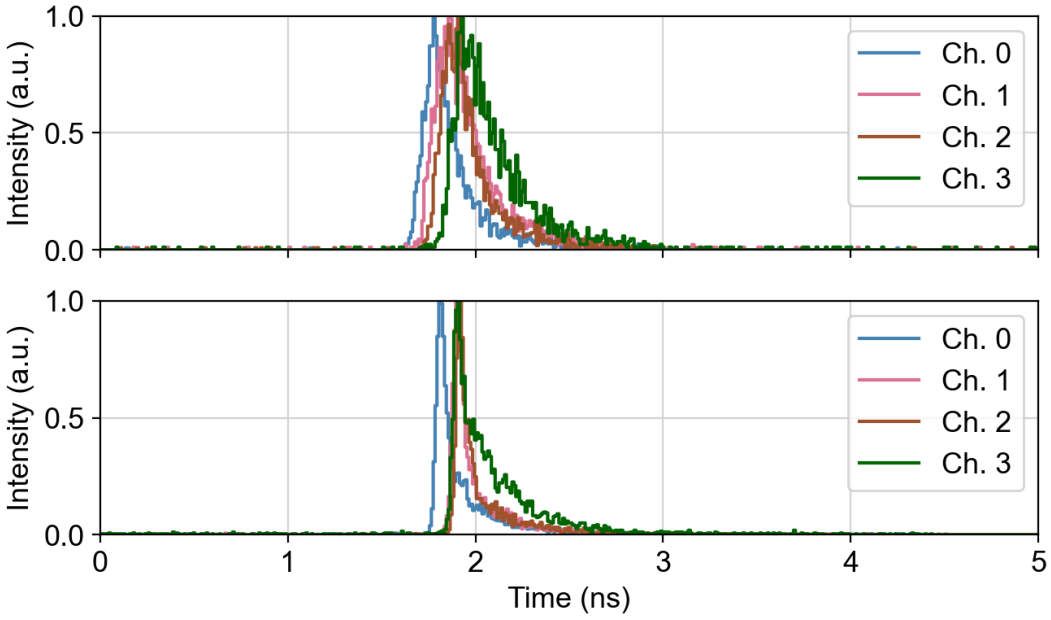


Figure 4.3: Timing characteristics of the optical pulses emitted by the four VCSELs of the LMU EQM recorded before (top) and after (bottom) the TID radiation tests.

Polarization Analysis has been performed, similarly to the spectral and timing characterization, in pulsed operation mode. To determine and evaluate the polarization states prepared by the EQM, we activate one of the four channel, i.e., a continuous stream of pulses containing photons with the same polarization is sent. This allows for the subsequent projection of the sent photons by this specific channel onto the six states $|H\rangle$, $|V\rangle$, $|+45\rangle$, $|-45\rangle$, $|L\rangle$, and $|R\rangle$. From the recorded countrates $\{R_H, R_V, \dots\}$ after the projection, the Stokes components (S_1, S_2, and S_3), which provide the complete description of the polarization state, can be reconstructed using

$$\vec{S}_N = \begin{pmatrix} 1 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} 1 \\ \frac{R_H - R_V}{R_H + R_V} \\ \frac{R_{+45} - R_{-45}}{R_{+45} + R_{-45}} \\ \frac{R_R - R_L}{R_R + R_L} \end{pmatrix}. \tag{4.1}$$

The measurement setup consists of a motorized QWP, a polarizer, and an APD. For a detailed description of the tomography procedure, please see Refs. [71, 72]. In table 4.2 the tomographic results of tests performed before and after TID irradiation are compared. The left part of the table represents the outcomes from the measurement recordings, while the right part are reconstructed states, i.e., the measured states rotated by an unitary transformation which minimizes the mean QBER for the standard BB84 bases of $|H\rangle/|V\rangle$ and $|+45\rangle/|-45\rangle$, respectively. The measured states are arbitrarily rotated because the optical fiber on our EQM is bent and arranged slightly differently after every handling or movement of the EQM, which lead to a change of the birefringence. Later in space, also the

orientation of the satellite towards the optical ground station might be rotated. Important here is only that the relative angles between the states remain constant which allows a later compensation using waveplates, a fiber polarization controller, or via liquid crystal retarders. The calculated states have not been experimentally confirmed by applying the calculated compensation setting here. Yet, the method was demonstrated before [71, 72].

The tomographic data show that the quality of the polarization states before and after the TID tests is unchanged and very satisfying. The preparation quality q (see equation (2.2)) is as high as 0.98 (ideally 1) and the mean QBER is below 1%. The consistency of the measured data is confirmed by a generally high degree of polarization (DOP).

Altogether, we state that the TID radiation tests had no influence on the polarization state preparation.

	Before TID Tests							
	Tomography outcome				Ideally compensated (calculated)			
Channel	0	1	2	3	0	1	2	3
S_1	0.622	-0.397	0.843	-0.817	0.975	-0.982	0.041	0.023
S_2	0.609	-0.762	-0.508	0.524	0.126	0.149	0.988	-0.989
S_3	0.456	-0.498	-0.111	0.192	-0.007	-0.007	-0.059	0.000
DOP	0.983	0.993	0.991	0.990	0.983	0.993	0.991	0.990
$\overline{\text{QBER}}$	-				0.8%			
q	0.98				0.98			
	After TID Tests							
Channel	0	1	2	3	0	1	2	3
S_1	-0.268	0.383	0.484	-0.477	0.989	-0.982	0.064	0.019
S_2	0.956	-0.877	0.361	-0.278	0.111	0.130	0.980	-0.992
S_3	0.057	0.283	-0.776	0.826	-0.002	-0.002	-0.049	0.000
DOP	0.995	0.990	0.983	0.993	0.995	0.990	0.983	0.993
$\overline{\text{QBER}}$	-				0.6%			
q	0.98				0.98			

Table 4.2: The polarization states of the LMU EQM before and after TID irradiation. (Left column) The measured Stokes components (S_1, S_2, and S_3) of the four channels without a compensation for their global rotation. (Right column) A calculated set of the four channels by applying an appropriate unitary transformation. Given this, the DOP and mean values for the QBER [71, 72] as well as for the preparation quality q (see equation (2.2)) can be calculated.

Secondary Voltage Characteristics have been recorded after every of the four TID runs. The QKD sender electronics requires three different voltage levels which are either directly supplied by the satellite bus (3.3 V) or are converted by a voltage step-down

chip (2.5 V and 1.2 V) on the electronics board. These power circuits are switched via a Hotswap-controlled N-Channel MOSFET. The 3.3 V line remains constant at 3.30 V during the campaign. Days after the radiation load we measured a slightly increased voltage of 3.37 V, which, however, has no effect on the functionality of the board. The 2.5 V and 1.2 V lines showed no change at all.

The TID load had no significant effects on the voltage control part of the EQM, which attests the reliability of the components chosen and the layout design.

4.1.3 Proton Radiation Tests

At an early stage of the project, proton radiation tests were performed. This campaign was also done together with colleagues from MPL Erlangen and under the supervision from OHB in Munich. The focus here was on testing a photonic integrated circuit (PIC, used by MPL) as well as materials used in the optics part of the LMU QKD sender. For the latter, the possible degradation of the polymer based foil-polarizer and the waveguide glass substrate (boro aluminosilicate glass) due to displacement damage (DD) effects has been investigated.

Test Facility and Methods

The proton radiation tests took place at the Helmholtz Center for Materials and Energy in Berlin. The facility provides a proton beam up to a particle energy of 72 MeV by a two stage accelerator system consisting of a Van-de-Graaf tandem accelerator (up to 5.5 MeV) and a cyclotron accelerator (5.5 MeV - 72 MeV).

The proton energy for the LMU material tests has been set to 30 MeV, which is in the lower but critical range of the proton energy spectra (up to 300 MeV, dominated by solar protons and protons trapped in the Earth magnetic field) potentially causing DD effects. Assuming a worst-case scenario for an 800 km sun synchronous orbit without any shielding, the proton flux has been estimated to be 3.5×10^9 p/cm^2 per year. At the accelerator, a proton flux of 5×10^6 p/cm^2 per second was chosen, which is two orders of magnitude higher as the expected orbital flux, but still represents a good trade-off between moderate test times and costs, while also not overtesting the samples. One set of samples was irradiated with a dose equivalent to one year in space and another one equivalent to three years.

Results

The transmittance of the 1-year sample of the glass substrate is unchanged and was 89.5% before and after the radiation. The 3-year sample shows a slightly reduced transmittance of 89.0%. The transmittance of the polarizer foil has insignificantly increased from 65.7% to 67.1% for the 1-year sample and to 67.6% for the 3-year sample. The extinction ratio of the polarizer foil was measured to be better than 1:10000 for the 1-year as well as for the 3-year sample, similar to a non-radiated one.

The materials investigated are nearly unaffected by the proton radiation. The slight change in transmittance can be neglected for our application.

4.1.4 Conclusion

We conclude that the TID tests of the EQM as well as the proton radiation tests revealed no relevant weaknesses regarding the functionality of the EQM or material degradation. The minor changes in the optical characteristics after the TID tests cannot be exclusively assigned to radiation effects and, if occurring in comparable scale, will not affect the operation of our QKD hardware in this mission.

4.2 Vibration Tests

The qualification of a satellite regarding vibration loads is mandatory for the acceptance on a rocket launch vehicle to avoid problems during the launch, which could be initiated even by smallest components. Besides for the acceptance for launch, the functionality of the hardware should also not be affected due to the vibration loads. The safety and reliability of the satellite hardware can be investigated by applying vibration loads as specified by the launch providers. The measurement procedure allows for the detection of weak points in the construction, the material choice, and all mechanical interfaces including screws, soldering, and adhesive joints.

In the following section, the outcomes of simulating the mechanical behavior of the sender design at an intermediate development state are discussed. Furthermore, the test facility and methods for the vibration qualification tests as well as the test results are presented.

4.2.1 Mechanical Simulations

For the critical design review of our QKD sender, we performed a modal and breaking load analysis using the *Ansys* simulation software (see figure 4.4).

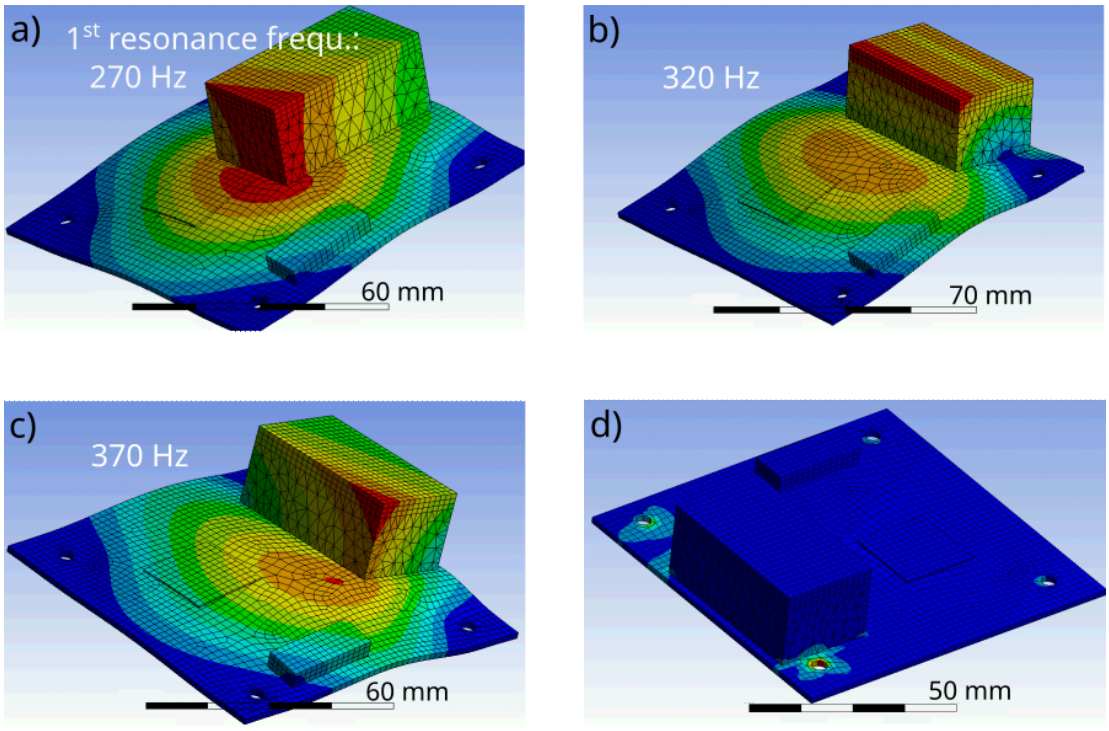


Figure 4.4: a) to c) Modal analysis of sender designs with different positions and orientations of the optical package. d) Breaking load analysis of the hardware configuration shown in c). The simulations have been performed with *Ansys*.

The first resonance frequency is strongly dependent on the position and orientation of the optical package on the printed circuit board (PCB). If placed centered with the short edge to one of the outer edges of the PCB, the first resonance frequency is at 270 Hz (see figure 4.4 a)). Rotating the optical package by 90° increases the first resonance to 320 Hz (see figure 4.4 b)). It can be shifted further to 370 Hz by positioning the optical package not centered but as close as possible to one of the fixation holes in the PCB (see figure 4.4 c)), which is the favored configuration. For this case, the simulation results in a maximum breaking load (also called "von Mises stress") of 134 MPa at the PCB fixation holes (see figure 4.4 d)). This is three times smaller than the ultimate stress point for the PCB material FR4, which is, slightly dependent on the manufacturer, well above 300 MPa. The mechanical simulations revealed no critical points and therefore, the hardware design has been pursued.

4.2.2 Test Facility and Methods

The vibration tests took place at IABG in Ottobrunn nearby Munich, where the four QUBE payloads have been tested in parallel in a joint campaign of MPL, DLR, and LMU (see figure 4.5). The EQM boards have been mounted on a 36 x 36 x 2.5 cm^3 aluminum plate and were equipped with an acceleration sensor each, which allows to measure the individual resonance behavior within the defined frequency range.

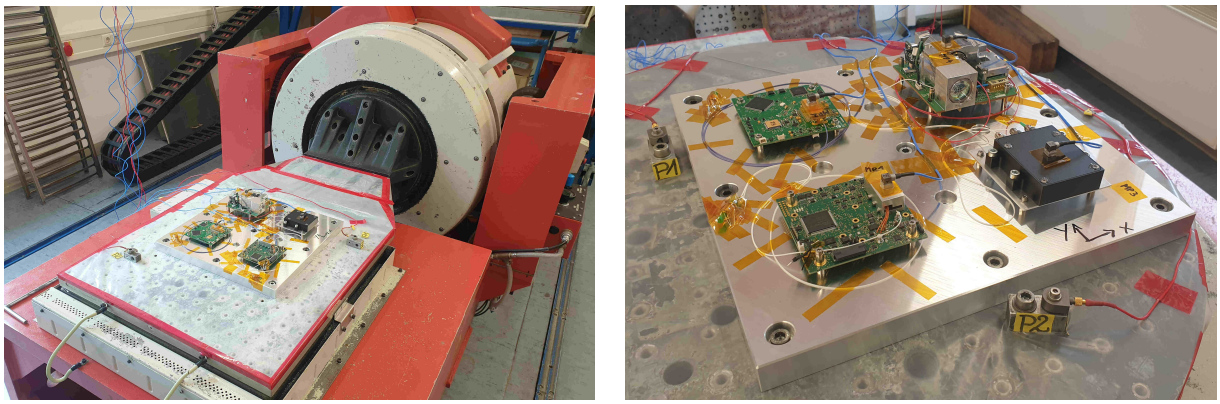


Figure 4.5: (Left) Joint vibration tests of the QUBE payload engineering models. (Right) Clockwise, starting from bottom left, the EQMs from LMU, MPL, DLR, and the wavelength-division multiplexing unit. The test procedure has been performed in X, Y, and Z orientation. The mechanical response has been monitored by acceleration sensors on each payload.

The vibration loads are defined by the qualification level for a Vega launch [135] (see table 4.3 (a) and (b)). Vega is a launch vehicle designed for the launch of small satellites into LEO and built in cooperation of the Italian Space Agency (ASI) and the European Space Agency (ESA). The loads on a Vega are higher compared to a Falcon 9 by SpaceX [136].

(a) Sine vibration	Frequency [Hz]:	8-70	70-125			
	Acceleration [g]:	2.5	1.25			
(b) Random vibration	Frequency [Hz]:	20-50	100	200-500	1000	2000
	Excitation [g^2/Hz]:	0.016	0.032	0.080	0.038	0.016
(c)	for X, Y and Z-axis: 1) Resonace search (5 - 2000 Hz, 0.5 g, 2 octaves/minute) 2) Sine vibration (5 - 125 Hz, max. 2.5 g, 2 octaves/minute) 3) Resonace search (same parameter as 1)) 4) Random vibration (20 - 2000 Hz, 8.84 g RMS, duration: 120 s) 5) Resonace search (same parameter as 1))					

Table 4.3: Spectrum for (a) sine vibration load, tuned to 2 octave/minute and (b) random vibration corresponding to 8.84 g RMS with a duration of 120 s per axis. The loads correspond to the qualification level for a Vega launch. (c) Test sequence performed in Z-, Y- and X-axis.

A pass of the vibration qualification on Vega level therefore also qualifies for a launch with a Falcon 9. Restrictions can occur if the launch provider uses deployment systems which again increase the qualification requirements. The sine and random vibration loads are applied between control resonance searches with low load (see table 4.3 (c)), which, in the case of the damage, e.g., loosening/breaking of parts, tearing of screws, or cracks in the PCBs, can give a hint at which sequence and for which axis the damage occurred.

4.2.3 Vibration Tests Results and Conclusion

The vibration tests had no impact on the functionality of the LMU EQM. There is no sign of a mechanical damage as the resonance characteristics of the hardware are identical before and after the test procedure for all three axes (see figure 4.6). The optical power at the fiber output and the signal from the internal photo diode of the sender remained identical for all four channels before and after the vibration tests (see figure 4.7). Two short intermediate functional tests after the Z and Y axis runs showed no relevant change in the optical response. The pulsing behavior was also not affected by the vibration tests.

In conclusion we state that the vibration loads on Vega level did not affect the LMU QKD sender. The general functionality as well as the mechanical and optical properties did not change due to the vibration tests.

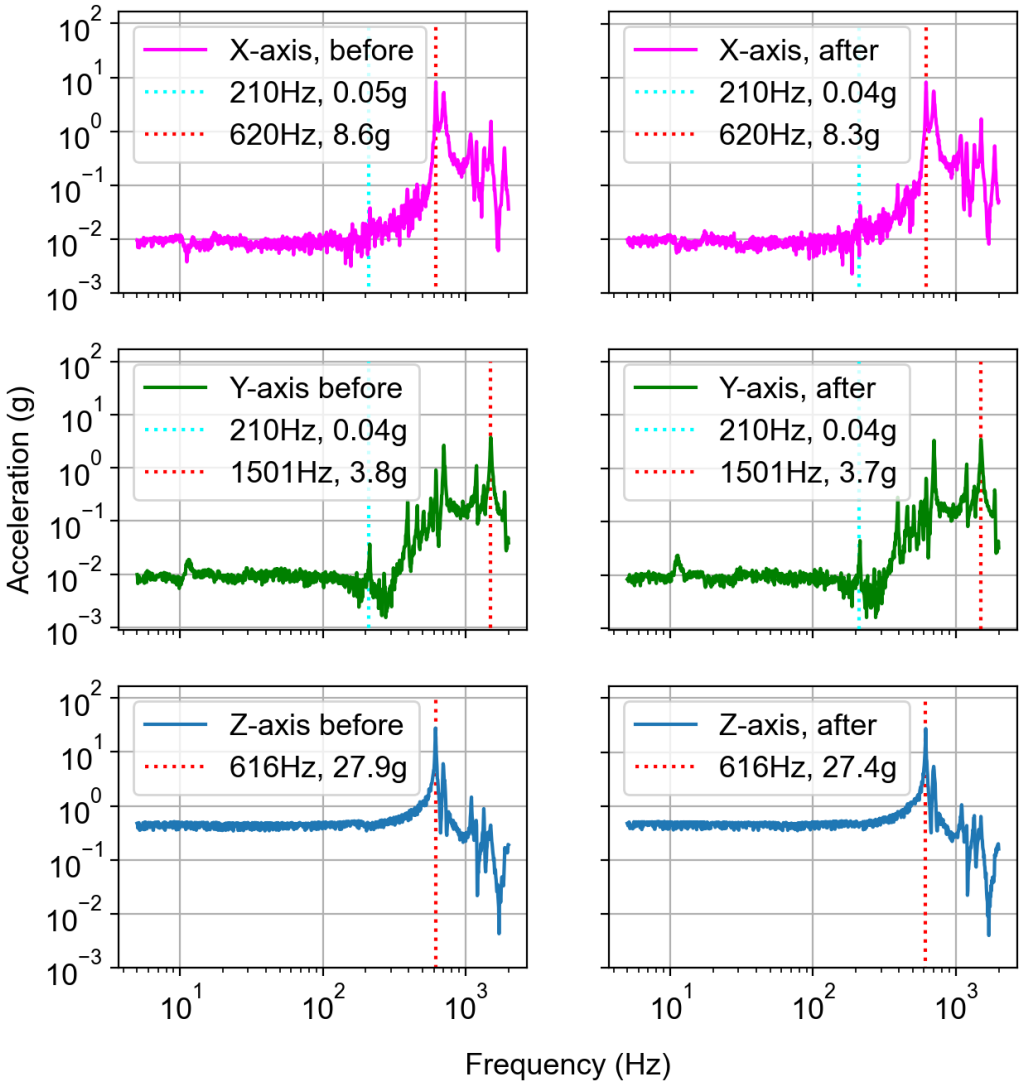


Figure 4.6: Mechanical response of the LMU engineering model before and after the sine and random vibration loads (see table 4.3 (c) 1) and 5)) in X-, Y-, and Z-direction. The vertical lines in cyan and red mark the first and the most distinct resonances.

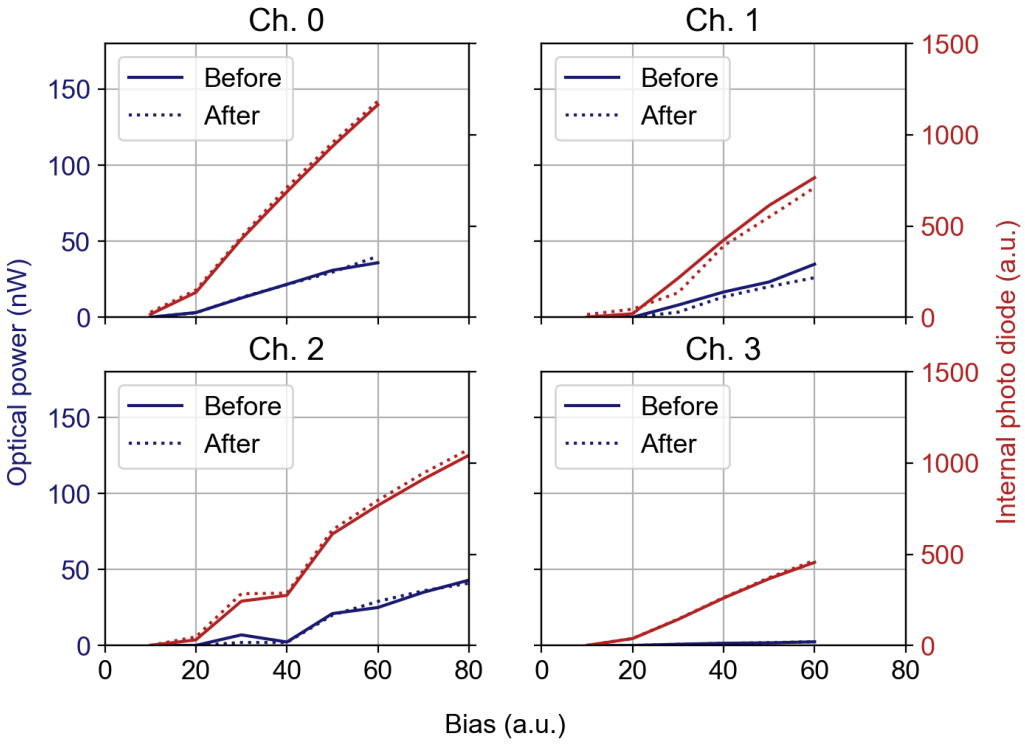


Figure 4.7: The optical power of the four channels of the LMU EQM at the fiber output (blue) and the response from the internal photo diode (blue) in continuous wave operation before and after the vibration tests.

4.3 Thermal Cycles under Vacuum Condition

We tested our QKD hardware under vacuum conditions and for thermal cycles, as satellites on a LEO constantly change between being illuminated by the sun or being the Earth shadow. The goal of this tests was to reveal possible problems regarding the mechanical interfaces, the selection of components and materials, and irregularities in the operative as well as the functional behavior. A simulation of thermal characteristics of the whole satellite to predict the expected temperature range which the different satellite parts are exposed to, is very complex and was not practical within the project timeline. In-orbit measurements of the UWE-3 mission by our colleagues from the ZfT Würzburg show that the temperature of this satellite's side panels vary between $-25\,^{\circ}\mathrm{C}$ and $+29\,^{\circ}\mathrm{C}$, however, the temperature range inside the satellite is by far smaller, e.g., the temperature of the battery varies only between $+4.5\,^{\circ}\mathrm{C}$ and $+9.5\,^{\circ}\mathrm{C}$ [137]. We expect a comparable temperature range also for the inside of QUBE, but extend the range for the tests to also account for the temperature variations during the satellite transport and waiting times at the launch location to $-10\,^{\circ}\mathrm{C}$ and $+60\,^{\circ}\mathrm{C}$.

Besides the temperature issue, the vacuum condition can change the properties of materials due to outgassing or the functionality of active components, which can be investigated also with the thermal vacuum chamber (TVC) test setup presented in the following.

4.3.1 Thermal Vacuum Chamber (TVC) Setup

To test the robustness and the behavior of our LMU EQM under thermal cycles in vacuum, a thermal vacuum chamber (TVC) has been built. It features full electrical connectivity to the EQM, i.e., power supply and controlling over the UNISEC bus [67] as well as feedthroughs for optical fibers allowing for monitoring and analysis of the optical signals outside the chamber[6] (see figure 4.8).

The TVC has an outer radius of 18 cm and a depth of 10 cm. By employing a pre- and turbo-pump system, the pressure can be reduced to about 2×10^{-6} mbar. The temperature can be set between about $-10\,^{\circ}\mathrm{C}$ and $+60\,^{\circ}\mathrm{C}$ via a thermoelectric cooler (Peltier device), squeezed between two copper plates. One of the plates is acting as an interface to the hardware to be cooled or heated, while the other one provides the interface to three standard heat pipes for the heat transfer to the outside of the chamber. The minimum temperature of $-10\,^{\circ}\mathrm{C}$, measured on the EQM, can be reached only when the EQM is turned off. After turning on the EQM, its power consumption of about 2W leads to a warming of the EQM board to about $-1\,^{\circ}\mathrm{C}$ (see figure 4.9).

Besides the three internal temperature sensors on the EQM, additional sensors mounted on the chamber inner wall, at both sides of the copper plate, a dummy board, the EQM electronics board, and the optics package are used for monitoring and debugging. The temperatures stated in this section are taken from the additional sensor at the EQM

[6] The interface part of this setup has been designed during a Semester's thesis by Jorge Rosano in a collaboration between LMU and TU Munich [138].

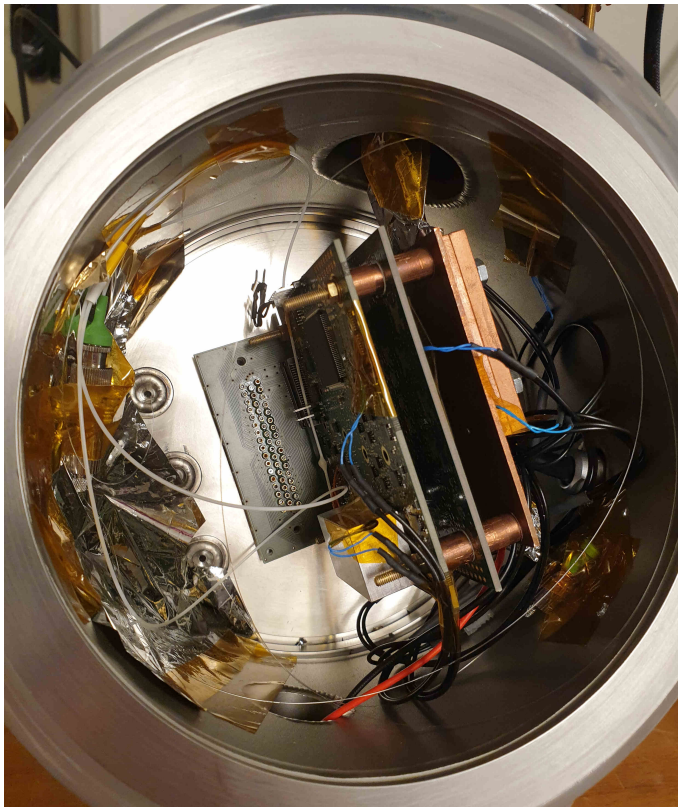


Figure 4.8: Thermal Vacuum Chamber at the LMU in Munich with (from left to right) the LMU engineering model, a dummy board (placeholder and temperature monitoring) and the copper heating/cooling plate. The back flange contains three fiber feedthroughs and a 50-pin electrical connector supporting UNISEC bus [67] operation.

electronics board. However, we observed that this sensor returns a higher temperature as the internal sensors. This is because of the worse thermal contact of the additional sensor, which was connected without thermally conductive paste inside the TVC, while the internal sensors have a good thermal contact over a soldering joint. The output values of the internal sensors and of the additional sensor on the EQM board show a linear dependence over the whole temperature range investigated, which allows the calibration of the additional sensor by $T_{int} = 1.3 \times T_{add}$ - 4.6 K.

4.3.2 EQM Long-term TVC Tests

The long-term TVC tests of the EQM were split into two phases for data acquisition: A stability analysis of the polarization state for the first about 90 h and spectra as well as intensity recordings during a second phase of about 70 h. The reason for this separated sequence was to preserve the stability of the tomographic measurement procedure. The vacuum and measurement setup was unchanged during the different measurement runs, thus without even the slightest changes of the hardware configuration, e.g., bending of

the fibers. The two sequences were performed right after another without changing the pressure, leading to an overall time of the EQM in the chamber of over 160 hours.

Furthermore, we wanted to operate the EQM as close as possible in a realistic overflight scenario, i.e., mostly switched off and short operation times of only a few minutes[7]. This gave the chance to catch effects which do not occur if the EQM is running for a longer time and therefore in thermal equilibrium.

Polarization Stability

Within the first 90 h of the EQM in the TVC we performed nine times a full polarization state tomography of the polarization states prepared by the EQM in pulsed mode with typical laser driver parameters (see figure 4.9).

Unfortunately, channel 2 of the EQM did not work properly for the runs with low temperature, which cannot be fully explained, but tend to be a problem of the electrical connection of the VCSEL. The temperature has been varied between $-1\,^{\circ}\mathrm{C}$ and $37\,^{\circ}\mathrm{C}$ simulating two warm-cold-cycles. The temperature spikes at the measurement points are caused by the heat buildup of the EQM due to its power consumption of approximately 2 W. The tomography procedure has been started about 1 min after switching on the EQM and has taken another 5 min for measuring all four channels.

The polarization states show a slight drift over time which however, by accounting for the long intervals between the measurements and the temperature range of almost $40\,^{\circ}\mathrm{C}$, can be nevertheless seen as very stable. Furthermore, we expect that these drifts do not have their origin in the state preparation on the EQM itself but in the stability of the fiber used for guiding the optical signals from the EQM to the outside of the TVC. Only the runs with a complete set of BB84 states recorded (Run1, Run4, and Run5) are suitable to calculate the preparation quality q (see equation (2.2)) and a mean value for the source intrinsic QBER [71, 72]:

	q	$\overline{\text{QBER}}$	$\overline{\text{DOP}}$
Run 1	0.98	0.6%	99.5%
Run 4	0.98	0.6%	99.6%
Run 5	0.98	0.7%	99.3%

The state preparation quality as well as the QBER are nearly constant for the different runs and close to optimally reachable values. In the runs where channel 2 was not working, the remaining polarization states show no significant changes. Hence, it can be expected that also for channel 2, comparably good results for q and QBER could have been achieved. Altogether we state that the polarization state generation stability is not affected by typical temperature changes under vacuum conditions.

[7] During an overflight sequence all payloads of the satellite are, because of the limited battery capacity, turned on as short as possible. For a typical overflight we expect an operating time of not much longer than 10 min.

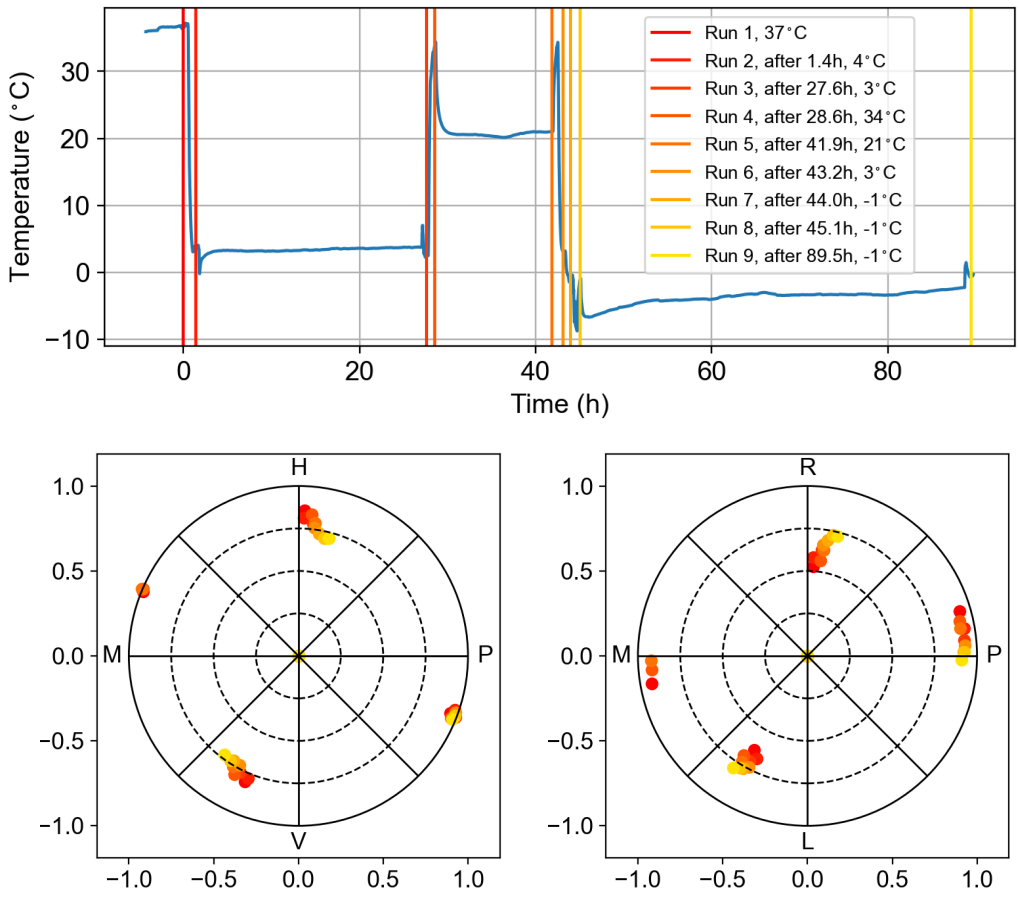


Figure 4.9: (Top) Temperature profile covering two warm-cold-cycles during almost 90 h test time. The vertical lines mark the points in time when a polarization state tomography has been performed. (Bottom) Outcomes of the polarization state tomography. The measured Stokes components are projected onto the equatorial (left) and circular/anti-diagonal (right) plane of the Poincaré sphere.

VCSEL Spectral Characteristics

During the second data acquisition phase of about 70 h, the spectra of the four VCSELs on the EQM have been measured eight times at temperatures between −2 °C and +64 °C (see figure 4.10). There, channel 2 showed a different behavior as during the polarization stability characterizations. The channel 2 once did work at low temperatures (Run 8) and once did not work (Run 1). Furthermore, this channel did sometimes not respond at higher temperatures, e.g., for Run 4 at 27 °C. With a high probability the electrical connection of the VCSEL from channel 2 seems to be not ideal, comparable to a cold solder joint.

In general, the four VCSELs of the EQM show a good overlap and the same temperature dependence regarding the wavelength. The measured temperature dependence of the wavelength is 0.06 nm/K, which is slightly below the value of 0.07 nm/K, stated by

the manufacturer. Evidently, the TVC tests have not revealed unexpected effects of the spectral characteristics.

Optical Response Characteristics

During the second data acquisition phase of the TVC test, besides the spectral characteristics (see the paragraph before), also the optical response of the VCSELs in continuous wave and in pulsed mode has been recorded (see figure 4.11). We observed a behavior of our optics module which is sometimes hard to interpret. For this reason, before discussing the measurement data in more detail, an overview of how different effects can affect the behavior should be given:

- The optical output power of the EQM at the fiber output depends on the coupling losses from the VCSELs to the waveguides and from the waveguide chip to the fiber. These two couplings are independent from each other, i.e., temperature-based effects due to thermal expansion of components or adhesive joints can either lead to higher/lower losses at both couplings or the overall loss is oppositely affected by them. Under unfavorable configurations, even the four channels can behave differently when, for example, the coupling of the four VCSELs into the waveguides strongly differs.

- The optical output power of the bare VCSELs is supposed to show a certain temperature dependence, which was not characterized beforehand, but should be investigated in future versions.

- We observed that some of the VCSELs change their optical mode profile with changing bias current. This behavior can on the one hand influence the coupling into the waveguide and on the other hand be correlated with a change of the degree of polarization.

- The internal photo diode on the EQM only collects stray light, i.e., light which is either not blocked by the polarizers or not coupled into the waveguides. The effects described before can influence the stray light intensity. Furthermore, the temperature dependence of the photo diode was not characterized, which should be also considered in future versions.

The channels 0 and 1 of the EQM behave somehow as expected in continuous wave (CW) operation, with a clear lasing threshold measurable at the fiber output as well as with the internal photo diode. After the cold-warm-cold-cycle ($-2\,^{\circ}\mathrm{C}$, $+64\,^{\circ}\mathrm{C}$, $-2\,^{\circ}\mathrm{C}$), channel 0 showed a reduced output power, although the optical power measured by the internal photo diode is unchanged, which is an indication for a slightly changed mechanical configuration probably having an impact on the coupling. The optical output power of channel 1 is higher after the cold-warm-cold-cycle and the internal photo diode shows a lower value. The channels 0 and 1 also behave differently during the warm phase: The optical output power stays constant for channel 0 but it goes down for channel 1, while the

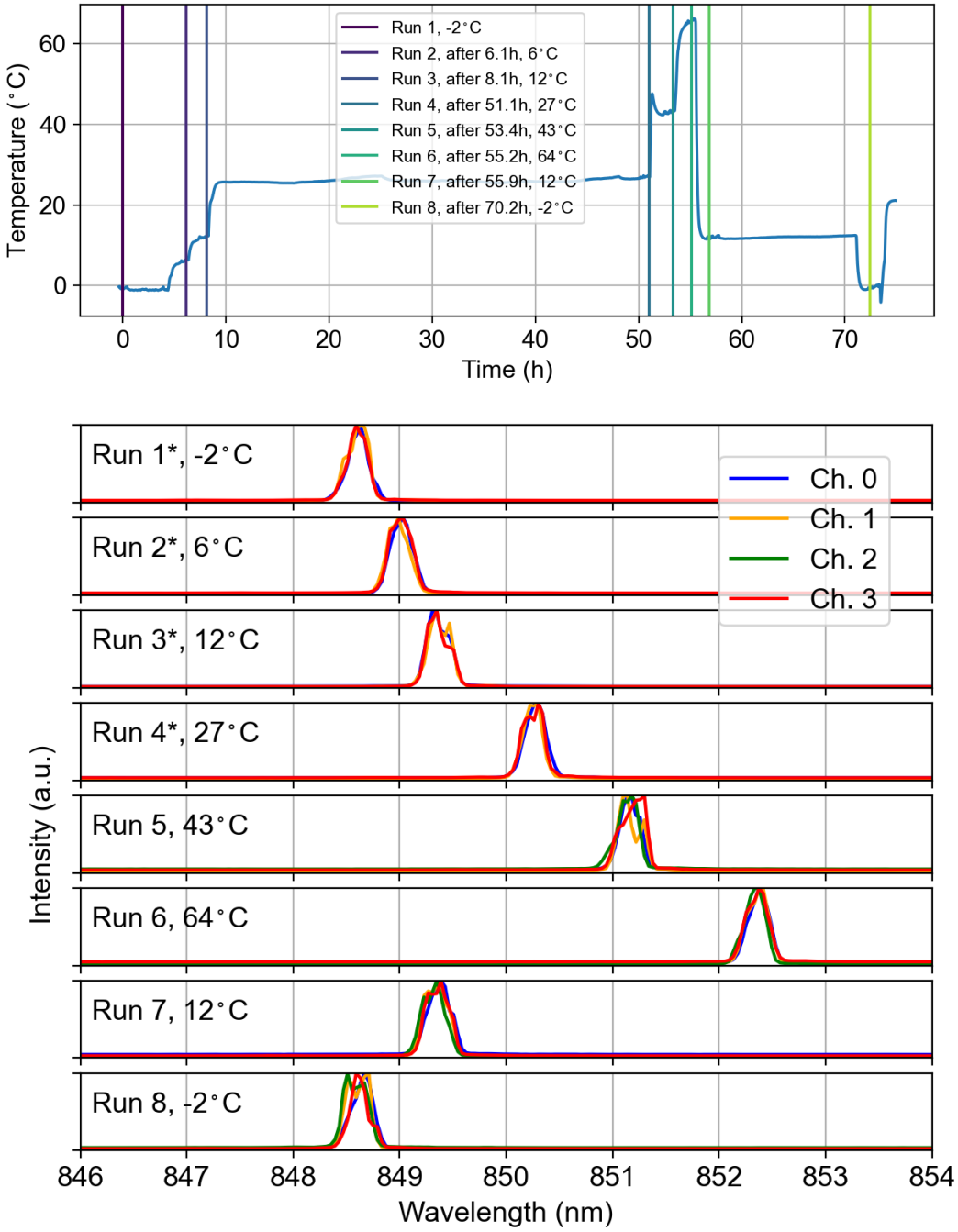


Figure 4.10: (Top) Temperature profile of the long-term TVC tests over 70 h. The vertical lines mark the points in time when the data acquisition for the VCSEL spectra and optical response (see figure 4.11) has been performed. (Bottom) Spectra of the VCSELs for the eight measurement runs. For the runs 1 to 4, the VCSEL corresponding to channel 2 was not working.

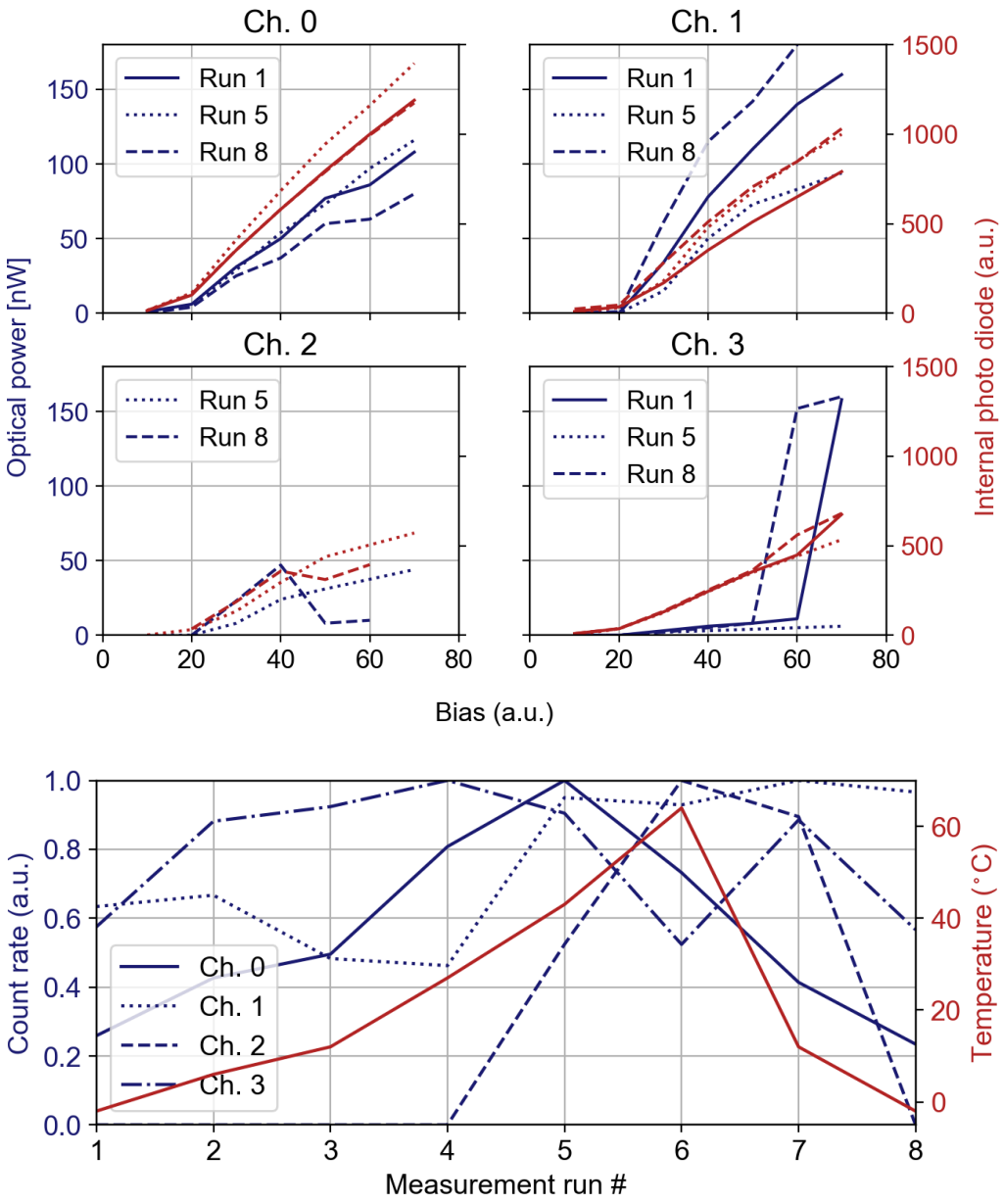


Figure 4.11: (Upper four graphs (Ch. 0 to Ch. 3)) Optical output power measured at the fiber output (blue) and with the EQM internal photo diode (red) in continuous wave operation (constant bias, zero modulation) for three representative TVC measurement runs, acquired at the same points in time as the spectral characteristics recordings (see figure 4.10). (Bottom) Temperature (red) and APD count rate (blue) of the four channels in pulsed mode (bias below lasing threshold, modulation on) for the eight TVC measurement runs. For the runs 1 to 4, the VCSEL of channel 2 was not working.

internal photo diode outputs a higher value for both. This effect could be explained by a higher optical output of the VCSELs at higher temperature but again, a slightly changed coupling configuration. Channel 2 did not work at the first run at low temperature (Run 1) but worked after reaching −2 °C again at Run 8. The optical output is constantly increasing with increasing bias for the higher temperature but shows a drop at higher biases for the lower temperature, which cannot be explained satisfyingly. Channel 3 shows a constant increase of the light captured by the photo diode but a jump in intensity for higher biases at low temperatures, which could be explained by a change in the optical mode profile causing a better coupling into the waveguide.

In pulsed mode (see figure 4.11 (Bottom)), the light generation of the VCSELs is too weak for the internal photo diode but the optical output of the module measured by an APD tend to follow the trend to higher optical output at higher temperatures. Channel 3, however, shows a drop in intensity at high temperatures and the optical output of channel 1 stays nearly constant after cooling down.

Temperature Dependence of the Driving Electronics

As the optical response of the Sender EQM during the thermal vacuum tests cannot be fully explained, we also investigated if the laser driving currents show a certain temperature dependence. Therefore, an identical sample to the EQM electronics, but without VCSELs and further optics attached, has been varied in temperature between 26 °C and 44 °C while the laser driver output was probed. We could not observe a remarkable change in the voltage output characteristics over the whole temperature range. Although the EQM has not been exclusively electrically characterized under different temperatures and the temperature range in this test is smaller than compared to the tests of the EQM in the TVC, we state that the driving current characteristics shows no indication for a relevant temperature dependence.

4.3.3 TVC Tests Conclusion

While the electronic functionality as well as the polarization and spectral characteristics of the QKD sender EQM behave stable or at least in an expected manner during the TVC tests, relevant issues regarding the optical intensity response and the partial inactivity of one channel has been revealed. No completely satisfying explanations could be given to both problems. Although further investigations might provide helpful insights, the test results are, especially in the context of the *New Space* development ansatz, promising and does not mean that this type of QKD sender design is unsuited for space missions. The stable long-term operation in CW mode is on the one hand not required for this type of module and on the other hand, active temperature stabilization as well as better monitoring are powerful tools to improve and handle the stability characteristics. Furthermore, the characterization, and especially the determination of the laser driver parameter in QKD mode, should be done at different temperatures to identify issues regarding the stability of the optical output power (see section 5.2).

Chapter 5

Characterization of the QKD Sender Flight Model

The qualification tests of the QKD sender EQM, presented in the last chapter, revealed no show-stopping issues of our hardware design. Based on this, we have built the QKD sender flight model (FM) using identical components and assembly methods as for the EQM. In this chapter, the results of its optical characterization are presented. Furthermore, the determination and analysis of driving parameter sets, required for a QKD-near operation mode, is shown. The measurements have been performed with the final flight hardware, with the consequence of being forced to find a trade-off between on the one hand testing and confirming its space suitability and on the other hand not damaging it.

5.1 Optical Characteristics

In the following section, results regarding the pulse timing, spectral properties, the optical response of the VCSELs, and the preparation quality of the polarization states, are discussed.

5.1.1 Timing Characteristics

The timing characteristics of the LMU FM has been recorded and analyzed along the same procedure and similar methods as for the qualification tests of the LMU EQM (see section 4.1.2).

We observe short and well-shaped optical pulses with a nearly identical length of about 150 ps FWHM, however, temporarily not overlapping (see figure 5.1). The pulses coming from channel 2 and 3 are separated most, accounting to about 200 ps. This is caused by non-optimally set hard-wired meander combinations (see section 3.1.2), which have been chosen on the basis of the satisfying timing characteristics of the EQM (see figure 4.3), built and characterized before the completion of the FM. Apparently, a better combination of the meander combinations could have been chosen and a resoldering would

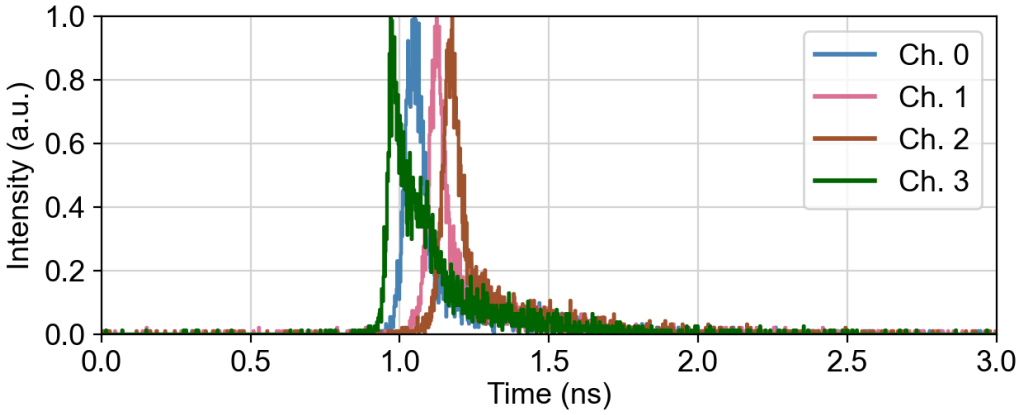


Figure 5.1: Timing characteristics of the optical pulses emitted by the four VCSELs of the LMU FM.

have been possible. However, we decided to keep this configuration to avoid risking a damage of the FM on the finish line. We are aware of the, with the presented timing characteristics of the FM, widely open QKD side channel, which must be closed in future versions.

In principle, the meander solution provides a good opportunity to passively manipulate the timing of the individual channels. However, there are limitations achieving a certain delay range while at the same time enabling a fine tuning on the order of picoseconds. Furthermore, for every tuning step solder bridges must be removed or set, which is a non-optimal procedure for a final flight hardware. We decided for this type of time delaying, as electronics delay chips[1] usually consume relatively much power, which limits their suitability for our Cube-Satellite.

5.1.2 Spectral Characteristics

The spectral characteristics of the LMU FM has been recorded and analyzed similarly to the procedure and methods as for the qualification tests of the LMU EQM (see section 4.1.2). To analyze the temperature dependence of the wavelength, we put the FM onto a temperature controllable copper plate and varied the temperature within a moderate range between 22 °C and 42 °C. The temperature has been measured by the three internal temperature sensors on the FM.

The four VCSELs emit a narrow peak of approximately 0.3 nm around the center wavelength of 850 nm at room temperature and show a linear temperature dependency of 0.06 nm/K. The VCSELs corresponding to channel 0 and channel 2 show a good spectral overlap while channel 1 and 3 are separated by about 0.2 nm in wavelength.

In contrast to the spectra of the four VCSELs of the EQM (see figure 4.2 and figure 4.10), which in general show a good overlap, the VCSELs of the FM array are non-ideal

[1] Former works in our group showed the well working timing adjustment based on delay chips [63].

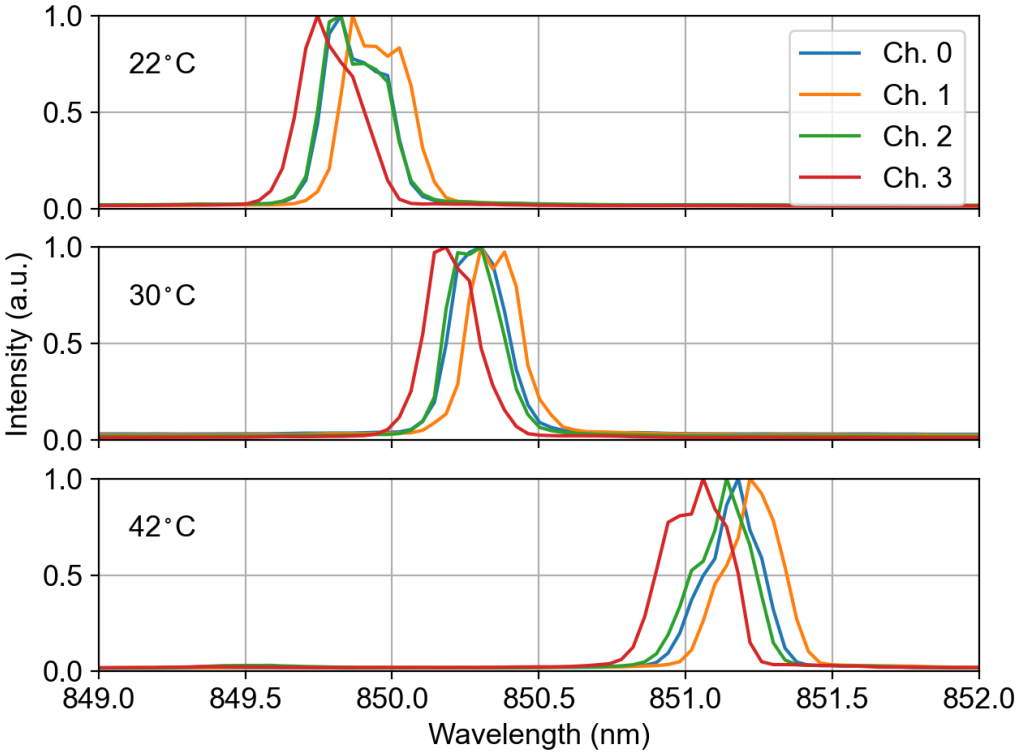


Figure 5.2: Spectral characteristics of the optical pulses emitted by the four VCSELs of the LMU FM. The temperature has been set to 22 °C, 30 °C and 42 °C.

with respect to a spectral QKD side channel. We were also forced, similar as for the temporal mismatch, to accept this flaw as a change of the optics hasn't been an option because of the project timeline. A change of only the VCSEL array is not possible with the developed optics assembly procedure (see section 3.2), here, the whole optics must be replaced. This problem can be solved by a better and more accurate selection of the VCSEL array before the optics assembly. However, for this, first a method to probe and spectrally analyze the diodes in pulsed mode before further assembly steps must be developed.

5.1.3 VCSEL Response Curves

The optical response of the four VCSELs of the FM has been recorded and analyzed in continuous wave (CW) and pulsed mode over a wide range of possible bias and modulation settings at room temperature (see figure 5.3).

For CW operation we observe a nearly linear rise of the optical output power with increasing bias after a clear lasing threshold. With exception of channel 3, this characteristics is observed at the fiber output as well as with the internal photo diode. Channel 3 is, regarding the optical output power, the weakest of the FM module. The coupling of the light from the corresponding VCSEL into the waveguide however should not be signifi-

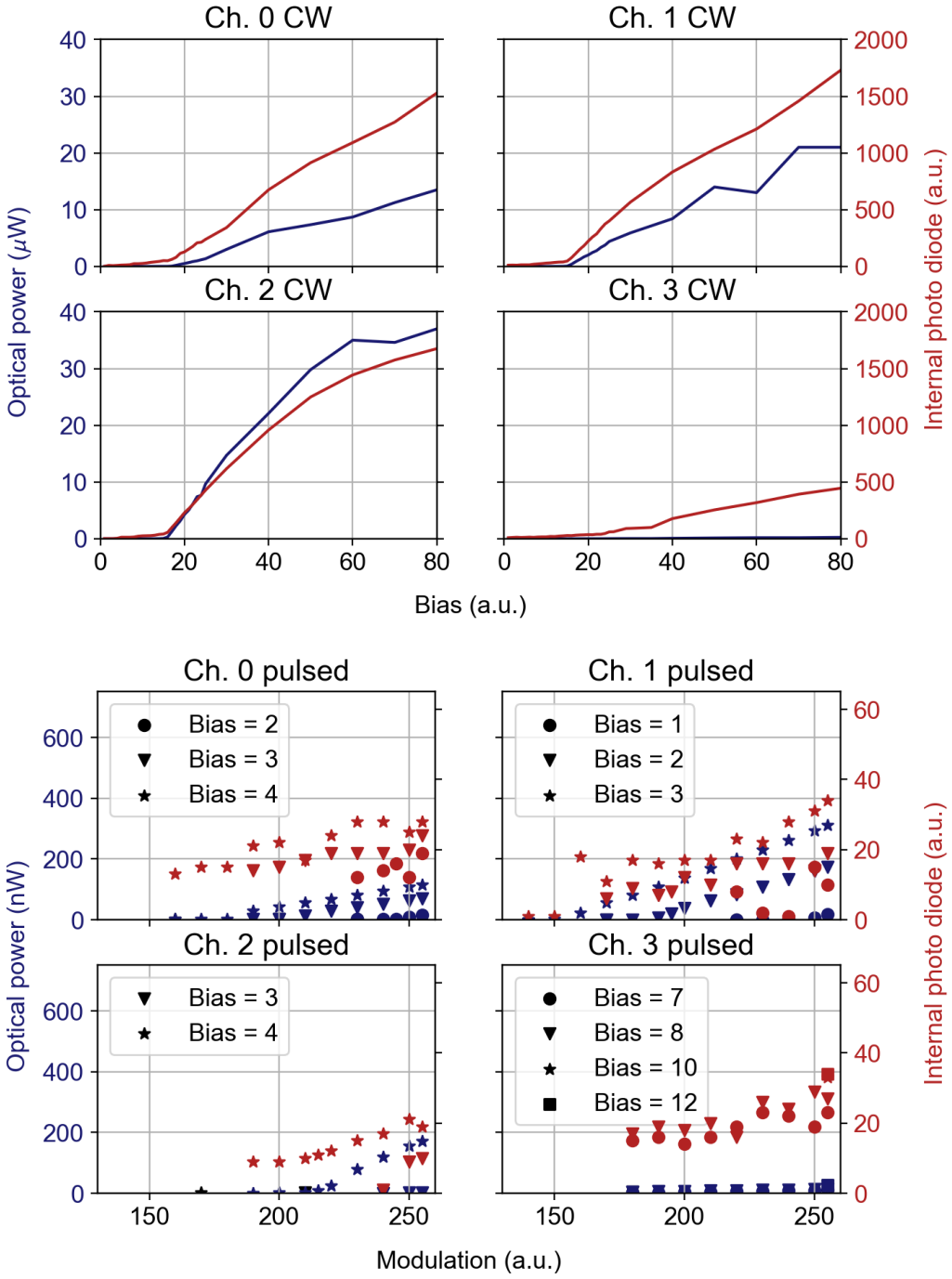


Figure 5.3: Optical response of the LMU FM in continuous wave (CW) (top) and pulsed mode (bottom). For the latter, the bias is kept below the lasing threshold while the modulation is varied. The optical output power is measured at the fiber output using a powermeter and with the internal photo diode, respectively.

cantly worse compared to the three other channels, which all show a higher optical output power. The pitch of the VCSELs on the array and the inputs of the waveguide circuit are perfectly fitting by construction, therefore, the coupling of only one channel cannot be completely different from the three remaining ones if those are comparable. One possibility is that the polarizer of this channel is not optimally positioned, therefore hindering a good coupling into the waveguide. This argument is substantiated by the significantly lower degree of polarization of only this channel (see table 5.1). Another possibility is an impurity at one of the surfaces after the VCSEL of channel 3, i.e., either at the microlens, the polarizer stripe, and/or the waveguide input.

For pulsed mode, with increasing bias and modulation, a higher optical output for all four channels is observed. Although also here channel 3 shows by far the lowest optical output power, it is still enough to find appropriate driving parameters to run sequences with adequate pulse brightness (see table 5.2).

5.1.4 Preparation Quality of the Polarization States

We performed a quantum state tomography (setup and method explained in section 4.1.2 and Ref. [72]) of the four polarization states of the FM in pulsed mode (see table 5.1). The measured states are rotated because of the birefringence of the optical fiber, which was random, but fixed for the data acquisition. By applying an appropriate polarization compensation, the states can be rotated back to $|H\rangle, |V\rangle, |+45\rangle$, and $|-45\rangle$.

	Tomography outcome				Ideally compensated			
Channel	0	1	2	3	0	1	2	3
S_1	0.347	-0.542	-0.646	0.644	0.965	-0.985	0.035	0.046
S_2	0.891	-0.706	0.603	-0.500	0.171	0.182	1.009	-0.945
S_3	0.219	-0.461	-0.488	-0.479	-0.039	-0.039	-0.003	-0.003
DOP	0.981	1.002	1.009	0.946	0.981	1.002	1.009	0.946
$\overline{\text{QBER}}$	-				1.2%			
$\overline{\text{q}}$	0.98				0.98			

Table 5.1: Polarization States of the LMU FM: S_1, S_2, and S_3 represent the Stokes components reconstructed from the measured tomographic data (left part) and a calculated set of states by applying an appropriate unitary transformation (right part). Given this, the DOP and mean value for the QBER [71, 72] as well as for the preparation quality q (see equation (2.2)) can be calculated.

We observe a low mean QBER of 1.2% and an almost ideal preparation quality q of 0.98. The degree of polarization (DOP) of channel 1 and channel 2 are slightly greater than 1, which is in principle an unphysical state, however, is explainable with the measurement accuracy[2]. Channel 3 shows a significantly lower DOP, which is accompanied by a comparably low optical output power of this channel. For further discussions regarding this, please see section 5.1.3. Despite this fault, the output polarization states of the FM are of good quality and very well suited for the QKD experiments with QUBE.

[2]By assuming a Poissonian distributed error of the count rates measured during the state tomography, the impact on the DOP is only in the fourth decimal place. Most probably a misalignment of the quarter wave plate or the polarizer in the tomography setup caused a slight but tolerable systematical error.

5.2 Determination of Driving Parameter

The following section details the determination of the operation parameters for the LMU FM by calibrating and testing it using a BB84 receiver and single photon detectors.

We decided to implement the BB84 protocol with a balanced basis choice. Therefore, the laser driver parameters (laser biases and modulation currents) must be tuned such that each of the four channels has the same optical output power. This calibration must be performed during sending a random pulse sequence, i.e., the four laser diodes are randomly pulsed with a repetition rate of 100 MHz - similar as in the QKD scenario. We observed that sequentially determined parameter sets, namely activating and optimizing one channel after another while the remaining three channels are off, cannot be used for random sequences. For such parameter sets, the pulse brightness of the four channels may change significantly [70], when used for random mode, with the consequence of missing the targeted proportion of the four polarization states sent. The reason for this behavior is the very sensitive optical response of the VCSELs in the mode we operate them during pulsing, where we keep the bias current below threshold and apply strong short modulation pulses above threshold [139].

The random pulse sequence is analyzed by a standard BB84 polarization receiver, which projects, after a passive basis choice by a balanced beam splitter, either on $|H\rangle\,/\,|V\rangle$ or $|+45\rangle\,/\,|-45\rangle$ (see section 2.3). The QKD sender is equipped with a 0.5 m long single mode (SM) fiber and an additional 5 m SM fiber with a manual fiber polarization controller for compensating the unitary rotation along these fibers.

At the time when the laser driver parameter sets have been determined, the final attenuation of the wavelength-division multiplexer (see section 2.2.4) and of the optical sender terminal OSIRIS (see section 2.2.3), in both cases the flight model, as well as of all fiber connections in between, have not been yet characterized. For this reason, we started with searching for the maximally reachable optical output power and furthermore three additional parameter sets, which enable a brightness variation of about two orders of magnitude (see table 5.2). As a consequence of the observed temperature dependence of the optical output power during the TVC tests (see section 4.3), we tested the parameters under different temperatures. For that we mounted the FM onto a temperature-controllable copper plate and performed (except for the maximum intensity set) the characterization measurements at system temperatures of 26 °C, 31 °C, and 40 °C. The temperature was monitored by the three internal sensors on the FM. At a room temperature of 21 °C, without active cooling or heating, and ambient air pressure, the thermal equilibrium of the electronics due to its waste heat is about 31 °C.

The determination of appropriate laser driver parameter of the QKD sender flight model was mainly affected by channel 3, because there the optical output power as well as the optical response on different driving parameters was by far the lowest (see figure 5.3 and table 5.2). The parameter set with the highest optical output power (PS-6) is therefore indicated by a high bias value and the highest possible modulation value (b9, m255) for channel 3. The procedure for the parameter set determination is, first, to turn on all four laser driver lines in random mode and further, detecting and analyzing the sent signals at

Parameter Set	VCSEL 1; 2; 3; 4	26 °C	31 °C	40 °C
PS-1	b4, m219; b3, m195; b4, m220; b8, m200	0.2 nW		
PS-2	b4, m231; b3, m206; b4, m240; b8, m212	0.5 nW		
PS-3	b4, m238; b3, m212; b4, m246; b8, m220	5.0 nW	-	-
PS-4	b4, m238; b3, m212; b4, m246; b8, m240	-	5.0 nW	-
PS-5	b4, m238; b3, m212; b4, m248; b8, m240	-	-	5.0 nW
PS-6	b4, m242; b3, m217; b4, m249; b9, m255	-	10.0 nW	-

Opt. output power sender (measured)	Mean photon number μ (calculated)	
	Sender	Exaperture satellite
0.2 nW	8.5	0.3
0.5 nW	21.3	0.7
5.0 nW	212.8	6.7
10.0 nW	425.7	13.5

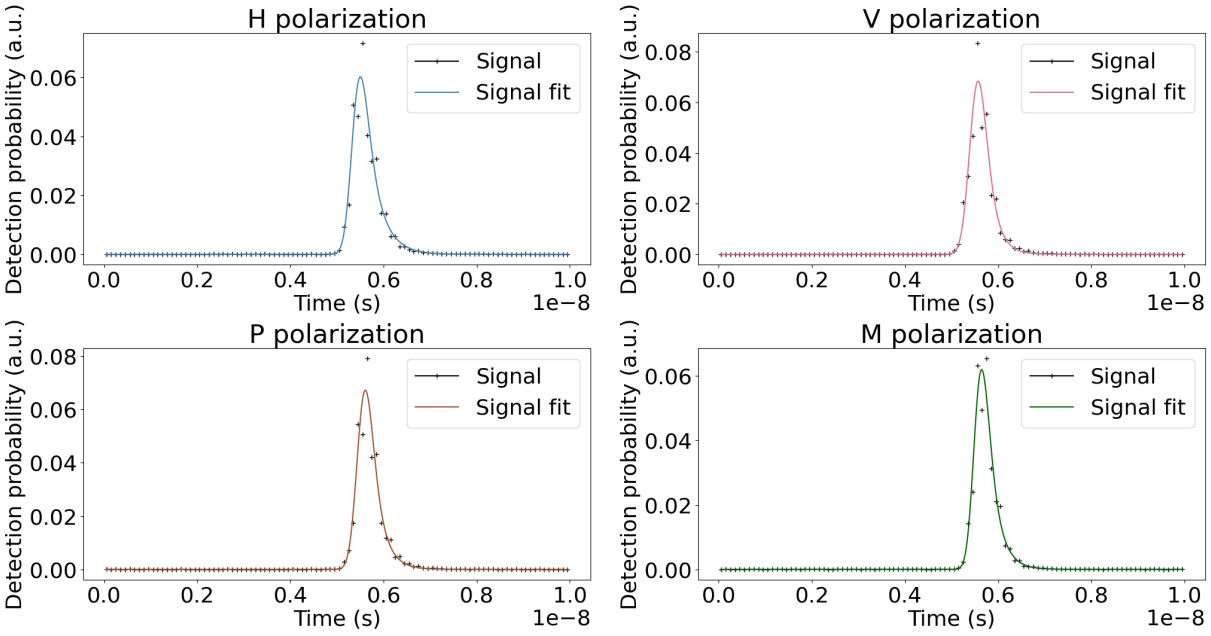
Table 5.2: Parameter sets (PS) for the laser driver settings bias (b) and modulation (m). The output power in random pulsed mode can be varied between 0.2 nW and 10 nW. For achieving a balanced brightness of the four channels, only at an optical output power of 5 nW, minor adjustments of the modulation depending on the temperature are necessary (PS-3 - PS-5). From the measured optical output power of the sender, the mean photon number μ can be calculated. To determine μ exaperture of the satellite, the losses at the wavelength division multiplexer (−2 dB) and at OSIRIS (−13 dB) must be taken into account.

the receiver while the laser driver parameters are tuned iteratively [70]. By this, parameter sets can be found, where the brightness of the optical pulses matches between the four channels (see figure 5.4). At this point it should be noted that the measurement of the optical output power was performed with a standard powermeter in combination with a highly sensitive photosensor, however, the parameter setting is made via the BB84 analyzer and APDs. To avoid unnecessary dis- and reconnecting and mounting, we were forced to go for a tradeoff of performed measurements and hardware modifications. For this reason, PS-6 was not tested under temperature changes and the output power of PS-1 to PS-5 is only reconstructed by the relative change of the APD detector count rate and the known attenuation at the BB84 receiver.

From the recorded detection events, we determine an overall average QBER (number of wrong detections divided by the sum of detection within the corresponding basis) of 1.3%. Note that this value already includes all imperfections of the sender and receiver as well as the polarization compensation.

In conclusion we can state that the overall brightness as well as the relative intensities of the four channels show nearly no temperature dependence over the considered temperature range. For a constant optical output power of our sender flight model, only minor changes

at the parameter sets PS-3 to PS-5 in the modulation of channel 2 and channel 3 have to be made. We are aware that the temperature range where the FM has been tested is smaller and does also not cover lower temperatures, as they are expected in space. Here, we also were forced to find a tradeoff of not overtesting the FM but still getting confidence about its behavior and stability in different ambient conditions.



State \ Det.	H	V	+45	−45	QBER
H	169357	4230	115916	70379	2.4%
V	2128	176964	119141	94531	1.2%
+45	65657	80370	170909	1600	0.9%
−45	76430	66429	788	151458	0.5%
				$\overline{\text{QBER}}$:	1.3%

Figure 5.4: The optical pulses of the QKD sender flight model (random pulsed mode) analyzed and detected by a BB84 receiver. Equally high detection probabilities for the four polarization states indicate a balanced brightness for the four lasers. From the detector countrates, the QBER related to each channel of the sender can be directly determined. The optical losses between sender output and receiver were not characterized here as for this measurement only the relative intensity between the channels has been varied. Shown here are the optical pulses and counts per second belonging to the parameter set 5 (PS-5, see table 5.2).

Chapter 6

Integration and Characterization of the Satellite

As shown in the two previous chapters, our QKD sender has been qualified for the usage in the QUBE satellite and the built sender flight model (LMU FM) promises optical characteristics well suited for this mission. This chapter comprises the integration and the optical characterization of the QUBE satellite flight model (QUBE FM).

6.1 Satellite Flight Model Integration

The mostly separately developed and built flight hardware of all project partners has been assembled at the clean room of the ZfT in Würzburg. The overall satellite structure as well as an overview of the to be integrated payload and operational modules is detailed in section 2.2.

The first payload which has been integrated into the QUBE FM main structure was the LMU FM. At this point in time the satellite has been only equipped with the backplane, the electric power system (EPS), and the on-board controller (OBC) (see figure 6.1 (left)). The most important criterion at the first step of its integration has been to ensure the perfect fit of the four mechanical fixation points and the electrical connector with the UNISEC[67] bus. The optical fiber of the LMU FM was temporarily fixed on the board. A first powering and commanding over UNISEC approved the correct interfacing and subsequent functional tests showed no noteworthy problems.

In the next steps, the FM of the MPL has been integrated according the same procedure as the FM of the LMU, followed by the attitude determination and control system (ADCS), the communication module (COMM), and the star tracker sensor. The OSIRIS terminal and the wavelength division multiplexer (WDM) unit has been mounted as the last components. The optical fiber network around the WDM unit, as well as the dedicated twisted pair clock line between the LMU, MPL, and OSIRIS module have been connected and fixed via Kapton and adhesive joints as one of the last integration steps before closing the satellite with the outer solar panels (see figure 6.1 (right)).

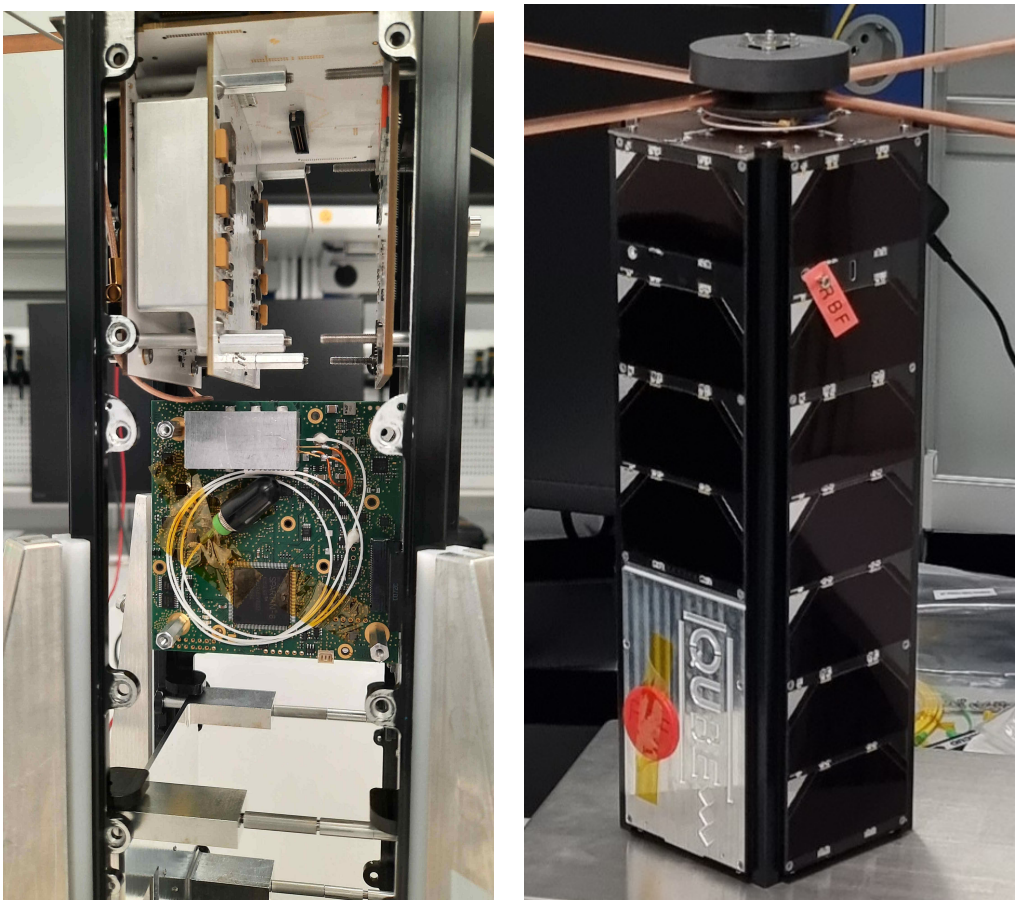


Figure 6.1: (Left) The LMU QKD sender FM (LMU FM) as the first payload and in general one of the first parts integrated in the QUBE FM. At this stadium, the LMU FM has been mechanically fixed and electrically connected via the UNISEC [67] interface. The optical fiber has been temporarily fixed on the board and the dedicated clock line, which is to be connected to the socket at the bottom right of the LMU FM, has not been attached yet. (Right) The fully integrated QUBE satellite FM. The red cover on the bottom protects the opening of the star tracker sensor.

6.2 Satellite Optical Characteristics

This section describes the optical characterization of the LMU FM in the fully integrated satellite FM, where we performed a quantum state tomography of the polarization states ex-aperture of the satellite, i.e., behind the last lens of the optical terminal. Furthermore, the output characteristics of the modulated OSIRIS beacon beam for synchronization purposes is shown.

6.2.1 Synchronization Channel

In general, QKD requires synchronized clocks of sender and receiver, which in our scenario are the clocks generated by the quantum payloads on the satellite and of the QKD receiver on ground. We implement this by modulating the 1550 nm tracking laser of the OSIRIS terminal with the QKD sender clocks. From the signal received at the optical ground station, the sender clock can be recovered. Precisely synchronized clocks do not only enable time bin matching but also allow for time filtering of the incoming QKD signals. This is a crucial factor to reduce the contribution of background photons in the detection recordings, which increase the capability of secure key rate generation (see section 2.4).

With the given pulse duration of about 150 ps of the LMU QKD sender signals, unfortunately not overlapping and separated by about 200 ps (see section 5.1.1), still a sub-ns acceptance time window is reasonable. This requires that the synchronization between satellite and optical ground station shows a jitter not larger than a few hundred ps. Due to the limited bandwidth of the available signal lines on the UNISEC bus in the satellite, we decided to implement a dedicated clock line with a twisted pair cable enabling the transmission of low voltage differential signals (LVDS) between the QKD senders and OSIRIS. The clock generated at the LMU FM is fed through the PCON module, which enables the switching between LMU and MPL clock (see section 2.2). We tested the signal integrity of the electrical clock signal generated on the LMU FM by probing at the last of all connectors in the line and set clock speeds of 10 MHz and 100 MHz (see figure 6.2 (Top)). We observe steep rising and falling edges but also a certain overswinging, which is more distinct at faster clock speeds. The overswing is in a tolerable range and below critical switching thresholds of subsequent parts. The cycle-to-cycle jitter of the signal is only 15 ps and 14 ps for 10 MHz and 100 MHz, respectively, read off the full width at half maximum (FWHM) of the cycle-to-cycle jitter envelope recorded.

The modulated beacon signal from OSIRIS has been analyzed using a fast photo sensor and an oscilloscope (see figure 6.2 (Bottom)). At a modulation speed of 10 MHz, an acceptably shaped clock signal can be detected - its cycle-to-cycle jitter is 154 ps FWHM. The laser diode used in OSIRIS is not designed for fast modulation, therefore, at a clock speed of 33 MHz only a sinusoidal response can be detected, however, its jitter is still only 134 ps FWHM.

Altogether, we state that the whole line for clock synchronization, starting at the clock generation over its electrical and optical transmission, fulfills our requirements regarding stability and precision.

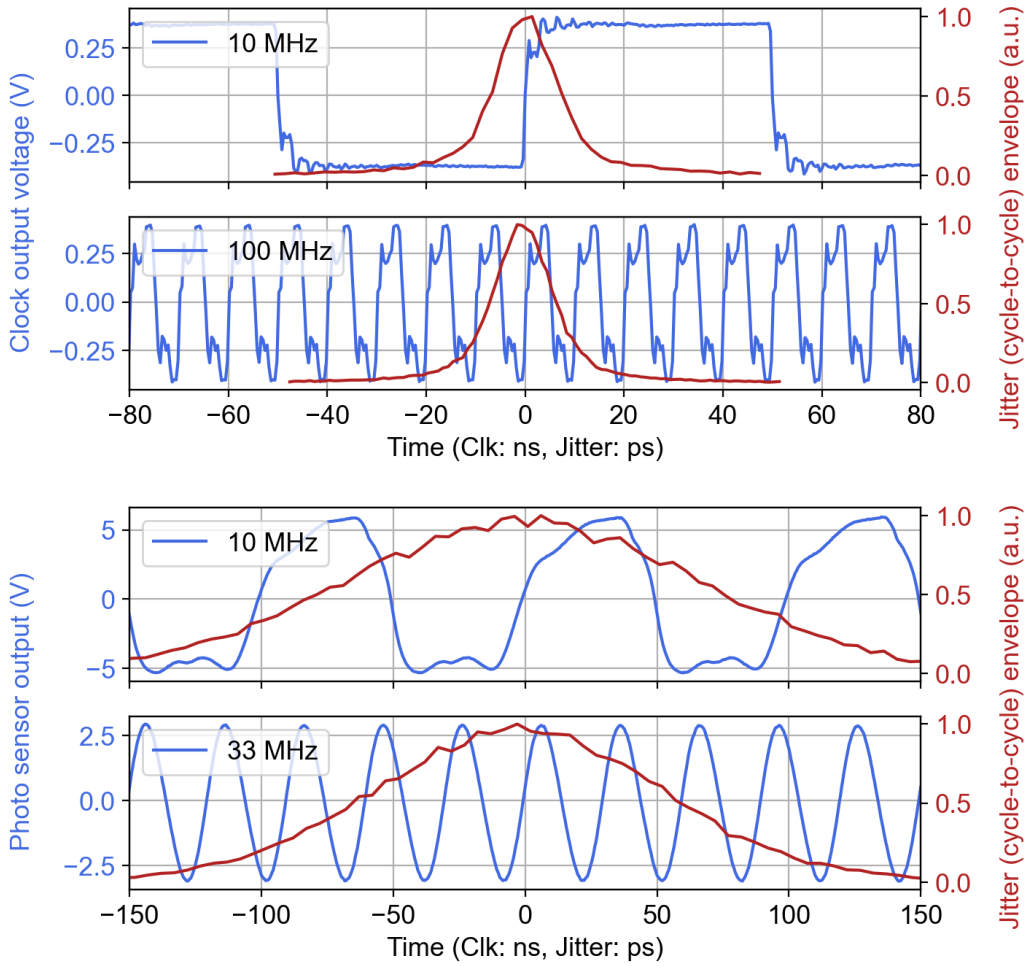


Figure 6.2: (Top) In blue, the low voltage differential signal (LVDS) clock generated at the LMU FM at the end of the dedicated twisted pair clock line for clock speeds of 10 MHz and 100 MHz directly recorded by an oscilloscope. In red, the envelope of the recorded cycle-to-cycle jitter of the clock signal. (Bottom) In blue, the output of a fast photo sensor capturing the 1550 nm beacon beam modulated by the clock signal generated on the LMU FM with 10 MHz and 33 MHz.

6.2.2 Quantum Signal Output

We performed a quantum state tomography of the polarization states emitted by the completely integrated satellite FM following the method explained in section 4.1.2 and Ref. [72]. This allows for investigating the polarization state quality exapterture of OSIRIS, i.e., after the generation and transmission through the whole optical path in the satellite including WDM unit, for the first time in the project. The operation mode of the QKD sender was set to pulsed mode emitting weak coherent pulses with a brightness comparable to a QKD like scenario.

In table 6.1, the tomographic results, comprising the polarization sates in Stokes representation as well as its degree of polarization (DOP), the mean QBER and the polarization preparation quality q are presented. The ideally compensated states are numerically reconstructed by applying an appropriate polarization compensation. For details to this method please see section 4.1.2 as well as in Refs. [71, 72].

	Tomography outcome				Ideally compensated			
Channel	0	1	2	3	0	1	2	3
S_1	0.122	0.262	-0.936	0.906	0.948	-0.979	-0.210	-0.138
S_2	0.952	-0.921	-0.290	-0.100	-0.215	-0.144	0.961	-0.933
S_3	-0.169	0.261	0.139	-0.268	0.084	0.084	-0.110	-0.110
DOP	0.976	0.993	0.989	0.950	0.976	0.993	0.989	0.950
$\overline{\text{QBER}}$	-				2.2%			
$\overline{\text{q}}$	0.94				0.94			

Table 6.1: Polarization states of the QUBE FM exaperture OSIRIS. S_1, S_2, and S_3 represent the Stokes components reconstructed from the measured tomographic data (left part) and a calculated set of states by applying an appropriate unitary transformation (right part). From this, the DOP and mean value for the QBER [71, 72] as well as for the preparation quality q (see equation (2.2)) can be calculated.

The overall quality of the analyzed polarization states is satisfying, as the mean QBER is only 2.2% and the preparation quality q is very high with its value of 0.94. The slight increase of the QBER and reduction of q compared to the source intrinsic values of 1.2% and 0.98, respectively (see section 5.1.4), is in an acceptable range in view of the transmittance through the very elaborated subsequent WDM unit and QSIRIS. The expected mean photon numbers (μ) exaperture of the satellite for different parameter settings in pulsed mode are stated in table 5.2. In total, the prepared polarization states emitted by the QUBE satellite FM are well suited for our planned QKD experiments.

Chapter 7

Conclusion and Outlook

This thesis reports the development, the construction, and the qualification of a highly compact QKD sender, which has been integrated into the 3-unit ($30 \times 10 \times 10\,\mathrm{cm}^3$) Cube-Satellite QUBE. This satellite is also equipped with an optical terminal, which enables the downlink to an optical ground station on Earth. With QUBE, a wide spectrum of tests of the QKD sender and its interplay with the other satellite components under real space conditions is possible. Due to the limited electrical power and space available in such a nanosatellite, strict requirements regarding size, weight, and power consumption (SWaP) were formulated on all payloads. Former works in our group, aiming at the miniaturization of a QKD sender for hand-held applications, provided the basic concept especially for the optics part. Here, an improved design has been developed and implemented by sophisticated assembly methods. By this we could reduce the dimensions of the sender optics to just about $3 \times 3 \times 20\,\mathrm{mm}^3$. The design of the sender has been also affected by the requirements regarding its robustness, as its application in a space mission comes along with harsh environmental influences due to radiation in space, vacuum, thermal fluctuations along the orbit, and vibration loads during the launch.

In total we built two sender modules using identical parts and assembly processes: an engineering qualification model (EQM) and the flight model (FM). The optical output states of the latter has been carefully characterized before and partly also after its integration into the satellite. The EQM, however, has been also tested regarding the aforementioned criteria due to the different influences during the mission. We could not observe a strong dependency of the functionality of the sender through the test loads. Also the tests performed with the self-built thermal vacuum chamber showed a remarkable stability of the polarization states, however, also raised the issue that the change of the output optical power with varying temperature is not always consistent. This is for sure an issue which has to be investigated closer in future versions of the sender, however, is not a showstopper for the proposed sender design in general. Here, thanks to the small size of the optics, this problem can be overcome by a temperature stabilization of this small volume, which is not yet implemented in QUBE but is in principle possible even on Cube-Satellites. The optical characterization measurements of the finally assembled satellite show promising results regarding the quality of the output polarization states and a low QBER of only

2.2%. Currently, a launch of the satellite is foreseen for the first half of 2023 and therefore first downlinks can be expected in the second half of 2023.

During this work, several issues appeared which either have not been completely finished or could be improved within QUBE but also should be addressed within the already initiated follow-up mission QUBE II. The usage of a VCSEL-array with four diodes, each designated for one of four polarization states, has the advantage that all subsequent parts of the optics are passive, i.e., activating the four individual channels is much simpler than using active phase or amplitude modulators. However, this scheme also has the disadvantage that, in unfavorable configurations, the wavelength as well as all other relevant degrees of freedom of the four VCSELs do not fully overlap, which opens a side-channel in the context of QKD. Possible remedies for the spectral mismatch are a better pre-selection of the VCSELs, wavelength filtering, as well as treating this imperfection in the QKD theory. A similar problem is the temporal overlap of the optical pulses. In QUBE, we use passive meander circuits on the electronics for the generation of the short electrical signals, which do not consume additional power. However, their handling is cumbersome, and the fine-tuning capabilities do not reach the accuracy and flexibility compared to former schemes using programmable delay lines. For QUBE II, most probably again the active solution has to be investigated. The assembly of the optics includes a step where the bonding wires get connected using an electrically conductive adhesive. The first problem of this technique is that relatively many steps have to be performed by hand, which on the one hand is time consuming and on the other hand reduces the reproducibility. At this point, a machine-based bonding technique should be considered. The determination of the driving parameter sets was performed iteratively by hand, which is comparably time consuming and should be automatized. So far, the optical output of the satellite has been characterized only in continuous-wave operation of the sender. Here, the driving parameter in pulsed mode should also be tested, which requires a slightly extended version of the analysis setup as used for the characterization measurements presented in this work.

At the optical ground station, the receiver setup has to be finalized and furthermore the influence of the telescope on the polarization states during the tracking of the satellite has to be characterized. Here also the polarization compensation requires an update to a more automatized controlling of the motorized compensation wave plates.

Especially regarding QUBE II, the key rate simulation needs to be adapted to include finite-statistics effects. Furthermore, the electronics has to be extended by the capabilities for post-processing and for the generation of decoy pulses. A possibility for improving the key rate performance would be to increase the actual repetition rate of 100 MHz, however, here the pulsing behavior of the VCSELs regarding stability and correlations has to be considered.

In this work substantial hardware developments of a low-SWaP QKD sender within the Cube-Satellite mission QUBE were made. They can provide important results regarding the suitability of such hardware for space missions and has the potential to serve as a key component in performant, but also economic QKD networks based on satellites.

Bibliography

[1] B. Schneier, *Applied Cryptography*. Wiley, 1996.

[2] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. CRC Press, 2015.

[3] L. Kruh and C. Deavours, "The commercial enigma: Beginnings of machine cryptography," *Cryptologia*, vol. 26, no. 1, pp. 1–16, 2002. DOI: 10.1080/0161-110291890731. [Online]. Available: https://doi.org/10.1080/0161-110291890731.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "Cryptographic communications system and method," *UNITED STATES PATENT*, vol. US 4405829 A, 1983.

[5] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Review*, vol. 41, no. 2, pp. 303–332, 1999.

[6] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017. DOI: 10.1038/nature23461. [Online]. Available: https://doi.org/10.1038/nature23461.

[7] D. Joseph *et al.*, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, 2022. DOI: 10.1038/s41586-022-04623-2. [Online]. Available: https://doi.org/10.1038/s41586-022-04623-2.

[8] W. Castryck and T. Decru, "An efficient key recovery attack on sidh," *Cryptology ePrint Archive, Paper 2022/975*, 2022. [Online]. Available: https://eprint.iacr.org/2022/975.

[9] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, pp. 644–654, 1976.

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 1 2002. DOI: 10.1103/RevModPhys.74.145. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.74.145.

[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, 3 2009. DOI: 10.1103/RevModPhys.81.1301. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.81.1301.

[12] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, pp. 595–604, 2014. DOI: 10.1038/nphoton.2014.149.

[13] S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020. DOI: 10.1364/AOP.361502. [Online]. Available: http://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012.

[14] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983, ISSN: 0163-5700. DOI: 10.1145/1008908.1008920. [Online]. Available: http://doi.acm.org/10.1145/1008908.1008920.

[15] C. H. Bennett and G. Brassard, "Quantum cryptography : Public key distribution and coin tossing," *International Conference on Computer System and Signal Processing, IEEE,*, pp. 175–179, 1984. [Online]. Available: http://ci.nii.ac.jp/naid/20001457561/en/.

[16] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Phys. Rev. A*, vol. 59, pp. 4238–4248, 6 1999. DOI: 10.1103/PhysRevA.59.4238. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.59.4238.

[17] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, p. 057 901, 5 2004. DOI: 10.1103/PhysRevLett.92.057901. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.92.057901.

[18] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, p. 037 902, 3 2002. DOI: 10.1103/PhysRevLett.89.037902. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.89.037902.

[19] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Reference-frame-independent quantum key distribution," *Appl. Phys. Lett.*, vol. 87, p. 194 108, 19 2005. DOI: 10.1063/1.2126792. [Online]. Available: https://doi.org/10.1063/1.2126792.

[20] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, 6 1991. DOI: 10.1103/PhysRevLett.67.661. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.67.661.

[21] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, 5 1992. DOI: 10.1103/PhysRevLett.68.557. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.68.557.

[22] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, p. 010 303, 1 1999. DOI: 10.1103/PhysRevA.61.010303. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.61.010303.

[23] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 db loss limit," *Phys. Rev. Lett.*, vol. 89, p. 167 901, 16 2002. DOI: 10.1103/PhysRevLett.89.167901. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.89.167901.

[24] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, p. 170 504, 17 2004. DOI: 10.1103/PhysRevLett.93.170504. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.93.170504.

[25] A. Vakhitov, V. Makarov, and D. R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," *Journal of Modern Optics*, vol. 48, no. 13, pp. 2023–2038, Nov. 2001. DOI: 10.1080/09500340108240904. [Online]. Available: https://doi.org/10.1080/09500340108240904.

[26] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nature Photonics*, vol. 4, pp. 686–689, 2010.

[27] V. Makarov, A. Anisimov, and J. Skaar, "Effects of detector efficiency mismatch on security of quantum cryptosystems," *Phys. Rev. A*, vol. 74, p. 022 313, 2 2006. DOI: 10.1103/PhysRevA.74.022313. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.74.022313.

[28] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors," *New Journal of Physics*, vol. 13, no. 7, p. 073 024, 2011. [Online]. Available: http://stacks.iop.org/1367-2630/13/i=7/a=073024.

[29] M. Rau *et al.*, "Spatial mode side channels in free-space qkd implementations," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 187–191, 2015, ISSN: 1077-260X. DOI: 10.1109/JSTQE.2014.2372008.

[30] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," *Proceedings 39th Annual Symposium on Foundations of Computer Science*, pp. 503–509, 1998. DOI: 10.1109/SFCS.1998.743501.

[31] R. Schwonnek *et al.*, "Device-independent quantum key distribution with random key basis," *Nature Communications*, vol. 12, no. 1, 2021. DOI: 10.1038/s41467-021-23147-3. [Online]. Available: https://doi.org/10.1038/s41467-021-23147-3.

[32] W. Zhang *et al.*, "A device-independent quantum key distribution system for distant users," *Nature*, vol. 607, no. 7920, pp. 687–691, 2022. DOI: 10.1038/s41586-022-04891-y. [Online]. Available: https://doi.org/10.1038/s41586-022-04891-y.

[33] D. P. Nadlinger *et al.*, "Experimental quantum key distribution certified by bell's theorem," *Nature*, vol. 607, no. 7920, pp. 682–686, 2022. DOI: 10.1038/s41586-022-04941-5. [Online]. Available: https://doi.org/10.1038/s41586-022-04941-5.

[34] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," *SPIE Proceedings*, 2005. DOI: 10.1117/12.606489. [Online]. Available: https://doi.org/10.1117/12.606489.

[35] M. Peev *et al.*, "The SECOQC quantum key distribution network in vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075 001, 2009. DOI: 10.1088/1367-2630/11/7/075001. [Online]. Available: https://doi.org/10.1088/1367-2630/11/7/075001.

[36] M. Sasaki *et al.*, "Field test of quantum key distribution in the tokyo qkd network," *Opt. Express*, vol. 19, no. 11, pp. 10 387–10 409, 2011. DOI: 10.1364/OE.19.010387. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-19-11-10387.

[37] Q. Zhang, F. Xu, L. Li, N.-L. Liu, and J.-W. Pan, "Quantum information research in china," *Quantum Science and Technology*, vol. 4, no. 4, p. 040 503, Nov. 2019. DOI: 10.1088/2058-9565/ab4bea. [Online]. Available: https://doi.org/10.1088/2058-9565/ab4bea.

[38] M. Mehic *et al.*, "Quantum key distribution: A networking perspective," *ACM Computing Surveys*, vol. 53, no. 5, pp. 1–41, 2020. DOI: 10.1145/3402192. [Online]. Available: https://doi.org/10.1145/3402192.

[39] S. Wang *et al.*, "Twin-field quantum key distribution over 830-km fibre," *Nature Photonics*, vol. 16, no. 2, pp. 154–161, 2022. DOI: 10.1038/s41566-021-00928-2. [Online]. Available: https://doi.org/10.1038/s41566-021-00928-2.

[40] R. Ursin *et al.*, "Entanglement-based quantum communication over 144 km," *Nature Physics*, vol. 3, pp. 481–486, 2007. DOI: 10.1038/nphys629.

[41] T. Schmitt-Manderbach *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, p. 010 504, 1 2007. DOI: 10.1103/PhysRevLett.98.010504. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.98.010504.

[42] S. Nauerth *et al.*, "Air-to-ground quantum communication," *Nature Photonics*, vol. 7, pp. 382–386, 2013. DOI: 10.1038/nphoton.2013.46.

[43] J.-Y. Wang *et al.*, "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," *Nature Photonics*, vol. 7, no. 5, pp. 387–393, 2013. DOI: 10.1038/nphoton.2013.89. [Online]. Available: https://doi.org/10.1038/nphoton.2013.89.

[44] S.-K. Liao *et al.*, "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, pp. 43–47, 7670 2017. DOI: 10.1038/nature23655. [Online]. Available: https://doi.org/10.1038/nature23655.

[45] J. Yin *et al.*, "Satellite-to-ground entanglement-based quantum key distribution," *Phys. Rev. Lett.*, vol. 119, p. 200 501, 20 Nov. 2017. DOI: 10.1103/PhysRevLett.119.200501. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.119.200501.

[46] S.-K. Liao *et al.*, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, p. 030 501, 3 2018. DOI: 10.1103/PhysRevLett.120.030501. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.120.030501.

[47] G. Vallone *et al.*, "Experimental satellite quantum communications," *Phys. Rev. Lett.*, vol. 115, p. 040 502, 4 2015. DOI: 10.1103/PhysRevLett.115.040502. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.115.040502.

[48] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Information*, vol. 3, no. 1, 2017. DOI: 10.1038/s41534-017-0031-5. [Online]. Available: https://doi.org/10.1038/s41534-017-0031-5.

[49] D. Oi *et al.*, "CubeSat quantum communications mission," *EPJ Quantum Technology*, vol. 4, no. 1, 2017. DOI: 10.1140/epjqt/s40507-017-0060-1. [Online]. Available: https://doi.org/10.1140/epjqt/s40507-017-0060-1.

[50] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, "Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite," *Nature Photonics*, vol. 11, no. 8, pp. 502–508, 2017. DOI: 10.1038/nphoton.2017.107. [Online]. Available: https://doi.org/10.1038/nphoton.2017.107.

[51] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, "Low cost and compact quantum key distribution," *New Journal of Physics*, vol. 8, no. 10, pp. 249–249, 2006, ISSN: 1367-2630. DOI: 10.1088/1367-2630/8/10/249. [Online]. Available: http://iopscience.iop.org/1367-2630/8/10/249.

[52] Y. Li *et al.*, "Space-bound optical source for satellite-ground decoy-state quantum key distribution," *Optics Express*, vol. 22, no. 22, p. 27 281, 2014, ISSN: 1094-4087. DOI: 10.1364/OE.22.027281. [Online]. Available: http://www.opticsinfobase.org/abstract.cfm?URI=oe-22-22-27281.

[53] D. M. Benton, P. M. Gorman, P. R. Tapster, and D. M. Taylor, "A compact free space quantum key distribution system capable of daylight operation," *Optics Communications*, vol. 283, no. 11, pp. 2465–2471, 2010, ISSN: 0030-4018. DOI: 10.1016/j.optcom.2009.10.039. [Online]. Available: http://dx.doi.org/10.1016/j.optcom.2009.10.039%20http://www.sciencedirect.com/science/article/pii/S0030401809010141.

[54] D. Lowndes, S. Frick, A. Hart, and J. Rarity, "A low cost, short range quantum key distribution system," *EPJ Quantum Technology*, vol. 8, p. 15, 1 2021. DOI: 10.1140/epjqt/s40507-021-00101-2. [Online]. Available: https://doi.org/10.1140/epjqt/s40507-021-00101-2.

[55] G. Vest *et al.*, "Quantum key distribution with a hand-held sender unit," *Phys. Rev. Applied*, vol. 18, p. 024 067, 2 2022. DOI: 10.1103/PhysRevApplied.18.024067. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevApplied.18.024067.

[56] P. Sibson *et al.*, "Chip-based quantum key distribution," *Nature Communications*, vol. 8, p. 13 984, Feb. 2017, ISSN: 2041-1723. DOI: 10.1038/ncomms13984. [Online]. Available: http://www.nature.com/doifinder/10.1038/ncomms13984.

[57] K. Wei *et al.*, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," *Phys. Rev. X*, vol. 10, p. 031 030, 3 Aug. 2020. DOI: 10.1103/PhysRevX.10.031030. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevX.10.031030.

[58] D. Bunandar *et al.*, "Metropolitan quantum key distribution with silicon photonics," *Phys. Rev. X*, vol. 8, p. 021 009, 2 Apr. 2018. DOI: 10.1103/PhysRevX.8.021009. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevX.8.021009.

[59] M. Avesani *et al.*, "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," *npj Quantum Information*, vol. 7, p. 93, 1 2021. DOI: 10.1038/s41534-021-00421-2. [Online]. Available: https://doi.org/10.1038/s41534-021-00421-2.

[60] T. K. Paraïso *et al.*, "A photonic integrated quantum secure communication system," *Nature Photonics*, vol. 15, p. 850, 11 2021. DOI: 10.1038/s41566-021-00873-0. [Online]. Available: https://doi.org/10.1038/s41566-021-00873-0.

[61] H. Heidt, J. Puig-Suari, A. S. Moore, S. Nakasuka, and R. J. Twiggs, "Cubesat: A new generation of picosatellite for education and industry low-cost space experimentation," *Proceedings of the AIAA/USU Conference on Small Satellites, Logan, UT, USA*, 2000.

[62] C. Nieto-Peroy and M. R. Emami, "Cubesat mission: From design to operation," *Applied sciences*, vol. 9, no. 15, p. 3110, 2019, ISSN: 2076-3417.

[63] G. Mélen, "Integrated quantum key distribution sender unit for hand-held platforms," Dissertation (2016), Ludwig Maximilian University Munich.

[64] G. Vest *et al.*, "Design and evaluation of a handheld quantum key distribution sender module," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 131–137, May 2015, ISSN: 1077-260X. DOI: 10.1109/JSTQE.2014.2364131.

[65] M. Smit *et al.*, "An introduction to InP-based generic integration technology," *Semiconductor Science and Technology*, vol. 29, no. 8, p. 083 001, 2014. DOI: 10.1088/0268-1242/29/8/083001. [Online]. Available: https://doi.org/10.1088/0268-1242/29/8/083001.

[66] C. Gabriel *et al.*, "A generator for unique quantum random numbers based on vacuum states," *Nature Photonics*, vol. 4, pp. 711–715, 10 2010. DOI: 10.1038/nphoton.2010.197. [Online]. Available: https://doi.org/10.1038/nphoton.2010.197.

[67] UNISEC, "Cubesat subsystem interface definition," Interface Definition Version 1.0, UNISEC-Europe Office Würzburg (2017).

[68] H. A. MacLeod, *Thin-Film Optical Filters*. CRC Press, 2010. [Online]. Available: https://doi.org/10.1201/9781420073034.

[69] J. Luhn, "Handheld quantum key distribution," Master's Thesis (2017), Ludwig Maximilian University Munich.

[70] M. Auer, "Implementation of decoy state qkd," Master's Thesis (2020), Ludwig Maximilian University Munich.

[71] T. Vogl, "Mobile free space quantum key distribution for short distance secure communication," Master's Thesis (2016), Ludwig Maximilian University Munich.

[72] P. Freiwang, "Towards hand-held quantum key distribution," Master's Thesis (2017), Ludwig Maximilian University Munich.

[73] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982. [Online]. Available: http://dx.doi.org/10.1038/299802a0.

[74] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology — EUROCRYPT '93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings*, T. Helleseth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423, ISBN: 978-3-540-48285-7. DOI: 10.1007/3-540-48285-7_35. [Online]. Available: http://dx.doi.org/10.1007/3-540-48285-7_35.

[75] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, "Demystifying the information reconciliation protocol cascade," *Quantum Info. Comput.*, vol. 15, no. 5–6, pp. 453–477, 2015.

[76] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," *Phys. Rev. A*, vol. 67, p. 052303, 5 2003. DOI: 10.1103/PhysRevA.67.052303. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.67.052303.

[77] R. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, 1962, ISSN: 0096-1000. DOI: 10.1109/TIT.1962.1057683.

[78] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," *2009 IEEE International Symposium on Information Theory*, pp. 1879–1883, 2009. DOI: 10.1109/ISIT.2009.5205475.

[79] A. R. Dixon and H. Sato, "High speed and adaptable error correction for megabit/s rate quantum key distribution," *Scientific Reports*, vol. 4, no. 1, p. 7275, 2014. DOI: 10.1038/srep07275. [Online]. Available: https://www.nature.com/articles/srep07275.

[80] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995, ISSN: 0018-9448. DOI: 10.1109/18.476316.

[81] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130 503, 13 2012. DOI: 10.1103/PhysRevLett.108.130503. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.108.130503.

[82] X. Ma and M. Razavi, "Alternative schemes for measurement-device-independent quantum key distribution," *Phys. Rev. A*, vol. 86, p. 062 319, 6 2012. DOI: 10.1103/PhysRevA.86.062319. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.86.062319.

[83] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, "Single photon quantum cryptography," *Phys. Rev. Lett.*, vol. 89, p. 187 901, 18 2002. DOI: 10.1103/PhysRevLett.89.187901. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.89.187901.

[84] R. Alléaume *et al.*, "Experimental open-air quantum key distribution with a single-photon source," *New Journal of Physics*, vol. 6, no. 1, p. 92, 2004. [Online]. Available: http://stacks.iop.org/1367-2630/6/i=1/a=092.

[85] T. Heindel *et al.*, "Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range," *New Journal of Physics*, vol. 14, no. 8, p. 083 001, 2012. [Online]. Available: http://stacks.iop.org/1367-2630/14/i=8/a=083001.

[86] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, pp. 1863–1869, 3 1995. DOI: 10.1103/PhysRevA.51.1863. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.51.1863.

[87] M. Dušek, O. Haderka, and M. Hendrych, "Generalized beam-splitting attack in quantum cryptography with dim coherent states," *Optics Communications*, vol. 169, pp. 103–108, 1999. DOI: http://dx.doi.org/10.1016/S0030-4018(99)00419-8. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0030401899004198.

[88] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, pp. 1330–1333, 6 2000. DOI: 10.1103/PhysRevLett.85.1330. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.85.1330.

[89] D. Gottesman, H. K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, 2004, p. 136. DOI: 10.1109/ISIT.2004.1365172.

[90] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, p. 057 901, 5 2003. DOI: 10.1103/PhysRevLett.91.057901. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.91.057901.

[91] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, p. 230 504, 23 2005. DOI: 10.1103/PhysRevLett.94.230504. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.94.230504.

[92] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, p. 230 503, 23 2005. DOI: 10.1103/PhysRevLett.94.230503. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.94.230503.

[93] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, p. 012 326, 1 2005. DOI: 10.1103/PhysRevA.72.012326. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.72.012326.

[94] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A*, vol. 61, p. 052 304, 5 2000. DOI: 10.1103/PhysRevA.61.052304. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.61.052304.

[95] H.-K. Lo, H. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, pp. 133–165, 2 2005. DOI: 10.1007/s00145-004-0142-y. [Online]. Available: https://doi.org/10.1007/s00145-004-0142-y.

[96] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state qkd protocol," *Appl. Phys. Lett.*, vol. 112, p. 17 114, 17 2018. DOI: 10.1063/1.5023340. [Online]. Available: https://doi.org/10.1063/1.5023340.

[97] C. C.-W. Lim, F. Xu, J.-W. Pan, and A. Ekert, "Security analysis of quantum key distribution with small block length and its application to quantum space communications," *Phys. Rev. Lett.*, vol. 126, p. 100 501, 10 Mar. 2021. DOI: 10.1103/PhysRevLett.126.100501. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.126.100501.

[98] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, "Finite key effects in satellite quantum key distribution," *npj Quantum Information*, vol. 8, p. 18, 1 2022. DOI: 10.1038/s41534-022-00525-3. [Online]. Available: https://doi.org/10.1038/s41534-022-00525-3.

[99] M. T. Gruneisen, M. B. Flanagan, B. A. Sickmiller, J. P. Black, K. E. Stoltenberg, and A. W. Duchane, "Modeling daytime sky access for a satellite quantum key distribution downlink," *Opt. Express*, vol. 23, no. 18, pp. 23 924–23 934, 2015. DOI: 10.1364/OE.23.023924. [Online]. Available: http://opg.optica.org/oe/abstract.cfm?URI=oe-23-18-23924.

[100] G. Mélen, W. Rosenfeld, and H. Weinfurter, "Impact of the slit geometry on the performance of wire-grid polarisers," *Opt. Express*, vol. 23, no. 25, pp. 32 171–32 178, 2015. DOI: 10.1364/OE.23.032171. [Online]. Available: http://www.opticsexpress.org/abstract.cfm?URI=oe-23-25-32171.

[101] R. Michalzik, *VCSELs: Fundamentals, Technology and Applications of Vertical Cavity Surface Emitting Lasers*. Springer, 2013.

[102] L. Y. Karachinsky *et al.*, "Reliability performance of 25 gbit 850 nm vertical-cavity surface-emitting lasers," *Semiconductor Science and Technology*, vol. 28, no. 6, p. 065 010, 2013. DOI: 10.1088/0268-1242/28/6/065010. [Online]. Available: https://doi.org/10.1088/0268-1242/28/6/065010.

[103] E. H. Land, "Some aspects of the development of sheet polarizers," *J. Opt. Soc. Am.*, vol. 41, no. 12, pp. 957–963, 1951. DOI: 10.1364/JOSA.41.000957. [Online]. Available: http://opg.optica.org/abstract.cfm?URI=josa-41-12-957.

[104] Y. Dirix, T. A. Tervoort, and C. Bastiaansen, "Optical properties of oriented polymer/dye polarizers," *Macromolecules*, vol. 28, no. 2, pp. 486–491, 1995. DOI: doi:10.1021/ma00106a011. [Online]. Available: https://doi.org/10.1021/ma00106a011.

[105] Y. Dirix, T. A. Tervoort, and C. Bastiaansen, "Optical properties of oriented polymer/dye polarizers. 2. ultimate properties," *Macromolecules*, vol. 30, no. 7, pp. 2175–2177, 1997. DOI: doi:10.1021/ma960808x. [Online]. Available: https://doi.org/10.1021/ma960808x.

[106] J. Birkmann, "Towards compact high-altitude-platform based quantum key distribution," Master's Thesis (2019), Ludwig Maximilian University Munich.

[107] K. M. Davis, K. Miura, N. Sugimoto, and K. Hirao, "Writing waveguides in glass with a femtosecond laser," *Opt. Lett.*, vol. 21, no. 21, pp. 1729–1731, 1996. DOI: 10.1364/OL.21.001729. [Online]. Available: http://opg.optica.org/ol/abstract.cfm?URI=ol-21-21-1729.

[108] A. Crespi *et al.*, "Integrated photonic quantum gates for polarization qubits," *Nature Communications*, vol. 2, no. 1, p. 566, 2011. DOI: 10.1038/ncomms1570. [Online]. Available: https://doi.org/10.1038/ncomms1570.

[109] C. Sonnleitner, "Towards a practical integrated qkd sender," Master's Thesis (2018), Ludwig Maximilian University Munich.

[110] L. D. Edmonds, C. Barnes, and L. Scheick, "An introduction to space radiation effects on microelectronics," publication 00-06 (2000), NASA Jet Propulsion Laboratory (JPL), California. [Online]. Available: https://parts.jpl.nasa.gov/pdf/JPL00-62.pdf.

[111] R. Baumann and K. Kruckmeyer, "Radiation handbook for electronics," Dallas (2020), Texas Instruments. [Online]. Available: https://www.ti.com/radbook.

[112] S. Bourdarie and M. Xapsos, "The near-earth space radiation environment," *IEEE Transactions on Nuclear Science*, vol. 55, no. 4, pp. 1810–1832, 2008. DOI: 10.1109/TNS.2008.2001409.

[113] F. Sexton, "Destructive single-event effects in semiconductor devices and ics," *IEEE Transactions on Nuclear Science*, vol. 50, no. 3, pp. 603–621, 2003. DOI: 10.1109/TNS.2003.813137.

[114] J. R. Schwank *et al.*, "Radiation effects in mos oxides," *IEEE Transactions on Nuclear Science*, vol. 55, no. 4, pp. 1833–1853, 2008. DOI: 10.1109/TNS.2008.2001040.

[115] R. Pease, "Total ionizing dose effects in bipolar devices and circuits," *IEEE Transactions on Nuclear Science*, vol. 50, no. 3, pp. 539–551, 2003. DOI: 10.1109/TNS.2003.813133.

[116] J. Srour, C. Marshall, and P. Marshall, "Review of displacement damage effects in silicon devices," *IEEE Transactions on Nuclear Science*, vol. 50, no. 3, pp. 653–670, 2003. DOI: 10.1109/TNS.2003.813197.

[117] M. Shaneyfelt, P. Dodd, B. Draper, and R. Flores, "Challenges in hardening technologies using shallow-trench isolation," *IEEE Transactions on Nuclear Science*, vol. 45, no. 6, pp. 2584–2592, 1998. DOI: 10.1109/23.736501.

[118] N. A. Dodds *et al.*, "Effectiveness of sel hardening strategies and the latchup domino effect," *IEEE Transactions on Nuclear Science*, vol. 59, no. 6, pp. 2642–2650, 2012. DOI: 10.1109/TNS.2012.2224374.

[119] J. W. Keller and N. M. Schaeffer, "Radiation shielding for space vehicles," *Electrical Engineering*, vol. 79, no. 12, pp. 1049–1054, 1960. DOI: 10.1109/EE.1960.6432974.

[120] W. Fan, C. Drumm, S. Roeske, and G. Scrivner, "Shielding considerations for satellite microelectronics," *IEEE Transactions on Nuclear Science*, vol. 43, no. 6, pp. 2790–2796, 1996. DOI: 10.1109/23.556868.

[121] D. V. Reames, "Particle acceleration at the sun and in the heliosphere," *Space Science Reviews*, vol. 90, pp. 413–491, 1999. DOI: https://doi.org/10.1023/A:1005105831781.

[122] M. Xapsos, C. Stauffer, G. Gee, J. Barth, E. Stassinopoulos, and R. McGuire, "Model for solar proton risk assessment," *IEEE Transactions on Nuclear Science*, vol. 51, no. 6, pp. 3394–3398, 2004. DOI: 10.1109/TNS.2004.839159.

[123] B. Rossi, "Cosmic rays," New York, McGraw-Hill (1964).

[124] M. Shea and D. Smart, "A comparison of energetic solar proton events during the declining phase of four solar cycles (cycles 19–22)," *Advances in Space Research*, vol. 16, no. 9, pp. 37–46, 1995, ISSN: 0273-1177. DOI: https://doi.org/10.1016/0273-1177(95)00312-3. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0273117795003123.

[125] E. Benton and E. Benton, "Space radiation dosimetry in low-earth orbit and beyond," *Nuclear Instruments and Methods in Physics Research Section B: Beam Interactions with Materials and Atoms*, vol. 184, no. 1, pp. 255–294, 2001, Advanced Topics in Solid State Dosimetry, ISSN: 0168-583X. DOI: https://doi.org/10.1016/S0168-583X(01)00748-0. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0168583X01007480.

[126] G. Badhwar and P. O'Neill, "Galactic cosmic radiation model and its applications," *Advances in Space Research*, vol. 17, no. 2, pp. 7–17, 1996, Proceedings of the Meetings F2.6 and F2.7 of COSPAR Scientific Commission F which was held during the Thirtieth COSPAR Scientific Assembly, ISSN: 0273-1177. DOI: https://doi.org/10.1016/0273-1177(95)00507-B. [Online]. Available: https://www.sciencedirect.com/science/article/pii/027311779500507B.

[127] G. D. Reeves *et al.*, "Electron acceleration in the heart of the van allen radiation belts," *Science*, vol. 341, no. 6149, pp. 991–994, 2013. DOI: 10.1126/science.1237743. [Online]. Available: https://www.science.org/doi/abs/10.1126/science.1237743.

[128] F. J. Pavón-Carrasco and A. De Santis, "The south atlantic anomaly: The key for a possible geomagnetic reversal," *Frontiers in Earth Science*, vol. 4, 2016. DOI: 10.3389/feart.2016.00040. [Online]. Available: https://www.frontiersin.org/article/10.3389/feart.2016.00040.

[129] S. Huston and K. Pfitzer, "A new model for the low altitude trapped proton environment," *IEEE Transactions on Nuclear Science*, vol. 45, no. 6, pp. 2972–2978, 1998. DOI: 10.1109/23.736554.

[130] *Total dose steady-state irradiation test method*, European Space Agency.

[131] *Mil-std-883 test method standard*, Microcircuits, Department of Defense.

[132] *Test procedures for the measurement of single-event effects in semiconductor devices from heavy ion irradiation*, Electronic Industries Association (EIA)/JESD57.

[133] *Standard guide for the measurement of single event phenomena (sep) induced by heavy ion irradiation of semiconductor devices*, ASTM International.

[134] M. Zeitlmair, "A hybrid plasmon-solid-state single-photon source," Dissertation (2021), Ludwig Maximilian University Munich.

[135] *Vega user manual issue 4 - revision 0*, Arianespace, April 2014.

[136] *Falcon user guide*, SpaceX, September 2021.

[137] S. Busch, "Robust, flexible and efficient design for miniature satellite systems," Dissertation (2016), Julius-Maximillians-Universität Würzburg.

[138] J. Rosano Nonay, "Characterisation of a thermal-vacuum-chamber for measurements with a transmitter for quantum key distribution," Semester's Thesis (2019), Ludwig Maximilian University Munich and Technical University Munich.

[139] H. Ko, B.-S. Choi, J.-S. Choe, K.-J. Kim, J.-H. Kim, and C. J. Youn, "Critical side channel effects in random bit generation with multiple semiconductor lasers in a polarization-based quantum key distribution system," *Opt. Express*, vol. 25, no. 17, pp. 20 045–20 055, 2017. DOI: 10.1364/OE.25.020045. [Online]. Available: http://www.osapublishing.org/oe/abstract.cfm?URI=oe-25-17-20045.

List of Abbreviations

ADCS	Attitude Determination and Control System
CME	Coronal Mass Ejection
DD	Displacement Damage
DLR	Deutsches Zentrum für Luft- und Raumfahrt (Engl. German Aerospace Center)
DLR IKN	DLR Institut für Kommunikation und Navigation (Engl. DLR Institute of Communications and Navigation)
EPS	Electric Power System
EQM	Engineering Qualification Model
FM	Flight Model
FPGA	Field-Programmable Gate Array
GCR	Galactic Cosmic Rays
InP	Indium Phosphide
LEO	Low Earth Orbit
LMU	Ludwig–Maximilians–Universität
MPL	Max Planck Institute for the Science of Light
OBC	On-board Controller

OGS	Optical Ground Station
OSIRIS	Optical Space Infrared Downlink System
PCB	Printed Circuit Board
PCON	Payload Controller
PIC	Photonic Integrated Circuit
QBER	Quantum Bit Error Ratio
QRNG	Quantum Random Number Generator
RMS	Root Mean Square
SEE	Single Event Effects
SET	Single Event Transient
SPE	Solar Particle Event
SWaP	Size, Weight and Power
TEC	Thermal Expansion Coefficient
TMTC	Telemetry and Telecommand
TID	Total Ionization Dose
UNISEC	University Space Engineering Consortium
UV	Ultraviolet
VCSEL	Vertical-Cavity Surface-Emitting Laser
WDM	Wavelength-Division Multiplexer
WGC	Waveguide Glass Chip
ZfT	Zentrum für Telematik (Engl. Center for Telematics)

Acknowledgments

An erster Stelle möchte ich meinem Professor Harald Weinfurter für die Möglichkeit zur Promotion in seiner Arbeitsgruppe danken. Es gab mir ein sehr gutes Gefühl, dass ich mit meinen Anliegen jederzeit bei Dir anklopfen und auf Deinen konstruktiven Rat zählen konnte. Hervorheben möchte ich, dass Probleme und Lösungsansätze bis ins kleinste Detail diskutiert werden konnten, obwohl es Dein voller Terminkalender oft eigentlich nicht hergegeben hätte. Da mich—Stand jetzt—QKD nicht loslässt, hoffe ich weiterhin auf Deine offene Tür.

Ein besonderer Dank gilt meinem Postdoc Lukas Knips. Ehrlich gesagt, fällt es mir nicht leicht die folgenden Worte zu schreiben, ohne dabei in Überschwang zu geraten. Dein Einsatz, Deine fachlichen Fähigkeiten, aber vor allem Deine über alle Maßen große Empathie und Dein Feinsinn sind einmalig. Dass Du mich in der Zeit meiner Promotion begleitet hast, ist einfach eines der wertvollsten Geschenke in meinem Leben.

In den ersten drei Jahre in der Arbeitsgruppe wurde ich intensiv von Wenjamin Rosenfeld betreut. Auch Dir gilt mein besonderer Dank, denn Du hast nicht nur den Grundstein zu dieser Arbeit gelegt, sondern mich nachhaltig geprägt. Ich sehe es als Privileg, einen Teil der Zeit für diese Arbeit unter Deiner Obhut verbracht haben zu dürfen.

Meinen QKD-Mitstreitern Michael Auer, Adomas Baliuka und Rengaraj Govindaraj danke ich für die tolle Zusammenarbeit im Team. In unserer Arbeitsgruppe herrscht ein großartiges Klima, und ich möchte mich ausnahmslos bei jeder und jedem von Euch dafür bedanken, auch bei meinen ehemaligen Kolleg:innen. Ein derart offenes, hilfsbereites und herzliches Umfeld findet man mit Sicherheit nicht oft. Von technischer Seite an der LMU danke ich dem Team um Herrn Aust, sowie Philipp Altpeter und Christian Obermayer.

Das QUBE-Satelliten-Projekt ist nur dank der guten Zusammenarbeit verschiedener Institutionen möglich—dazu zählen das DLR IKN und OHB in Oberpfaffenhofen, die Kolleg:innen vom MPL bzw. der FAU in Erlangen und dem ZfT in Würzburg. Vielen Dank für Euren andauernden Einsatz, um dieses Projekt hoffentlich erfolgreich abzuschließen.

Zu guter Letzt möchte ich auch meiner Familie und meinen Freunden danken: Ihr habt immer an mich geglaubt und mich jederzeit unterstützt!