# Air to Ground Quantum Key Distribution

**Sebastian Nauerth**


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

2013

# Air to Ground Quantum Key Distribution

**Sebastian Nauerth**

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

vorgelegt von
Sebastian Nauerth
aus München

München, den 19. Juli 2013

Erstgutachter: Prof. Harald Weinfurter
Zweitgutachter: Prof. Ulf Kleineberg
Tag der mündlichen Prüfung: 21. Oktober 2013

# Abstract

For confidential communication, today, a variety of extremely secure encryption algorithms are readily available. These techniques, however, always require a secret key shared between sender and receiver. The only way to exchange such a key for two distant parties unconditionally secure is quantum key distribution (QKD). Moreover, a key, once generated using QKD, can be analyzed for its integrity and discarded – in parts or completely – in case the transmission was intercepted.

The operating distance of QKD systems, however, is limited to a few hundreds of km due to the attenuation in the channel and detector noise. Yet, satellite based systems could provide efficient links for global scale QKD. While both classical optical satellite downlinks and long range terrestrial free-space QKD were shown successfully, a quantum key exchange with a rapidly moving platform is still missing. The presented work closes this gap with a first experimental demonstration of a BB84 QKD transmission from an airplane at a speed of 290 km/h to ground.

The experiment could be realized supplementing the system for classical free-space optical (FSO) communication operated by the German Aerospace Center (DLR) with QKD hardware: A transmitter for BB84 polarization encoded faint pulse QKD at a wavelength of 850 nm was designed and integrated in the free-space experimental laser terminal 2 (FELT2) carried by a Dornier 228 turboprop airplane and an according QKD receiver was mounted to the optical ground station (OGS) located near Munich, Germany.

A first challenge of this demonstration was to enable sufficient coupling of the transmitter and receiver telescope. This required an enhancement of the pointing system as for QKD applications the transmitter power may not be increased to compensate for high channel attenuation. Further, the polarization encoding necessitates a precise compensation scheme for mutual rotations of the encoding bases in the aircraft and on the ground. This was complicated by the moving pointing mirrors in the FELT2 which gave rise to varying circular polarization components, too. A third challenge was the integration of the QKD hardware itself as the host FSO system was never intended to accommodate additional optics.

The quantum key exchange with the aircraft could successfully be accomplished in a flight campaign over a distance of 20 km. The advanced pointing and tracking system enabled a stable sifted key rate of 145 bit/s for the whole 10 min aircraft passage. The observed quantum bit error ratio (QBER) was as low as 4.8 % with a technical QBER (without detector and background noise) of only 1.8 %. This proves for a precise compensation of the polarization rotations in the quantum channel. Finally, by integrating QKD hardware into an existing FSO system, the suitability of QKD as an add-on could be shown.

With the high angular speed of the aircraft the obtained results are representative for links to satellites in low earth orbit (LEO), high-altitude platforms and intercontinental planes, which together will form the basis of a global scale trusted node quantum network for secure communication.

# Zusammenfassung

Für vertrauliche Kommunikation stehen heute eine Vielzahl von extrem sicheren Verschlüsselungsverfahren zur Verfügung. Diese erfordern jedoch stets einen geheimen Schlüssel der Sender und Empfänger bekannt ist. Die einzige Möglichkeit jedoch, einen solchen Schlüssel unbedingt sicher auszutauschen, bietet die Quantenschlüsselverteilung (quantum key distribution, QKD). Darüber hinaus kann ein Schlüssel, der mit Hilfe der QKD erzeugt wurde, auf seine Integrität untersucht und, falls die Übertragung abgehört wurde, ganz oder teilweise verworfen werden.

Die Reichweite von QKD-Systemen ist jedoch durch die Kanalabschwächung und das Detektorrauschen auf wenige 100 km begrenzt. An Bord eines Satelliten hingegen, könnten QKD-Systeme global effiziente Verbindungen ermöglichen. Während sowohl klassische optische Satellitenlinks als auch terrestrische freiraumoptische (free-space optical, FSO) QKD über große Distanzen bereits gezeigt wurden, fehlt ein Quantenschlüsselaustausch mit einer schnellen, mobilen Plattform noch. Die vorgelegte Arbeit schließt diese Lücke mit einer ersten experimentellen Demonstration einer BB84 QKD-Übertragung von einem Flugzeug bei einer Geschwindigkeit von 290 km/h zum Boden.

Das Experiment konnte durch eine Erweiterung des Systems zur klassischen FSO-Kommunikation des Deutschen Zentrums für Luft und Raumfahrt (DLR) mit Hardware zur Quantenkryptographie realisiert werden. Dazu wurde ein Sender für polarisationskodierte BB84 QKD mit abgeschwächten Laserpulsen (Wellenlänge 850 nm) entwickelt und in das „free-space experimental laser terminal 2" (FELT2) an Bord des Flugzeugs (Dornier 228) integriert. Ein passender QKD-Empfänger wurde an der optischen Bodenstation montiert.

Eine erste Vorraussetzung dieser Demonstration war, eine hinreichende Kopplung der Teleskope zu garantieren. Dazu war eine Verbesserung der Zielvorrichtungen nötig, da die Sendeleistung in der QKD nicht angehoben werden kann um hohe Kanalabschwächung auszugleichen. Weiter erforderte die Polarisationskodierung eine präzise Kompensation der gegenseitigen Verdrehung der Kodierbasen im Flugzeug und am Boden. Dies wurde durch die sich bewegenden Zielspiegel des FELT2 erschwert, durch die auch zirkulare Polarisationskomponenten auftraten. Eine dritte Herausforderung war die Integration der QKD-Komponenten selbst, da das FSO-System des DLR nie für zusätzliche Optik vorgesehen war.

Der Quantenschlüsselaustausch mit dem Flugzeug konnte über eine Distanz von 20 km in einer Flugkampagne erfolgreich durchgeführt werden. Die präzise Zielsteuerung ermöglichte dabei eine stabile Schlüsselrate (gesiftet) von 145 bit/s während eines ganzen 10-minütigen Vorbeiflugs. Dabei betrug die Quantenbitfehlerrate (QBER) lediglich 4.8 %. Die technische QBER (ohne Detektor- und Hintergrundrauschen) von 1.8 % zeigt die präzise Kompensation der Polarisationsrotationen im Quantenkanal. Schließlich unterstreicht die hier erfolgte Integration die Eignung von QKD zur Erweiterung bestehender FSO-Systeme.

Die Resultate dieses Experiments sind, nicht zuletzt auf Grund der hohen Winkelgeschwindigkeit des Flugzeugs, repräsentativ für Verbindungen zu Satelliten, Höhenplattformen und Flugzeugen auf interkontinentalen Strecken, die zusammen die Basis eines globalen Quanten-Netzwerks zur sicherer Kommunikation bilden werden.

# Contents


**1 Introduction** **1**

**2 Quantum Key Distribution** **7**
2.1 BB84 Protocol . . . . . 8
2.2 Classical Post-processing . . . . . 8
2.2.1 Error Correction . . . . . 9
2.2.2 Privacy Amplification . . . . . 9
2.2.3 Authentication . . . . . 10
2.2.4 Realistic Devices . . . . . 10

**3 Experiment Setup** **13**
3.1 DLR Host System Hardware . . . . . 15
3.1.1 Flight Terminal . . . . . 15
3.1.2 Optical Ground Station . . . . . 16
3.1.3 Additional Radio Links . . . . . 18
3.2 Pointing and Tracking . . . . . 18
3.2.1 Fine Pointing . . . . . 18
3.2.2 Beacon and QKD Beam Coalignment . . . . . 21
3.3 QKD Transmitter – Alice Module . . . . . 22
3.3.1 Alice Module Electronics . . . . . 23
3.3.2 Alice Module Optics . . . . . 27
3.3.3 Pulse Intensity Calibration . . . . . 34
3.3.4 Module Integration . . . . . 36
3.3.5 Airworthiness Certification . . . . . 38
3.4 QKD Receiver – Bob Module . . . . . 38
3.5 Polarization Management . . . . . 40
3.5.1 Polarization Rotations Flight Terminal . . . . . 42
3.5.2 Spatial Polarization Rotations . . . . . 42
3.5.3 Polarization Rotations OGS . . . . . 44
3.5.4 Compensation Model and Polarization Controller . . . . . 44
3.6 Timestamping Electronics . . . . . 46
3.7 Software . . . . . 46

3.7.1 Alice Control . . . 46
3.7.2 Online Filtering and Sifting . . . 48

**4 Field Tests and Flight Campaign 51**
4.1 Ground to Ground Testing . . . 51
4.2 Calibration of Coalignment and Beam Divergence . . . 53
4.2.1 Scheme for Online Pointing Error Compensation . . . 54
4.2.2 Measurement of QKD Beam Divergence . . . 54
4.3 Experimental Flights . . . 55
4.3.1 Atmospheric conditions . . . 56
4.3.2 Spectral Filtering . . . 56
4.3.3 Flight Track . . . 59
4.3.4 In Flight Pointing Optimization . . . 60
4.3.5 Key Exchange . . . 60

**5 Results and Analysis 63**
5.1 Raw Event Rates and Signal Recovery . . . 63
5.1.1 Transmitter – Receiver Synchronization . . . 64
5.1.2 Diode Delay Compensation . . . 65
5.1.3 Temporal Signal Statistics and Filtering . . . 65
5.2 Transmission Parameters . . . 67
5.2.1 Channel Attenuation . . . 67
5.2.2 Sifted Key Rate and QBER . . . 69
5.2.3 Pointing Stability . . . 74
5.2.4 Polarization Compensation . . . 74
5.3 Secure Key Rate after Privacy Amplification . . . 76
5.3.1 Weak Coherent Pulses and Decoy States . . . 76
5.3.2 Secure Key Rate Evaluation . . . 79
5.4 Discussion . . . 81
5.4.1 QKD Transmitter and Receiver . . . 83
5.4.2 Classical Subsystem . . . 85
5.4.3 Secure Key Rate . . . 86

**6 Summary and Outlook 89**

**References 95**

**Abbreviations 105**

# Chapter 1

# Introduction

Cryptography has come a long way from first transposition ciphers , which, almost 4000 years ago, were produced by exchanging letters according to a fixed table only. Today, modern block ciphers and even asymmetric private/public key schemes secure an immense amount of global communication. The motivation, however, did not change over time. Now and then, people want or have to exchange information in a confidential and secure way. They want to make sure that their opponents – known or unknown – do not find out about the content of their communication and, equally important, that the message is authentic, comprising the authenticity of its sender/receiver as well as its content.

Two weaknesses, however, are common to all conventional schemes, from ancient times until now: First, for every secret communication, the sender and the receiver, traditionally called Alice and Bob, have to find a compromise: Depending on their skills and available technology, they choose a cryptographic protocol with acceptable effort. In doing so, they will also take into consideration the potential risks of the information becoming public, and the assumed motivation, skills and technical possibilities of their adversary. Obviously, false estimations about the means of an opponent will lead to insufficient security measures and, in fact, all conventional cryptographic schemes crucially rely on assumptions about the technological and financial situation of the adversary and on the mathematical complexity of the algorithm itself. One exception to this argument is an encryption scheme called one-time pad which was shown to be information theoretically secure, as long as a key equal in length with the message is used [1]. This excessive key requirement, however, is also the reason why the one-time pad is only rarely used.

This is connected to the second weakness of conventional cryptographic schemes which is the secure exchange of a *secret key* between Alice and Bob: Cryptography based on publicly known and well tested encryption algorithms combined with a hard to guess key has proven to enable highest security measures – proprietary techniques partly relying on security by obscurity often suffered from design flaws and could be broken within short time. The high security level of modern encryption

algorithms (e.g. advanced encryption standard (AES) [2, 3]), however, makes the key exchange the weakest link in the security chain. Moreover, once Alice and Bob have established a symmetric key, there is no way to determine its integrity. This is largely independent of the method they chose: If they sent the key written on paper or stored on a hard drive, they have to trust their couriers and storage facilities to efficiently prevent the fabrication of copies by an illegitimate party. In case they used a mathematical technique, for example the Diffie-Hellman key exchange [4] or the public key method invented by Rivest, Shamir and Adleman (RSA, [5]), to generate a shared key using an otherwise public channel, then again they have to trust the assumed computational complexity of the algorithm. This mathematical approach is usually implemented in today's encrypted communication over the Internet and the security of the algorithms is based on the problem of factoring large numbers which as of today can not be accomplished in polynomial time. The assumed hardness of this and other mathematical problems exploited in conventional cryptography, however, could not be proven.

Quantum key distribution (QKD) [6–9] offers a solution to the key distribution problem and thereby enables the application of the information theoretically secure one time pad. The absolute security of QKD could be proven for a variety of protocols and the laws of quantum mechanics are the only restriction an adversary is assumed to be liable to. This is in sharp contrast to the assumptions and estimations made in case of conventional encryption algorithms. Additionally, using QKD, the amount of information an eavesdropper may have gained in the key distribution process can be quantified by measurable parameters – first and foremost the observed transmission noise. This enables an evaluation of the integrity of a generated key before it is used to actually encrypt sensitive data. It has to be noted, however, that there remains the often implicit assumption that a system, while theoretically feasible, can actually be implemented with reasonable effort as described by the protocol.

Unfortunately, QKD is not immediately compatible with today's communication technology as it requires a *quantum* channel between Alice and Bob. Such a channel preserves the physical states of the quantum entities, the qubits, usually realized with photons, sent to generate a secret key.

With a quantum channel over a distance of 30 cm the first demonstration of QKD [7, 10] in 1989 became the starting point of a rapid development of this new technology enabling successively longer distances and secure key rates. Soon, also optical fibers were found to provide efficient quantum channels. Yet, noise, especially from the detectors, and the increasing attenuation in the quantum channel limit the maximum distance for a successful quantum key generation in either case – as a matter of fact, the qubits cannot be amplified on their way. As of today, in fiber QKD, there are experiments using superconducting single photon detectors to demonstrate distances up to 250 km [11–15]. In order to exchange secret keys over even longer distances or to enable QKD networks as demonstrated in [16, 17], trusted nodes can connect two or more point-to-point links. The only way to overcome this

trusted node topology and thereby the need for secure switch sites, however, is a future quantum repeater which is currently under investigation [18–20].

Experiments using a free-space quantum channel established between two telescopes have similarly pushed the limits in distance and secure key rate. After a first real live demonstration on the 23 km distance between two mountains [21] and first daylight key exchanges on 1.6km [22] and 10 km distance [23], soon the direct line of sight between the two Canary islands Teneriffe and La Palma was discovered as an ideal testbed. There, on a distance of 144 km, QKD has been performed [24–26] as well as entanglement distribution [27] and even quantum teleportation [28]. These techniques, recently also demonstrated on a 97 km free-space channel [29, 30], enable the generation of a shared secret key, too.

The grand goal of long distance free-space QKD is, of course, a satellite based system acting as a trusted node, which would allow for a key exchange on a global scale. Enabling QKD on horizontal distances beyond the effective thickness of the atmosphere, however, is usually considered to be even harder concerning fluctuations compared to a satellite-to-ground link mainly propagating in vacuum. The results of earth bound experiments thus often are quoted to evaluate the feasibility of QKD with satellites [31, 32] and QKD system components for the application in space are proposed and tested [33].

Yet, all QKD experiments so far were performed with stationary transmitters and receivers only. Clearly, for satellite based qkd this can only be partly representative. In classical free-space communications, however, the situation is different: High bandwidth data links between an aircraft and a ground station have been demonstrated [34, 35] as well as links to and from satellites in low earth orbit (LEO) [36–38]. Additionally inter satellite links, both LEO–LEO and inter orbit to satellites in a geosynchronous orbit (GEO), are already developed [39] to provide high speed data backbones.

In this work [40, 41], both these worlds – long distance quantum communication and free-space optical data links to moving platforms – shall be combined in a first experiment proving the feasibility of QKD from an airplane to an optical ground station. The demonstration is enabled by the recent advances in both fields and intends to constitute a major milestone on the way to QKD applications in space. The aircraft as an experimental platform further allows for an evaluation of the possibilities and requirements of quantum key distribution with different kinds of air vehicles. Especially unmanned aerial vehicles (UAVs) and balloons, which are proposed to enable temporary communication networks for short time events or in urban and disaster areas, could be supplemented by QKD capabilities to provide secure key exchange in addition to data communication. The experiment aims to facilitate the integration of QKD on all current and future communication devices operating on a direct line of sight and thus is projected as an add-on to an existing optical communication system.

Supplementing an existing communication platform gives rise to several challenges as the host system, the optical terminal in the aircraft and the ground station telescope, was initially not intended to support add-ons. Moreover, the classical link has to remain operational even with the QKD hardware installed. As a consequence, modifications to the classical components were confined to be least invasive and compromises had to be adopted in order to meet the space and power limitations imposed by the host system. Additionally, the airworthiness certification process demanded for the transmitter hardware to remain unchanged already about nine months before the flight campaign and also imposed other constraints concerning laser safety and electrical connections.

Another major challenge are the more accurate pointing requirements to be met compared to classical free-space communication. While a classical system can, to some extent, compensate power losses with increased transmitter intensity, this is not true for quantum communications. Additionally, in contrast to the classical case, the achievable secure key rates in QKD are directly connected to the channel attenuation. The QKD beam thus will be collimated much narrower then the classical communication laser in order to collect as much signal as possible at the receiver's aperture, which in turn requires an extremely accurate pointing.

As the polarization of photons is well preserved in the atmosphere even on long distances [42], this degree of freedom is most often used in free-space quantum communications to encode information. In a mobile scenario, however, this gives rise to a third difficulty of the projected experiment: The polarized photons prepared at the transmitter travel through a system of lenses and mirrors at either end of the optical link. When they reach the receiver, they appear rotated depending on the relative orientations of the transmitter and receiver and the according pointing mirror positions. In addition to these mere spatial rotations, varying birefringence of optical components when used at different angles of incidence give rise to circular polarizations, too. In order to still obtain meaningful results from polarization measurements at the receiver, all these rotations have to be compensated somewhere in the optical channel. The receiver's polarization reference frame has to become equivalent to the reference used for preparation. Therefore, in this work, especially because of the unpredictable orientation of the aircraft in the presence of wind and turbulence, a polarization compensation scheme has to be developed and implemented. It has to be noted, that for future satellite QKD, this task is investigated theoretically [43], yet, the satellites ephemeris provides very precise a priori trajectories as a basis for the calculation which are not available in the aircraft scenario.

In this thesis, after a short introduction to the QKD basics and the BB84 [7] protocol, chapter 3 describes the experiment hardware consisting of the classical host system and the QKD add-ons and modifications. The next chapter is dedicated

to the ground to ground tests and the actual flight campaign while experimental results are analyzed and discussed in chapter 5 followed by a summary and outlook.

# Chapter 2

# Quantum Key Distribution

The properties of single quanta governed by the laws of quantum mechanics open up new possibilities of information processing and communication. The transition from classical bits '0' and '1' to qubits, quantum mechanical two level systems, enables also the storage of superpositions of the two states.

QKD [6, 8, 9] is the most mature technology in quantum information and also the first one applied commercially [44]. In QKD, qubits are used to encode and exchange information over a quantum channel to establish a shared secret in a provably secure way between two parties traditionally called Alice and Bob. This is enabled by the quantum mechanically no-cloning theorem and the fact that any measurement on a quantum entity necessarily makes a possible superposition state collapse to the measurement outcome. Thus, in contrast to conventional key agreement schemes, QKD does not rely on any assumptions on the power and capabilities of a potential attacker.

Another real advantage QKD offers is its ability to provide an upper bound on the information an eavesdropper may have gained as a function of the observed transmission noise, the quantum bit error ratio (QBER). This makes it possible to check an exchanged key for its integrity prior to its application for the encryption of sensitive data. Conversely, in the classical world, one cannot tell whether a key is secret, was partly compromised or even copied completely. Moreover, if the transmitted key turns out to be only partly secure, it is possible to extract a shorter, yet secure key using classical post processing.

Necessary prerequisites for QKD are a preferably quantum source of randomness for Alice and Bob, a classical communication channel between them and some small amount of initially shared secret for authentication. The latter is required to rule out any man-in-the-middle attack from the beginning. Later in the transmission, part of the generated key has to be reinvested for this purpose. The term quantum key growing is sometimes used to stress the necessity for a pre-shared secret and the fact that QKD is the only way to securely increase the amount of shared secrecy remotely.

Further methods of quantum information include for example quantum teleportation [45, 46], quantum simulation [47] and most prominently quantum computation [48, 49], i. e., the development of a quantum computer, which was shown to enable a significant speedup for certain classical problems and thereby threatens all public key cryptography schemes. For example, with the help of Shor's algorithm [50], numbers can be factorized in sub-exponential time. This has already been demonstrated experimentally for the number 15 [51, 52].

## 2.1 BB84 Protocol

The BB84 protocol for quantum key exchange proposed by Charles Bennett and Gilles Brassard was the first to be invented and also the first to be implemented [10]. Its intuitive approach makes it still the most comprehensible and distinct method to generate a shared secret key by sending single quanta, i.e., qubits. While these can be realized with a variety of different quantum entities and according two level subspaces, the relevant implementation here are photons (with their state of polarization), which are sent through a free-space quantum channel established between Alice and Bob.

For the key exchange, Alice and Bob agree on an encoding of the classical bits '0' and '1' in two orthogonal, and maximally conjugate bases called "rectilinear" (+) and "diagonal" (×) respectively. The first is defined by the horizontal and vertical polarization ($|H\rangle, |V\rangle$), the latter by the polarizations along $\pm 45°$ relative to $|H\rangle$ ($|+45\rangle, |-45\rangle$). This ensures that a qubit prepared in one basis does not reveal any information about the encoded bit when measured in the other basis.

The protocol then works as follows: Using two bit of randomness, Alice chooses a bit value and one of the two bases, × or +. She encodes her qubit accordingly and sends it through the quantum channel to Bob. He, in the same way, chooses randomly a basis for measurement and records its outcome '0' or '1'. They repeat these steps until they have acquired the desired amount of data before they proceed with the entirely classical post processing: Over the classical channel, Alice announces which basis she used for every qubit she sent. Bob replies with a list of time slots in which both have chosen (by chance) the same basis and received a signal at all. Only these qubits can lead to meaningful results and will form the so called "sifted key". The remaining signals are discarded as in case of differing bases, Bob's measurement results are completely random.

## 2.2 Classical Post-processing of the Sifted Key

While the sifted keys of Alice and Bob should in principle be identical, noise will always cause a certain amount of errors. While these errors normally result from detector noise, stray light and small misalignments, it is always assumed that an

eavesdropper is responsible for the complete observed QBER and has gained the according amount of information. Thus, the sifted key cannot directly be used to confidentially encrypt a secret message. It is the task of the classical post-processing to distill a *symmetric* and *secret* key from the sifted key obtained in the quantum transmission.

### 2.2.1 Error Correction

The process of error correction, also called "reconciliation", eliminates differing bits from Alice's and Bob's sifted keys to establish actual symmetric keys. However, this can not be performed without disclosing some information about the sifted key. This has to be compensated later in privacy amplification and thus reduces the key length. The minimum amount of data that has to be sacrificed depends on the error rate $e$ and is given by the binary entropy function $H_2(e)$ [53]

$$H_2(e) = -e \log_2(e) - (1-e) \log_2(1-e) \ . \tag{2.1}$$

However, this is only a theoretical minimum and actual algorithms are designed to perform as close to this so called Shannon limit as possible. For a long time, CASCADE [54] was used in reconciliation being specifically invented for quantum cryptography. It is designed to disclose as few bits as possible. Recently, however, protocols often implement low density parity check (LDPC) codes [55, 56]. They require a good a priori estimation of the error rate, but can then perform extremely efficient [57].

Another subtlety remains which again costs valuable key bits: All efficient error correction protocols have a small yet finite probability to fail, in which case Alice's and Bob's keys still differ in one or more bits even after error correction. After the privacy amplification step to follow, this would result in completely different keys and thus render the message unreadable for the recipient. Even more important, a key containing errors might not be covered by security proofs and the cipher produced with such a key might be vulnerable [58]. Thus, verification of the successful error correction is an important step of the QKD protocol.

### 2.2.2 Privacy Amplification

For this stage of the classical post processing a short identical key, shared between Alice and Bob, is required. Yet, due to the non vanishing QBER, they have to assume that a possible eavesdropper already has some knowledge about the string. The task of privacy amplification [59, 60] is to distill a secret key reducing the information of an adversary to an arbitrarily small amount.

The information that may have leaked to en eavesdropper is upper bounded again by the binary entropy function $H_2(e)$. This means that in total, together with

the bits disclosed in the error correction process, a secure fraction

$$R = 1 - 2H_2(e) \tag{2.2}$$

of the sifted key can be distilled to be used as a secret key. Yet, this relation only holds for the ideal protocol with an infinite long sifted key and an optimal error correction algorithm. In the analysis in chapter 5, the necessary variations to equation (2.2) will be described.

If this fraction $R$ is positive, this means, if the amount of leaked information is less then the number of sifted key bits, a secure key can be distilled using two-universal hash functions [61]. A class of functions which when chosen randomly are are on average input independent. They reduce the key length as needed and produce an output string which is maximally dependent on all input bits. As a rule of thumb, a single bit flip at the input string flips half the bits of the hashed output.

### 2.2.3 Authentication

While the communication during post-processing can be done publicly, all messages from Alice to Bob and vice versa have to be authenticated. For a public channel, this means that both the origin and the content of every message have to be verified.

The authenticity of the origin ensures the identity of the respective sender and prevents that an illegitimate party can secretly inject messages. For this purpose, an initially shared secret is inevitable. For absolute security, this affords that Alice and Bob have at least met once before.

The authenticity of the content guarantees that the message was not altered on its way and thus is still identical to the transmitted version.

Both these tasks can be accomplished information theoretically secure by authentication protocols such as [62]. They need, however, a non negligible amount of key (in the beginning from the pre-shared secret) to agree on a secret, two-universal hash function [61] and to encrypt the hash tag, i.e., the result of the hash function when applied to the message.

### 2.2.4 Realistic Devices

Originally, idealistic implementations were considered by protocol security proofs [63, 64]. The theoretic models for QKD systems originally did not incorporate any imperfections or experimental necessities of real devices like noise, multi photon signals, asymmetries in the detector channels, finite data sets, etc. However, there are constantly new proofs developed which incorporate many characteristics of real world devices and show up ways to handle them in the privacy amplification step [9, 65–69].

Still, imperfect or even controllable detectors at Bob's site or so called "side channels" like insufficient quality of the Alice state preparation [70] are often a major

vulnerability and some of them could even been effectively exploited experimentally, which is referred to as “quantum hacking” [71–75]. These demonstrations, however, never do nor can they target the protocols but always the specific hardware. The vulnerabilities used can in principle be eliminated as the underlying theory is proven to be secure. Yet, an “unconditional secure” key exchange still remains to be demonstrated [76] and also throughout this work, there will be details pointed out that spoil the security of the key exchange in this demonstration.

# Chapter 3

# Experiment Setup

The realization of QKD from an airplane to a ground station naturally breaks down into two branches: First, a classical system has to establish and maintain a stable, optical link between the communication partners. Second, a QKD transmitter can use this link as a quantum channel to exchange qubits with a receiver on the other side. Therefore, it is obvious to approach this experiment as an integration of quantum hardware with a system for classical airborne laser communication.

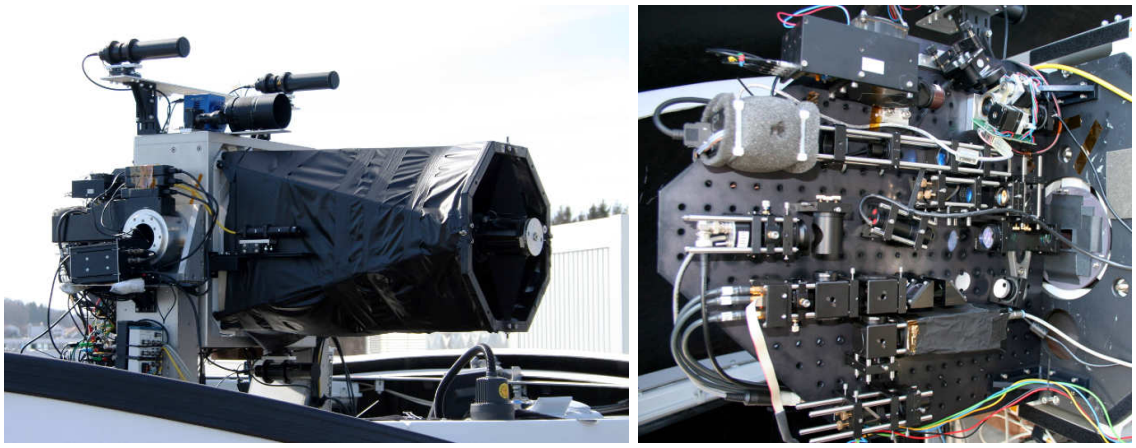
This work [40, 41], thus, was enabled by a collaboration with the German Aerospace Center (DLR) in Oberpfaffenhofen, Germany. The free-space experimental laser terminal 2 (FELT2, fig. 3.1) mounted in a Dornier 228 turboprop short take-off and landing type aircraft and the optical ground station (OGS, fig. 3.2) of the DLR's Institute of Communications and Navigation constitute an ideal classical host system [34, 77]. Initially built for high speed data communications in large area survey scenarios, it is able to provide Fast Ethernet data rates over a stable optical channel for distances of up to 120 km. Moreover, the OGS located in Oberpfaffenhofen near Munich, Germany already demonstrated laser communications with satellites in LEO [36] and a stratospheric balloon [78].

To make the DLR system capable of exchanging quantum keys, a transmitter for polarization encoded, faint pulse QKD according to the BB84 protocol [7] at a wavelength of 850 nm was developed and integrated.

The chosen polarization encoding was already demonstrated to be robust also under non-lab conditions [21, 23, 25] – especially when compared with techniques requiring stable interferometers for state generation and analysis. Moreover, for polarization encoding it is not necessary to couple the received light into single mode fiber, which would certainly introduce severe losses. However, in this mobile scenario, polarization encoding necessitates a scheme for compensation of the constantly changing effective birefringence of the optical channel. This results from the varying relative orientation of transmitter and receiver and especially the pointing mirrors. The polarization compensation will be discussed in section 3.5. Depolarization and consequently noise due to the atmospheric propagation of the

(a) (b)

**Figure 3.1:** The free-space experimental laser terminal 2 (FELT2) mounted in the aircraft. **a**: Dornier Do 228 turboprop aircraft used to carry out this experiment. The inset magnifies the optical dome underneath the aircraft fuselage housing the coarse pointing assembly (see fig. 3.4). **b**: The terminal inside the aircraft cabin covered by the white safety hood. In the foreground, the rack with power supplies and laptops is visible.



(a) (b)

**Figure 3.2:** The optical ground station (OGS) Oberpfaffenhofen. **a**: The telescope with the framework covered to reduce background noise from stray light. **b**: The optical breadboard attached to the back of the main mirror. The board is moving with the telescope. It was covered in black tissue during the experiment.

photons is not to be expected [42]. Dielectric coatings of the optical elements and especially the dicroic mirrors, however, are a source of noise due to small polarization dependent properties.

The qubits in this experiment are mimicked by Poissonian pulses with a mean photon number per pulse of 0.5 and special care was taken to calibrate and control this intensity. Nevertheless, there is a non negligible fraction of pulses containing more then one photon. This requires a decoy state protocol extension [79–81] necessary to become robust against attacks on the poissonian photon number of the faint pulses [82]. In this first demonstration, however, this was not implemented. Yet, all parameters necessary to judge the QKD system's performance assuming an additional decoy extension are accessible and thus the achievable secure key rate can be calculated for the decoy state method, too.

At the time of this experiment, data communication was possible unidirectionally only. Therefore, the optical link could unfortunately not be used as the classical channel for sifting and post processing, as this demands for bidirectional operation. Current development of the system, however, aims to implement bidirectional links, too. Nevertheless, the classical data link was usable even with the QKD extension implemented in the DLR system, and could be applied to synchronize the QKD hardware aboard the airplane and at the ground.

## 3.1 DLR Host System Hardware

Before add-ons and modifications for this experiment are described in detail, in this section, a brief overview of the host system is given. For clarity, figure 3.3 shows a block diagram of the hardware and also indicates, the QKD components and interfaces.

### 3.1.1 Flight Terminal

The airborne terminal houses the optical breadboard mounted shock insulated to the seat rails of the cabin above a tunnel through the aircraft fuselage. On the outside, a motorized Kepler telescope (coudé path, see fig. 3.4) is mounted in an optical dome. The breadbord contains everything that is needed for the operation of the optical link. Namely optics, detectors and an inertial measurement unit (IMU) for pointing and tracking, laser diodes and a fiber amplifier for data transmission and further electronics like an embedded computer, ultra high frequency (UHF) modem and a variety of sensors. In flight, the system has to be covered and is then controlled via Ethernet connections using a laptop. The data signal to modulate the laser is interfaced differentially with logic voltage levels according to low-voltage positive emitter-coupled logic (LVPECL). The communication laser simultaneously serves as a beacon for the ground station to track on. The setup of the flight terminal as

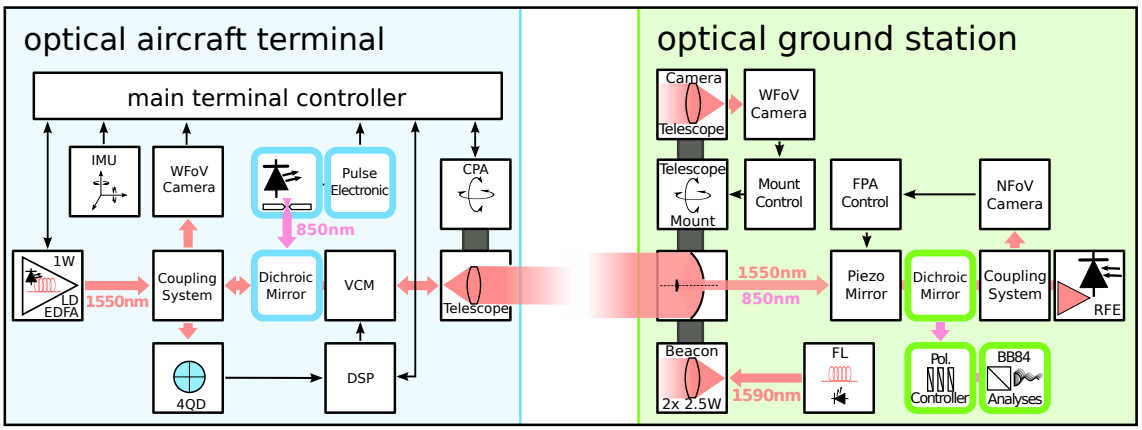



**Figure 3.3:** Block diagram of the DLR host system with the integration of the QKD hardware indicated (colored boxes). Laser diode and erbium doped fiber amplifier (LD EDFA), inertial measurement unit (IMU), digital signal processor (DSP), wide field of view (WFoV) camera, narrow field of view (NFoV) camera, four quadrant diode (4QD), coarse pointing assembly (CPA), voice coil mirror (VCM), fiber laser (FL), and receiver front-end (RFE).

modified for this experiment will be described in section 3.3. Figures 3.5 and 3.9 give an overview of the terminal optics and control system.

### 3.1.2 Optical Ground Station

The ground station is located on the rooftop of a DLR building next to the special airport Oberpfaffenhofen. The 40 cm Cassegrain telescope is azimuth-elevation mounted in a clam shell type housing (see fig. 3.2). This allows in principle for an unrestricted observation in the full hemisphere[1]. Behind the main mirror an optical breadboard moving together with the telescope is attached. All optical components for communication, tracking and beam analysis are mounted there. Two fiber collimators are attached right and left of the main mirror, emitting the beacon laser beams, the airplane can track on. The diversity gained from two beacons, which cannot be resolved by the FELT2 optics, improves the pointing stability in the presence of scintillations. A more detailed discussion of the OGS as tailored for this experiment is presented in section 3.4. An overview of the ground station is given in figure 3.6 hardware.

[1] In the north, the view was obscured below a certain height due to the buildings superstructure. This was, however, not hindering the experiment, as the airspace regulations required the aircraft to operate south of the OGS anyway.

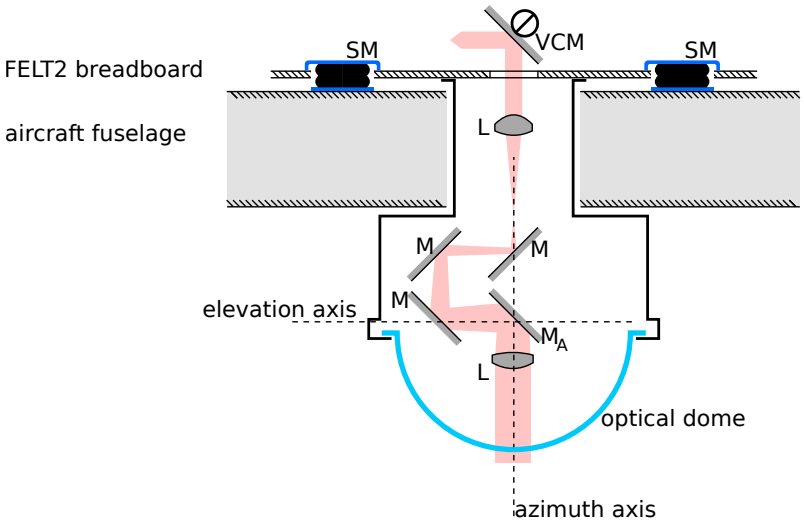



**Figure 3.4:** Section view of the tunnel and the optical dome illustrating the shock insulating mounting (SM) of the optical breadboard and the coudé beam path between the lenses of the Kepler telescope: For azimuthal rotation all mirrors ($M_{(A)}$) rotate together around the vertical axis. The elevation angle, limited to a maximum of 5° above the horizon, is defined by the angular position of the mirror $M_A$ around the horizontal axis. Fine and fast corrections to the pointing are enabled by the voice coil mirror (VCM). A specialty of the coudé beam path is the rotation of the field of view with the azimuth angle. This will also be apparent in the polarization compensation later. The two lenses (L) act as a factor 2 beam expander for the terminal beacon at $\lambda = 1550\,\mathrm{nm}$.

### 3.1.3 Additional Radio Links

Apart from the optical link, the DLR communication system is equipped with an UHF modem that allows for bidirectional data communication at a rate of 9600 bit/s. This link is realized with a small helix antenna underneath the aircraft fuselage and a tracking Yagi-antenna on the ground. The speed is sufficient to transmit the aircraft GPS position, orientation and heading to the ground station with an update rate of 5 Hz. Communication and coordination of the experiment between the ground station operators and the crew aboard the aircraft was mainly accomplished via satellite phones.

## 3.2 Pointing and Tracking

Establishing and maintaining a stable and efficient optical channel was the main task of the classical host system. In order to acquire a link, at first, the OGS receives the aircraft GPS position via the UHF link and aims its telescope at the according direction. Thereby, the aircraft is illuminated with the beacon lasers attached to the OGS telescope.

At the same time, the FELT2 calculates the direction to the OGS with the help of the on-board inertial measurement unit (IMU) and the CPA performs a scan around this direction. To gain some robustness against other light sources in the vicinity of the OGS, the beacon lasers are modulated with 2 kHz. Once the OGS beacon is in the field of view (FoV) of the FELT2 InGaAs-camera (FoV 48 mrad), coarse tracking begins to keep the spot in the center using the DC brush-less motors that drive the coudé mechanics.

Now, the FELT2 beacon (divergence 3 mrad), which is also modulated to transmit the payload data, illuminates the OGS. Thereby, the CPA InGaAs-camera mounted to the OGS telescope frame with its FoV of 12.8 mrad can track the aircraft.

This pointing and tracking setup provides a mean pointing error of 500 µrad. For classical communication from the aircraft to the ground, this prove to be sufficient and the demonstration of Ethernet speeds over a distance of 120 km was accomplished in this configuration [34].

### 3.2.1 Fine Pointing

In classical communications, the transmitter power can be adjusted in a wide range to overcome the channel attenuation. Moreover, the available power allows for wide beam divergences, which produce a large footprint on the ground. This leads to less critical pointing requirements while the necessary signal power at the receiver can still be maintained. When performing a quantum key exchange, however, this is not possible as one has to adhere to the low mean intensities of less than one photon per pulse: Only the single photon pulses can be used for key generation and their

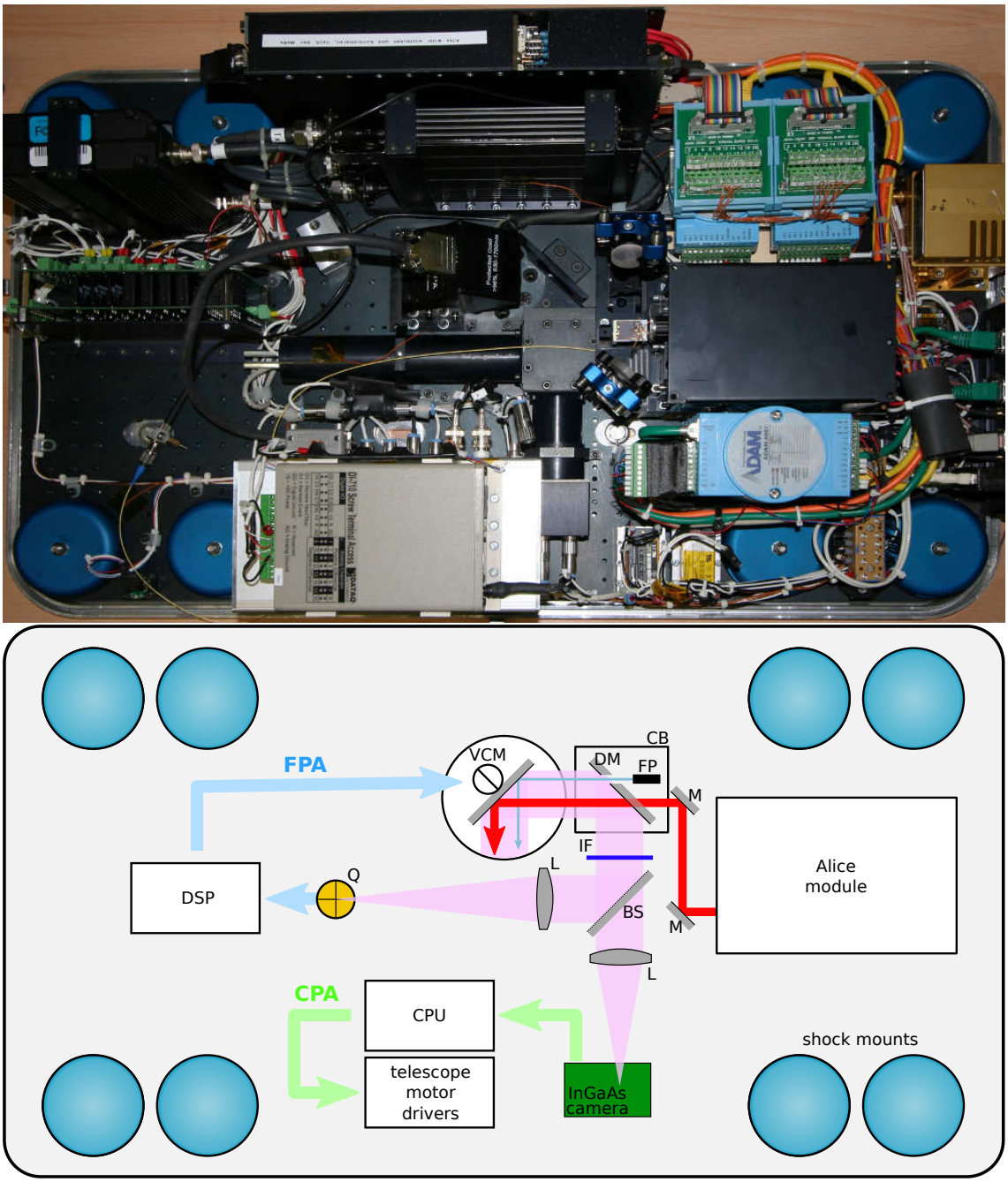



**Figure 3.5:** Photo and simplified scheme of the FELT2 terminal setup. the voice coil mirror (VCM) reflects the light to and from the motorized telescope underneath the aircraft (fig. 3.4) to the coupling block (CB, fig. 3.16). There, a dichroic mirror (DM) overlaps the incoming beacon with the terminal beacon, which passes through a 4 mm hole and the QKD beam from the Alice module (fig. 3.9). The incoming light is reflected at the CB, spectrally filtered (IF) and, after a beam splitter (BS), focused (L) onto a quadrant diode (Q) and an InGaAs-camera respectively. These are part of the two control loops for pointing and tracking: 1. (green) The coarse pointing assembly (CPA) consisting of the InGaAs-camera, the terminal controller (CPU) and the motorized telescope in the optical dome. 2. (blue) The fine pointing assembly (FPA) consisting of the quadrant diode, a digital signal processor (DSP) and the VCM.

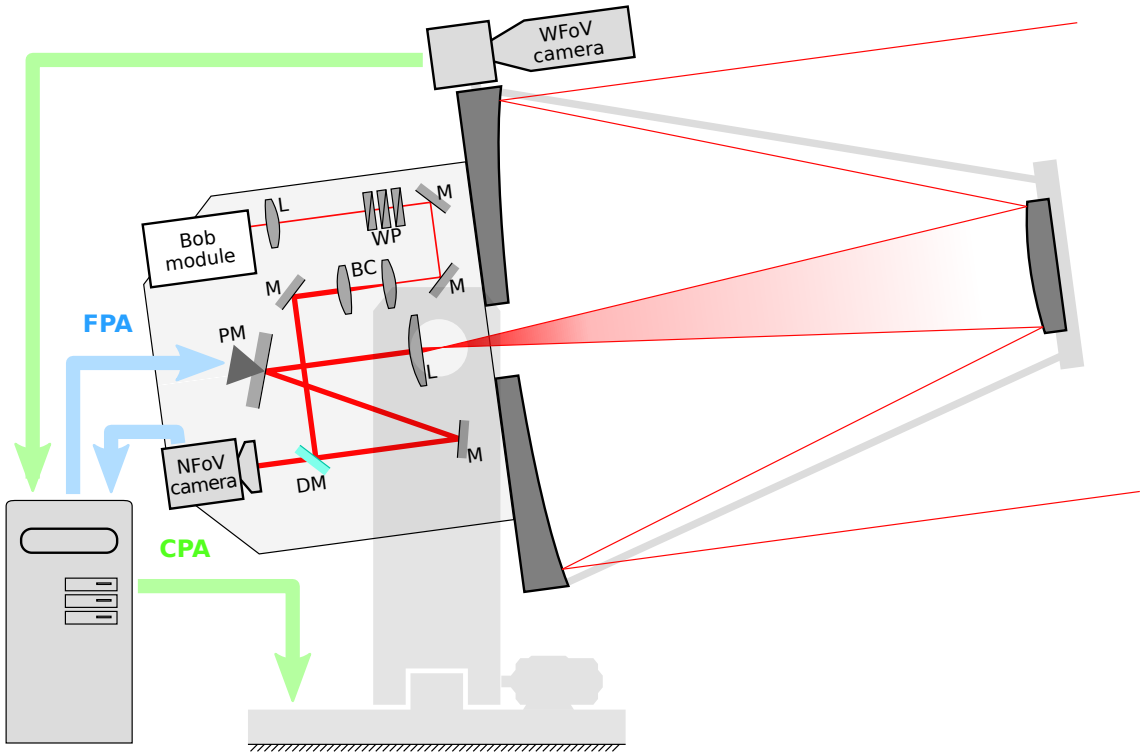



**Figure 3.6:** Simplified scheme of the OGS telescope and optics. After a collimation lens (L) and the piezo actuated mirror (PM), the incoming light is spectrally divided at the dichroic mirror (DM). The 1550 nm light from the FELT2 beacon is analyzed by a narrow field of view (NFoV) InGaAs-camera the 850 nm QKD beam is compressed (BC), polarization corrected by the set of motorized wave plates (WP) and focused into the bob module (fig. 3.17).

fraction in all pulses would rapidly vanish if the pulse intensity was increased (see § 5.3.1).

It is, thus, crucial that the link efficiency is maximized by a small beam divergence and a stable pointing. Therefore, an additional FPA was developed and installed by the DLR both in the FELT2 and the OGS [83]. The complete setup visualizing the fine and coarse pointing control loops of the FELT2 is shown in figure 3.5 and the configuration at the OGS is depicted in figure 3.6, respectively.

For the FELT2 the FPA [84] consists of a ⌀1 mm quadrant diode[2], a DSP and a voice coil actuated mirror. In analogy to the coils in loudspeakers, the term "voice coil" describes an electric coil within a static magnetic field which tilts the mirror depending on the electric current running through the coil.

At the ground station, the FPA is realized with an InGaAs-camera (FoV 960 µrad), a piezo actuated mirror and a computer system to close the control loop. In order to increase the bandwidth of this regulation, only a small window is actually read from the camera sensor at a frame rate of 400 Hz and analyzed to find the pointing deviation. The effective focal length of 4 m and the 30 µm pixel pitch of this camera result in an angular resolution of 7.5 µrad/pixel.

For both systems – the flight terminal and the ground station counterpart – it has to be stressed, that these fine and coarse control loops only operate locally. This means, they only correct for errors of the receiving direction, i.e., the "visual ray". Here, the term "local" refers to the fact that both, the position sensitive device acquiring the error signal and the respective steering mirror to compensate these errors are at the same end of the communication link. The transmitted beams are adjusted only once to be parallel to this visual ray on a testbed and there is no control loop for online compensation of any residual misalignment possible.

### 3.2.2 Beacon and QKD Beam Coalignment

The pointing method described above crucially relies on the parallel alignment of the incoming beacon when it hits the center of the quadrant diode or the FPA camera and the outgoing laser beam. In other words, one has to ensure manually that the transmitters of each system actually point into the exact same direction its receivers operate on. The straight forward strategy for calibration is to track a fixed target emitting a beacon laser and adjust the own beacon to hit this target, too. With increasing distance, of course, this adjustment gets more and more precise as angular errors result in increasingly larger displacements.

For the beacon lasers of the FELT2 and the OGS, however, this coalignment is only moderately critical due to their wide divergences: The FELT2 laser can be calibrated on a distance of 50 m where it already produces a beam diameter of 15 cm and the OGS beacons are overlapped with the receiver direction using its coarse tracking

[2]The effective focal length of the optical system focussing on the quadrant diode is 300 mm. This corresponds to a FoV of 3.3 mrad

camera on the wall of a building about 1 km away. Together with the large power range of the respective sources, the wide beam divergence ensures that even with slightly misaligned beacon lasers, the opposite side can still receive a sufficiently strong signal.

Yet, for the QKD beam both these arguments fail: Neither can one afford a wide divergence which leads to signal loss at the receiver aperture nor increase the pulse intensity. Thus, for a successful key exchange, a most accurate coalignment is crucial. Precision kinematic mirror mounts with enhanced stability are therefore used to couple the Alice beam onto the pointing axis and to provide the least susceptibility to vibrations and shocks. Still, the coalignment of the QKD beam emerged to be a major challenge of this experiment as is described later in chapter 4.

## 3.3 The airborne QKD Transmitter – Alice

To keep the QKD add-on as modular as possible, the design intention for the transmitter was a self contained module that could also be integrated into other optical systems or used in QKD only experiments.

In this demonstration, the flight terminal was chosen to host the QKD transmitter, called the Alice module. This decision is based on the available telescope apertures of the flight terminal (30 mm) and on the ground station (40 cm) to achieve maximum coupling. Sending the qubits in this direction is favorable as the strongest fluctuations of the atmosphere are near the ground and then occur at the end of the quantum channel. There, their effect on the beam direction is less severe. Moreover, the collection efficiency of the 3 cm aperture is worse in the reverse scenario or would impose excessive demands on the tracking accuracy.

The flight terminal initially was not intended to host additional hardware. Therefore, spacing for the Alice implementation was rather tight. Additionally, the free-space optical path within the terminal had to be kept short to maximize the mechanical stability of the QKD source relative to the classical optical detectors responsible for pointing and tracking. Consequently, the solution depicted in figure 3.5 is a compromise of these considerations with spacing constraints and the necessity to keep some parts of the classical system removable with the carefully aligned QKD hardware installed: Some screws for the assembly of the terminal in the aircraft are hidden underneath the main coupling block and the voice coil mirror. Yet, in the chosen implementation, the system is sensitive to a bending of the optical breadboard as this affects the classical and the quantum part differently.

For the actual overlapping of the QKD beam with the existing optics, the so called coupling block of the classical system was chosen. This component, at the same time, defines the maximum QKD full beam diameter within the terminal to 7.5 mm and requires an off axis alignment. In section 3.3.4, the coupling of the QKD beam will be explained in more detail.

While shock mounts are used to maximally decouple the optical setup from the aircraft fuselage (visible in fig. 3.4), during taxiing these mounts are frequently driven to their hard stops which results in severe shocks to the optical setup. In flight a significant amount of vibration was to be expected, too, and a detailed analysis reveals the rotating four blade propellers as the main source of mechanical noise at 25.4 Hz and 101.4 Hz (the vibration spectrum is available in [34]). Therefore, a first concern in the design of the QKD transmitter was the mechanical stability even under harsh conditions.

In addition to the QKD operation mode, the Alice module was equipped with the ability to emit a continuous wave (cw) or slowly modulated laser beam with (relative) high intensity (up to $\approx 4\times1.3\,\mathrm{mW}$) in order to facilitate first link acquisitions and the pointing fine tuning in-flight. This could be achieved by mounting the attenuator, which reduces the pulse intensities for QKD operation to the single photon level, on a remote-controlled servo arm (see fig. 3.10). Additionally, a photodiode was placed on this arm and could be brought into the beam path for verification and electronical recalibration of the pulse intensities in flight.

### 3.3.1 Alice Module Electronics

The Alice electronics are grouped in two devices: The voltage generation from the 12 V supply provided by the host system and the actual control board integrated into the Alice module, respectively. The former contains voltage regulators for 5 V and 3.3 V with capacitive and inductive filtering and is separated to reduce the heat input and noise contamination into the main module. Figure 3.7 shows a block diagram of the main board. A micro controller (`ATmega324p`) interfaces between the USB port (`FT232r`) and the field-programmable gate array (FPGA) (`SPARTAN 3e`) and controls all periphery components like the servo arm and the laser driver bias and modulation currents. Additionally, it collects system health data like operating voltages and temperatures of the electronics and the Alice module chassis. Finally, it controls the self calibration for precise QKD pulse intensities.

Unfortunately, the Alice pulse repetition frequency of 10 MHz could not directly be transmitted for synchronization via the optical link due to its bandwidth limitations. Therefore, the 100 MHz signal which clocks the FPGA is fed to the classical system for modulation of the data and beacon laser. In section 5.1.1 the synchronization will be described in more detail.

#### Generation of Short Pulses

The short pulses fed to the laser drivers are produced directly in the FPGA: The main clock signal of 100 MHz is delayed in a so called digital clock manager (DCM) and XOR-ed with the original clock. The pulse width of the resulting signal is basically the DCM delay and can be programmed via the USB connection in slightly

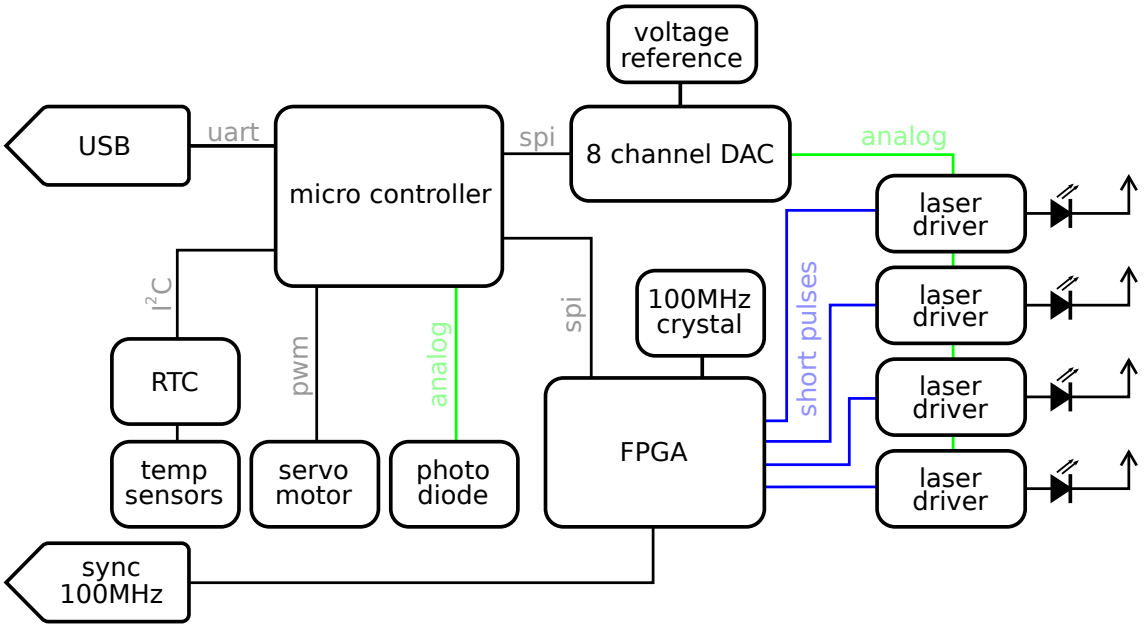



**Figure 3.7:** Block diagram of the Alice module main electronics. The FPGA generates short pulses in a pseudo random pattern of adjustable length to feed the laser drivers. These are programmed individually for a DC bias and additional modulation current with analog values from the 8 channel digital to analog converter (DAC). The main clock is derived from a 100 MHz crystal and forwarded by the FPGA to the host system for synchronization with the ground station. The micro controller ($\mu$C) manages communication with a laptop over USB and handles the temperature sensors, the servo motor, the real time clock (RTC), the DAC and the programming of parameters into the FPGA. Moreover, an internal ADC in the micro processor measures the voltage of the reverse biased photo diode. Peripheral connections: universal asynchronous receiver and transmitter (uart), serial peripheral interface (spi), pulse width modulation (pwm), inter-integrated circuit ($I^2C$).

varying steps of approximately 20 ps length. Still in the FPGA, the short pulses are distributed to four AND-gates realized in look-up tables which control the laser diode to fire and at the same time reduce the repetition rate to 10 MHz. The performance of the FPGA gates, however, limits the minimum pulse width at full amplitude of the laser driver output to about 850 ps. With this setting, the laser pulses produce a 1 ns (FWHM) pulse as detected by an avalanche photo diode (APD) (see fig 3.8). Deconvolution with the APD jitter of $400 \pm 50$ ps [85] results in a true laser pulse width of 0.9 ns resembling the electronic pulse length.

In the beginning dedicated adjustable delay integrated circuits (ICs) for the generation of the short pulses and for compensation of time shifts between each of the four channels were projected, however, they could not be populated on the circuit board in this experiment because of their power consumption. The introduced heat into the module could not have been exchanged with the ambiance outside the FELT2. As a result, the pulses for each diode are individually shifted relative to the 10 MHz beat (see fig. 3.8). While, in this stage of the experiment, this can be corrected in the post processing (see section 5.1.2), for a secure key, however, it is vital to maximally overlap the emitted pulses in every degree of freedom and avoid any distinguishability which could lead to side channels [70–72].

### Pseudo Random Bit Sequence

In principle, true random numbers have to be used to generate the qubit sequence as demanded by the protocol. Only then, a secure key can actually be produced. Yet, as the host system provided only unidirectional communication, the qubits were prepared according to a pseudo random bit Sequence (PRBS). This allowed for a fast and easy sifting of the received signal even without classical communication: At the ground station, the used PRBS was known and Bob could easily find the correct offset by a cross correlation.

This was realized by the implementation of a 16 bit linear feedback shift register (LFSR) [86] in the FPGA with a reset counter programmable for a pattern length between 4 bit and 255 bit. Unfortunately, during the flight tests, which started with a consecutive pattern of all four diodes only, there was no time left to try longer PRBS sequences as well.

### Laser Pulse Intensity

The exact brightness of the pulses is determined by two parameters that are controlled with two currents $i_B$ and $i_M$ into the laser driver ICs. They set a bias current $I_B = 85 \times i_B$ through the laser diodes and a modulation current $I_M = 85 \times i_M$, added to $I_B$ during a pulse. Both $i_B$ and $i_M$ are adjusted individually for all four drivers by the micro controller via an eight-fold DAC. A series resistor $R_{\text{ser}}$ translates the DAC voltage $U_{\text{DAC}}$ to a current into the drivers and its value determines the

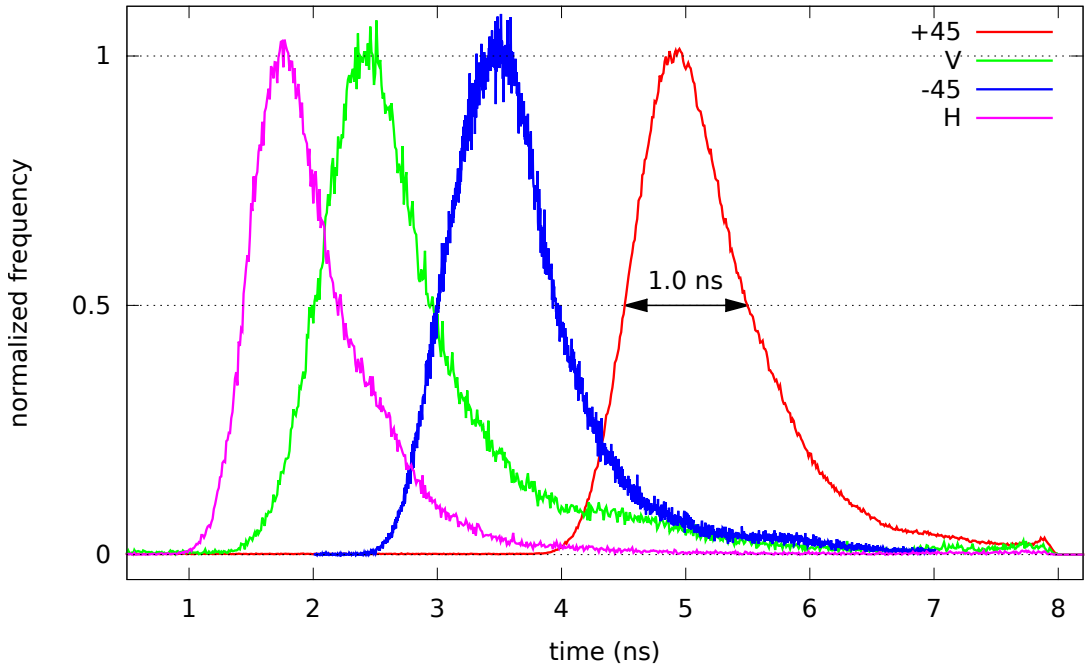



**Figure 3.8:** Alice laser pulses of the four laser diodes measured as a time histogram of APD pulse delays relative to the 10 MHz repetition frequency. Note that this measurement includes the APD temporal jitter of $400 \pm 50$ ps. The individual delays occur because the delay ICs could not be used due to their power consumption. The slightly varying pulse length is due to different diode and coupling efficiencies and according different modulation values for the laser drivers.

maximum for $I_B$ and $I_M$ respectively. As the programming pins of the laser driver IC are kept at 1.2 V, the output currents are calculated according to

$$I_{B,M} = \frac{1.2\ \mathrm{V} - U_{\mathrm{DAC}}}{R_{\mathrm{ser}}} \times 85\ . \tag{3.1}$$

For increased precision and stability, the full DAC resolution of 12 bit is mapped to voltages from 0 V to 1.25 V and $U_{\mathrm{DAC}}$ is derived from a dedicated voltage reference IC.

While $R_{\mathrm{ser}}$ for the modulation current is chosen for the maximum output modulation of up to 85 mA, the series resistors for the bias are selected to provide the full resolution for current values up to 21 mA in order to allow for precise setting below and at the laser threshold of the diodes. Additionally, for bright beam operation, the micro controller can bypass the bias DAC programming with a FET transistor to set the maximum allowed laser diode current of 35 mA.

### 3.3.2 Alice Module Optics

To implement the BB84 protocol, pulses with four polarizations equally distributed on a great circle of the poincaré sphere have to be prepared. As laser diodes are intrinsically linearly polarized well (typically 1:1000), it is straight forward to use four diodes with their polarization transformed to the states $|H\rangle$, $|V\rangle$ and $|+45\rangle$, $|-45\rangle$ for the two encoding bases as described in section 2.1. A schematic overview of the setup is presented in figure 3.9 and a stereoscopic view is shown in figure 3.10.

#### BB84 State Preparation

In the Alice module the four laser diodes are mounted in collimation packages, which allow for a precise collimation using an aspheric lens with $f = 11$ mm focal length. The diodes were selected to have similar emission spectra. Their nominal emission wavelength is 850 nm at 10 mW of laser power, figure 3.11 shows their spectra in pulsed operation. The variations in their wavelength distributions will have to be eliminated by a narrow interference filter to make all four diodes indistinguishable and to disable side channel attacks on the qubit wavelength. However, in order to achieve stable pulse intensities, this would require to control the laser diode temperatures and thus, was not implemented here.

Each pair of diodes is rotated by 90° against each other and their light is combined using a polarizing beam splitter. For the diagonal bases, a half wave plate rotates the polarization of one pair of diodes by 45° before both beams are combined on a beam splitter and directed to a spatial filter. The resulting polarizations were measured with the Alice module mounted in the FELT2 after the terminal dome using the polarimeter. In table 3.1, the resulting angles are listed. As the worst deviation of 2.2° from the nominal angle would result in an error rate of only 0.15 %, there is no significant contribution to the total QBER to be expected due to the state preparation.

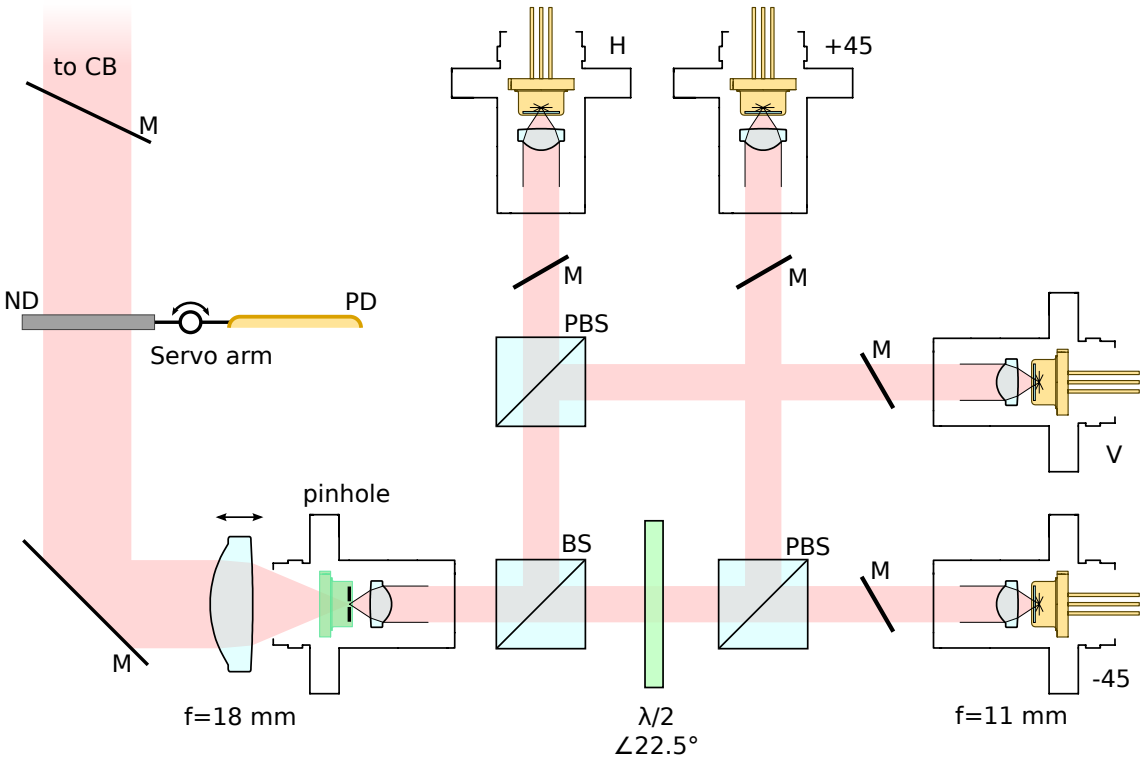



**Figure 3.9:** Optical setup of the QKD transmitter (Alice module, see also fig. 3.10 for an isometric view). Four Laser diodes (H, V, +45°, -45°) are mounted in collimation tubes perpendicular to the optical breadboard. Their light is combined using two polarizing beam splitters (PBS) and a simple beam splitter cube (BS). A half wave plate ($\lambda/2$) is used for the basis rotation from $\{H, V\}$ to $\{\pm 45°\}$. A spacial filter, built from the same collimation tube with a 5 µm pinhole in a laser diode dummy package (fig. 3.12) selects the mode to be collimated by the final lens ($f = 18\,\text{mm}$). The servo arm can optionally insert the attenuator (ND) or the Photodiode (PD) before the light is directed to the coupling block (CB, see fig. 3.16). The four mirrors (M) on the right allow for an assembly perpendicular to the breadboard and, together with the degrees of freedom of the collimation tubes, enable the coupling through the spacial filter.

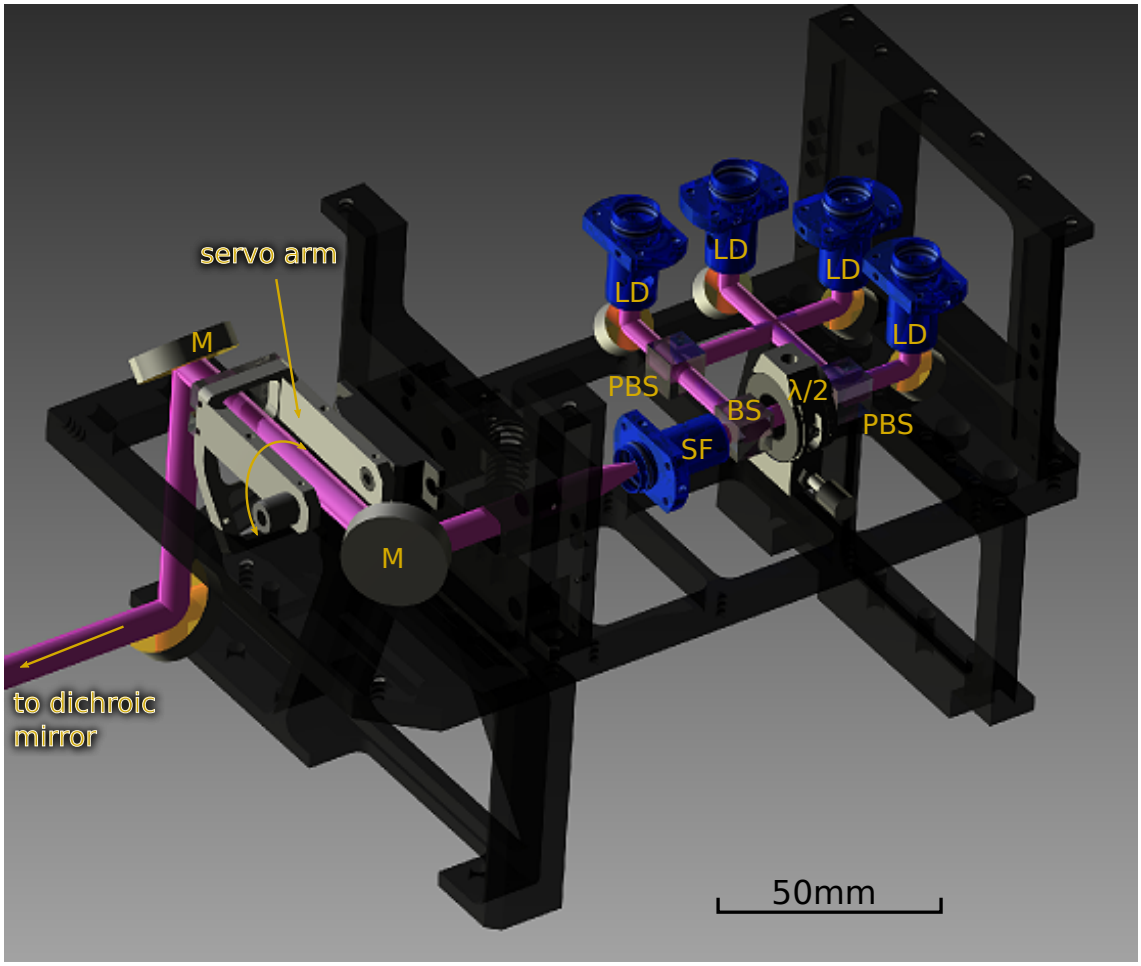



**Figure 3.10:** CAD render image of the Alice module optical setup as detailed in figure 3.9. One can see the four laser diode collimators (LD), the normal (BS) and polarizing (PBS) beam splitters, the quarter wave plate ($\lambda/2$), the spatial filter (SP), the servo arm and the mirrors used for beam alignment (M). Between these two mirrors, the beam passes the servo arm with the attenuator and the calibration photo diode. The electronics and most of the structure is hidden to reveal the optics within. The module has to be mounted elevated as the fiber amplifier of the classical system is located between the two support columns.

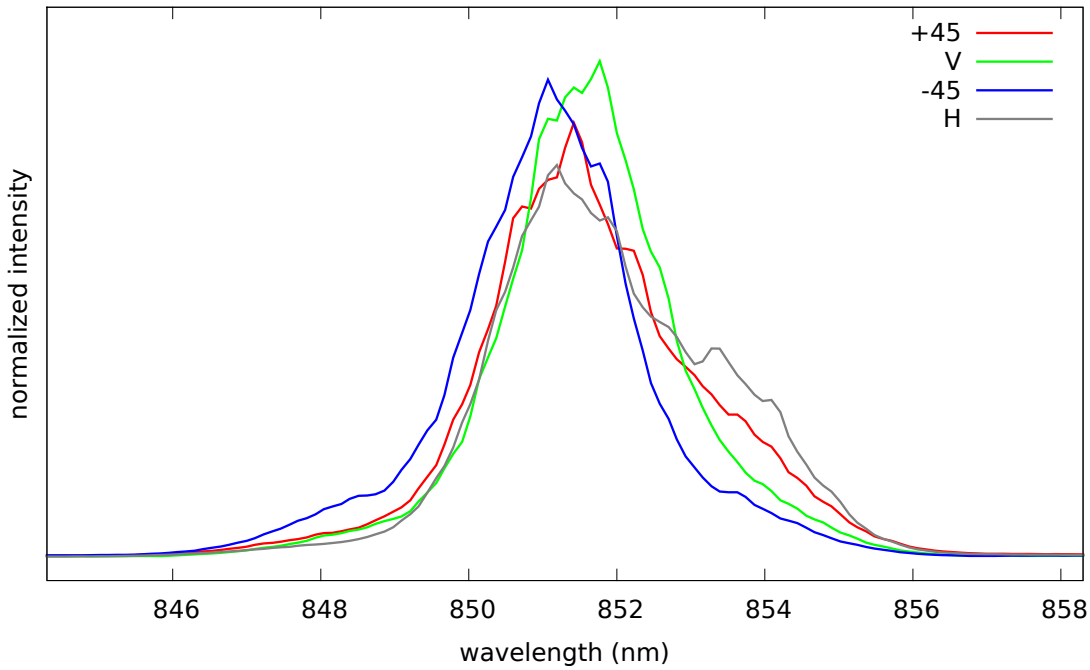



**Figure 3.11:** Spectra of the four laser diodes in pulsed mode mounted in the Alice module normalized for equal emission power. Registered with a spectrometer coupled to the Alice module output.

**Table 3.1:** Measurement of the Alice polarization states after the optical dome of the terminal.

| **laser diode** | **pol. azimuth** (°) | **pol. elevation** (°) | **linear pol. error** (°) |
|---|---|---|---|
| $\|-45\rangle$ | -46.1 | 0.2 | -1.1 |
| $\|V\rangle$ | 89.4 | 0.1 | -0.6 |
| $\|+45\rangle$ | 47.2 | 0.1 | 2.2 |
| $\|H\rangle$ | -0.4 | -0.4 | -0.4 |

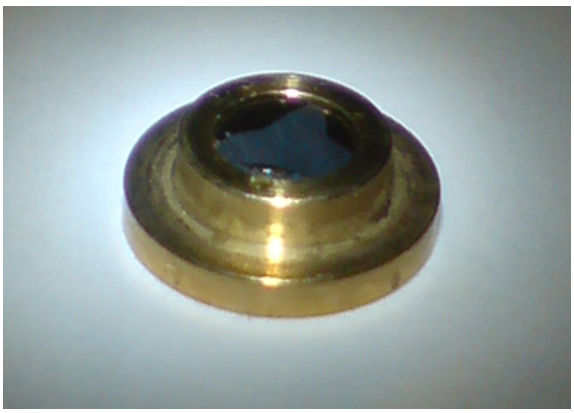


**Figure 3.12:** Dummy laser diode package with pinhole mounted in place of the laser emitter. For spatial filtering another laser diode collimation tube is used, equipped with this dummy diode. This prove to be a compact solution for a stable mounting of the pinhole while still providing the necessary degrees of freedom to adjust the accepted beam divergence and direction.

### Spatial Filtering and Collimation

For the security of the QKD transmission, it is essential that the modes of the four laser diodes are indistinguishable and a setup using different diodes for some or all of the polarization states is intrinsically prone to state preparation side channels. For the spatial degree of freedom, this vulnerability can be avoided by filtering the combined light of the diodes with a short piece of single mode fiber. Yet, this causes unpredictable polarization rotations if the fiber is bended or otherwise stressed. Nevertheless, in [70, 87], such a filter with temperature stabilization could be demonstrated. The space and power requirements as well as the desired transmittance, however, do not allow an adoption of this technique here. Therefore, a free-space spatial filter was implemented for this experiment as this also promises to be more robust against temperature changes and mechanical vibrations. However, true indistinguishability of the four diodes had to be sacrificed and the according side channel remains to be closed at this stage of the experiment.

The spatial filter is realized focusing the light on a $d = 5\,\mu\text{m}$ pinhole, which is mounted in a laser diode dummy package (fig. 3.12). Thereby, the same collimation package as for the laser diodes can be used in reverse. This allows for the precise alignment of the focusing and the filter axis. As the diffraction limited waist of the focusing lens ($f = 11\,\text{mm}$) is slightly smaller than the pinhole diameter, best results were obtained slightly out of focus. Then, the center maximum of the Airy diffraction pattern behind the circular aperture nicely approximates a Gaussian beam profile.

After the spatial filter, the pinhole diffraction pattern is collimated by an $f = 18\,\text{mm}$ aspheric achromat (diameter 9 mm). As the subsequently available aperture

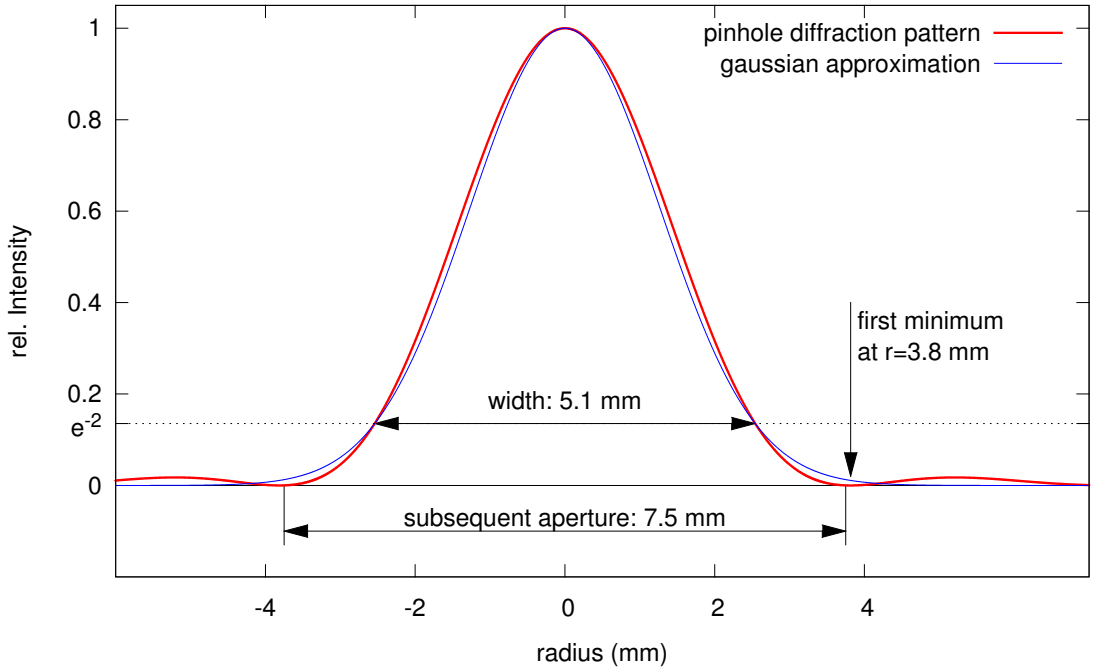



**Figure 3.13:** Diffraction pattern (red) calculated for a 5 µm circular pinhole in a distance of 18 mm and an approximated Gauss peak (blue) of the same width.

in the FELT2 terminal is limited to 7.5 mm (see fig. 3.16), the focal length $f$ is chosen such that the first minimum of the pinhole diffraction pattern has also the same 7.5 mm diameter. Figure 3.13 shows the calculated diffraction pattern for a 5 µm pinhole in the distance $f$. The resulting collimated beam has a diameter of 5.1 mm at $1/e^2$ level.

Figure 3.14 representatively displays the beam profiles of the four diodes as out of the Alice module and without further optics (the exit aperture is defined by the collimation lens holder with a diameter of 8 mm). They were captured on a canvas in a distance of 50 m using a linear CCD camera. Variations of the power distribution in the beam are due to non planar wave fronts in the pinhole diameter and are sensitive to mechanical stress on the Alice module framework and temperature changes of the structure. This might be improved with a still smaller pinhole. Yet, a smaller pinhole was not used here to avoid a possible blockage during the experiment by small dirt particles in the rough and possibly dusty environment to be expected during the ground to ground tests, the assembly in the aircraft, and the flight campaign.

The power transmission of the spatial filter was reasonably stable at about 20 %. Loosing half of the laser power at the beam splitter, this leads to 1 mW CW power at the Alice module output for each laser diode at its nominal maximum power.

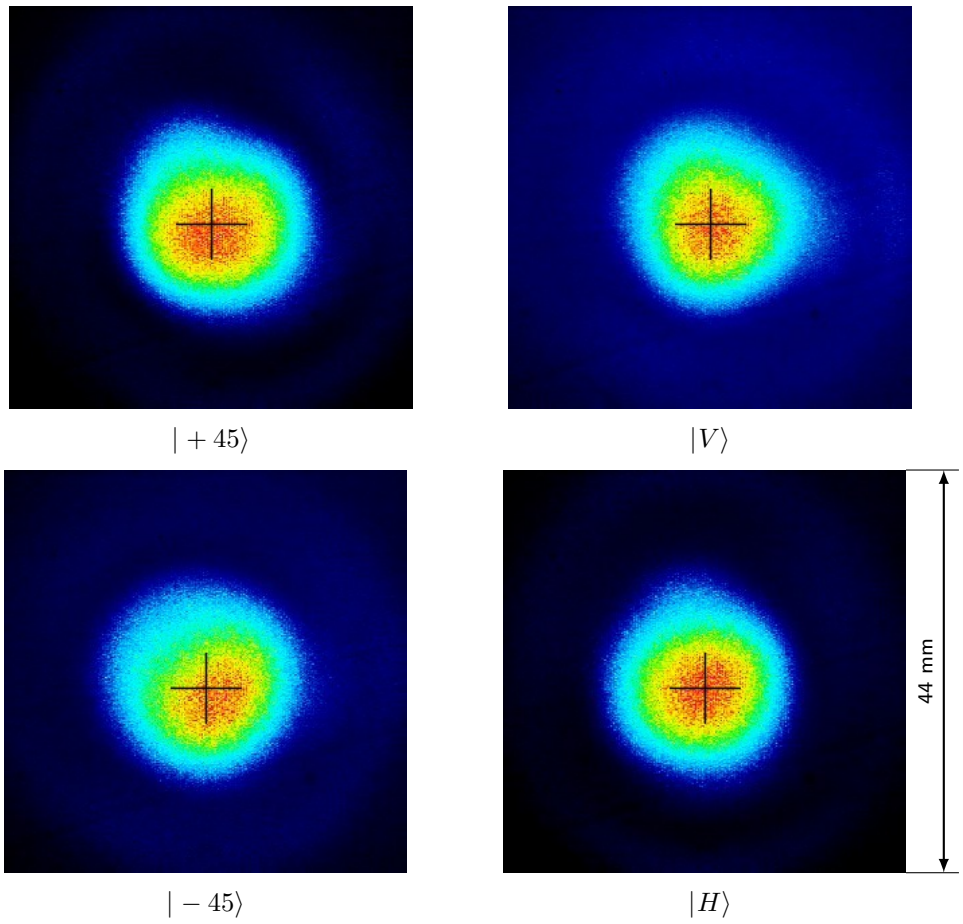



**Figure 3.14:** Modes of the four laser diodes registered in a distance of 50 m behind the spatial filter on a canvas using a linear CCD camera. The cross marks a fixed position on the screen.

Finally the telescope implemented in the FELT2 coarse pointing assembly widens the beam and at the same time reduces its divergence. A beam at the design wavelength of 1550 nm is expanded in the telescope by a factor of 2. For the QKD beam at 850 nm, this means, it has to enter the telescope slightly divergent in order to leave it collimated. An optical simulation (Zemax) resulted in a final beam diameter at the telescope output of 12.2 mm at $1/e^2$ level. For a perfect Gaussian beam, this would result in a diffraction limited divergence of 88 µrad (full angle). Due to the constraints of the host system, the QKD beam can enter the telescope only parallel to its axis (shifted by $\approx 4$ mm, see fig. 3.16 in § 3.3.4). As a consequence, the beam is also slightly cut by the exit aperture of 30 mm. Therefore, a diffraction limited divergence is not to be expected and the actual value is determined experimentally over a distance of 300 m (see section 4.2.2).

#### Attenuation

In contrast to previous four or eight laser diode implementations of a BB84 QKD transmitter [16, 25, 87–89], the combination of the laser diode modes on the one hand and the attenuation to mean intensities below one photon per pulse on the other hand could be separated in the present design. This makes mean pulse intensities from 0 to a few million photons per pulse possible by selecting the according attenuating filter and additionally offers the possibility to emit a bright beam for alignment purposes.

Therefore, the final optical component of the Alice module is the remotely removable attenuator, which is made from two stacked filters of absorptive Schott glass with 27.8 dB and 30.8 dB attenuation respectively (58.6 dB in total). The characterization of these filters was done by measuring their extinction with a 10 mW laser beam at 850 nm and a power meter. While the exact brightness is controlled electronically with the value of $I_B$, this defined attenuation (together with further losses within the Alice enclave) brings down the intensity of the laser diode pulses to the single photon level for QKD operation. To avoid any angular deviation of the QKD beam when the attenuator is inserted into the beam path, the filters were especially selected for a vanishing wedge angle.

### 3.3.3 Pulse Intensity Calibration

The mean photon number per pulse sent by Alice is crucial to comply with the protocol and consequentely for the security of the distributed key. The fraction of multi photon pulses can only be estimated for a precise intensity of the pulses. Therefore, the Alice module was equipped with a photo diode (PD) to allow for calibration and measurement of this parameter in flight. Mounted on a remote controlled servo arm, this PD can be brought into the beam path and the laser power can be measured with the help of an ADC. For an increased dynamic range,

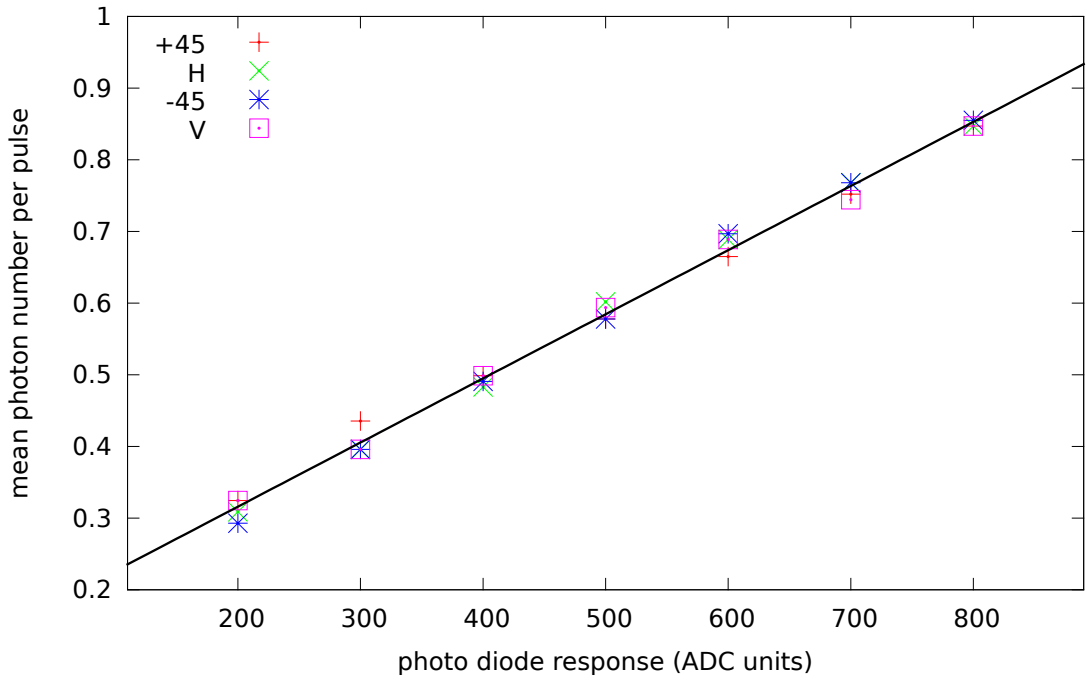



**Figure 3.15:** Mean photon number $\mu$ of the Alice pulses after 67.1 dB attenuation measured by focusing the Alice beam onto an APD when the laser diodes are electronically adjusted to induce a certain response on the calibration photo diode (PD). The straight line is a linear fit.

the PD bias resistor can be selected in software. This allows to measure the power of the bright cw beams, too.

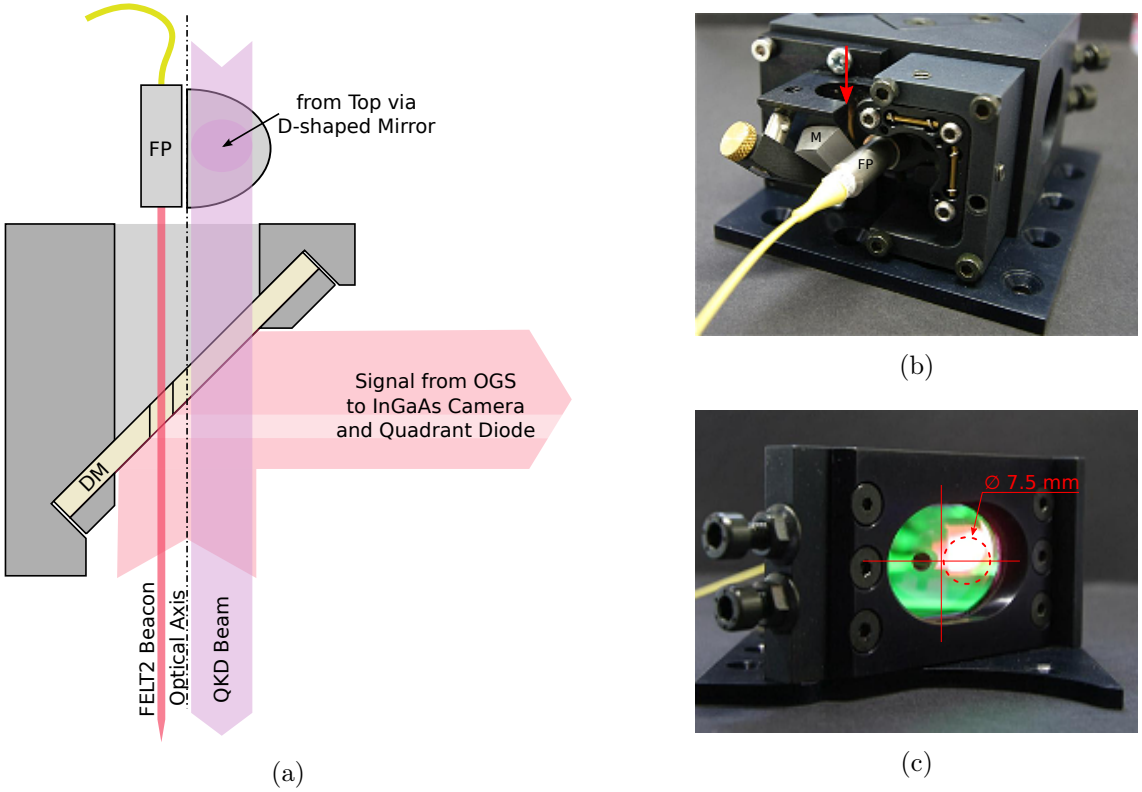
The relationship between the mean photon number per pulse (after the attenuator) and the response on the photodiode when placed in the beam (instead of the attenuator) enables the calculation of the actual laser pulse brightness from the ADC reading. This was measured beforehand in the lab using an APD to determine the attenuated pulse intensity. In figure 3.15, the mean photon number per pulse $\mu$ is plotted against the ADC value. $\mu$ is calculated for the total attenuation of 67.1 dB between the Alice output and the exit from the glass dome. Additional losses to the main attenuator are due to an extra attenuating filter (4.8 dB, could not be mounted on the servo arm due to a lack of space there) and the FELT2 optics (3.7 dB). With this information, the micro controller is able to perform a search for the bias current value – the modulation current was kept maximal – resulting in pulses with a mean intensity of exactly 0.5 photons.

Due to the high efficiency of the mode combination of the four diodes, small bias currents were sufficient to produce the desired pulse intensities. As a consequence, there was no background measurable between the pulses when the diodes were switched off well below their laser threshold. This constitutes a big advantage compared to prior experiments [87], where the large attenuation of the diode coupling sometimes forced high bias currents close to the laser threshold. This resulted in a much worse signal to noise ratio due to a non vanishing brightness in the "off" state.

### 3.3.4 Module Integration

To interface the QKD transmitter with the FELT2 optics, the coupling block (CB, fig. 3.16) was chosen. There, the original setup provided two fiber ports to emit beacon lasers with different divergences. They were both mounted to the back of the CB pointing through two holes in the CB mirror. By passing the bright beams (2 W peak) through holes in the coupling mirror, possible stray light, which might occur on the surfaces of a dicroic mirror and then disturb the tracking sensors, can be avoided.

For classical communication experiments, only one of the two fiber ports was used at a time. Thus, for this demonstration, it was possible to remove one of them in order to make room for the QKD beam coupling. For this purpose, a D-shaped mirror was mounted to the back of the CB providing a beam access from the top (fig. 3.16). Additionally, the CB silver mirror was replaced with a dichroic mirror transmitting light with a wavelength of $\lambda = 850$ nm to allow for a beam diameter beyond the 4 mm hole. Consequently, for the remaining fiber port only one hole was drilled in this new mirror. A disadvantage of this configuration is the off axis access to the terminal optical system which, however, could not be avoided without major modifications of the terminal.




(a) (b) (c)

**Figure 3.16:** FELT2 Coupling block. **a:** Schematic view of the coupling block where the incoming signal from the OGS is overlapped with the terminal beacon and the QKD signal. **b:** Back view. While the original design symmetrically uses two fiber ports (FP) with different divergences for the beacon laser, in this experiment one was exchanged for a D-shaped mirror (M) providing access for the QKD beam from the top (red arrow). **c:** Front view. The dichroic mirror replacing the original silver mirror with two holes. The QKD beam passes the dichroic coating in the dotted circle. It is at this component where the maximum possible full diameter of 7.5 mm of the QKD beam in the FELT2 is defined. The cross marks the axis of the FELT2 optical system.

### 3.3.5 Airworthiness Certification

The FELT2 host system already implements the requirements for the airworthiness certification, for instance shielding of laser radiation from the aircraft personnel and passengers and a fire-retardant housing.

During the design and construction process of the Alice module as an add-on to the FELT2, special considerations had to be taken to keep the flight terminal certifiable as a whole. Specifically, the demand for a robust and trustworthy mechanical setup to minimize the chance of parts breaking apart in turbulent flight situations. Moreover, cables and other plastics used had to meet applicable standards, to limit the emission of toxic gasses in case of fire.

Most challenging, however, were laser safety considerations regarding the QKD beam. The beam diameter and minimal divergence had to be specified by a measurement report as the basis for the calculation of the applicable safety distance. For static applications, this is the "extended nominal ocular hazard distance" (NOHDe). Within this distance, somebody using binoculars or a consumer grade telescope might be at risk when looking into the laser source. The NOHDe for the QKD transmitter, however, is much longer than the intended flight height due to its narrow divergence. Yet, in this airborne scenario, a prolonged exposition to the beam can be excluded because it is practically impossible to track an arbitrary observer accidentally. Therefore, a maximum exposure time of 100 ms could be argued for this experiment and the safety distance could be reduced to 800 m. Note that the host system communication and beacon laser has a much higher maximum power of 2 W peak. Due to the longer wavelength of 1550 nm and the much wider divergence, however, eye safety is already reached in a distance of 376 m even for prolonged exposition.

As the requirements from the airworthiness certification are primarily binding to the pilot, a switch had to be installed in the cockpit that cuts and clears power to the terminal laser systems. The aircraft operating manual was supplemented with the documentation of the new switch and instructions that oblige the pilot to disable the laser systems when flying below 800 m or in situations when other air traffic comes closer than this distance.

## 3.4 The QKD Receiver – Bob

The analysis of the transmitted qubits takes place in the Bob module. It houses all optics necessary to passively select a basis out of $\{|H\rangle, |V\rangle\}$ and $\{|+45\rangle, |-45\rangle\}$ at a beam splitter and subsequently measure the polarization of the incoming, ideally single photon pulses using polarizing beam splitters and APDs in Geiger mode. This module design has been used in experiments before [16, 88, 90] and an illustration of the internal setup is depicted in figure 3.17.

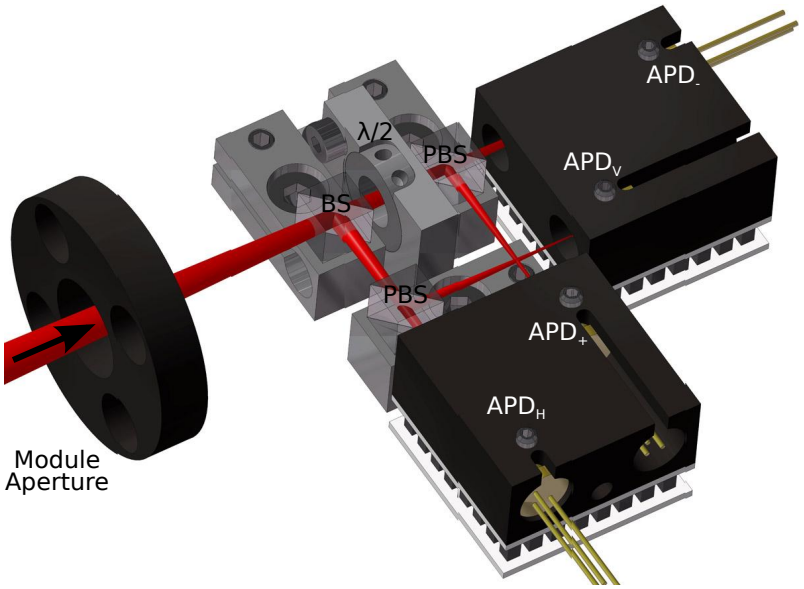



**Figure 3.17:** Illustration of the Bob module optical setup. The receiver implements two polarization analyzers with a polarizing beam splitter (PBS) and two silicon APDs each. At a first non polarizing beam splitter (BS), the incoming qubit is either reflected to the analyzer orientated in the $\{|H\rangle, |V\rangle\}$ basis, or transmitted. In this case, the polarization is rotated by a $\lambda/2$ wave plate set at 22.5° before the light enters the second analyzer, resulting in a measurement in the $\{|+45\rangle, |-45\rangle\}$ basis. Peltier elements underneath the APD mounting blocks are used to cool the diodes and thereby reduce dark count events.

The silicon APD detectors (PerkinElmer C30902S) are cooled with Peltier elements to −20 °C. At this temperature they show a dark count rate of about 500 $s^{-1}$ each. The efficiency was previously measured to be around 38 % [85]. The APDs are passively quenched with a 390 kΩ resistor, leading to a significant dead time of about 0.5 µs after a detection event [89]. Due to the low count rate to be expected in this experiment, however, this is tolerable.

The Bob module electronics consists of controllers that maintain the APD temperature, adjustable high voltage supplies for the biasing of the APDs and the pulse detection circuit. The latter implements a threshold trigger for each channel and a subsequent pulse shaping, which extends the output pulse length to 20 ns.

An overview of the complete OGS optical setup is sketched in figure 3.6: After passing the telescope, the beam is collimated and the fast piezo actuated mirror compensates for small fluctuations in the mean arriving wavefront direction as described in section 3.2. The classical signal is then transmitted at a dichroic mirror while the QKD beam gets reflected, compressed by a factor of 2 and finally, after polarization correction, focused onto the APDs in the Bob module with an $f = 75$ mm lens. All together, this defines a field of view for the Bob module of 83 µrad calculated from the detector diameter of 500 µm and the effective focal length of the telescope system of 6 m. At the location of the aircraft in a distance of 20 km this translates to a diameter of 1.7 m and efficiently reduces the stray light susceptibility of the QKD system. An interference filter (see also § 4.3.2) mounted in front of the Bob module further reduces the remaining background.

The coalignment of the Bob module optical axis to the main telescope axis was done at a distance of 500 m. On the rooftop of a nearby building, a calibration target was installed, emitting both the 1550 nm beacon and an 850 nm test signal from a common open fiber end. With the OGS tracking this target, the receiving direction of the Bob module could be manually overlapped with the telescope axis by adjusting the mirrors on the OGS breadboard.

## 3.5 Management of Polarization Rotations in the Quantum Channel

One of the underlying principles of QKD security is, that a measurement on the qubits provides only meaningful results when performed in the correct bases. This means in reverse, that the receiver has to use the exact same reference frame for his measurement as was used for preparation of the states. Contrary to stationary systems, in a mobile or even airborne scenario as in this experiment, this is not trivially accomplished: The polarizations may appear rotated at Bob's due to the relative orientation of the aircraft and the ground station telescopes. Moreover, phase shifts, which are introduced polarization dependently by the optical components of the pointing systems, give rise to circular components, too. Therefore,

to enable a low noise polarization encoded quantum transmission, it is crucial to compensate these effects somewhere in the quantum channel using for example a set of wave plates. However, as the aircraft changes its orientation relative to the OGS permanently, new angular positions for these wave plates have to be determined for a successful compensation – ideally continuously.

The first approach to realize a polarization compensation scheme was to measure the actual polarization rotation of the quantum channel at the receiver with the help of a bright ($\approx 1\,\mathrm{mW}$) calibration signal from the transmitter. This can be achieved by once in a while sending the two non orthogonal states $|H\rangle$ and $|45\rangle$ for a short time each and measure the polarizations actually arriving at the Bob module. The necessary calibration intervals depend on the trajectory of the airplane. On the projected circular path, however, no fast changes are to be expected. The exact time before a recalibration needs to be determined in flight.

For this scheme, a compact polarimeter[3], offering a dynamic range from $-60\,\mathrm{dBm}$ to $10\,\mathrm{dBm}$, was mounted on the ground station. A remote controlled flip mirror was installed to direct the received signal onto this polarimeter on demand. The phase shifts introduced by the flip mirror and one additional mirror were measured once to enable the calculation of the polarization as it enters the Bob module.

This strategy would in principle enable a complete characterization of the birefringence of the quantum channel and thereby allow to calculate angular positions for the wave plates to compensate for all polarization rotations. In the ground to ground tests, however, it was difficult to obtain reliable measurements from the polarimeter within integration times of 1 s to 3 s. While the high dynamic range of the device was perfect for this scenario, the measurement principle proved to be not suited in the presence of fluctuations (see § 4.1). Therefore, a closed loop control could not be realized.

The alternative option therefore was an open loop control of the polarization compensation depending on a careful characterization of the relevant system components. Especially in view of finite key effects (see § 5.3.2), an advantage of this approach is, that there is no need for calibration intervals and the quantum transmission does not have to be interrupted.

The overall polarization rotation in the quantum channel can be decomposed into the following effects:

i. static birefringence within the flight terminal

ii. phase shifts introduced at the moving pointing mirrors of the flight terminal due to the varying angle of incidence

iii. phase shifts introduced passing the optical dome, possibly depending on the position on the dome (i.e. the pointing direction)

[3]model: Thorlabs `PAN5710IR1`

iv. spatial rotation of the aircraft around the beam axis.

v. static birefringence of the OGS optics. (Note that the spatial orientation of the OGS telescope is not relevant here as it moves as a whole.)

All these distortions to the polarization can either be measured beforehand, if necessary depending on the pointing direction of the flight terminal, or calculated from live data in flight. This shall be explained in more detail in the following.

### 3.5.1 Polarization Rotations in the Flight Terminal (i to iii)

In the flight terminal, the QKD beam is reflected by several fixed mirrors and passes a dicroic mirror as well as two lenses which are coated for telecom wavelengths. All these components can cause *static* polarization rotations. The mirrors in the pointing system, however, introduce effective phase shifts depending on their orientation, i.e., depending on the terminal pointing direction. The glass dome may introduce distortions depending on the position the beam passes, too. Therefore, the combined effect on the polarization of the FELT2 terminal optics including the glass dome was measured for all relevant pointing directions in the lab. This was done using the polarimeter mentioned above to determine the birefringent effects on the two polarizations $|H\rangle$ and $|45\rangle$ sent by Alice.

The result (fig. 3.18) was used to model the polarization effects within the FELT2 depending on the pointing elevation ($\vartheta$) and azimuth ($\varphi$) as a rotation $R_{\mathrm{FELT}}(\vartheta, \varphi)$. As it turns out, the terminal dome does not seem to introduce any severe birefringence – at least without any air stream[4]. Additionally, the phase shifts introduced by the pointing mirrors cancel out. Therefore, only the geometric rotation of the field of view with the azimuth angle, a feature of the coudé beam path, remains and a simple linear model suffices.

To additionally provide information about the current direction of the FELT2 pointing mirrors to the compensation algorithm working at the OGS, the data protocol for transmitting the aircraft GPS and heading data via the UHF radio link was extended for the two pointing angles $\vartheta$ and $\varphi$. With a repetition frequency of 5 Hz, this data enables a nearly instant calculation of new angular positions for the wave plates.

### 3.5.2 Spatial Polarization Rotations (iv)

The only entirely spatial rotation of the qubit polarization that remains to be compensated is the rotation of the aircraft around the beam axis (iv). For distances

[4]The gradient of the air stream velocity is known to cause some birefringence. The effect is, however, supposed to be very small [91]

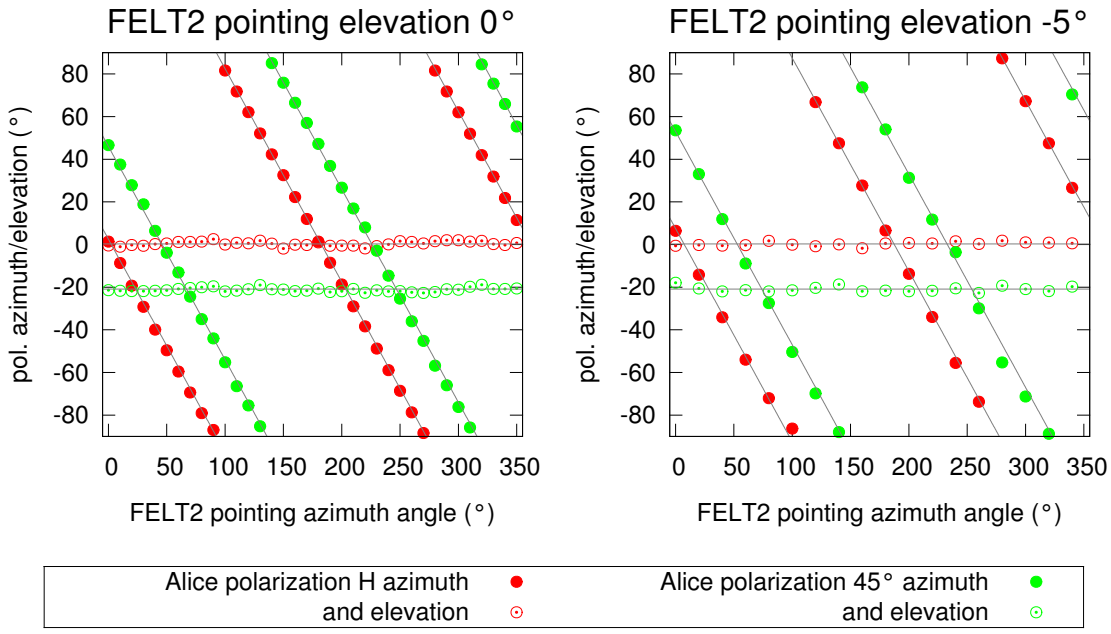



**Figure 3.18:** Polarization measurement for Alice states $|H\rangle$ and $|45\rangle$ after the FELT2 glass dome for relevant pointing directions of the flight terminal. The resulting polarizations are characterized by their azimuth and elevation on the Poincaré sphere. Due to the limited flight altitude to be expected, the circular path of the aircraft and the distance to the OGS only small negative pointing elevation angles are relevant. The gray lines indicate the modeled behavior.

much greater than the flight altitude and on the projected circular path around the OGS, the beam axis almost coincides with the aircraft pitch axis, the transverse horizontal axis. As a consequence, most of the time the pitch angle – the rotation around this axis – is small owing to the fact that the airplane does not follow steep trajectories. Because in this experiment there is also not much variation of this angle, the actual pitch value $\delta$ was reported by the pilot and manually entered in the control algorithm as a linear rotation $R_{\text{spatial}}(\delta)$ of the polarization reference frame.

### 3.5.3 Polarization Rotations OGS (v)

Because the OGS telescope with all subsequent optics is moved as a whole to change the pointing, its orientation relative to the arriving photons is unchanged and only static polarization effects have to be considered at Bob's. In order to measure them, the OGS tracking was locked on a dummy laser source on a rooftop at a distance of 500 m. The Bob module was exchanged for the polarimeter and a polarizer was placed in the beam right behind the main mirror. The overall birefringence of all components up to the Bob module was then measured with horizontal and 45° settings of this polarizer, which allows to calculate the static rotation $R_{\text{OGS}}$ of the polarization reference frame at the OGS.

### 3.5.4 Compensation Model and Polarization Controller

In summary, all distortions listed in 3.5 are now characterized and either invariant or parametrized by angles accessible during the flight experiment. The overall polarization distortion can thus be calculated as

$$R(\vartheta, \varphi, \delta) = R_{\text{OGS}}\, R_{\text{spatial}}(\delta)\, R_{\text{FELT}}(\vartheta, \varphi) \tag{3.2}$$

For compensation, first two quarter wave plates followed by a half wave plate are used. Angular positions for these elements are calculated from the rotation $R(\vartheta, \varphi, \delta)$ every 200 ms and sent to the free-space polarization controller (fig. 3.20) mounted on the OGS breadboard right in front of the Bob module (fig. 3.6). The strategy for calculation of the wave plates' angular positions (illustrated in fig. 3.19) first rotates the great circle containing the Alice polarizations in a way that makes it cut the poles of the Poincaré sphere. This can always be accomplished deterministically with a quarter wave plate orientated perpendicular to the intersection of this great circle with the equatorial plane and is easily calculated as a set of cross products. The intersection of the rotated circle with the equatorial plane defines the orientation of the second quarter wave plate, resulting in all four Alice polarizations rotated back to the equator of the Poincaré sphere. The final half wave plate then brings them back to their initial positions. Extra care has to be taken in order not to alter the

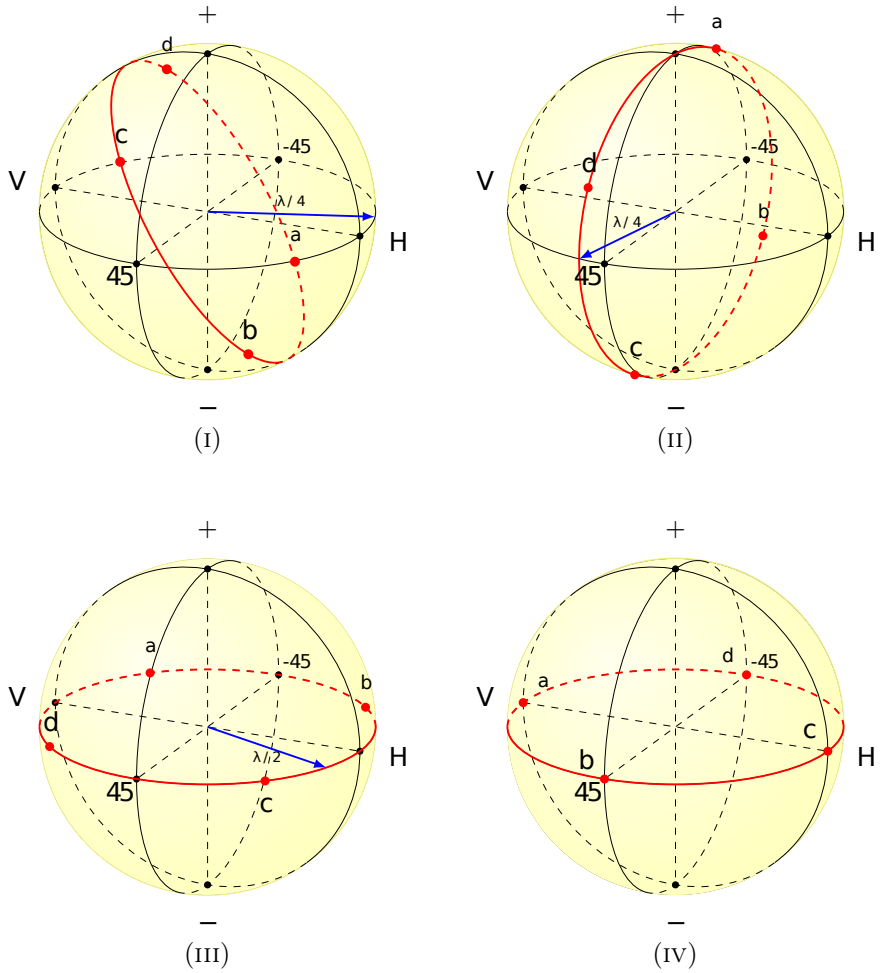



**Figure 3.19:** Illustration of the strategy to compensate an arbitrary rotation of the Alice states $|V\rangle$, $|45\rangle$, $|H\rangle$, $|-45\rangle$, resulting in the polarizations $a$, $b$, $c$, $d$ on the Poincaré sphere. (I) A first quarter wave plate is oriented perpendicular to the intersection of the equator and the great circle (red) described by the received polarizations. (II): The circle now intersects the poles of the Poincaré sphere and a second quarter wave plate is orientated along the circle's intersection with the equator. (III): All polarizations $a$-$d$ are now linear and a final half wave plate is adjusted to make up for the rotation within the equator and arrive in the compensated situation depicted in (IV). Note that following this strategy, the angular positions of the wave plates are only defined modulo $\pi$ and it has to be ensured by the correct orientation of the last half wave plate that the cyclic sequence of the four polarizations is not destroyed.

sequence ($|H\rangle \rightarrow |45\rangle \rightarrow |V\rangle \rightarrow |-45\rangle$) of polarizations around the Poincaré sphere by the correct orientation of the final half wave plate (see fig. 3.19).

## 3.6 Timestamping Electronics

All detector events from the Bob module are timestamped and saved to allow for later analysis of the received signal. The analysis is facilitated, if both Alice and Bob already operate synchronously. For this purpose, the Alice clock is distributed over the classical optical channel by modulating the flight terminal data and beacon laser. At the OGS, this signal is fed into a phase-locked loop (PLL) and finally used as a clock for the FPGA to timestamp the signals. Running at 200 MHz, the FPGA assigns the number of cycles since start as a coarse timestamp (48 bit) to every event. This allows for over 390 h of operation without overflow. A carry chain is used to interpolate these 5 ns intervals to get a fine granular timestamp with a bin size of $\approx 56$ ps, a technique explained for example in [92]. The resulting integers, together with the detector number are packed in a 64 bit value and transmitted via USB to a computer.

## 3.7 Software Experiment Control and Online Evaluation

A number of software modules were created to control the hardware components involved in this experiment. Moreover, for online evaluation of the QKD transmission, a complex suite was developed, which is able to perform a local QKD sifting process with the help of the known PRBS sequence and allows to log and visualize all transmission parameters in real time.

### 3.7.1 Alice Control

The software to control the Alice module entirely runs on the embedded micro controller. A serial terminal on a laptop is used to communicate with the module over a USB connection. The available commands comprise:

- Functions to measure temperature, supply voltages and maximum available laser power (coupling of the mode filter) and to report the operating status.
- Selection and activation of different slow and bright blink patterns useful for signal acquisition and alignment.
- Control of the motorized arm to place the photodiode or the attenuator in the beam.

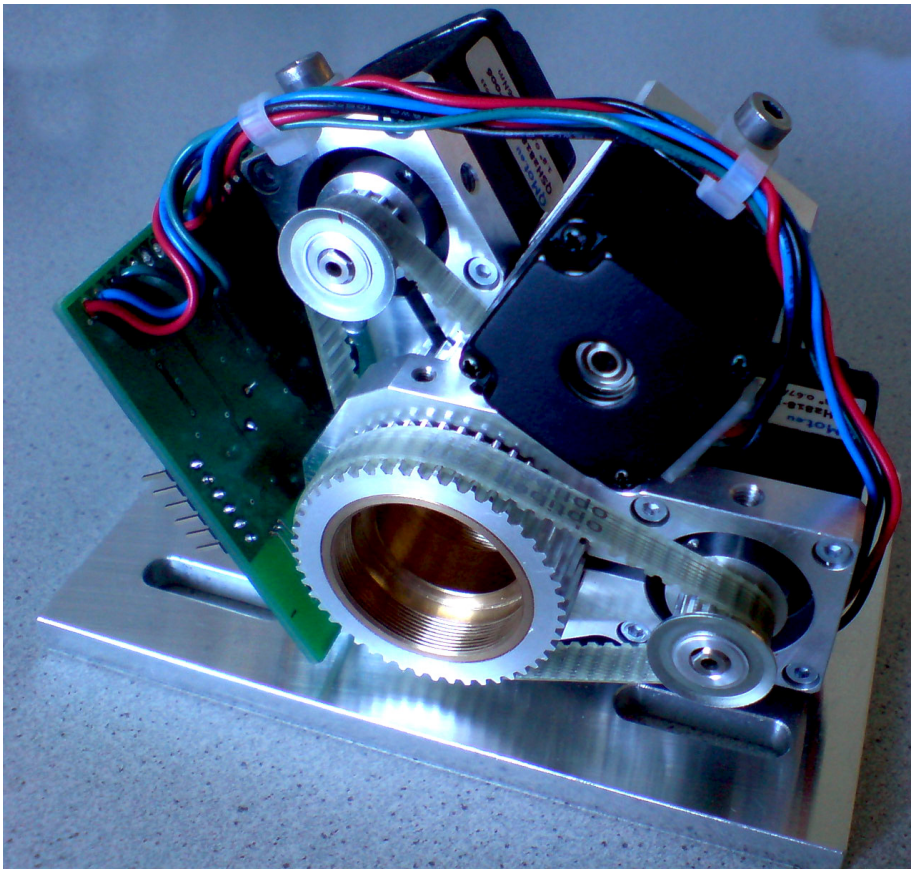


**Figure 3.20:** Three-fold motorized rotation mounts for free-space polarization transformations. The design is trimmed for a small footprint and little weight as it is moving with the OGS telescope. Still, the ability to accommodate common 1 in optics (here wave plates) was preserved. Reference switches (hall sensors with neodym magnets in the rotating wheels) enable calibration for absolute positions after a power cycle. The unit is controlled via a USB connection.

- Setting of the laser diode bias and modulation currents. Additionally, the bias current control can be bypassed and set to the maximum operating current for the laser diodes in order to produce a bright cw beam.

- Measurement and calibration of the QKD pulse brightnesses.

- Polarization pattern and PRBS length selection.

The real time clock built into the module provides accurate human readable timing information, which is displayed with all commands and messages from the module. This allows to use the logfile of the serial terminal in the experiment evaluation.

### 3.7.2 Online Filtering and Sifting

The main online evaluation tool is a software that reads in the data from the timestamping FPGA, logs it and determines basic parameters like count rates. Additionally it executes the sifting. This process is facilitated as Alice and Bob both know the PRBS used to prepare the qubits and therefore, no additional classical communication is needed. Note, however, that for a secure exchange of a truly random key, a classical channel between Alice and Bob is needed which has to be authenticated properly.

#### Synchronization and Filtering:

The first task is to synchronize receiver and transmitter. This is facilitated by the Alice clock being transmitted as a 100 MHz signal via the classical link to Bob. Therefore, the timestamping on the ground already works synchronously. Because the QKD-pulse repetition frequency is only 10 MHz, Bob has to divide the transmitted clock accordingly. A time histogram of the received events then allows him to determine the phase/delay of the qubits arrival within the resulting 100 ns intervals. This delay is composed of an integer multiple of 10 ns due to the frequency division with arbitrary remainder and an overall fixed delay. The latter is accumulated from the time needed for pulse processing at Alice and Bob relative to the delays in the clock distribution via the classical channel and the clock recovery for the Bob timestamping unit. Note that the time of flight of the photons, namely the distance from the airplane to the ground station, is irrelevant, as the clock is transmitted via the same channel as the quantum signal. Once synchronized, an online coarse time filtering of the recorded events eliminates the majority of clicks from dark counts or stray light and assigns the filtered events to transmitter time slots.

### Sifting

As a next step, the sifting can be performed: While this usually involves communication between Alice and Bob, due to the unidirectional classical link, this process is done locally in this demonstration on the basis of the commonly known PRBS. By a cross correlation of the PRBS with the received signal for multiple delays of 100 ns, the polarization pattern phase is determined and Bob discards the events measured in the wrong basis to obtain the sifted key. At this stage, the QBER can be calculated. While privacy amplification, necessary to actually distill a secure key, is not performed online, estimates for the main parameters allowing to judge the QKD performance – attenuation and QBER – are immediately available during the experiment.

# Chapter 4

# Field Tests and Flight Campaign

While the actual flight tests are the main subject and the highlight of this work, the preparations in the preceding months were equally important. Besides the design, the assembly and the integration of the QKD hardware as described in the last chapter, characterization and extensive testing of the combined system was done in ground to ground tests to lay the best possible foundations for a successful flight experiment. In fact, the strategies for compensation of the polarization rotations and the need for the fine calibration of the QKD pointing in flight emerged from these tests. Starting from the moment the whole system was ready to leave the lab, this chapter shall describe the last steps to and including the experimental flights.

## 4.1 Ground to Ground Testing

In the ground to ground tests preceding the experimental flights, tests on different distances were performed to primarily evaluate the performance of the bidirectional pointing and the coalignment of the QKD beam with the tracking axis between the terminal and the OGS. Further tests also concerned the QKD beam collimation, the polarization compensation and the clock synchronization from Alice to Bob.

These field trials were performed using a test vehicle already equipped with a power generator and the antennas (GPS, UHF) needed for the FELT2. The flight terminal was mounted on a lab trolley and secured in the vehicle with the door open. Beyond static tests, this also allowed trials at moderate speed of the FELT2. Up to 30 km/h could be achieved for several seconds, which corresponds to an angular speed of up to 3 mrad/s and is comparable to the conditions during flight.

Figure 4.1 gives an overview of the test links. In distances of $d_a = 330\,\mathrm{m}$, $d_b = 2.5\,\mathrm{km}$ and $d_c = 4.6\,\mathrm{km}$ around the OGS in Gilching 23 km west of Munich, Germany, locations were found providing a direct line of sight to the OGS telescope. Dynamic tests, however, were only possible on $d_b$.

The first issue that emerged in the field trials concerned the polarization compensation scheme and led to the strategy as detailed in section 3.5.4. Even

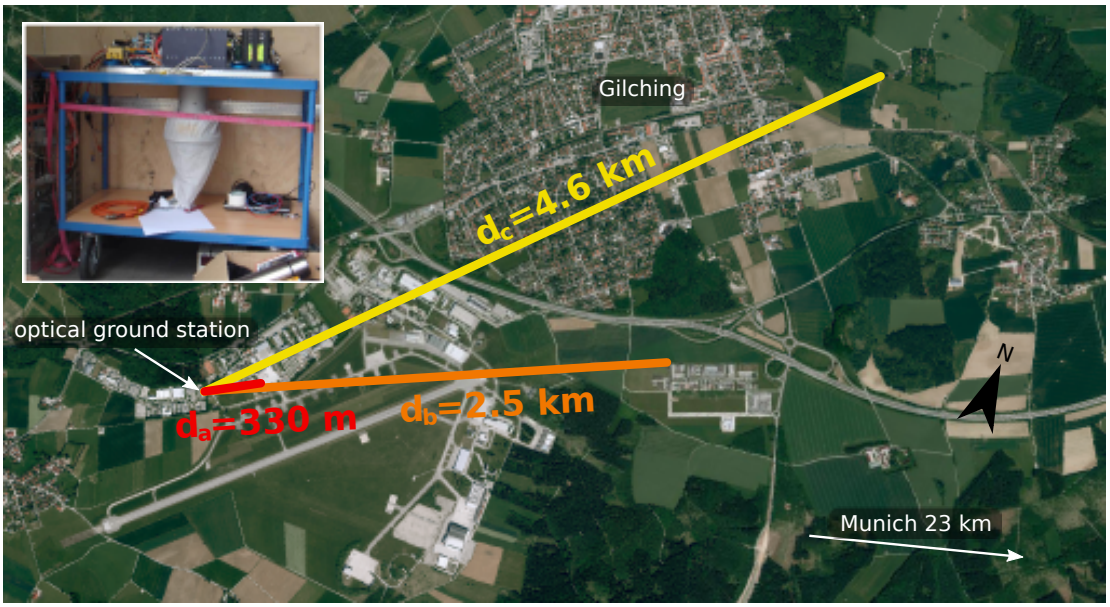





**Figure 4.1:** Location of the ground to ground test distances used to evaluate the correct operation of the system . The short link $d_a$ was also used to line up the Alice pointing relative to the tracking axis before every flight. On $d_b$, the pointing and tracking could also be tried dynamically with the test vehicle accelerating on about 100 m. The inset shows the FELT2 mounted on the lab trolley in the car.

though prior lab tests with simulated fluctuations were positive, it turned out that the polarimeter was not able to provide reliable measurements of the polarizations received over the free-space link within an acceptable time. This was attributed to the work principle of the device [93]: Using only one photodiode, the polarimeter measures the polarization with the help of a rotating quarter wave plate and a fixed polarizer. The resulting signal is a combination of two sine curves and is evaluated for their relative phases and amplitudes to obtain the polarization orientation. While this measurement technique could in principle offer some robustness against asynchronous fluctuations, this was not the case and even with long measurement times (i.e., many revolutions of the wave plate) the acquired precision on the polarization angles was worse than $\pm 5^\circ$ what finally made a quasi closed loop scheme impossible.

While all other classical and quantum subsystems could be enabled without major obstacles, the calibration of the crucial QKD beam coalignment with the classical pointing axis (see also section 3.2.2) turned out to be sensitive to even the slightest deformation of the FELT2 breadboard.

## 4.2 Calibration of Coalignment and Beam Divergence

Preset in the lab on a distance of 50 m, the QKD pointing could be adjusted on the field test distances for optimal overlap with the pointing axis while the tracking system was in operation. The custom optical breadbord of the FELT2, however, turned out not to be stiff enough to maintain the alignment reliable over time scales beyond a day: The slightest stress on the FELT2 setup manifested itself by a deviation of the crypto beam causing a nearly complete loss of signal. While the shock mounts mediate or damp most of the forces that potentially change the shape of the breadboard, deviations of the QKD pointing relative to the classical system were especially evident when tying together the cables connecting the terminal to the laptops, antennas and power supplies. While this could be avoided, there was still the possibility that the coalignment would get lost in flight due to single shocks or temperature expansion of individual components.

To provide the best possible coalignment in the beginning of each experiment, it was readjusted right before every flight. For this procedure, the short test distance $d_a$ to the airfield was used, where the aircraft could be placed in a direct line of sight to the OGS. There, a target (fig. 4.2) was placed with a beacon laser emitting from an open fiber end in its center. The FELT2 could track this target and the position of the QKD beam was visualized using an infrared capable linear camera. The image was sent via wireless LAN back to the aircraft in real time, where it enabled an adjustment of the Alice pointing for best possible overlap with the tracking axis.

While this procedure ensures an optimal setting right before the aircraft engines start, there is no guarantee that it is maintained until the QKD transmission actually takes place. Therefore, a scheme for in flight fine calibration was developed.

### 4.2.1 Scheme for Online Pointing Error Compensation

To compensate systematic Alice pointing errors, which might arise during taxiing, takeoff and due to varying temperatures in the terminal, a possibility to fine adjust the QKD beam pointing in flight had to be developed.

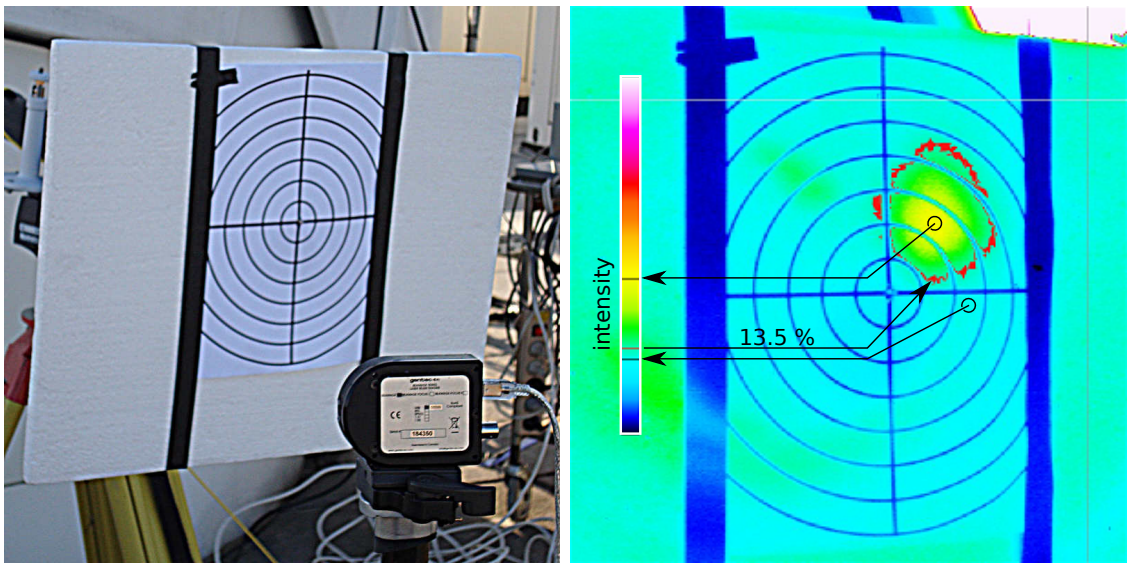
The solution makes use of the wide divergence of the FELT2 laser (3 mrad) compared to the QKD beam with a divergence of 182 µrad only: In the FELT2 FPA control loop, normally the DSP aims to keep the incoming light on the center of the quadrant diode controlling the voice coil mirror accordingly (explained in fig. 3.5). Here, the DSP firmware was altered to accept an offset vector $\mathbf{c} = (c_x, c_v)$, which was subtracted from the error signal[1]: Rather than on the center $(0, 0)$ of the quadrant diode, the control loop aims to keep the focused OGS beacon at $\mathbf{c}$. This results in an intentional error of the FELT2 receiver orientation, which, however, is not critical due to the wide field of view of the FELT2 fine tracking system (3.3 mrad). The accompanying small misspointing of the terminal beacon does not harm the operation of the classical system, either: Due to its wide divergence, enough light can still be caught by the OGS tracking and data communication sensors.

In this way, the fine control of the QKD pointing could be enabled in software and no changes to the already certified terminal hardware were necessary.

### 4.2.2 Measurement of QKD Beam Divergence

The divergence of the beam was set and measured here by reducing the beam diameter as much as possible moving the collimation lens in front of the pinhole (fig. 3.9). Of course, this strategy does not converge exactly to the minimum divergence possible because the theoretically smallest beam diameter in the distance of $d_a = 300$ m occurs for an intermediate waist near to the terminal. As this waist, is only slightly smaller than the telescope aperture, the divergence is only a few µrad wider compared to the optimal case (see section 3.3.2). In the experiment, however, much wider beams were observed on the target than theoretically predicted. This is because the beam, as prepared by Alice, is not perfectly gaussian and the FELT2 terminal optics is entered only parallel to the axis. Hence, it is not clear, to which extent gaussian beam propagation is applicable. To get an estimate for the actual divergence of the QKD beam, the $1/e^2$ level was visualized on the camera image 4.2(b)

[1] These coordinates do not represent linear distances on the quadrant diode but rather voltage differences between its top and bottom (left and right respectively) halves. The resulting beam displacement is not linear and strongly depends on the focus shape. Therefore, there is no reliable relation between the actual angular variation and the values of $\mathbf{c}$.




(a) (b)

**Figure 4.2:** Calibration of the Alice alignment relative to the tracking axis. **a:** In the center of the target, an open fiber end emits a beacon the FELT2 can track on. Once the tracking is locked, the infrared capable camera makes the Alice beam visible on the target. **b:** From the linear camera image, one can deduce the $1/e^2 \approx 13.5\,\%$ boundary of the Alice beam marked here in red with the help of the color bar. The distance of the target rings is $\Delta r = 20\,\text{mm}$. By adjusting the coupling mirrors of the Alice, the QKD beam could be centered on the target to establish the coalignment.

and the diameter $d(330\text{ m}) \approx 60\,\text{mm}$ could be measured with the help of the target rings. From this, the divergence angle of the QKD beam is derived geometrically to be 182 µrad which corresponds to the divergence of a Gaussian beam with diameter 6 mm at the $1/e^2$ level. The beam diameter in a distance of 20 km, i.e., at the OGS is 3.6 m.

Under good seeing conditions, the Fried parameter can be well above $r_0 = 10\,\text{cm}$ which would allow a telescope with aperture $d > r_0$ to reach an angular resolution of 8.5 µrad. This shows, that the collimation of the beam in the current configuration is indeed limited by the effective telescope aperture and not by the turbulence in the atmosphere. Thus, significant improvements are possible with larger telescopes.

## 4.3 Experimental Flights

As the experiments had to be performed in the dark to reduce the noise due to stray light, the flight campaign had to take place in winter in order to leave enough time

between sunset around 18:00 and the closing of the special airport Oberpfaffenhofen at 21:00. Furthermore, the dates were chosen to be around new moon to avoid this source of background stray light, too.

At first, the flights were planned in the beginning of November 2010. Due to delays in the airworthiness certification process, however, these dates had to be abandoned and the experimental flight campaign was finally scheduled in the week from February 28 to March 4 2011 (new moon on March 4).

While the first day was reserved for the system integration into the aircraft and the final certification, four flights were planned on the remaining days. Due to insufficient weather conditions, some starts had to be canceled as for aircraft operation according to the visual flight rules (VFR) a certain minimum visual range and distance from clouds has to be maintained. Fortunately, the opportunity of additional flights in the following week opened up. Table 4.1 and Figure 4.3 give an overview of the campaign with the three flights actually carried out and a brief description of the results.

### 4.3.1 Atmospheric conditions

During the final flight at which the QKD demonstration analyzed in chapter 5 was performed, it was slightly hazy. There was a closed cloud cover restricting the flight altitude to $\approx 1100\,\mathrm{m}$ above ground. Direct light from the first quarter moon (located in the west, elevation 30.8° at 19:55) thus was shaded. A diffuse illumination, however, was produced by the clouds which also reflected the Munich and suburban lights.

### 4.3.2 Spectral Filtering

To suppress background light, an interference filter was used. However, as neither this filter nor the Alice laser diodes were temperature controlled, filters with different central wavelengths were tried in the experiment to maximize signal coupling. During the key transmission analyzed here, the ambient temperature at the OGS was 7.6 °C and the temperature of the laser diodes was 44.1 °C to 44.8 °C (fig. 4.5). This led to an increase in the emitted wavelengths and a shift to the blue of the interference filter. Under these conditions, a filter with a nominal central wavelength of 860 nm and a width of 10 nm (full-width at half-maximum (FWHM)) was found to provide the best results (see § 3.4). The rather wide spectral width of this filter was chosen to account for temperature fluctuations and the resulting relative variations between the filter and the laser diodes.

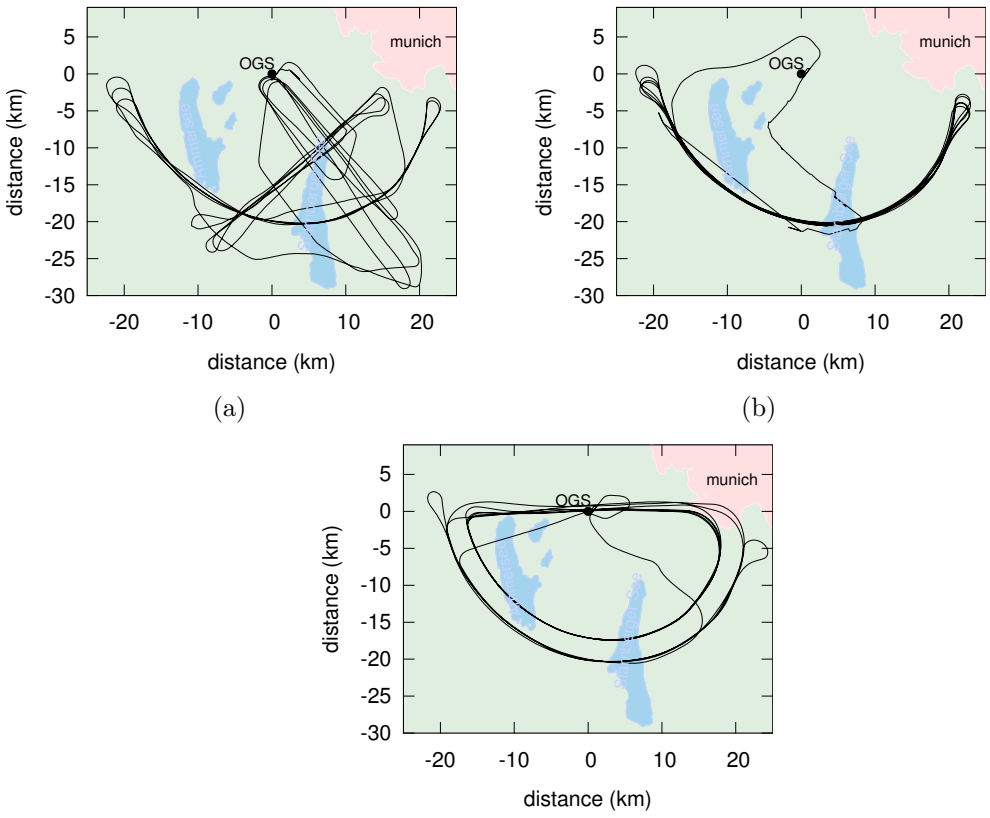



**Figure 4.3:** Flight tracks for all three flights. **a:** First flight performed on March 2. The pointing and tracking on circular, radial and tangential paths was tested and had still to be optimized. The correction of the fine pointing as explained in section 4.2.1 was tested. The most stable results could be obtained on the circular paths which were, thus, used exclusively on the following days. **b:** Second flight, March 3. Slowly modulated bright light and also pulses with a mean intensity of 50 photons could successfully be registered at the ground station. Further experience with the fine pointing compensation was gained. **c:** Third flight, March 9. On the first two passages (note the two turning loops) the pointing was optimized. It emerged, that the compensation values were different and the results for the clockwise track were better. Thus all following passages were performed clockwise. On the way back along the diameter, the plane went at a higher speed, therefore it only took about 6 min. This time was used for recalibration of the Alice pulse intensities. On the third passage a QKD transmission with mean intensity of 1 photon per pulse was achieved for 12 min which showed a mean error rate of 4 % at a mean sifted key rate of 450 bit/s. On the fourth passage, the data analyzed in chapter 5 was obtained with a mean pulse intensity of 0.5 photons per pulse. After three further passages which were used to optimize the telescope coupling, a cable of the telemetry antenna at the OGS broke and no further experiments could be performed. Especially the tracks with smaller radius (18 km) could not be tested as the repair on the ground took too long.

**Table 4.1:** Overview of the flight campaign schedule with brief results.

| | **date** | | **results** |
|---|---|---|---|
| Mo | 28.2.2011 | mounting of terminal into aircraft | final certification |
| Di | 1.3.2011 | flight canceled (bad weather conditions) | |
| Mi | 2.3.2011 | first flight | tracking and pointing optimization |
| Do | 3.3.2011 | second flight | bright CW and pulsed tests (50 photons/pulse) |
| Fr | 4.3.2011 | flight canceled (technical problems OGS[†]) | |
| Mo | 7.3.2011 | flight canceled (technical problems sat phone[‡]) | |
| Di | 8.3.2011 | flight canceled (bad weather conditions) | |
| Mi | 9.3.2011 | third flight | QKD operation (0.5 photons/pulse) |

[†] Due to the failure of a PCI real time clock in one of the OGS computers, the controlling LabVIEW software refused to work. The issue could not be resolved in time.

[‡] For this day, only a newer version of the satellite phone was available. Unfortunately it was not compatible with the external antenna mounted on the aircraft. This issue was discovered to late and as a consequence, the experiment coordination would not have been possible in flight.

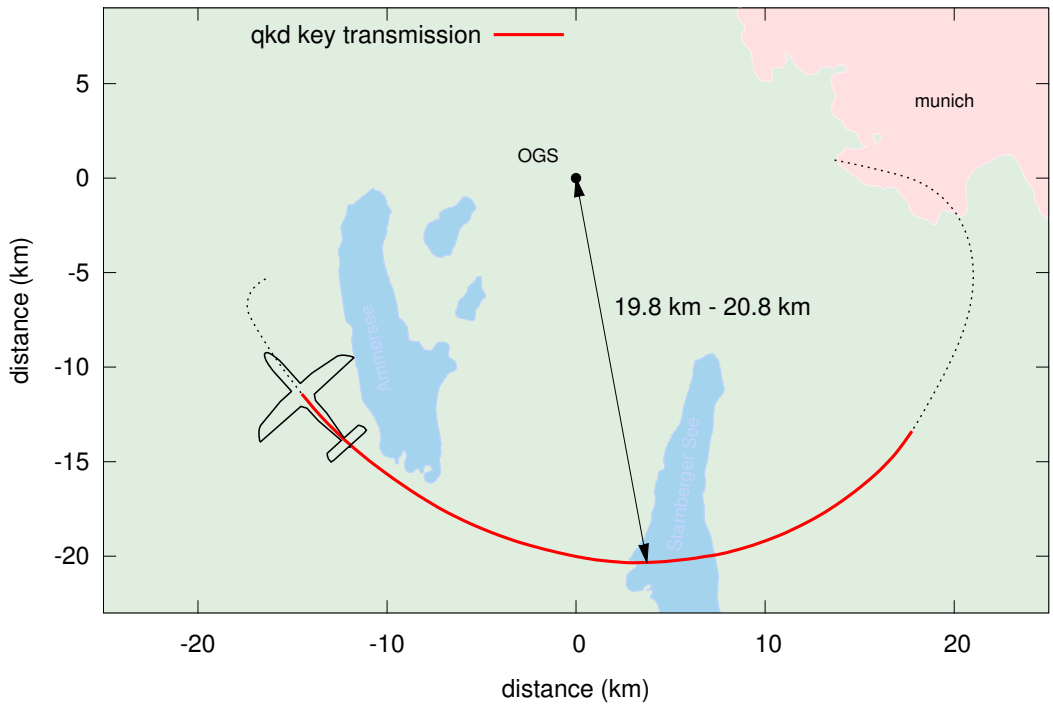



**Figure 4.4:** Flight track followed during the key exchange. Due to airspace regulations concerning the Munich airport, the plane could not go far north of the OGS. Therefore, the experiment was performed on half circles around the OGS. The red line marks the duration of 604 s of the actual key exchange analyzed in chapter 5.

### 4.3.3 Flight Track

For the first experiment, a circular flight track around the OGS was planned, as the relative position between the aircraft and the OGS does not change much in this scenario. Only small fluctuations due to turbulences and a slight variation from the tangential orientation due to wind are to be expected. Therefore, the circular track promises to be most friendly concerning pointing optimization as planned in section 4.2.1 and also eliminated the need for a refocusing of the OGS telescope. Moreover, a manual compensation of the polarizations could have worked in case the automatic system described in section 3.5 had failed. Other tracks had been projected (tangential, radial) and approved by the air traffic control. There were, however, no QKD experiments performed on these tracks due to a lack of time.

The aircraft was not allowed to go far north of the OGS, as there already begins the airspace controlled by the Munich airport. Hence, the actual track was the southern half circle illustrated in figure 4.4. Moreover, slight variations of the coalignment with the telescope pointing to the right or to the left of the aircraft

made it favorable to only fine adjust for one direction and taking the short way back along the west-east diameter.

For the track radius, a compromise had to be found: At a distance of 20 km, the minimum possible aircraft speed of around 290 km/h translates to an angular speed of 4.0 mrad/s. While a smaller distance in principle promises increased coupling for the QKD beam, higher angular speeds would have degraded the OGS pointing accuracy due to the telescope mount starting to vibrate. The flight height was 1100 m above ground governed by the meteorological conditions, as the VFR demand a certain vertical distance to the cloud cover.

With the given parameters, one passage along the half circle takes about 13 min and the way back to the start about 8.5 min. On the narrow curved path in the beginning and the end of the circular track, the aircraft roll angle (longitudinal axis) can get large. As the elevation angle of the CPA is limited to about 5° above its horizon, there are regions where no link is possible. Furthermore, considering a short time for link acquisition, the usable experiment time per passage is about 10 to 12 min.

### 4.3.4 In Flight Pointing Optimization

Once the aircraft reached its final height and the telescope link was established successfully, the first task in flight was a fine adjustment of the QKD pointing to eliminate any residual alignment errors. As described in section 4.2.1, a pointing control offset vector $\mathbf{c}$ was searched, optimizing the Alice-Bob coupling. For this purpose, the Alice attenuator was swung out and a slowly modulated periodic pattern was sent with all four laser diodes at full power (2 s on – 0.5 s off). This produced a distinctive response at the receiver that also allowed to distinguish background and signal contribution. The OGS operators announced the receiver count rates over satellite phone back to the aircraft, where the offset vector $\mathbf{c}$ was recursively modified and optimized. After some experience from the second flight, on the third flight this process could be completed during the first two passages.

### 4.3.5 Key Exchange

Immediately prior to the key exchange, the Alice pulse intensities were calibrated to $\mu = 0.5$ photons/pulse. Table 4.2 shows the measurements of $\mu$ after this calibration and directly after the key exchange. The table reveals a slight decrease of the pulse intensities during the experiment of 2 % to 4 %. The reason is most likely the temperature change of 0.8°C in the relevant time interval (see fig. 4.5).

The Alice QKD transmitter was enabled right at the beginning of the passage and the key exchange began as soon as a stable link was established. The tracking was lost 604 s later and the key exchange thereby terminated. Unfortunately, soon after this transmission, a cable feeding the OGS telemetry antenna broke and could

**Table 4.2:** Mean photon number per pulse measured for the four Alice laser diodes directly before and after the key transmission with the integrated photodiode.

| **time** | **polarization state** | | | | |
|---|---|---|---|---|---|
| | $\|+45\rangle$ | $\|V\rangle$ | $\|-45\rangle$ | $\|V\rangle$ | mean |
| (hh:mm:ss) | (photons/pulse) | | | | |
| 19:48:36 | 0.50 | 0.50 | 0.48 | 0.50 | 0.49 |
| 19:59:18 | 0.48 | 0.49 | 0.48 | 0.48 | 0.48 |

not be fixed in the remaining time before the airplane had to land ($\approx$20:45). This is why further tests – projected with a longer PRBS as described in section 3.3.1 – could not be performed anymore.

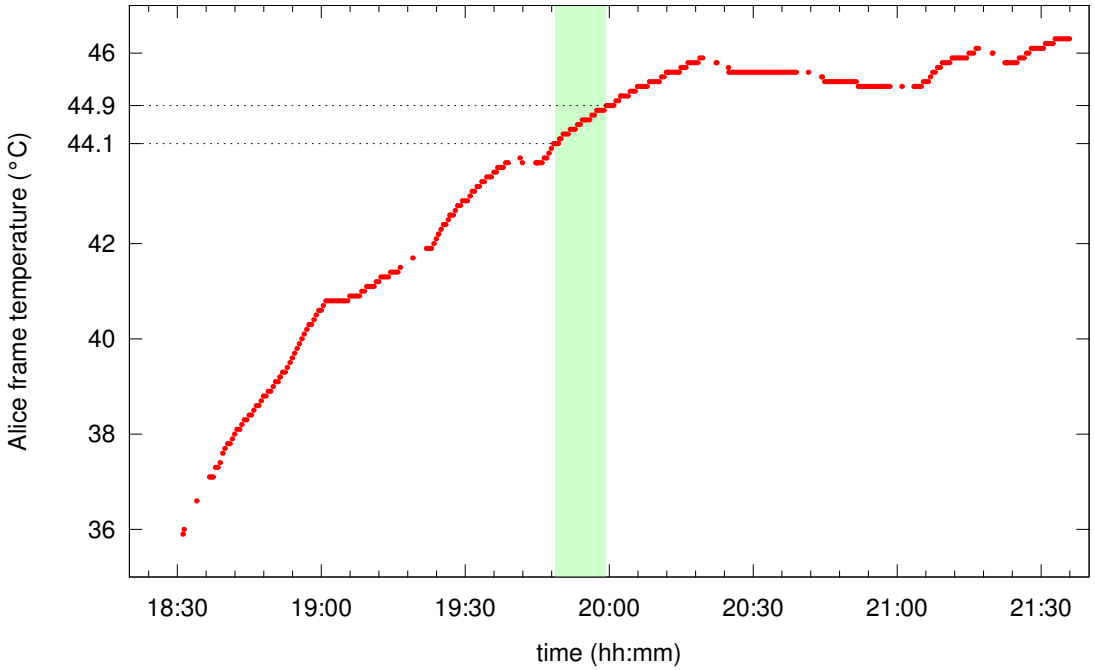



**Figure 4.5:** Temperature of the Alice framework close to the laser diode mounts for the duration of the experiment. During the key exchange (area shaded green) there was a temperature increase of 0.8°C.

# Chapter 5

# Results and Analysis

This chapter is dedicated to the post processing and analysis of the data generated in the flight experiments. While there was an online synchronization and sifting done, this was primarily intended to provide fast feedback about the QKD performance and estimates for the transmission parameters. Here, a more detailed and adapted analysis will be described allowing for optimization of the filtering in order to maximize the final key rate [40].

In this experiment, however, technological simplifications were adopted. While the solutions are in principle practicable and have already been shown, the main focus here was to enable the demonstration with only about one year of preparation and in the limited time, the aircraft was available for experiments. Therefore, the secure key rate achievable in this experiment has to be calculated based on assumptions, which are detailed here.

For evaluation of the quantum transmission, the raw data files as produced by the Bob timestamping unit were used. Using custom software written in `C`, the relevant intervals were extracted, count rates evaluated, filter applied, and finally, all quantities relevant for the QKD post processing were determined. Further calculations and optimizations were done in Mathematica.

## 5.1 Raw Event Rates and Signal Recovery

During the demonstration, the receiver detectors experienced a significant background event rate of $r_0 \approx 3500\,\mathrm{s}^{-1}$ all together when pointing into the night sky. Roughly half of this background was caused by stray light, the other half was due to detector dark counts. When the tracking is locked on the aircraft terminal, an additional background source becomes visible: The anti-collision beacon flash tubes located on top and underneath the aircraft fuselage. These red lights produce short (1 ms to 3 ms) bright flashes with a frequency of 0.5 Hz to 1 Hz and may not be turned off during flight. Their pattern is clearly visible in Bob's raw count rate (fig. 5.1). The red and green navigation lights at the wingtips, however, do not

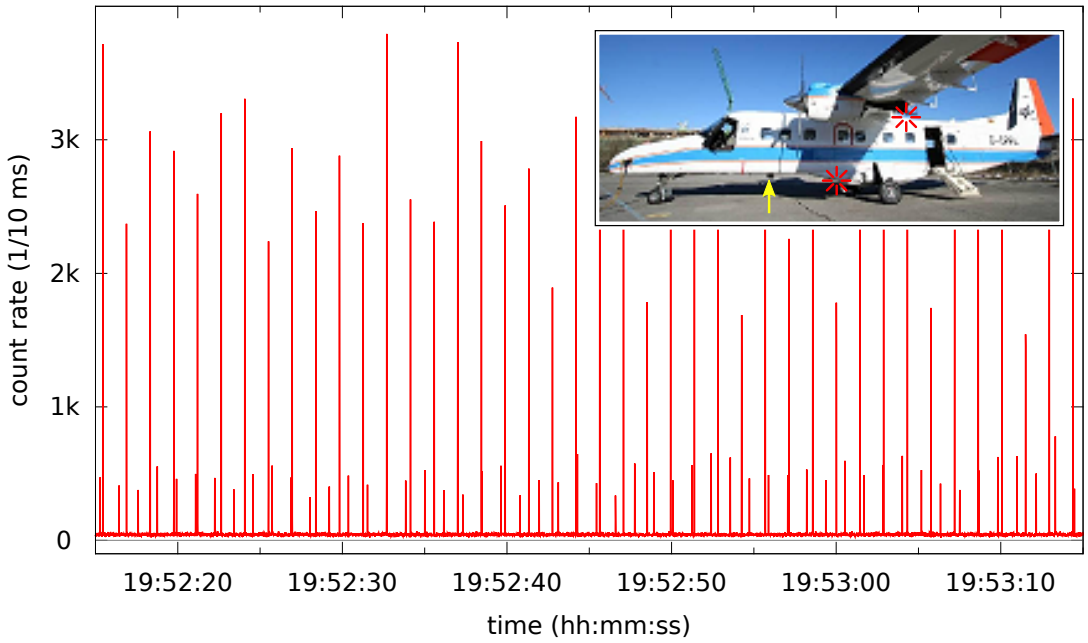



**Figure 5.1:** Raw detector count rate for a representative interval of 30 s. The signal is dominated by the anti collision flashes which appear as short spikes of 1 ms to 3 ms length. The inset displays the location of the two flash tubes (red stars), which can be distinguished due to their amplitude and their slightly different frequencies. The brighter one is located near the optical dome (yellow arrow) underneath the aircraft, the other is located on the back of the fuselage.

contribute significantly to the dark count rate. The cabin lighting was disabled as far as possible to avoid additional noise from light shining through the aircraft windows.

Before any further analysis, the raw signals are filtered to remove the anti collision flashes. This is done by a simple threshold filter, which discards intervals of 10 ms in case the count rate is higher than on average. However, with the frequencies of the flashes being about 0.69 Hz and 0.85 Hz, 1.5 % of the transmission time is discarded.

### 5.1.1 Transmitter – Receiver Synchronization

In order to perform a signal recovery and subsequently the sifting, a transcription of the events registered in units of real time has to be performed to associate measured signals to time slot numbers shared between Alice and Bob. Yet, as the Alice clock is transmitted via the classical optical link as a 100 MHz signal, the whole system is operated in principle synchronously. Only the phase of the 10 MHz repetition

frequency remains to be determined. As described in section 3.7.2, this phase can be retrieved from a time histogram of the registered events to fully synchronize the system.

The remaining task is to find the start condition in the data stream. While this is typically accomplished by the introduction of synchronization headers in the sent stream [88], here the cyclic nature of the transmitted signal allows to find the sequence start by a cross correlation of the time filtered string with the original PRBS (see also § 3.3.1).

### 5.1.2 Diode Delay Compensation

As mentioned already in section 3.3.1, the originally projected emitter coupled logic (ECL) delay ICs could not be assembled on the main electronics board in the Alice module due to their significant heat dissipation. This results in an individual delay between the diode emission times and the 10 MHz beat (see fig. 3.8), which has to be taken into account when time filtering the receiver events. As in this experiment, the four polarizations were sent sequentially, this is straight forward: A histogram of the events over their arrival times modulo 400 ns (i.e. four time slots) reveals the mean time shifts for each diode and time filtering is done around these positions. In this way, the compensation of the delays is applied on the transmitted pulses and does not influence the QBER. Significant individual delays of the four receiver channels are not considered here as no such evidence could be found in the time histograms of the received signals.

### 5.1.3 Temporal Signal Statistics and Filtering

The received clicks, even though synchronized, show an accumulated time jitter on their timestamps. This is due to a combination of the jitter in the clock interface from the Alice module to the FELT2, the optical transmission, the interfacing and clock recovery at the ground station, and of course the APD detection of the signal in the Bob module. Figure 5.2 shows a histogram of the detection times relative to the Bob clock. The width of 1.2 ns (FWHM) can be directly compared to the width of the transmitter pulses as documented in section 3.3.1 (fig. 3.8) as the same APD jitter is included in both measurements. Again assuming Gaussian statistics, a deconvolution determines the time jitter of the clock synchronization system alone to 0.66 ns.

Once the synchronization is established, time filtering can suppress background events significantly: Accepting only events from the Bob module within a time window of width $\tau_f$ around the expected time of arrival in the $f = 10\,\mathrm{MHz}$ beat, the fraction of all registered background and dark counts which actually enter the raw key data is reduced to $\tau_f f$. While, evidently from figure 5.2, the signal to noise ratio (SNR) is best for narrow time filtering. However, the more restrictive the

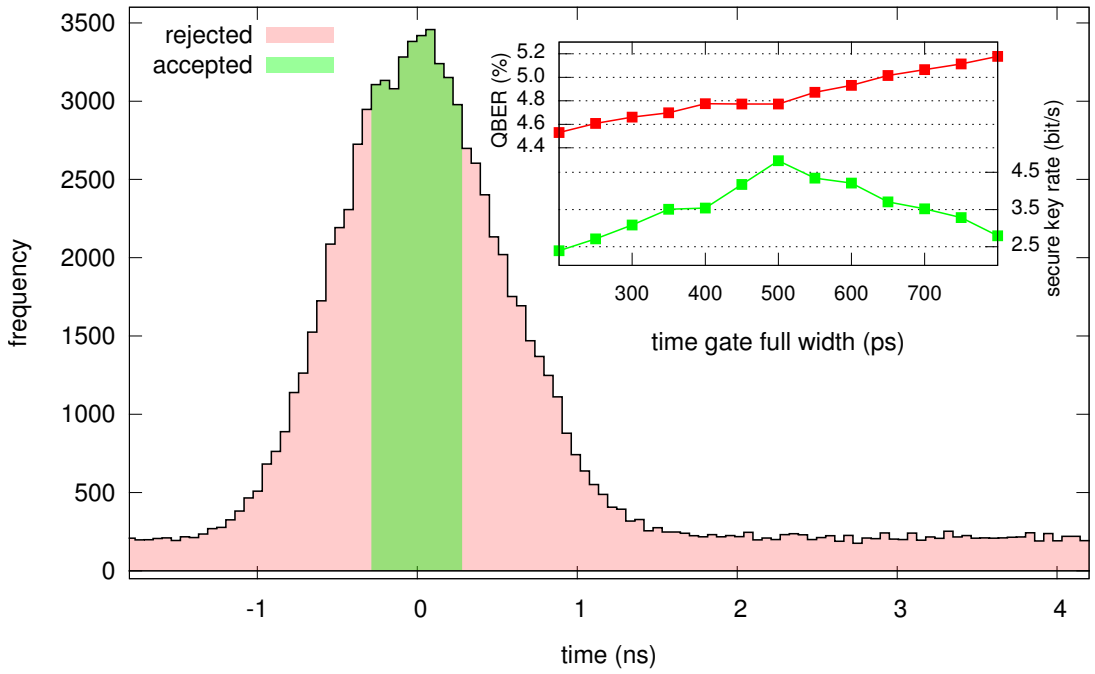



**Figure 5.2:** Time histogram of the Bob detections relative to the expected arrival times. The green region visualizes the time filtering with an acceptance window full width of 0.5 ns. Events in the red region are discarded in the time filtering. Timestamps are corrected for delays of individual diodes due to the Alice pulse generation. The inset shows the QBER and the secure key rate to be expected after privacy amplification over the time gate width (detailed in § 5.3.2).

applied filtering is, the more signal counts are discarded, too. As a consequence, one has a trade-off between raw key rate or length and the amount of noise, which is here observed as QBER. The final figure of merit is of course the secure key rate distillable from the raw data in privacy amplification. The situation for this experiment – forestalled the analysis in section 5.3.2 – is depicted in figure 5.2: A time window of 0.5 ns maximizes the final secure key rate. The signal loss due to this restrictive filtering is 4.2 dB, however, it yields a QBER of 4.77 % as the background probability in these short time windows is only $r_0\tau_f = 1.75 \times 10^{-6}$ with the background event rate $r_0$.

Subsequently to the time filtering, a second filter is applied in software to eliminate intervals with poor signal to noise ratio: For every second, the registered timestamps are histogrammed modulo 100 ns similar to figure 5.2. If the contrast between the maximum of the histogram (for increased stability averaged over several histogram bins) and the noise background drops below an empirically determined threshold, the data of this second is discarded. This eliminates transmission intervals suffering from short signal faints or high background, which would otherwise contribute sifted key with a QBER of approximately 50 %. The usable transmission time is reduced by this filter by 29 nonconsecutive seconds to $T = 575\,\mathrm{s}$. Starting from an overall transmission duration of 604 s, this corresponds to a factor of 0.95. However, it has to be stressed that this is no post selection of intervals with low QBER, as the filter is applied before the sifting. Otherwise, an eavesdropper might be able to have Bob discard individual intervals by selectively introducing noise and construct an attack thereof.

## 5.2 Transmission Parameters

### 5.2.1 Channel Attenuation

An intuitive estimate for the channel attenuation $\eta$ can be formulated as the fraction of detection events after time filtering $N_t$ over the number of sent pulses $T \times f$ and the mean photon number per pulse $\mu$:

$$\eta \approx \frac{N_t}{T f \mu} \tag{5.1}$$

Here, $\eta$ shall comprise all attenuation from outside the Alice enclave to the received signals accepted after filtering. The above estimate, however, disregards the threshold behavior of the single photon detectors, which leads to a different channel transmittance $\eta_i$ for every $i$-photon state [94]:

$$\eta_i = 1 - (1 - \eta)^i \tag{5.2}$$

**Table 5.1:** Terminology: yield ($Y$) and gain ($Q$) values.

| Symbol | Quantity | Description |
|---|---|---|
| $Y_i$ | yield | the probability to register a sent pulse that initially contained $i$-photons. The $Y_i$ describe the quantum channel, their values, however, might be arbitrarily modified by an adversary. |
| $Q_i$ | gain | the yield times the probability that Alice actually sends an $i$-photon pulse |
| $Q_\mu$ | gain | probability to register an event due to a pulse sent with mean intensity $\mu$ (sum over $Q_i$, see eq. (5.4)). |

This expresses the probability that at least one of $i$ photons in the original pulse triggers a detector click. It is thus necessary to investigate the calculation of the channel attenuation in more detail[1].

Starting point is the so called Yield $Y_i$, the probability to obtain a detection event from an $i$-photon pulse emitted from Alice [94] or in other words the attenuation for $i$-photon pulses:

$$\begin{aligned} Y_i &= Y_0 + \eta_i - Y_0\eta_i \\ &\approx Y_0 + \eta_i, \end{aligned} \tag{5.3}$$

with the probability for a dark count event $Y_0$ in case Alice did not send a pulse. The product of two small terms can be omitted here.

The actual registered fraction $Q_\mu$ of the sent poissonian states with mean photon number $\mu$ – the only figure directly accessible from the experiment to calculate the attenuation – can then be written as [94]

$$Q_\mu = \sum_{i=0}^{\infty} Q_i = \sum_{i=0}^{\infty} Y_i \frac{\mu^i \mathrm{e}^{-\mu}}{i!} \tag{5.4}$$

$$\overset{\text{eqs. (5.2), (5.3)}}{=} Y_0 + 1 - \mathrm{e}^{-\eta\mu} \tag{5.5}$$

$Q_\mu$ is called the gain of pulses with mean intensity $\mu$; the $Q_i$ are the gain of $i$-photon pulses respectively. However, the $Q_i$ are not accessible from the experiment, as the actual photon number of a pulse leaving Alice is only defined on average and

[1] The ad hoc estimation for the channel attenuation in eq. (5.1) actually delivers good results as will be shown after equation (5.6) . Nevertheless, the calculation of the attenuation shall be used to introduce the quantities needed later.

**Table 5.2:** Contributions to the overall attenuation. The attenuation of beam wander and broadening was calculated and found to be negligible in this scenario [83].

| | | |
|---|---|---|
| time filtering | −4.2 dB | see section 5.1.3 |
| detector efficiency | −4.2 dB | APD efficiency [85] |
| interference filter | ≈ −3 dB | peak transmission −2.2 dB |
| OGS optics | −3 dB | non ideal optics [83] |
| atmospheric att. | −6 dB | simulation [83], visibility 50 km |
| OGS collection eff. | −15 dB | link budget calculations [83] |
| tracking losses | −4 dB | link budget calculations [83] |
| diode coupling losses | −2 dB | link budget calculations [83] |
| estimated total att. | −41.4 dB | |
| observed total att. | −42.7 dB | see equation (5.6) |

once the pulse has arrived at Bob's its photon number might have changed due to the channel attenuation. The meaning of yield and gain values is summarized in table 5.1.

The channel attenuation can now conveniently be calculated from (5.4) with the values from the experiment $Q_\mu = 2.86 \times 10^{-5}$ and $Y_0 = 1.75 \times 10^{-6}$:

$$\eta = \frac{-\ln(1 - Q_\mu + Y_0)}{\mu} = 5.37 \times 10^{-5} = -42.7 \text{ dB} \tag{5.6}$$

For comparison, the estimation according to equation (5.1) yields $\eta \approx 5.73 \times 10^{-5} = 42.4\,\text{dB}$.

As already mentioned, this value comprises all attenuating effects between the FELT2 terminal dome, which represents the border of the secure Alice enclave, and the registered events after time filtering. The complete link budget is summarized in 5.2. Especially the contributions to the attenuation due to atmospheric effects (attenuation, turbulence) are simulated values only, yet all contributions sum up to −41.4 dB which is close to the observed value of −42.7 dB.

### 5.2.2 Sifted Key Rate and QBER

After the synchronization and time filtering as described above (§ 5.1.1), the BB84 protocol can proceed with the sifting process. The resulting sifted key is constructed

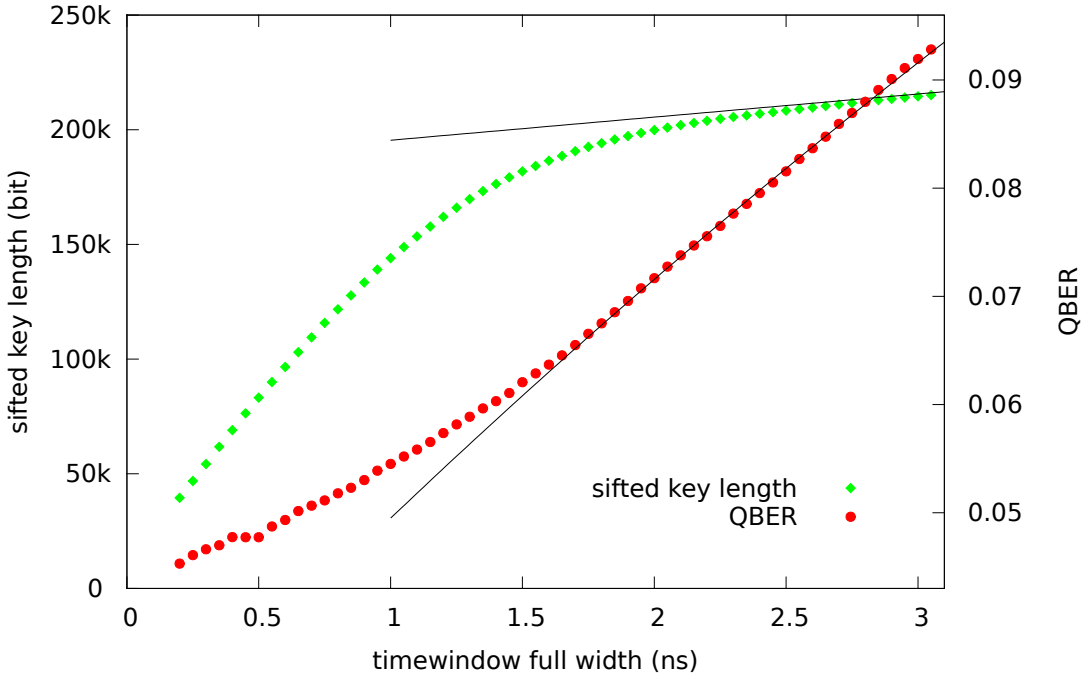



**Figure 5.3:** QBER and sifted key length over the time filtering full window width $\tau_f$. The straight lines indicate the behavior for $\tau_f$ longer than the width of the received pulses. As the acceptance window is widened, more and more signal can be accepted, but at the same time, more background events contribute to the sifted key. At some point, the gain in sifted key is entirely due to background events and the slope becomes proportional to the background count rate. Similarly, the QBER increases due to the successively larger fraction of background events in the sifted key and would eventually saturate at 0.5.

from all qubits Bob detected and for which his basis choice agrees with Alice's and should ideally be identical for both partners. Yet, in the presence of noise, it is inevitable that a certain number of errors occur in the sifted key, which give rise to the so called quantum bit error ratio QBER. As already indicated in section 5.1.3, the actual sifted key rate $\dot{N}_\mathrm{s}$ and the QBER after time filtering are dependent on the filtering parameter $\tau_f$. The rates for the analyzed data set are depicted in figure 5.3 for 0.2 ns $\leq \tau_f \leq$ 3 ns. The asymptotic behavior of the sifted key length is nicely correlated with the background event rate $r_0$ as for $\tau_f$ larger than the received pulse width

$$\frac{\delta N_\mathrm{s}}{\delta \tau_f} = \frac{r_0 N_\mathrm{sent}}{2} \tag{5.7}$$

holds – half of the background events occur in the "wrong" basis and thus do not contribute. $N_\mathrm{sent} = Tf = 5.75 \times 10^9$ (for $T = 575\,\mathrm{s}$ and $f = 10\,\mathrm{MHz}$) is the total number of signals sent and at the same time the number of receiver time slots in the usable experiment time $T$. The ordinate intersection estimates (hypothetical) the total number of signals after sifting $N_\mathrm{rec}/2 = 185360$ present in the data set (without background events and before time filtering – this number is of course not accessible as a perfect signal filtering is not possible).

Similarly, the QBER increases with $\tau_f$ as the SNR gets worse. Its evolution for large $\tau_f$ indicated in figure 5.3 is

$$e = \frac{E_\mathrm{sig} + \tau_f r_0 N_\mathrm{sent}/2}{N_\mathrm{rec} + \tau_f r_0 N_\mathrm{sent}}, \tag{5.8}$$

which estimates the QBER $e$ as the fraction of erroneous bits due to signal ($E_\mathrm{sig}$) and background events in the total number of bits. (5.8) would eventually saturate and approach 0.5 for larger $\tau_f$ corresponding to the case of a sifted key composed almost entirely from background events. The constant number $E_\mathrm{sig}/N_\mathrm{rec}$ can be regarded as the QBER of the signal in the absence of background events. In the notation introduced above, one can also calculate this technical error as [95]:

$$e_\mathrm{tech} = \frac{eQ_\mu - Y_0/2}{(1 - \mathrm{e}^{-\eta\mu})} \tag{5.9}$$

For the optimal $\tau_f = 0.5\,\mathrm{ns}$ (see analysis in section 5.3.2), the QBER and the sifted key rate are plotted in figure 5.4 for intervals of one second per data point. The mean sifted key rate is $\dot{N}_\mathrm{s} = 145\,\mathrm{s}^{-1}$ ($N_\mathrm{s} = 82308$ for the whole passage) and the mean QBER is $e = 4.8\,\%$. The technical error according to equation (5.9) evaluates to $e_\mathrm{tech} = 1.8\,\%$. This shows the significant contribution of background noise in this experiment, but also proves the polarization compensation to work fine.

An analysis of the sifted key reveals that the distribution of "0" and "1" in the sifted key is biased ($p(0) = 42\,\%$ and $p(1) = 58\,\%$ respectively, see also tab. 5.3). This reduces the extractable randomness, which is given by the min entropy [96]

$$h_\infty(p) = -\log_2 p_\mathrm{max} \tag{5.10}$$

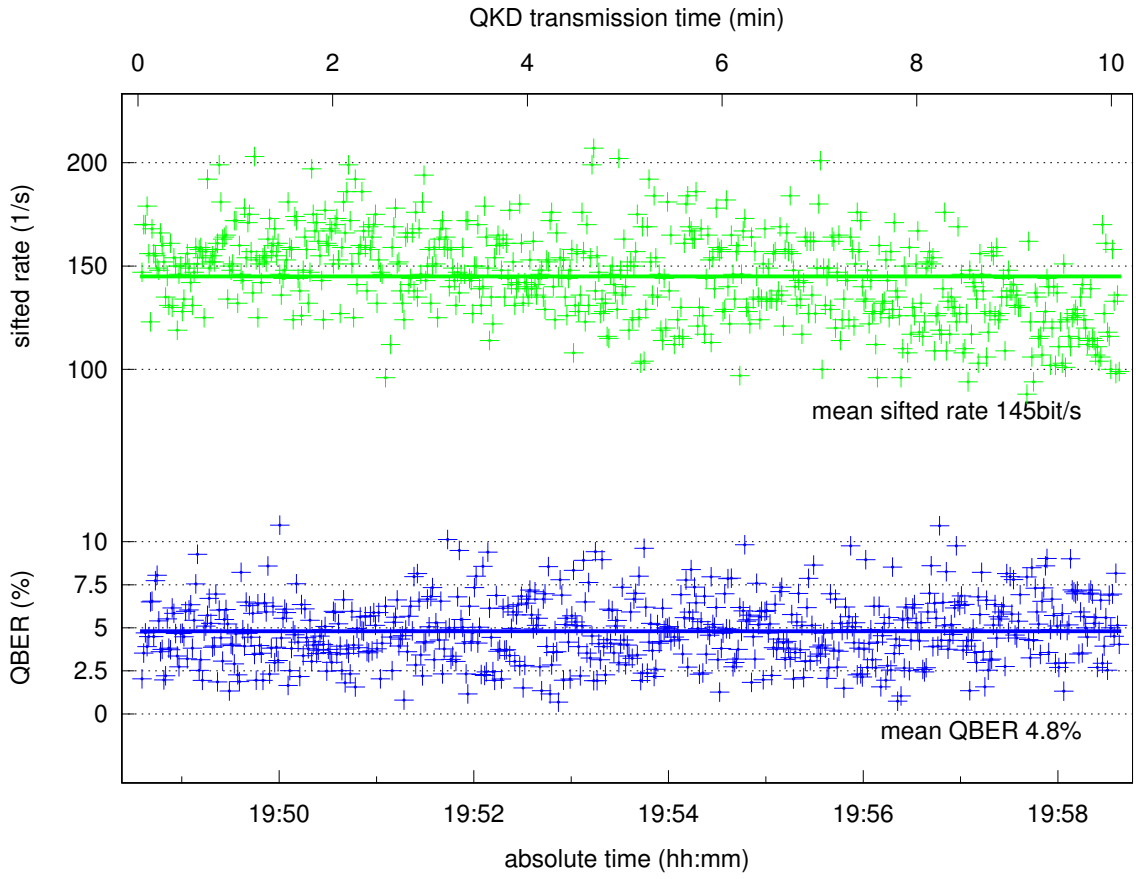



**Figure 5.4:** Sifted key rate (green) and QBER (blue) during the QKD transmission. Each point marks the average value for one second. Bold lines indicate mean values.

**Table 5.3:** Distribution of bit and basis values in the sifted key.

| | | **basis** | | **sum** |
|---|---|---|---|---|
| | | $\{H, V\}$ | $\{\pm 45\}$ | |
| **bit** | 1 | 32.5% | 25.5% | 58% |
| | 0 | 14% | 28% | 42% |
| **sum** | | 46.5% | 53.5% | |

of one sifted key bit to $h_\infty(0.42) = 0.786$ and has to be taken into account in privacy amplification. However, balancing the efficiencies of the four channels by additional attenuators in the stronger ones would reduce the size of the sifted key by 16 % only.

Similarly, the bases Bob used to measure are not equally distributed. 46.5 % of the sifted key bits were measured in the $\{\pm 45\}$ basis compared to 53.5 % measured in the $\{H, V\}$ basis. This asymmetry could increase the success probabilities for an eavesdropper in guessing the right basis. However, there are techniques to quantify this advantage for an attacker and to incorporate it in privacy amplification [66].

The reason for these aberrations are non uniform APD efficiencies of the four APDs, not perfectly balanced beam splitters in the Bob module and the attenuation introduced by the half wave plate for the diagonal basis. It is preferable and practicable to eliminate these asymmetries in the hardware compared to any post processing. Therefore, these effects will not be included in the evaluation of the achievable secure key rate.

Note that the classical communication normally involved in the sifting to agree on a subset of the sent bits as key bit candidates could be omitted here as firstly, Bob knows the PRBS used to generate the qubit stream and secondly Alice does not need to know the final key in this demonstration. It has to be stressed, however, that the classical channel would be readily available to perform this protocol task whenever QKD is implemented as an add-on for a conventional bidirectional communication system. Also here, the host system is fully operational even with the QKD hardware installed. Yet, the FELT2 at this stage only provides a unidirectional channel from the airplane to the ground, which is used here to transmit the clock. Current

development of the DLR system, however, will enable bidirectional communication soon.

### 5.2.3 Pointing Stability

The sifted key rates depicted in figure 5.4 already prove a stable pointing for the whole passage of about 10 min. The pointing accuracy of the terminal could further be characterized by the InGaAs-camera of the FELT2: As this device is not part of the pointing control loop, which uses the quadrant diode only to generate an error signal, it delivers an independent measure for the mean pointing error. Unfortunately, the camera's resolution is not sufficient for a precise determination of the pointing, as the OGS beacon remains on the center pixel most of the time. This means that only an upper bound of 150 µrad can be specified for the mean pointing error corresponding to the angular width of one camera pixel. The typical tracking accuracy of the OGS being stationary and therefore not subject to severe vibrations is about 20 µrad [83].

### 5.2.4 Polarization Compensation

The low technical error rate calculated in section 5.2.2 above, together with the fact that there was no manual interaction performed during the key transmission, already shows that the polarization compensation could be accomplished well with the designed strategy and hardware. Furthermore, there seem to be no severe systematic deviations in the compensation scheme as manual variation of the compensation parameters during prior passages could not improve the QBER.

The dynamic performance of the setup, however, can only be judged by the data in figure 5.4 and figure 5.5 together. The latter shows the actual pointing directions in the FELT2 for the duration of the QKD transmission together with the calculated orientations of the compensating wave plates. While the elevation angle is nearly stationary apart from noise, there is a variation of about 15° in the azimuth mirror position. This clearly shows the necessity of the online polarization control even on the circular path as the azimuth angle translates directly to the (linear) rotation of the polarization (see fig. 3.18) and would have caused directly a QBER of about 6.7 % in absence of other error sources. The main cause for the deviation of the aircraft orientation from the tangential direction was wind coming from the east.

While on the circular path the compensation scheme performed well, almost exclusively the effects of the azimuth rotation of the coudé beam path were relevant in this experiment. These lead to a rotation of the FoV and at the same time of the polarization, however, only around the axis perpendicular to the equator of the Poincaré sphere. This idealized situation would require the quarter wave plates to rotate exactly like the FoV and the half wave plate to rotate half the way. In the experiment, however, the distortions to the polarization were more complex so that

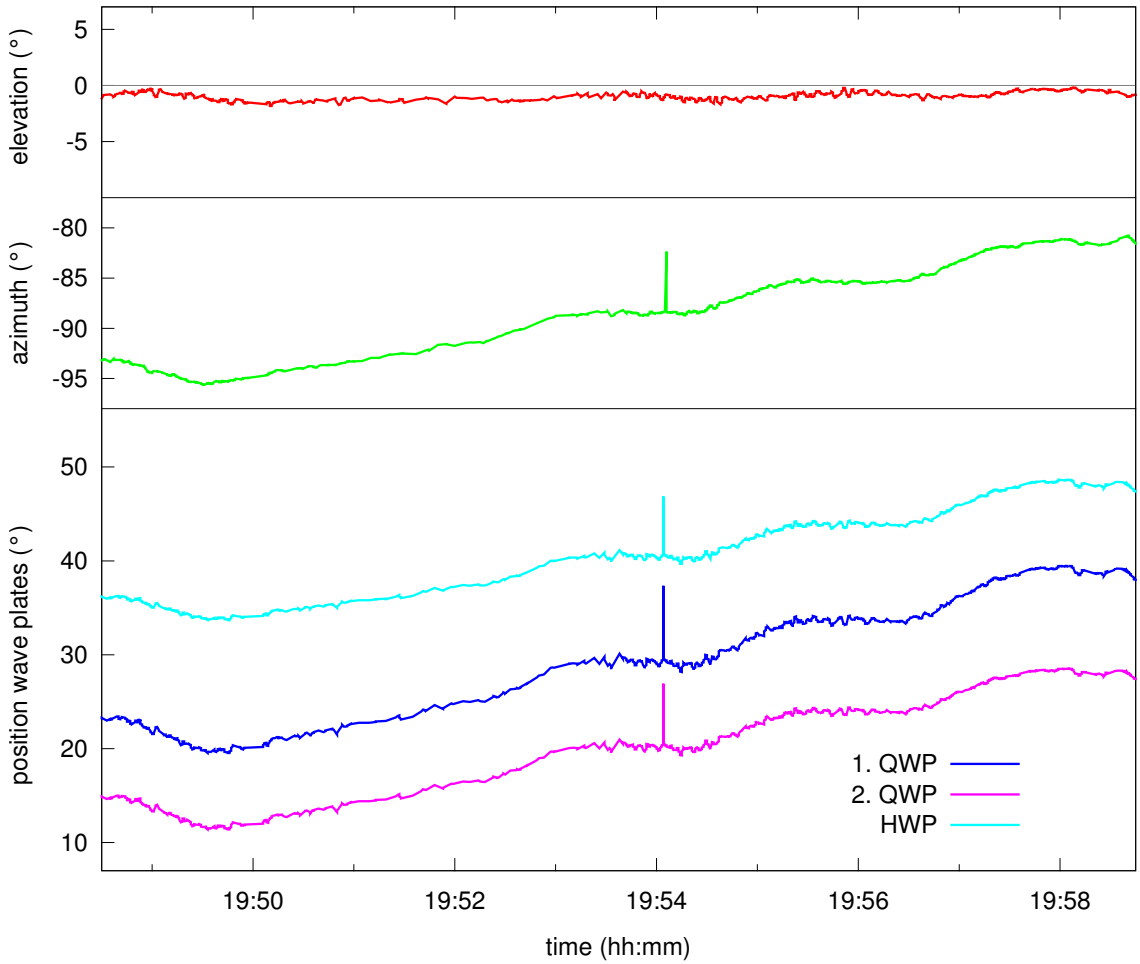



**Figure 5.5:** Angular positions of the FELT2 elevation and azimuth coarse pointing mirrors and the wave plates for polarization compensation for the duration of the QKD transmission. The variation of the azimuth in spite of the circular path is due to the wind coming from the east and the distance between the OGS and the center of the aircraft trajectory (the airport coordinates programmed in the aircraft auto pilot). The spike at 19:54 results from an uncaught transmission error of the UHF link.

this pure behavior is not apparent from figure 5.5 for the second quarter and the half wave plate.

As a consequence of the circular path, it is not possible to fully judge the performance of the compensation scheme for arbitrary polarization rotations on basis of the data aquired in this experiment. This will have to be characterized in a next step to enable future non circular trajectories of the airplane which will cause more complex polarization rotations. An important task will also be to identify and eliminate numerical weaknesses of the strategy described in section 3.5.4 under pathological starting conditions.

## 5.3 Secure Key Rate after Privacy Amplification

The sifted key rate together with the QBER and the repetition frequency, provide comprehensible and objective information about the performance and potential of a QKD system. For the final figure of merit of a QKD experiment, however, the actual *secure* key rate has to be evaluated. As mentioned in the introduction to this chapter, here, a hypothetical secure key rate will be calculated for this system achievable once all remaining elements will be implemented.

### 5.3.1 Weak Coherent Pulses and Decoy States

In this experiment, QKD is implemented using weak coherent pulses (WCPs), as the preparation of true single photon pulses requires a comparably huge technological overhead [97–99]. Yet, a WCP fundamentally contradicts the idea of a qubit, which is by definition a single quantum entity. Nevertheless, WCPs are widely used in quantum key distribution experiments [15, 25, 95, 100] and with the decoy state encoding and analysis [80, 81], a specialized measure was invented to upper bound the fraction of multi photon pulses, which led to raw key bits. With this estimation, the extractable secure key rate from weak pulse QKD can be calculated following the lines of [66].

WCPs exhibit a Poissonian photon number distribution. Namely the probability $P_\mu(n)$ to find $n$ photons in a pulse of mean intensity $\mu$, measured in photons per pulse, is given by

$$P_\mu(n) = \frac{\mu^n \mathrm{e}^{-\mu}}{n!} \ . \tag{5.11}$$

Therefore, also pulses with more than one single photon occur inevitably with a non zero probability $P_\mu(n > 1) = 1 - \mathrm{e}^{-\mu} - \mu \mathrm{e}^{-\mu}$ and the key bit candidates they produce are insecure. An obvious exploit of this effect would be to strip off one photon from all these pulses, store them, and measure them after Alice and Bob reveal their measurement bases while at the same time blocking parts of or even all single photon pulses (confer *Photon Number Splitting* [82, 101, 102]).

In a first attempt to still enable a secure key distribution with WCPs, one could eliminate as many bit of information from the raw key as multi photon pulses were sent (estimated from the Poissonian distribution), regarding these as *tagged* [66] and thus known to the adversary usually called Eve. This simple strategy, however, would fail to produce secure key even for moderate channel attenuation: Once $P_\mu(n \geq 2) \geq \eta$, one has to assume that no single photon events at all contributed to the raw key and consequently discard it completely.

The theory introducing decoy states provides much tighter estimations for the fraction of raw key bits resulting from multi photon events. This enables QKD with WCPs on much longer distances: While the key generation rate $R$ for WCP-based systems according to [66] drops with $(\mathrm{e}^{-\eta})^2$ (for optimal $\mu$), with decoy state encoding the relation is $R \propto \mathrm{e}^{-\eta}$ and the ranges become comparable to systems equipped with true single photon sources [80, 81] which show the same dependency in $\eta$ (see fig. 5.6).

For the decoy method, $m$ different decoy states with mean intensities $\nu_i$, $i < m$ are sent through the quantum channel, randomly alternating with the signal pulses. While an adversary could in principle measure the photon number of a pulse, this gives him no possibility to determine the class, signal or $i$-decoy, the pulse belongs to. The probability to find an $n$-photon pulse is non zero for all mean pulse intensities. Therefore any attempt to suppress single photon pulses necessarily affects all pulse classes equally but will change their photon number distribution differently. After the transmission, Alice announces which pulses were of which class and together with Bob calculates the gain values $Q_\mu$ and $Q_{\nu_i}$ for all $m$ classes separately. In case of any photon-number depending attack, they will notice different changes in the gain values $Q_\mu$ and $Q_{\nu_i}$ which allow them to tightly estimate the gain of single photon pulses $Q_1$. Of course, an essential assumption here is, that all mean pulse intensities are equally attenuated in the channel.

As mentioned before, decoy state encoding was not implemented here and the demonstrated transmission is therefore susceptible to the powerful photon number splitting attack. Yet, the experimental results allow for an evaluation of the secure key generation rate under the assumption that decoy states had been sent as described in the remaining part of this section.

With the additional information Alice and Bob get from the decoy state analysis about the photon number statistics for all pulse classes, they can calculate the secure key generation rate $R$ following Ma et al. [94]. The calculation combines the decoy state method with the work of Gottesman et al. [66]:

$$R \geq \frac{1}{2}\Big(Q_1\big(1 - H_2(e_1)\big) - Q_\mu f(e_\mu) H_2(e_\mu)\Big) \tag{5.12}$$

$e_\mu$ is the QBER on signal states and $e_1$ the error ratio on single photon pulses only. $f(e_\mu)$ is the efficiency of the error correction algorithm relative to the Shannon

limit [53]. Note that, following the lines of [94], the secret key is distilled exclusively from the signal pulses with intensity $\mu$ and thus, in the following $Q_1$ is considered the single photon gain of this pulse class only.

Analogous to equation (2.2), the above relation can be understood quantitatively in the following way: The secure key generation rate $R$ is lower bounded by the gain of true single photon pulses contributing to the raw key reduced by the amount of information an eavesdropper might have gained as indicated by the QBER on these single photon pulses ($-Q_1 H_2(e_1)$). Furthermore, the information disclosed during privacy amplification $Q_\mu f(e_\mu) H_2(e_\mu)$ has to be eliminated (subtracted). Finally the factor 1/2 is due to the decoy protocol only providing useful results in case of matching bases.

Of course, neither $e_1$, the error rate of single photon pulses, nor $Q_1$, the corresponding gain of signal pulses (eq. (5.4)), is directly accessible in the experiment. Even photon number resolving detectors at Bob's could not determine the number of photons in the initial pulse sent by Alice. Yet, the decoy theory provides tight bounds $e_1^U \geq e_1$ and $Q_1^L \leq Q_1$ in the respective worst case direction, which enable a calculation of a lower bound on the secure key rate.

Generally, an infinite number of decoy intensities $\nu_i$ would be optimal, however, it is impossible to determine an infinite number of $Q_{\nu_i}$ with the necessary precision on a finite experimental data set. In the following, the description is therefore restricted to the so called vacuum+weak decoy protocol using only two intensities $\nu_0 = 0$ and $\nu_1 = \nu < \mu$, which is optimal for finite transmission durations [81]. Then, the aforementioned worst case bounds $e_1^U$ and $Q_1^L$, assuming Poissonian photon number statistics of the sent pulses, take the form [94]

$$Q_1^L = \frac{\mu^2 \mathrm{e}^{-\mu}}{\mu\nu - \nu^2}\Big(Q_\nu \mathrm{e}^{\nu} - Q_\mu \mathrm{e}^{\mu}\frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\Big) \leq Q_1 \tag{5.13}$$

and

$$e_1^U = \frac{e_\mu Q_\mu - {}^1\!/_2 Y_0 \mathrm{e}^{-\mu}}{Q_1^L} \geq e_1 \ . \tag{5.14}$$

Substituting these estimates back into equation (5.12) provides a lower bound on the secure key rate. This only depends on quantities which were either set prior to the experiment (the pulse intensities $\mu$ and $\nu$) or can be measured in the key exchange (the gains $Q_\mu$ and $Q_\nu$, the error rate $e_\mu$, and the probability of dark counts ($Y_0$, measured when Alice sent vacuum pulses $\nu_0$).

In this way, the decoy method enables the substitution of a true single photon source with a transmitter preparing WCPs while preserving the security of the distributed key and at the same time the dependence of the key generation rate $R$ on $\eta$. Moreover, the optimal pulse intensity for a wide range of channel attenuation is close to $\mu = 0.5$ [94] and the transmitters can be operated in the GHz regime [100]. Therefore, as of now, decoy QKD systems usually outperform setups that encode

*single* photons, as there the mean intensities per pulse often suffer from poor collection efficiency and the repetition rate is limited.

### 5.3.2 Secure Key Rate Evaluation

#### Parameter Optimization

For the present experiment, the calculation of the maximum secure key rate is based on the values of the mean pulse intensity $\mu$, the QBER $e_\mu$, the gain of signal states $Q_\mu$, the yield of vacuum pulses $Y_0$, and the total channel attenuation $\eta$, which were all measured in the experiment.

For the evaluation according to the decoy state protocol, additionally, a decoy pulse intensity $\nu$ has to be chosen and the corresponding gain $Q_\nu$ is calculated from equation (5.4). Furthermore, the frequencies of decoy and vacuum pulses, $P_\nu$ and $P_0$, in the sent stream have to be determined. In this offline analysis, an optimization in Mathematica is used to find the set of parameters resulting in the highest secure key rate according to equation (5.12).

However, for an infinite long key exchange, the secure key rate is maximized for vanishing decoy and vacuum pulse frequencies and a near zero decoy pulse intensity [94]. While these would indeed be the optimal parameters, this is only true as long as the necessary quantities for the equations (5.12) to (5.14) can be determined with a reasonable accuracy, too. Of course, this is not practicable for $\nu$, $P_\nu$ and $P_0$ close to 0 and for a reasonable statement about the secure key rate in this experiment, one has to consider the finite amount of signal received, which inevitably leads to noise in the measured parameters. Therefore, assuming a Gaussian error distribution, all measured gain values and the QBER in equations (5.12) to (5.14) are substituted with according worst case estimations by $s_d$ standard deviations (STD) [95]:

$$\begin{aligned} Q_{\mu,\nu} \;\rightarrow\; Q^{\pm}_{\mu,\nu} \;&=\; Q_{\mu,\nu} \quad \left(1 \pm \frac{s_d}{\sqrt{N_{\text{sent}} P_{\mu,\nu} Q_{\mu,\nu}}}\right) \\ e_\mu \;\rightarrow\; e^{\pm}_{\mu} \;&=\; e_\mu \quad \left(1 \pm \frac{s_d}{\sqrt{N_{\text{sent}} P_{\mu} Q_{\mu} e_{\mu}}}\right) \end{aligned} \tag{5.15}$$

With these substitutions, a confidence interval of one STD $s_D = 1$, and a time filter window width of $\tau_f = 0.5\,\text{ns}$ an optimization for maximum secure key rate delivers practicable parameters $\nu$, $P_\nu$, and $P_0$ for operation of a decoy QKD system:

$$\nu = 0.076, \quad P_\nu = 12.8\ \%, \quad P_0 = 9.5\ \% \tag{5.16}$$

The result of the optimization heavily depends on the total amount of signal that could be registered. Therefore, $\tau_f$ is a crucial parameter here, too (see § 5.1.3): For a wider filtering window, i.e. a larger $\tau_f$, the sifted key gets longer, which makes the worst case estimations in equation (5.15) less restrictive. On the other hand, this would result in a slightly higher QBER which, at the same time, decreases the secure key rate. Consequently, the optimization was done for different time filtering windows in 50 ps steps. The result was already given in figure 5.2 (page 66) where the secure key rate, plotted together with the QBER over $\tau_f$, shows a maximum for $\tau_f = 0.5\,\text{ns}$.

### Secure Key Rate

Operating the QKD system supplemented with the ability to send decoy states and using $\mu = 0.5$ and the parameters in equation (5.16) on the quantum channel as observed in the experiment (i.e. with the same noise and attenuation) would result in an asymptotic secure key rate of 7.9 bit/s calculated according to equations (5.12) to (5.14). Considering the repetition rate of $f = 10\,\text{MHz}$ this corresponds to a secure key generation rate per sent qubit of $7.9 \times 10^{-7}$.

In this calculation, statistical noise in the parameter estimation is neglected (see below). Furthermore, information leaks via side channels are not considered in this evaluation as these can be made arbitrarily small by technological means.

### Finite Key Considerations

In a realistic scenario, the number of signals received will always be finite. Moreover, the block size in privacy amplification, i.e., the number of bits which are processed at once, may be limited due to the available memory and processing power especially in high rate QKD applications. This gives rise to statistical fluctuations on the measured parameters which enter the secure key rate calculation and was soon recognized [67] to impose security flaws when not handled properly: For example, the information leakage indicated by the observed QBER via the binary entropy function in equation (5.12) might be smaller than Eve's actual information gain in case she was lucky to cause less errors in Bob's signals on a specific finite sample. Only asymptotically, the frequency of quantum bit errors becomes equal to the ratio of errors in the sifted string, the QBER, and allows for a secure calculation of the information leakage.

An ad hoc approach to incorporate these effects uses the worst case estimations from equation (5.15) [95]: For $s_d = 1$ the secure key rate for this experiment drops from 7.9 bit/s to 4.8 bit/s. Yet, this confidence interval is obviously to small for a truly secure key as there remains a probability, adhering to the assumed Gaussian distribution, of 31.7 % for each measured parameter to exceed its assumed worst case boundary. In this case the information gain of an eavesdropper would remain underestimated. A confidence interval on the parameters of ten STDs is often used

**Table 5.4:** Secure key length and rate of this experiment asymtotically and for a worst case estimation of the measured parameters by one and two STD. For comparison, the asymtotic key rate of a true single photon QKD transmitter with the same mean intensity $\mu = 0.5$ is given.

| | **worst case est.** $s_d$ | **secure key rate** (bit/s) | **tot. length** (bit) |
|---|---|---|---|
| sifted key | | 145 | 82308 |
| decoy | asymtotically | 7.9 | 4484 |
| decoy | 1 std | 4.8 | 2724 |
| decoy | 2 std | 1.8 | 1021 |
| single photon QKD | asymtotically | 64 | 36329 |

for "unconditional" security [95]; $s_d = 10$ reduces the probability to underestimate the information leakage due to a single parameter to $1.5 \times 10^{-23}$. Unfortunately, for this experiment the secure key rate already almost vanishes for $s_d = 2$ (see tab. 5.4). In Figure 5.6, the key rate is visualized over the channel attenuation for 0, 1, and 2 STDs and compared to the case of a true single photon QKD transmitter with the same mean intensity $\mu = 0.5$.

Recent security proofs for QKD make use of an uncertainty relation for the so called min- and max-entropy [9, 68, 103] to derive secure key rates under realistic assumptions concerning finite key effects [104]. For decoy state QKD, however, this treatment of finite size effects is not yet completely solved. Proposals to accomplish this can be found in [105–109], however, the security considerations for the decoy parameters differ between these works and appear to be conservative. For the current experiment, an analysis along these lines does not allow for the distillation of a secure key.

## 5.4 Discussion

In this work, a first proof of principle demonstration of BB84 quantum key distribution from an airplane to ground could be successfully performed. This comprises the design and the seamless integration of QKD hardware into an existing system for classical communication, the precise compensation of mutual rotations of the polarization reference frame, and an accurate pointing to establish and maintain the quantum channel between the aircraft and the ground station telescope.

All parameters to judge the QKD performance of the system and the quantum channel could be measured and the calculation of the secure key rate under the

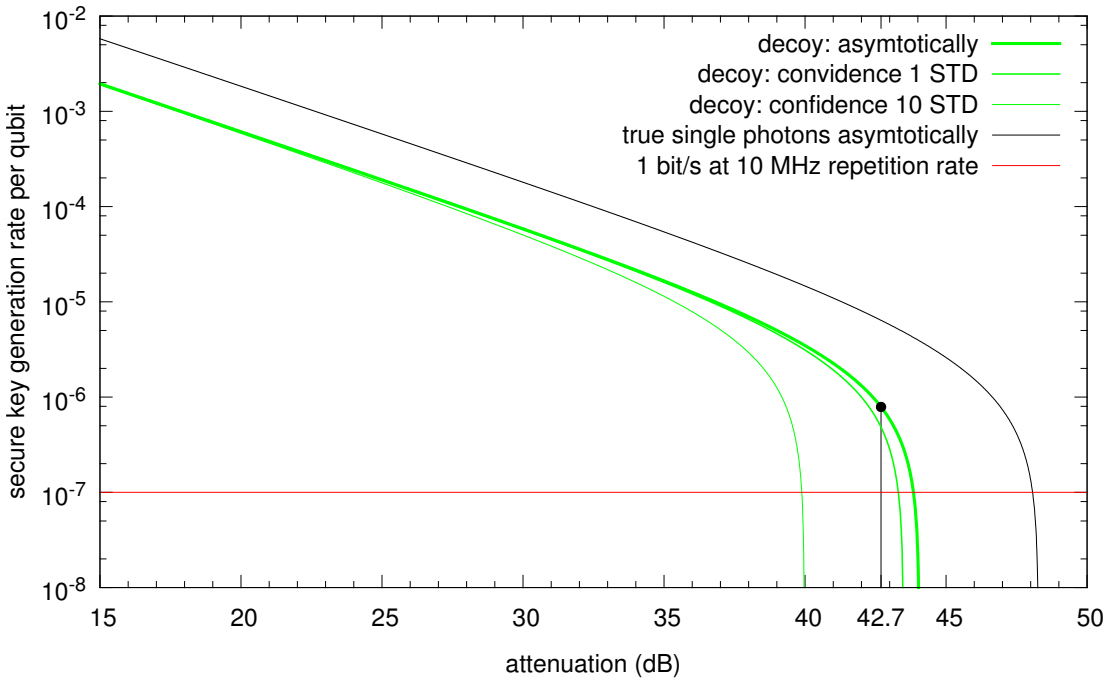



**Figure 5.6:** Secure key generation rate per sent qubit depending on the channel attenuation for a decoy state analysis of this experiment with worst case estimations of 0 (asymtotic case), 1 and 10 STDs. The dot marks the observed result. While for one STD, the drop in key generation rate is only about 2 dB, for 10 STDs confidence intervall no secure key can be distilled at all. For comparison, also the expected secure key rate of true single photon QKD operating on the same channel and with the same mean intensity is visualized. For clarity, the red line marks the key generation rate of 1 bit/s at the used repetition frequency of 10 MHz.

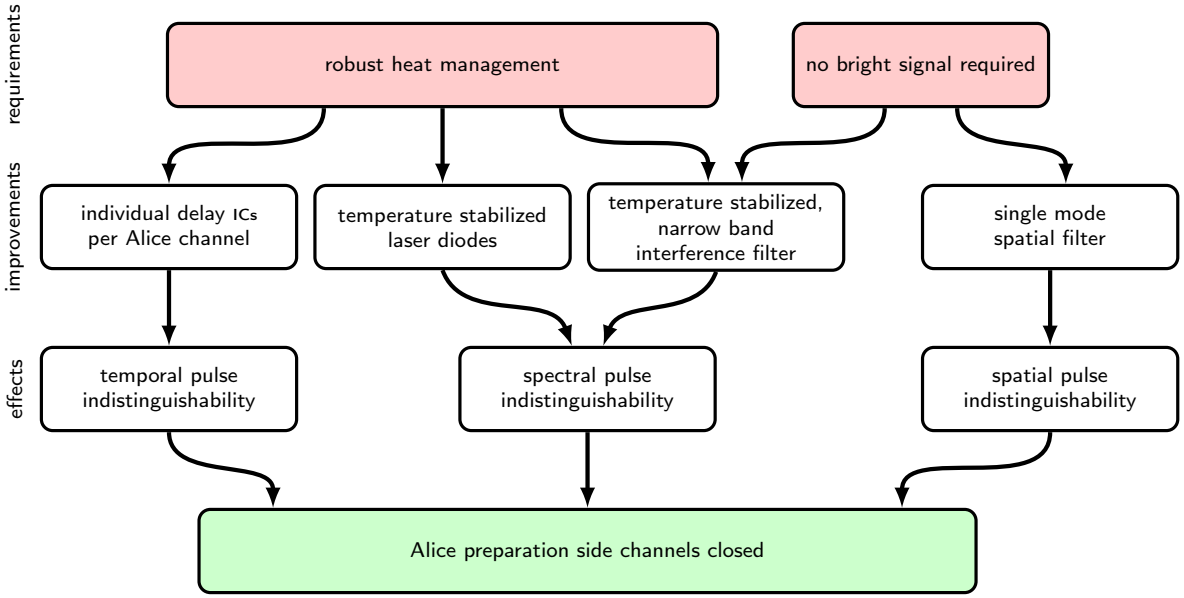



**Figure 5.7:** Future improvements in order to eliminate preparation side channels of the Alice module. Once, a robust heat management is established for the FELT2 and bright signals are no longer required from the QKD transmitter, the spatial, spectral and temporal side channels can be eliminated.

assumptions detailed in section 5.3.2 shows that for example more than 10 symmetric keys for the classical encryption scheme AES256 [2, 3] – 256 indicates the key length in bit – can be exchanged in one aircraft passage (see tab. 5.4, 1 STD).

The application of the information theoretically secure one time pad encryption scheme [1] requires a key of the same length as the data to be encrypted. Therefore, the achieved secure key rate in this experiment would allow for a very limited communication only. Moreover, the system has to be improved to become robust against attacks on the photon number of the transmitter pulses or side channels in order to render the according assumptions in the analysis obsolete and finally arrive at an unconditionally secure system.

Therefore, on the way to a prototype for commercial and secure QKD applications, there are still several details to be addressed. These shall be discussed together with their implications on the performance of a next generation experiment in the following.

### 5.4.1 QKD Transmitter and Receiver

The limited experiment time of at most only four short flights was a major concern in the development of the Alice module for this experiment and the design aimed to make a complete failure of the module as unlikely as possible. Therefore,

simplifications and compromises in certain details had to be adopted in favor of the needed robustness that will have to be addressed in future experiments.

First of all, decoy states will have to be implemented in the Alice module. This can be accomplished using an eight channel transmitter module as developed and used in [16, 25] to produce the necessary decoy and signal states with four laser diodes each. The third intensity, the vacuum pulse, is trivially realized by suppressing the respective pulses completely. This approach, however, requires more complicated optics which is undesirable in view of miniaturization and industrial manufacturing. Thus, alternatively, decoy states could be produced electronically, for example by coupling two laser drivers to every laser diode, each calibrated to deposit a different pulse energy $\mathcal{E}_\mu$ and $\mathcal{E}_\nu$ respectively. In this way, decoy state preparation could be enabled for the Alice module built here, too, by mere exchange of the electronics board. On Bob's side, the integration of a decoy state analysis only requires for a slightly extended classical post processing (see § 5.3.1) which is a matter of software only.

In a next stage of the experiment, there will be no need for bright output powers. Operation in the mW range as well as pulsing with several hundreds of photons per pulse was incredibly helpful in the preparation of this experiment but can be omitted in the future with the experience acquired here. Therefore, a much more restrictive mode filter and a narrow interference filter can be afforded while still reliably providing the necessary QKD intensities in the sub single photon regime. Thereby, two severe side channels – the spatial and spectral distinguishabilities of the four laser diodes – can be eliminated at the same time (see fig. 5.7).

Further, a whole set of improvements is enabled once the FELT2 allows for heat exchange with the surrounding to dissipate the terminal excess heat: The temperature stabilization of the laser diodes and the interference filter mentioned above would guarantee stable output wavelengths and thus enable a more restrictive filtering at the receiver. In this way one would reduce the background noise in the signal significantly. Additionally, faster electronics enabled by better heat management would allow to reduce the QKD pulse length and to eliminate the delay between the four diodes, closing the third side channel associated with the photons degrees of freedom (see fig. 5.7). Finally, the repetition rate could be increased by possibly two orders of magnitude to above 1 GHz.

A future FPGA-based circuitry of Alice and Bob will make the implementation of the complete post processing straight forward: sifting, error correction and privacy amplification can easily be performed by modern FPGAs as well as the necessary communication, provided a bidirectional optical data channel is made available by the classical subsystem. Such an FPGA system could already be demonstrated by Zhang et al. [110]. Recently, also fast radio links for air to ground communication become available that could provide the classical back-channel for unidirectional optical systems, too (a prototype capable of up to a few Mbit/s was already tested during this experiment).

Finally, the Alice module will need a reliable source of true randomness for generation of the secret key. For this purpose, physical or even quantum random number generators [111] are by now readily available and can be interfaced to the FPGA. Yet, the BB84 protocol needs two bit of randomness for every qubit and the decoy method requires a small additional amount of randomness (depending on the distribution of decoy and signal states) to select one of the three pulse intensities. The required bit rate of a random number generator, therefore, is about a factor of 2 to 3 higher then the repetition rate of the QKD system. As commercial quantum random number generators are limited to rates of tens of MHz [44, 111, 112], for the time being, they will have to be parallelized or used to seed pseudo random number generators to enable a bit stream in the GHz regime. Nevertheless, quantum random number generators are being actively developed and bit rates well beyond 100 MHz have already been demonstrated [113, 114].

The above proposed modifications are necessary to establish the systems unconditional security: The increased sifted bit rate will allow for the rigorous analysis of finite key effects as envisioned in section 5.3.2 and the transmitter side channels can be eliminated. All these improvements are in principle practicable even in the constricted room on board of an aircraft or satellite.

### 5.4.2 Classical Subsystem

While the classical subsystem performed excellent for this demonstration, there are some points that have to be addressed in order to enable the complete BB84 protocol and to provide the environment for an *unconditionally secure* QKD transmitter.

First, as the classical optical link worked unidirectionally only at the time of this experiment, no online sifting could be performed. However, current development of the platform at the DLR will enable bidirectional communication even with a mobile ground station [115] so that the classical channel can be provided as requested by the protocol.

Another important issue is the thermal management of the airborne terminal already mentioned before to overcome design constraints for a new QKD transmitter. While the required power consumption for temperature stabilized components should not exceed a few Watt, a cooling mechanism will definitely be necessary to eliminate vulnerabilities due to the state preparation as analyzed in [70]. The heat exchange could be realized by a heat pipe connecting an interior heat sink with the aircraft or terminal outer skin cooled by the constant air stream of the moving aircraft. This strategy would also solve the laser safety considerations claimed by the authorities in conjunction with conventional ventilation slots through which laser radiation might escape under faulty conditions.

The pointing accuracy achieved here was sufficient with regard to the still relatively wide QKD beam as it was no major source of attenuation (see tab. 5.2). From Figure 5.4 the long term stability becomes evident, too. Apart from sub second

losses, there are no complete link failures during the whole passage and only a slight decrease of the sifted key rate is noticeable. Responsible for this are probably small imperfections of the beam alignment in the FELT2 relative to the systems axis, which also manifested themselves as different optimal values for the pointing control offset vector (see section 4.3.4) depending on the aircraft direction around the OGS – clock-wise or counter-clock-wise. Moreover, the optical system of a next experiment will have to guarantee perfect stability for the coalignment of the pointing axis and the QKD-beam without the need for manual tweaks in flight (see § 4.2.1) which can already be accomplished by a more stable optical breadboard.

Especially in view of a future satellite based application, the QKD beam will have to be much better collimated in order to bridge the longer distances with high efficiency. This will enforce larger effective transmitter apertures in the regime of 10 cm [116] and even better pointing accuracy. However, in this demonstration, a major challenge was to decouple the optical system, both passively using shock mounts and actively with the FPA, from the vibrating body of the aircraft, which is not necessary to that extent on board a satellite. There, even an open-loop pointing of the space terminal based on the known satellite trajectory is assumed to achieve a precision of already about 25 µrad [32]. The situation appears to be more demanding on board of the international space station (ISS) as the high activity there constantly excites a multitude of vibrational modes of which an estimated number of 5000 (200) are below 50 (15) Hz [117] starting from 0.06 Hz. These slow deformations of the structure of the ISS would need to be compensated by an FPA with sufficient angular range. Moreover, the mounting position of a future QKD-system on the ISS would have to be carefully chosen in order to minimize large amplitude angular vibrations.

On the ground, the OGS tracking will also benefit from the a priori known trajectory of a ballistic body in LEO as compared to the aircraft. Yet, a fast fine pointing will, nevertheless, be necessary to compensate the effects of air turbulence.

### 5.4.3 Secure Key Rate

The secure key rate calculated under the assumptions as detailed in section 5.3.2 is only meant to give an idea of the systems performance and to help identify the necessary improvements. Under a rigorous analysis, as mentioned in section 5.3.2, no secure key could be distilled from the quantum transmission. The main reasons are the limited key length and the reasonably high total QBER. Yet, for both these issues, there is much room for improvements (see also tab. 5.5):

The amount of raw key linearly increases with the system's repetition frequency, which promises advances of at least one to two orders of magnitude. On Bob's side, the detectors can handle much higher signal rates before dead time effects become relevant. The increased rates, however, will demand for a correspondingly better time synchronization of Bob's detectors to reliably assign signal events to transmitter time slots avoiding influence from stray light (already demonstrated in [118, 119]).

**Table 5.5:** Overview of future improvements to the experimental setups which will boost both the speed and thereby the security of the transmission by enabling secure key distillation under rigorous finite key analysis.

| **improvements** | **to enable** | **benefit** |
|---|---|---|
| quieter detectors, better spectral filtering | reduced background noise by factor 5 | QBER due to background noise $< 1\%$ |
| usage of full terminal exit aperture of 30 mm | narrower beam collimation, waist diameter 12 mm | 6 dB more signal at receiver, QBER due to background noise $< 1\%$ |
| faster Alice electronics | repetition rate of up to 1 GHz | up to 20 dB speedup in sifted key rate |
| reduced synchronization jitter | less signal loss in time filtering | up to 3 dB speedup in sifted key rate |

If this overall temporal jitter can be addressed, additionally the signal loss of 4.2 dB in the time filtering step can be reduced in favor of the sifted key length.

Furthermore, the optical coupling of the telescopes will have to be improved, which would also raise the signal to noise ratio. An advanced mode filter, i.e., beam preparation, together with optimized telescope optics will allow for a much narrower collimation. Even in case only the current telescope aperture of $d = 30$ mm is available, this then results in a diffraction limited full divergence of 90 µrad (waist $\omega_0 = 0.2d$). The corresponding beam diameter at the OGS telescope is 1.8 m, which gives about 6 dB more signal than the configuration demonstrated here.

In total, from the increased rates and enhanced optics of a next generation experiment, one can expect more then 26 dB increase in the raw signal rate at the slightly reduced total quantum channel attenuation of 37 dB, which would result in $10^7$ bit of sifted key from one aircraft passage.

Additionally, it will be important to improve the QBER. About two thirds of the errors are currently due to dark count events and stray light in roughly equal parts. Because in this application, APDs are needed with a reasonably large active area to allow for a minimum of residual pointing errors, they will always suffer from a significant dark count rate. Below 200 counts per second and detector seems, however, a realistic specification, which corresponds to a reduction of dark counts by a factor of 5. Furthermore, the contribution from stray light will be drastically

reduced by the narrow interference filter mentioned above. If there a conservatively estimated factor of 5 can be realized, too, this would result in half the total QBER compared to the value observed here and improve the asymptotic secure key rate under otherwise same conditions to 38 bit/s (+6.8 dB).

The results of the automatic polarization compensation could not be improved manually to arrive at lower QBER. Thus, polarization dependent reflectivities and transmissions due to the finite quality of the optical components and coatings will have to be eliminated or compensated where possible to further reduce the number of erroneous bits from actual signal events.

In summary, the estimated parameters for the sifted key length and QBER of a next generation QKD experiment on a channel as observed here allow for a secure key exchange even under state of the art finite key privacy amplification [105]. While the key generation rates would still only be in the regime of tens of bit/s (6 kbit/passage), more than 20 *unconditionally* secure keys for classical symmetric encryptors working on basis of AES256 can be provided in one aircraft passage.

# Chapter 6

# Summary and Outlook

In the presented experiment, the feasibility of a quantum key exchange according to the BB84 protocol between an aircraft and an optical ground station could be successfully demonstrated. To this aim, a transmitter for polarization encoded, faint pulse QKD was integrated with the free-space experimental laser terminal 2 (FELT2) of the DLR and the optical ground station in Oberpfaffenhofen near Munich, Germany was supplemented with an according quantum receiver.

With the aircraft at a distance of 20 km and flying at a speed of 290 km/h, sifted key could be generated at a rate of 145 bit/s. The observed QBER was 4.8 % and contained a significant contribution from stray light and dark counts (3 %). Assuming the implementation of the decoy state method, secure key can be distilled at an asymptotic rate of 7.9 bit/s. While at this point, finite key effects could not be rigorously be accounted for, thorough analysis reveals, that *unconditional* secure key at similar rates can be enabled in a next step of the experiment by advanced electronics and tighter filtering. Online sifting and post processing will immediately be possible once the classical host system allows for bidirectional communication, too.

The implementation of the QKD hardware could be realized as an add-on while the classical host system remained fully operational. Even though neither the FELT2 nor the OGS were intended to accommodate additional components, only minor changes were required in order to enable this demonstration. This underlines the suitability of QKD as a supplementary technology for classical communication devices.

Already in this demonstration, the quantum transmitter and receiver were designed as integrated modules and further miniaturization will allow for their implementation in nearly all classical communication systems operating on a direct line of sight: As of today, there is a variety of solutions for high speed data links, both free-space optical (FSO) and on basis of point-to-point directional radio. All these systems could implement cryptographic means to secure the communication

and thus could benefit from a QKD add-on. Additionally, it has to be stressed, that in contrast to frequent claims, narrow beam FSO links do not offer intrinsic security against eavesdropping as stray light produced at the transmitter or the receiver can be collected and analyzed with suitable telescopes.

With the fine pointing assemblys (FPAs) in the flight terminal and on the ground station, the DLR contributed an essential prerequisite to the success of this experiment. The stability as well as the absolute efficiency of the quantum channel could only be achieved with the advanced accuracy enabled by the additional fine and fast pointing facilities. The increased pointing performance will in turn also boost the classical communication speed and extend the possible operation ranges. For links to systems in LEO, the techniques employed here will certainly need some refinement to meet the even more critical accuracy requirements. This is, however, considered practicable [32] even under the space, weight, and power restrictions on board of a satellite.

The polarization encoding in this mobile scenario made a compensation scheme necessary to make up for mutual rotations of the transmitter's and receiver's reference frames. Even on the circular path, the online readjustment of the wave plates turned out to be vital in order to maintain low error rates. Finally, the small technical error of 1.8 % contributing to the overall QBER proofs a successful and precise polarization compensation. It has to be noted, however, that the design of the pointing system has substantial influence on the complexity of the polarization compensation. The coudé geometry of the FELT2 telescope produced rotations depending on the pointing direction which could be modeled and compensated well. There are, however, other configurations that might introduce more complex distortions. In fact the need for a compensation scheme can also be avoided partly or even entirely: If transmitter and receiver are both azimuth/elevation mounted and moved as a unit, there are no moving mirrors and the relevant rotations are entirely of spatial nature. In this case a single half wave plate is sufficient to reestablish the common reference frame. In [120], an otherwise similar QKD experiment linking to a hot-air balloon is presented which is, however, realized without any polarization compensation. This is possible as the vertical direction is always well defined for the balloon. For satellite terminals, the influence of a single tip/tilt mirror in front of the telescope is investigated and also reference beams are discussed, either at a different wavelength or time multiplexed [43].

The absolute security measures enabled by QKD systems certainly will not be the answer to the security issues of ordinary home or office computers and their communication via the internet. This is not only because the network topology necessary to provide a quantum channel for every terminal, essentially a quantum internet, would be excessively expensive. In fact, an adversary will always go for the weakest link in the security chain and in order to establish and maintain data integrity and confidentiality, a secure key exchange and a perfect encryption

algorithm are only two necessary prerequisites. Most attacks registered today target specific erroneous software implementations or the user himself by forging mails and websites. Moreover, the limited possible damage associated with eavesdropping on private communication, i.e., the risk usually does not even justify advanced conventional security hardware.

In an intermediate approach – without a quantum internet – users could exchange secure key using QKD in mobile devices with a terminal at their bank or other trusted organization. This key could later be used to authenticate and encrypt communication via the internet and thereby enable a greatly improved communication security. The idea is somehow similar to one time transaction authentication numbers (TANs) as used today only that the key length could be much longer (the necessity to type the key by hand drops) and the secure quantum distribution replaces the TAN letter. The development of such hand held QKD systems started already in 2006 [121] and with recent advances in wave guide optics becomes more and more feasible.

The cost-benefit analysis appears much different for the security of professional systems. Today, almost every day attacks on the information infrastructure of huge companies, universities and even governments are reported. Even more alarming are intrusions into systems controlling critical infrastructure like power grids, pipelines, offshore platforms, air traffic control or the railway network. Here, vulnerabilities in the data communication can possibly claim many human lives and most secure network infrastructure is indicated.

Indeed, QKD can improve the robustness of these delicate systems against attacks by providing unconditionally secure symmetric keys. Moreover, the results of this work proof QKD to be a feasible technology for mobile applications, too. Not only can the connection to the aircraft itself be secured. Regarding the flying unit as a trusted node allows to distribute key material in varying scenarios on a continental range. In some cases, especially when integrated with unmanned aircraft, free space QKD may also be cost effective compared to very expensive dark fibers.

Of course, QKD to and between satellites remains the grand goal for global secure communication. In fact, the conditions aboard a satellite in some respects are even advantageous compared to the aircraft scenario in the presented experiment: First, the trajectory of a satellite is usually known precisely and a second benefit is the absence of vibrations aboard a satellite which were severe in the presented scenario. Thereby, the pointing and tracking will be facilitated on both ends of the quantum channel. Moreover, the polarization rotations emerging from the satellite's orientation are deterministic and their compensation can be improved iteratively due to the repeating nature of its track.

With the successful polarization compensation in this highly dynamic demonstration and the observed attenuation comparable to the values anticipated in a LEO down link, this experiment constitutes a major milestone on the way to unconditionally secure communication on a global scale.

# Publications

The presented experiment is subject of the following publications:

- Air to Ground Quantum Communication
  S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick and H. Weinfurter
  *Nature Photonics* **7**, 382 (2013)

- Air to Ground Quantum Key Distribution
  S. Nauerth, F. Moll, M. Rau, J. Horwath, S. Frick, C. Fuchs, and H. Weinfurter
  in *Proceedings of the SPIE Quantum Communications and Quantum Imaging X 8518*, 85180D (2012)

- Communication System Technology for Demonstration of BB84 Quantum Key Distribution in Optical Aircraft Downlinks
  F. Moll, S. Nauerth, C. Fuchs, J. Horwath, M. Rau and H. Weinfurter
  in *Proceedings of the SPIE Optical Engineering+Applications 8517*, 851703 (2012)

Further publications:

- Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range
  T. Heindel, C. Kessler, M. Rau, C. Schneider, M. Fürst, F. Hargart, W. Schulz, M. Eichfelder, R. Roßbach, S. Nauerth et al.
  *New Journal of Physics* **14**, 083001 (2012)

- Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors
  H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth & H. Weinfurter
  *New Journal of Physics* **13**, 073024 (2011)

- High speed optical quantum random xnumber generation.
  M. Fürst, H. Weier, S. Nauerth, D. Marangon, C. Kurtsiefer & H. Weinfurter.
  *Optics Express* **18**, 13029 (2010)

- The SECOQC Quantum Key Distribution Network in Vienna
  M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fïst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden & A. Zeilinger
  *New Journal of Physics* **11**, 075001 (2009)

- Information leakage via side channels in freespace BB84 quantum cryptography
  S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier & H. Weinfurter.
  *New Journal of Physics* **11**, 065001 (2009)

# Bibliography


[1] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal* **28**, 656 (1949)

[2] NIST. *Advanced Encryption Standard* (2001)

[3] B. Schneier & P. Sutherland. *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, Inc. (1995)

[4] W. Diffie & M. E. Hellman. Multiuser cryptographic techniques. In *Proceedings of the national computer conference and exposition*, pages 109–112 (1976)

[5] R. L. Rivest, A. Shamir & L. M. Adelman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* **21**, 120 (1978)

[6] S. Wiesner. Conjugate coding. *ACM Sigact News* **15**, 78 (1983)

[7] C. H. Bennett & G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179 (1984)

[8] N. Gisin, G. Ribordy, W. Tittel & H. Zbinden. Quantum cryptography. *Review of Modern Physics* **74**, 145 (2002)

[9] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus & M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics* **81**, 1301 (2009)

[10] C. H. Bennett & G. Brassard. Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working. *SIGACT News* **20**, 78 (1989)

[11] C. Gobby, Z. Yuan & A. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters* **84**, 3762 (2004)

[12] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller & J. E. Nordholt. Long-distance quantum key distribution in optical fibre. *New Journal of Physics* **8**, 193 (2006)

[13] H. Takesue, S. Nam, Q. Zhang, R. Hadfield, T. Honjo, K. Tamaki & Y. Yamamoto. Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors. *Nature photonics* **1**, 343 (2007)

[14] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. Towery & S. Ten. High rate, long-distance quantum key distribution over 250km of ultra low loss fibres. *arXiv* quant-ph/0903.3907 (2009)

[15] D. Rosenberg, C. G. Peterson, J. W. Harrington, P. R. Rice, N. Dallmann, K. T. Tyagi, K. P. McCabe, S. Nam, B. Baek, R. H. Hadfield, R. J. Hughes & J. E. Nordholt. Practical long-distance quantum key distribution system using decoy levels. *New Journal of Physics* **11**, 045009 (2009)

[16] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fïst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden & A. Zeilinger. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics* **11**, 075001 (2009)

[17] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev & A. Zeilinger. Field test of quantum key distribution in the tokyo QKD network. *Optics Express* **19**, 10387 (2011)

[18] H.-J. Briegel, W. Dür, J. I. Cirac & P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters* **81**, 5932 (1998)

[19] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer & J.-W. Pan. Experimental demonstration of a BDCZ quantum repeater node. *Nature* **454**, 1098 (2008)

[20] M. Zwerger, W. Dür & H. Briegel. Measurement-based quantum repeaters. *Physical Review A* **85**, 062326 (2012)

[21] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster & J. G. Rarity. Quantum cryptography: A step towards global key distribution. *Nature* **419**, 450 (2002)

[22] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt & C. G. Peterson. Daylight quantum key distribution over 1.6 km. *Physical Review Letters* **84**, 5652 (2000)

[23] R. J. Hughes, J. E. Nordholt, D. Derkacs & C. G. Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics* **4**, 43 (2002)

[24] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter & A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature Physics* **3**, 481 (2007)

[25] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger & H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters* **98**, 010504 (2007)

[26] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein & A. Zeilinger. Feasibility of 300 km quantum key distribution with entangled states. *New Journal of Physics* **11**, 085002 (2009)

[27] A. Fedrizzi, R. Ursin, T. Herbst, M. Nespoli, R. Prevedel, T. Scheidl, F. Tiefenbacher, T. Jennewein & A. Zquantieilinger. High-fidelity transmission of entanglement over a high-loss free-space channel. *Nature Physics* **5**, 389 (2009)

[28] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin & A. Zeilinger. Quantum teleportation over 143 kilometres using active feed-forward. *Nature* **489**, 269 (2012)

[29] J. Yin, H. Lu, J.-G. Ren, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, Y. Jiang, X.-D. Cai, P. Xu, G.-S. Pan, J.-Y. Wang, Y.-A. Chen, C.-Z. Peng & J.-W. Pan. Teleporting independent qubits through a 97 km free-space channel. *arXiv* quant-ph/1205.2024 (2012)

[30] X.-M. Jin, J.-G. Ren, B. Yang, Z.-H. Yi, F. Zhou, X.-F. Xu, S.-K. Wang, D. Yang, Y.-F. Hu, S. Jiang, T. Yang, H. Yin, K. Chen, C.-Z. Peng & J.-W. Pan. Experimental free-space quantum teleportation. *Nature Photonics* **4**, 376 (2010)

[31] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto & P. Villoresi. Feasibility of satellite quantum key distribution. *New Journal of Physics* **11**, 045017 (2009)

[32] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell & C. G. Peterson. Satellite-based quantum communications. In *Proceedings of Updating Quantum Cryptography and Communications 2010*, pages 71–72 (2010)

[33] Z. Yan, E. Meyer-Scott, J.-P. Bourgoin, B. L. Higgins, N. Gigov, A. MacDonald, H. Hübel & T. Jennewein. Novel high-speed polarization source for decoy-state BB84 quantum key distribution over free space and satellite links. *arXiv* quant-ph/1211.3194 (2012)

[34] J. Horwath & C. Fuchs. Aircraft to ground unidirectional laser-communication terminal for high resolution sensors. In *Proceedings of the SPIE Free-Space Laser Communication Technologies XXI*, pages 919909–1 (2009)

[35] A. Biswas, J. Kovalik, M. W. Regehr & M. Wright. Emulating an optical planetary access link with an aircraft. In *Proceedings of the SPIE Free-Space Laser Communication Technologies XXII*, page 75870B (2010)

[36] N. Perlot, M. Knapek, D. Giggenbach, J. Horwath, M. Brechtelsbauer, Y. Takayama & T. Jono. Results of the optical downlink experiment KIODO from OICETS satellite to optical ground station Oberpfaffenhofen (OGS-OP). In *Proceedings of the SPIE Free-Space Laser Communication Technologies XIX and Atmospheric Propagation of Electromagnetic Waves*, pages 645704–1 (2007)

[37] Y. Takayama, M. Toyoshima, Y. Shoji, Y. Koyama, H. Kunimori, M. Sakaue, S. Yamakawa, Y. Tashima & N. Kura. Expanded laser communications demonstrations with OICETS and ground stations. In *Proceedings of the SPIE Free-Space Laser Communication Technologies XXII*, page 758703 (2010)

[38] R. Fields, D. Kozlowski, H. Yura, R. Wong, J. Wicker, C. Lunde, M. Gregory, B. Wandernoth & F. Heine. 5.625 gbps bidirectional laser communications

measurements between the NFIRE satellite and an optical ground station. In *Proceedings of the IEEE International Conference on Space Optical Systems and Applications (ICSOS)*, pages 44–53 (2011)

[39] R. Fields, C. Lunde, R. Wong, J. Wicker, D. Kozlowski, J. Jordan, B. Hansen, G. Muehlnikel, W. Scheel, U. Sterr et al. NFIRE-to-TerraSAR-X laser communication results: satellite pointing, disturbances, and other attributes consistent with successful performance. In *Proceedings of the SPIE Sensors and Systems for Space Applications III*, page 73300Q (2009)

[40] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick & H. Weinfurter. Air to ground quantum communication. *Nature Photonics* **7**, 382 (2013)

[41] S. Nauerth, F. Moll, M. Rau, J. Horwath, S. Frick, C. Fuchs & H. Weinfurter. Air to ground quantum key distribution. In *Proceedings of the SPIE Quantum Communications and Quantum Imaging X*, page 85180D (2012)

[42] D. H. Höhn. Depolarization of a laser beam at 6328 Å due to atmospheric transmission. *Applied Optics* **8**, 367 (1969)

[43] C. Bonato, M. Aspelmeyer, T. Jennewein, C. Pernechele, P. Villoresi, A. Zeilinger et al. Influence of satellite motion on polarization qubits in a space–earth quantum communication link. *Optics Express* **14**, 10050 (2006)

[44] ID QUANTIQUE SA. http://www.idquantique.com/

[45] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres & W. K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters* **70**, 1895 (1993)

[46] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter & A. Zeilinger. Experimental quantum teleportation. *Nature* **390**, 575 (1997)

[47] S. Lloyd et al. Universal quantum simulators. *Science* **273**, 5278 (1996)

[48] R. P. Feynman. Quantum mechanical computers. *Foundations of physics* **16**, 507 (1986)

[49] S. Lloyd et al. A potentially realizable quantum computer. *Science* **261**, 1569 (1993)

[50] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pages 124–134 (1994)

[51] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood & I. L. Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* **414**, 883 (2001)

[52] C.-Y. Lu, D. E. Browne, T. Yang & J.-W. Pan. Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits. *Physical Review Letters* **99**, 250504 (2007)

[53] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal* **27**, 379 (1948)

[54] G. Brassard & L. Salvail. Secret key reconciliation by public discussion. In *Proceedings of Eurocrypt: Advances in Cryptology*, volume 765, pages 410–423 (1993)

[55] R. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory* **8**, 21 (1962)

[56] D. MacKay & R. Neal. Near shannon limit performance of low density parity check codes. *Electronics letters* **32**, 1645 (1996)

[57] S. Chung, G. Forney Jr, T. Richardson & R. Urbanke. On the design of low-density parity-check codes within 0.0045 db of the shannon limit. *Communications Letters, IEEE* **5**, 58 (2001)

[58] Ø. Marøy, M. Gudmundsen, L. Lydersen & J. Skaar. Error estimation, error correction and verification in quantum key distribution. *arXiv* quant-ph/1210.6520 (2012)

[59] C. H. Bennett, G. Brassard & J.-M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing* **17**, 210 (1988)

[60] C. H. Bennett, G. Brassard, C. Crepeau & U. M. Maurer. Generalized privacy amplification. *IEEE Transaction on Information Theory* **41**, 1915 (1995)

[61] J. L. Carter & M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences* **18**, 143 (1979)

[62] M. N. Wegman & J. L. Carter. New hash function and their use in authentication and set equality. *Journal of Computer and System Sciences* **22**, 265 (1981)

[63] P. W. Shor & J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters* **85**, 441 (2000)

[64] D. Mayers. Unconditional security in quantum cryptography. *Journal of the ACM (JACM)* **48**, 351 (2001)

[65] H.-K. Lo & H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050 (1999)

[66] D. Gottesman, H.-K. Lo, N. Lütkenhaus & J. Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information and Computation* **5**, 325 (2004)

[67] H. Inamori, N. Lütkenhaus & D. Mayer. Unconditional security of practical quantum key distribution. *European Physical Journal D* **41**, 599 (2007)

[68] V. Scarani & R. Renner. Security bounds for quantum cryptography with finite resources. *Theory of Quantum Computation, Communication, and Cryptography* pages 83–95 (2008)

[69] C. Fung, K. Tamaki, B. Qi, H. Lo & X. Ma. Security proof of quantum key distribution with detection efficiency mismatch. *Quantum Information & Computation* **9**, 131 (2009)

[70] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier & H. Weinfurter. Information leakage via side channels in freespace BB84 quantum cryptography. *New Journal of Physics* **11**, 065001 (2009)

[71] V. Makarov, A. Anisimov & J. Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A* **74**, 022313 (2006)

[72] A. Lamas-Linares & C. Kurtsiefer. Breaking a quantum key distribution system through a timing side channel. *Optics express* **15**, 9388 (2007)

[73] Y. Zhao, C. Fung, B. Qi, C. Chen & H. Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A* **78**, 042333 (2008)

[74] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth & H. Weinfurter. Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors. *New Journal of Physics* **13**, 073024 (2011)

[75] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov & G. Leuchs. After-gate attack on a quantum cryptosystem. *New Journal of Physics* **13**, 013043 (2011)

[76] V. Scarani & C. Kurtsiefer. The black paper of quantum cryptography: real implementation problems. *arXiv* quant-ph/0906.4547v1 (2009)

[77] D. Giggenbach, J. Horwath & K. Markus. Optical data downlinks from earth observation platforms. In *Proceedings of the SPIE Free-Space Laser Communication Technologies XXI*, pages 719903–1 (2009)

[78] M. Knapek, J. Horwath, N. Perlot & B. Wilkerson. The DLR ground station in the optical payload experiment (STROPEX): results of the atmospheric measurement instruments. In *Proceedings of the SPIE Free-Space Laser Communications VI*, page 63041U (2006)

[79] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Physical Review Letters* **91**, 057901 (2003)

[80] X.-B. Wang. Beating the photon-xnumber-splitting attack in practical quantum cryptography. *Physical Review Letters* **94**, 230503 (2005)

[81] H.-K. Lo, X. Ma & K. Chen. Decoy state quantum key distribution. *Physical Review Letters* **94**, 230504 (2005)

[82] B. Huttner, N. Imoto, N. Gisin & T. Mor. Quantum cryptography with coherent states. *Physical Review A* **51**, 1863 (1995)

[83] F. Moll, S. Nauerth, C. Fuchs, J. Horwath, M. Rau & H. Weinfurter. Communication system technology for demonstration of BB84 quantum key distribution in optical aircraft downlinks. In *Proceedings of the SPIE Laser Communication and Propagation through the Atmosphere and Oceans*, page 851703 (2012)

[84] C. Fuchs. Fine tracking system for aeronautical FSO links. In *Proceedings of the ASI Ka and Broadband Communications, Navigation and Earth Observation Conference* (2009)

[85] T. Schmitt-Manderbach. *Long distance free Space quantum key distribution.* Ph.D. thesis, Ludwig-Maximilians-Universität München (2007)

[86] M. Goresky & A. Klapper. *Algebraic Shift Register Sequences.* Cambridge University Press (2012)

[87] S. Nauerth. *Freiraumoptische Quantenkryptographie.* diploma thesis, Ludwig-Maximilians-Universität München (2007)

[88] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer & H. Weinfurter. Free space quantum key distribution: Towards a real life application. *Fortschritte der Physik* **54**, 840 (2006)

[89] H. Weier. *European Quantum Key Distribution Network.* Ph.D. thesis, Ludwig-Maximilians-Universität München (2011)

[90] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares & C. Kurtsiefer. Daylight operation of a free space, entanglement-based quantum key distribution system. *New Journal of Physics* **11**, 045007 (2009)

[91] G. Boyer, B. Lamouroux & B. Prade. air-flow-birefringence measurement. *JOSA* **65**, 1319 (1975)

[92] J. Song, Q. An & S. Liu. A high-resolution time-to-digital converter implemented in field-programmable-gate-arrays. *Nuclear Science, IEEE Transactions on* **53**, 236 (2006)

[93] P. Williams. Rotating-wave-plate stokes polarimeter for differential group delay measurements of polarization-mode dispersion. *Applied Optics* **38**, 6508 (1999)

[94] X. Ma, B. Qi, Y. Zhao & H.-K. Lo. Practical decoy state for quantum key distribution. *Physical Review A* **72**, 012326 (2005)

[95] Y. Zhao, B. Qi, X. Ma, H. Lo & L. Qian. Experimental quantum key distribution with decoy states. *Physical Review Letters* **96**, 070502 (2006)

[96] R. Konig, R. Renner & C. Schaffner. The operational meaning of min-and max-entropy. *Information Theory, IEEE Transactions on* **55**, 4337 (2009)

[97] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J. Poizat & P. Grangier. Single photon quantum cryptography. *Physical review letters* **89**, 187901 (2002)

[98] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J. Roch, A. Beveratos, R. Brouri-Tualle, J. Poizat & P. Grangier. Experimental open-air quantum key distribution with a single-photon source. *New Journal of physics* **6**, 92 (2004)

[99] T. Heindel, C. Kessler, M. Rau, C. Schneider, M. Fürst, F. Hargart, W. Schulz, M. Eichfelder, R. Roßbach, S. Nauerth et al. Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range. *New Journal of Physics* **14**, 083001 (2012)

[100] Z. Yuan, A. Dixon, J. Dynes, A. Sharpe & A. Shields. Practical gigahertz quantum key distribution based on avalanche photodiodes. *New Journal of Physics* **11**, 045019 (2009)

[101] M. Dušek, O. Haderka & M. Hendrych. Generalized beam-splitting attack in quantum cryptography with dim coherent states. *Optics Communications* **169**, 103 (1999)

[102] G. Brassard, N. Lütkenhaus, T. Mor & B. C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters* **85**, 1330 (2000)

[103] M. Tomamichel & R. Renner. Uncertainty relation for smooth entropies. *Physical Review Letters* **106**, 110506 (2011)

[104] M. Tomamichel, C. Lim, N. Gisin & R. Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications* **3**, 634 (2012)

[105] J. Hasegawa, M. Hayashi, T. Hiroshima & A. Tomita. Security analysis of decoy state quantum key distribution incorporating finite statistics. *arXiv* quant-ph/0707.3541 (2007)

[106] M. Hayashi. Upper bounds of eavesdropper's performances in finite-length code with the decoy method. *Physical Review A* **76**, 012329 (2007)

[107] R. Cai & V. Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics* **11**, 045024 (2009)

[108] T. Song, J. Zhang, S. Qin & Q. Wen. Finite-key analysis for quantum key distribution with decoy states. *Quantum Information & Computation* **11**, 374 (2011)

[109] M. Hayashi & R. Nakayama. Security analysis of the decoy method with the bennett-brassard 1984 protocol for finite key lengths. *arXiv preprint arXiv:1302.4139* (2013)

[110] H.-f. Zhang, J. Wang, K. Cui, C.-l. Luo, S.-z. Lin, L. Zhou, H. Liang, T.-y. Chen, K. Chen & J.-W. Pan. A real-time QKD system based on FPGA. *Journal of Lightwave Technology* **30**, 3226 (2011)

[111] qutools GmbH. http://www.qutools.com/

[112] M. Fürst, H. Weier, S. Nauerth, D. Marangon, C. Kurtsiefer & H. Weinfurter. High speed optical quantum random xnumber generation. *Optics Express* **18**, 13029 (2010)

[113] C. Williams, J. Salevan, X. Li, R. Roy & T. Murphy. Fast physical random xnumber generator using amplified spontaneous emission. *Optics Express* **18**, 23584 (2010)

[114] M. Wahl, M. Leifgen, M. Berlin, T. Rohlicke, H. Rahn & O. Benson. An ultrafast quantum random xnumber generator with provably bounded output bias based on photon arrival time measurements. *Applied Physics Letters* **98**, 171105 (2011)

[115] A. Shrestha & M. Brechtelsbauer. Transportable optical ground station for high-speed free-space laser communication. In *Proceedings of the SPIE Laser Communication and Propagation through the Atmospher and Oceans*, page 851706 (2012)

[116] J. G. Rarity, P. R. Tapster, P. M. Gorman & P. Knight. Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics* **4**, 82 (2002)

[117] B. Tryggvason, W. Duval, R. Smith, K. Rezkallah, S. Varma, R. Redden & R. Herring. The vibration environment on the international space station: its significance to fluid-based experiments. *Acta Astronautica* **48**, 59 (2001)

[118] J. Bienfang, A. Gross, A. Mink, B. Hershman, A. Nakassis, X. Tang, R. Lu, D. Su, C. Clark, C. Williams, E. Hagley & J. Wen. Quantum key distribution with 1.25 gbps clock synchronization. *Optics Express* **12**, 2011 (2004)

[119] A. Restelli, J. C. Bienfang, C. W. Clark, I. Rech, I. Labanca, M. Ghioni & S. Cova. Improved timing resolution single-photon detectors in daytime free-space quantum key distribution with 1.25 GHz transmission rate. *Selected Topics in Quantum Electronics, IEEE Journal of* **16**, 1084 (2010)

[120] J. Wang, B. Yang, S. Liao, L. Zhang, Q. Shen, X. Hu, J. Wu, S. Yang, Y. Tang, B. Zhong et al. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *arXiv* quant-ph/1210.7556 (2012)

[121] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro & J. G. Rarity. Low cost and compact quantum key distribution. *New Journal of Physics* **8**, 249 (2006)

# Abbreviations

| | |
|---|---|
| **ADC** | analog to digital converter |
| **AES** | advanced encryption standard |
| **APD** | avalanche photo diode |
| **CPA** | coarse pointing assembly |
| **cw** | continuous wave |
| **DAC** | digital to analog converter |
| **DLR** | German Aerospace Center<br>(Deutsches Zentrum für Luft- und Raumfahrt e.V.) |
| **DSP** | digital signal processor |
| **ECL** | emitter coupled logic |
| **FELT2** | free-space experimental laser terminal 2 |
| **FoV** | field of view |
| **FPA** | fine pointing assembly |
| **FPGA** | field-programmable gate array |
| **FSO** | free-space optical |
| **FSO** | free-space optical |
| **FWHM** | full-width at half-maximum |
| **GEO** | geosynchronous orbit |
| **GPS** | global positioning system |
| **IC** | integrated circuit |

| | |
|---|---|
| **IMU** | inertial measurement unit |
| **ISS** | international space station |
| **LDPC** | low density parity check |
| **LEO** | low earth orbit |
| **LFSR** | linear feedback shift register |
| **LVPECL** | low-voltage positive emitter-coupled logic |
| **OGS** | optical ground station |
| **PRBS** | pseudo random bit Sequence |
| **QBER** | quantum bit error ratio |
| **QKD** | quantum key distribution |
| **RTC** | real time clock |
| **SNR** | signal to noise ratio |
| **STD** | standard deviation |
| **TAN** | transaction authentication number |
| **UAV** | unmanned aerial vehicle |
| **UHF** | ultra high frequency |
| **VFR** | visual flight rules |
| **WCP** | weak coherent pulse |

# Danksagung

An dieser Stelle möchte ich mich herzlich bei all jenen Menschen bedanken, die diese Arbeit ermöglicht und zum ihrem Gelingen beigetragen haben. Mein Dank geht insbesondere an:

- Herrn Prof. Weinfurter, für sein Vertrauen und die Möglichkeit selbstständig an diesem Experiment zu arbeiten.
- Herrn Dr. Krebs
- Meine Crypto-Kollegen Markus Rau und Stefan Frick sowie auch den Wissenschaftlern am DLR, vor allem Florian Moll, Christian Fuchs und Joachim Horwath, die dieses Experiment mit mir zusammen realisiert und durchgeführt haben. Danke für Euren Einsatz bei Tag und auch für die zahllosen Stunden in eisigen Nächten.
- Die Piloten, Mechanikern und Organisatoren des DLR-Flugbetriebs, die unsere Flugcampagne mit großem Wohlwollen betreut und dabei das ein oder andere Auge zugedrückt haben.
- Alle weiteren Kollegen aus der Arbeitsgruppe Weinfurter: Almut, Andreas, Christian (Horst), Christoph, Chunlang, Daniel, Daniel, Daniel, Davide, Florian, Fredrick, Gwenaelle, Harald, Johannes, Julian, Juliane, Jürgen, Kai, Lars, Lea, Lukas, Magdalena, Marion, Markus, Michael, Nikolai, Norbert, Pavel, Roland, Wenjamin und natürlich ganz besonders an meine Crypto-Vorgänger Tobias, Henning und Martin, die mich vor allem zu Beginn meiner Arbeit sehr unterstützt haben. Ich habe die Zeit sehr genossen und das liegt vor allem an Euch.
- Jürgen Aust und Thomas Großhauser und das Werstattteam der LMU, die mit großer Hilfsbereitschaft diverse Bauteile für das Experiment hergestellt haben.
- Meine lieben Freunde, die mich mit ihrem Interesse immer wieder neu motiviert haben.
- Meine Frau Magdalena, die Erfolge und Mißerfolge im Laufe meiner Promotion geteilt und mich dabei immer unterstützt hat. Sowie an meine Große, Lucia, und meine Kleine, Sophia, die ihrem Papa so viele Spielstunden abgetreten haben.