Long distance free-space quantum key distribution

Tobias Schmitt-Manderbach

München 2007

Long distance free-space quantum key distribution

Tobias Schmitt-Manderbach

Dissertation at the Faculty of Physics
of the
Ludwig–Maximilians–Universität München

Tobias Schmitt-Manderbach
born in München, Germany

München, 16. Oktober 2007

Erstgutachter: Prof. Dr. Harald Weinfurter
Zweitgutachter: Prof. Dr. Wolfgang Zinth
Tag der mündlichen Prüfung: 17. Dezember 2007

Zusammenfassung

Im Zeitalter der Information und der Globalisierung nimmt die sichere Kommunikation und der Schutz von sensiblen Daten gegen unberechtigten Zugriff eine zentrale Stellung ein. Die Quantenkryptographie ist derzeit die einzige Methode, die den Austausch eines geheimen Schlüssels zwischen zwei Parteien auf beweisbar sichere Weise ermöglicht. Mit der aktuellen Glasfaser- und Detektortechnologie ist die Quantenkrypographie aufgrund von Verlusten und Rauschen derzeit auf Entfernungen unterhalb einiger 100 km beschränkt. Prinzipiell könnten größere Entfernungen in kürzere Abschnitte aufgeteilt werden, die dafür benötigten Quantenrepeater sind jedoch derzeit nicht realisierbar. Eine alternative Lösung zur Überwindung größerer Entfernungen stellt ein satellitenbasiertes System dar, das den Schlüsselaustausch zwischen zwei beliebigen Punkten auf dem Globus mittels freiraumoptischer Kommunikation ermöglichen würde.

Ziel des beschriebenen Experiments war es, die Realisierbarkeit satellitengestützter globaler Quantenschlüsselverteilung zu untersuchen. Dazu wurde ein freiraumoptisches Quantenkryptographie-Experiment über eine Entfernung von 144 km durchgeführt. Sender und Empfänger befanden sich jeweils in ca. 2500 m Höhe auf den Kanarischen Inseln La Palma bzw. Teneriffa. Die kleine und leichte Sendeeinheit erzeugte abgeschwächte Laserpulse, die mittels eines 15-cm Teleskops zum Empfänger geschickt wurden. Die Empfangseinheit zur Polarisationsanalyse und Detektion der gesendeten Pulse wurde in ein existierendes Spiegelteleskop für klassische optische Kommunikation mit Satelliten integriert. Um die nötige Stabilität und Effizienz der optischen Verbindung trotz atmosphärischer Turbulenzen zu gewährleisten, waren die Teleskope mit einem bidirektionalen automatischen Nachführungssystem ausgestattet.

Unter Verwendung des Standard-BB84 Protokolls wäre aufgrund hoher optischer Abschwächung und Streulicht ein sicherer Schlüsselaustausch mittels abgeschwächter Laserpulse jedoch nicht möglich. Die Photonenzahlstatistik folgt bei abgeschwächten Laserpulsen der Poisson-Verteilung, sodaß ein Abhörer von allen Pulsen, die zwei oder mehr Photonen enthalten, ein Photon abspalten und dessen Polarisation messen könnte, ohne den Polarisationszustand der verbleibenden Photonen zu beeinflussen. Auf diese Weise könnte er Informationen über den Schlüssel gewinnen, ohne dabei detektierbare Fehler zu verursachen. Um diesen Angriff zu verhindern, wurde im vorliegenden Experiment daher die kürzlich entwickelte Methode der sog. „Täuschpulse“verwendet, d.h. die Intensität der vom Sender erzeugten Pulse wurde auf zufällige Weise variiert. Durch Analyse der Detektionswahrscheinlichkeit der verschiedenen Pulse läßt sich ein Abhörversuch der beschriebenen Art erkennen. Dadurch konnte trotz der Verwendung abgeschwächter Laserpulse die Sicherheit des ausgetauschten Schlüssels bei einer Abschwächung von ca. 35 dB im Quantenkanal gewährleistet und eine Schlüsselrate von bis zu 250 bit/s erreicht werden.

Unser Experiment wurde unter realen atmosphärischen Bedingungen und mit vergleichbarer Kanalabschwächung wie zu einem erdnahen Satelliten durchgeführt. Daher zeigt es die Realisierbarkeit von satellitengestützter weltweiter Quantenschlüsselverteilung mit einem technologisch vergleichsweise einfachen System.

Abstract

In the age of information and globalisation, secure communication as well as the protection of sensitive data against unauthorised access are of utmost importance. Quantum cryptography currently provides the only way to exchange a cryptographic key between two parties in an unconditionally secure fashion. Owing to losses and noise of today's optical fibre and detector technology, at present quantum cryptography is limited to distances below a few 100 km. In principle, larger distances could be subdivided into shorter segments, but the required quantum repeaters are still beyond current technology. An alternative approach for bridging larger distances is a satellite-based system, that would enable secret key exchange between two arbitrary points on the globe using free-space optical communication.

The aim of the presented experiment was to investigate the feasibility of satellite-based global quantum key distribution. In this context, a free-space quantum key distribution experiment over a real distance of 144 km was performed. The transmitter and the receiver were situated in 2500 m altitude on the Canary Islands of La Palma and Tenerife, respectively. The small and compact transmitter unit generated attenuated laser pulses, that were sent to the receiver via a 15-cm optical telescope. The receiver unit for polarisation analysis and detection of the sent pulses was integrated into an existing mirror telescope designed for classical optical satellite communications. To ensure the required stability and efficiency of the optical link in the presence of atmospheric turbulence, the two telescopes were equipped with a bi-directional automatic tracking system.

Still, due to stray light and high optical attenuation, secure key exchange would not be possible using attenuated pulses in connection with the standard BB84 protocol. The photon number statistics of attenuated pulses follows a Poissonian distribution. Hence, by removing a photon from all pulses containing two or more photons, an eavesdropper could measure its polarisation without disturbing the polarisation state of the remaining pulse. In this way, he can gain information about the key without introducing detectable errors. To protect against such attacks, the presented experiment employed the recently developed method of using additional "decoy" states, i.e., the the intensity of the pulses created by the transmitter were varied in a random manner. By analysing the detection probabilities of the different pulses individually, a photon-number-splitting attack can be detected. Thanks to the decoy-state analysis, the secrecy of the resulting quantum key could be ensured despite the Poissonian nature of the emitted pulses. For a channel attenuation as high as 35 dB, a secret key rate of up to 250 bit/s was achieved.

Our outdoor experiment was carried out under real atmospheric conditions and with a channel attenuation comparable to an optical link from ground to a satellite in low earth orbit. Hence, it definitely shows the feasibility of satellite-based quantum key distribution using a technologically comparatively simple system.

Contents

1 Introduction

> *"You see, wire telegraph is a kind of a very, very long cat. You pull his tail in New York and his head is meowing in Los Angeles. Do you understand this?*
> *And radio operates exactly the same way: you send signals here, they receive them there. The only difference is that there is no cat."*
>
> Albert Einstein, asked to explain radio.

Today, nearly a century later, the "meow" would be sequenced into 0s and 1s. Data digitalisation, and the rapid increase in the speed with which data can be sent and processed, form the technological basis for the "information society" and "information economy" in which we live and work [1]. With information becoming a more and more important resource for companies and countries, the desire is growing to protect information against unauthorised access. This is especially relevant in connection with the rising interest in sharing information in a globalised world. We as individual people, as well as the whole economy, heavily rely on the availability of electronic communications and electronic transactions — but also on its security. Against this background, it is of utmost importance to provide the means for reliable and secure communication channels.

This is the goal of cryptography. The name is derived from the Greek words $\kappa\rho\upsilon\pi\tau\acute{o}\varsigma$ for *hidden*, or *secret*, and $\gamma\rho\alpha\varphi\acute{\eta}$ for *writing*. From the early beginnings some 4000 years ago, when ancient Egyptians used modified hieroglyphs to conceal messages, the art of cryptography has undergone radical changes. The advent of computers has revolutionised both code making and code breaking. Nowadays, electronic communications rely on established and standardised encryption techniques, such as RSA and AES, whenever sensitive data, for example, credit card numbers, or personal identification numbers, are transmitted [2]. The security of these techniques, however, rests on complexity statements on the involved mathematical algorithms that are not yet proven. The threat of the existence and discovery of simpler algorithms might be abstract at present, just as is the menace of quantum computers becoming usable for realistic attacks. However, it is a fact, that the computational power available for a given amount of money still continues to rise exponentially, and thus the potential to crack longer and longer cryptographic keys. Encryptions that are considered safe today will likely be broken by a standard consumer PC in a few years' time, just like it has happened several times in the past [3, 4].

Classical cryptography can indeed provide an unbreakable symmetric secret-key cipher, the Vernam cipher [5], most often called one-time-pad. Provided the secret key is purely random, as long as the message itself, and used only once, the one-time-pad resists adversaries with unlimited computational and technological power [6]. The main drawback of the one-time-pad is the necessity to distribute a large amount of secret key material, and has prevented its wider use. It is at this point that quantum mechanics can offer a unique solution to the key distribution problem: Quantum key distribution (QKD) [7–9] provides currently the only way to exchange a crytographic key between two parties in an unconditionally secure fashion. Its security is not based on assumption on the adversary's limited technology, but rests on the validity of quantum mechanics itself: Unlike classical information, an unknown quantum state cannot be perfectly copied [10]. Thus, any eavesdropping attempt will disturb the transmitted quantum states — leading to errors, that are detectable by the legitimate users. A fundamental principle of QKD is that this error rate imposes a bound on the amount of information an adversary could have on the raw key. If the error rate is too high and jeopardising the secrecy of the key, the legitimate users discard the key and start anew. Otherwise, they apply a classical privacy amplification scheme to diminish the adversary's partial information on the final key arbitrarily close to zero.

Quantum key distribution has been implemented in a number of experiments mainly based on optical fibres (see e.g., [11–15] and references therein). Being the first technology of the field of quantum information to have reached some state of maturity, first commercial fibre-based QKD systems are already available on the market[1]. However, owing to the noise of available single-photon detectors together with losses and decoherence effects in the fibre, the distance that can be bridged with current technology is limited to the order of 100–200 km [16–20].

Several approaches have been proposed to overcome this problem. In principle, any large distance can be subdivided into smaller segments by introducing intermediate nodes. Secret keys are then exchanged first between adjacent nodes, followed by subsequent bitwise XOR-steps that combine two keys from neighbouring links into a single new one, until, finally, a secret key between the two initial end points is established. For this scheme to work, all intermediate nodes must be trustworthy. When the distance is long, a large number of trusted nodes are required. The requirement of trust can be dropped if the classical repeater stations are replaced by quantum repeaters to faithfully transfer the unknown quantum states via entanglement teleportation, thereby avoiding the conversion into classical information [21, 22]. Even though some of the key techniques involved have been demonstrated (e.g., entanglement swapping and entanglement purification), it seems fair to say, that a fully functional practical quantum repeater is still beyond current technology. Moreover, the individual segments between repeater stations would by far not be of global scale. Hence, an impractical large number of repeater stations would be required to bridge intercontinental distances.

[1] id Quantique, *http://idquantique.com*; MaqiQ Technologies, *http://www.magiqtech.com*

To overcome the distance restrictions, a satellite-based global key exchange system has been envisioned [23–27], allowing for key exchange between two arbitrary points on the globe. The idea is to establish an optical free-space link from a ground station to a dedicated satellite in earth orbit. As the satellite passes over different locations on earth, separate keys are exchanged with each ground station. Thus, a single satellite may cover a large portion of the earth's surface. Supposing that ground stations A and B want to establish a secret key, the satellite would have to store the key from ground station A securely until the ground station B came into view. This reduces the problem of many trusted nodes (necessary for a fibre-based connection) to just one trusted satellite. It should be noted, that even the satellite wouldn't need to be trustworthy if an entanglement-based quantum cryptographic scheme was employed [12, 28–37]. In this case, however, the two ground stations wishing to exchange a key must be in the satellites reach simultaneously. Depending on the specific orbit, and the location of the ground stations, this requirement may reduce the duration and number of available links drastically.

Free-space links between earth and a satellite benefit from the fact that most of the communication path is in empty space, where the photons can freely propagate, and only a short section of the path is in earth's atmosphere. Furthermore, the atmosphere provides low absorption in the spectral range of 600–850 nm, where good single-photon detectors are available, and exhibits almost no birefringence, which allows to encode the quantum information into the polarisation degree-of-freedom of photons.

Up to now, the longest free-space QKD demonstrations covered distances one order of magnitude shorter than in optical fibres [37–40]. Moreover, implementations based on entangled photons [37, 40, 41] or single photon sources [42–44] generally require a rather complicated and delicate setup, which is less suited to the mass, power, and complexity restrictions of a spaceborne transmitter module. A transmitter generating attenuated laser pulses is technologically much simpler, but even for average photon numbers well below one, the Poissonian nature of the laser photon statistics opens a back door for a photon-number-splitting (PNS) attack [45–47]: By removing a photon from all pulses containing two or more photons, and delaying the measurement of its state after bases announcement, an adversary can learn a significant portion of the key without introducing errors. In conditions of low channel transmittance, he may even obtain the full key. To avoid such leakage one has to strongly attenuate the laser pulses, approximately proportional to the link efficiency. Therefore, former QKD experiments using attenuated laser pulses did either not provide security against photon-number splitting attacks, or suffered from poor efficiency.

The recently developed idea of decoy state protocols [48–50] provides an elegant solution to this problem. Instead of using a fixed average photon number, the transmitter creates additional "decoy" pulses of various intensities. By comparing the receiver's detection probability of the individual pulse classes, the PNS attack can be detected. Thus, the decoy-state analysis opens the possibility for attenuated pulse systems to be secure over larger distances with an efficiency close to single-photon QKD. Not long ago,

decoy state protocols have seen first demonstrations in optical fibres [14, 15, 18, 19] and, at the same time, in free space [51].

The goal of the experiment presented in this thesis was to investigate the feasibility of satellite-based global quantum key distribution. This work describes the distribution of a quantum key over a real distance of 144 km between the Canary islands of La Palma and Tenerife. This free-space link provides a realistic test bed for optical communication to space: Even though the actual link distance is somewhat shorter than a link from a satellite in low earth-orbit (LEO) to a ground station (typically close to 350 km), the path length *through atmosphere* is already much larger. In fact, simulations suggest that the expected link transmittance from a LEO satellite will be comparable [27]. The simple and lightweight transmitter setup, based on attenuated laser pulses in combination with a decoy state scheme, was located on the island of La Palma. The quantum signal was transmitted over 144 km optical path at a mean altitude of 2400 m to the island of Tenerife. There, the quantum receiver was integrated into an existing telescope for classical optical satellite communications, the European Space Agency's Optical Ground Station (OGS). To achieve the necessary link efficiency and stability in the presence of slowly varying atmospheric influences, bidirectional active telescope tracking for continuous optimisation of the channel transmittance was implemented. Still, due to stray light and dark counts, secure communication over such a distance would not be possible anymore with the standard BB84 protocol. However, using the decoy-state analysis, the secrecy of the cryptographic key could be ensured.

Overview

This thesis is organised as follows. Chapter 2 establishes some required theoretical background on quantum key distribution. Different classes of attacks on the quantum channel are briefly reviewed, with emphasis on the photon-number-splitting attack that plays an important role in QKD schemes utilising attenuated pulses. This specific attack leads to poor performance of the standard BB84 protocol in scenarios involving high losses in the quantum channel. It is shown how this problem can be overcome with the help of decoy states and a refined data analysis. The specific protocol used in the experiment is laid out in greater detail. The chapter concludes with a brief description of the classical part of the protocol. Chapter 3 deals with the specific challenges of using the atmosphere as the quantum channel. Some fundamental principles and relevant effects associated with the propagation of a laser beam through the turbulent atmosphere are presented. Chapter 4 is devoted to the characterisation of the inter-island optical link. Measured losses and turbulence parameters are compared with predictions based on the theory presented earlier. The results indicate that active beam steering techniques are required to mitigate the deleterious effects of beam wander for our QKD experiment. Finally, the implemented telescope tracking system is presented. Chapter 5 introduces the experimental setup with its individual components. The ordering of the different

parts roughly reflects the temporal sequence of events, from the generation of the quantum signal, its transmission, up to its detection at the receiver. The characterisation of the individual building blocks allows to calculate the expected performance of our QKD system. In chapter 6, the procedure and aspects of data analysis and processing for the presented experiment are explained. The individual steps from the detection of raw events to the distillation of secret key bits are presented and analysed in detail, and associated problems are discussed. Chapter 7 summarises the experimental results and places them into the context of satellite-based QKD. Remaining challenges and future fields of work are identified as an outlook.

2 Theory of quantum key distribution

2.1 Security in QKD

It is the goal of quantum key distribution (QKD) to enable two distant parties, traditionally called *Alice* and *Bob*, to establish a common *secret key*, that is, a string of random bits which is unknown to an adversary, *Eve*. An important difference to classical key distribution schemes is that the security of the final key can actually be proven under a very limited number of logical assumptions. The strongest reasonable notion of security is *information-theoretic* security (also called *unconditional* security), which guarantees that an adversary does not get any information correlated with the key, except with negligible probability. A weaker level of security is computational security, where one only requires that it is difficult (i.e., time-consuming, but not impossible) for an adversary to compute information on the key. This is the type of security that is typically sought-after in classical cryptographic algorithms.

Under the sole assumption that Alice and Bob are connected by a classical authenticated[1] communication channel, secret communication - and thus also the generation of a secret key - is impossible [6]. This changes dramatically when quantum mechanics comes into play. Bennett and Brassard were the first to introduce a quantum key distribution scheme, which uses communication over a — completely insecure — quantum channel in addition to the classical channel [8]. This scheme is commonly known as the BB84 protocol, although foundations were already laid by Wiesner [7].

In general, a typical *prepare-and-measure*[2] quantum key distribution protocol consists of two phases:

Phase I: A physical apparatus generates quantum mechanical signals[3], which are distributed to, and eventually measured by the communicating parties. The measure-

[1] To rule out a man-in-the-middle attack where Eve impersonates Bob to Alice, and vice versa, Alice and Bob should authenticate the data sent in the classical channel. This requires a short pre-shared key.

[2] In a prepare-and-measure protocol, Alice simply prepares a sequence of single photon signals and transmits them to Bob. Bob immediately measures those signals; thus, no quantum computation or long-term storage of quantum information is necessary, only the transmission of single photon states.

[3] These signals are usually described by qubits. In practical QKD, flying qubits are always realised as photons. In the following, the term *qubit* is therefore often used equivalently with a two-level degree-of-freedom of a single photon.

ment results obtained by Alice and Bob represent classical data describing their knowledge on the prepared signals.

Phase II: Using their authenticated classical channel, Alice and Bob exchange information on their data, for example by sifting, error correction, or privacy amplification procedures.

A theoretical security and efficiency analysis of a QKD protocol provides statements on how exactly to convert the data obtained in phase I into a secret key in phase II.

QKD is generally based on the impossibility to observe a quantum mechanical system without changing its state. An adversary trying to wiretap the quantum communication between Alice and Bob would thus inevitably leave traces, which can be detected. Hence, a QKD protocol achieves the following type of security: As long as the adversary is passive, it generates a secret key. However, in case of an attack on the quantum channel jeopardising the security of the final key, the protocol recognises the attack and aborts the generation of the key with very high probability[4]. The public classical channel used in the second phase of the protocol needs to be protected against a man-in-the-middle attack. Otherwise, Alice may be unaware that she has accidentally exchanged a secret key with Eve instead of Bob, for example. To prevent this attack, Alice and Bob have to authenticate the data sent in the classical channel. Since the authentication of an N-bit message requires only $O(\log N)$ secret bits [52], Alice and Bob can generate more secret bits by QKD than bits are consumed for authentication during the protocol, provided they share a short initial key. Consequently, one should rather speak of QKD as *quantum key growing*.

2.2 QKD with the BB84 protocol

The BB84 protocol uses an encoding of classical bits in qubits, that is, two-level quantum systems. The encoding is with respect to one of two different orthogonal bases, called the *rectilinear* and the *diagonal basis*. These two bases are mutually unbiased (*maximally conjugate*) in the sense that any two states from different bases have overlap probability 1/2. Thus, a measurement in one of the bases reveals no information on a bit encoded with respect to the other basis. Very commonly, the signal states are realised as single photons in linear polarisation states, where horizontal $|H\rangle$ and vertical $|V\rangle$ polarisation states form the rectilinear basis, and the diagonal basis consists of polarisations along 45°, $|+45\rangle$, and 135°, $|-45\rangle$.

In the first step of the protocol, Alice chooses N random bits $X_1, ..., X_N$, encodes each of these bits into qubits using at random either the rectilinear or the diagonal basis, and transmits them to Bob via the quantum channel. Bob measures each of the qubits he receives with respect to (a random choice of) either the rectilinear or the diagonal basis

[4]The abortion probability is a security parameter, that can be chosen arbitrarily close to unity.

to obtain classical bits Y_i. The pair of classical bitstrings X and Y held by Alice and Bob after this step is called the *raw key* pair.

The remaining part of the protocol is purely classical, in particular, Alice and Bob communicate only classically from here on. First, in the *sifting step*, Alice and Bob announce their choices of bases used for the encoding and the measurement, respectively. Since only bits where the basis is the same for the encoding and for the measurement give a deterministic relation between signal and measurement outcome, they keep only those bits of the raw key, discarding all other ones. The result is called the *sifted key*.

In an experimental implementation, noise is always present leading to a certain bit error ratio in the sifted key even if the adversary is passive. However, as these errors are not distinguishable, even in principle, from errors caused by an attack, they have have to be attributed to eavesdropping activity. To be able to yield an error-free and secret key, the key distribution protocol has to be amended by two steps:

The first is the *reconciliation* (or error correction) step, leading to a key, shared by Alice and Bob. In an either one-way or interactive procedure, Alice and Bob exchange certain error correcting information on the sifted key strings X', Y'. In order to quantify the quantum bit error ratio[5] (QBER), i.e., the fraction of positions i in which X'_i and Y'_i differ, Alice and Bob either compare some small randomly chosen set of bits of their sifted key, or derive the QBER directly from the error correcting procedure. If the error ratio is too large — which might indicate the presence of an adversary — the protocol has to be aborted.

The second step deals with the situation that the eavesdropper has to be assumed to be in possession of at least some knowledge about the reconciled string, originating possibly both from an attack on the quantum signals, and from the error correcting information. Therefore, in the final step of the protocol, Alice and Bob apply two-universal hashing [53] to turn the (generally only partially secret) string X' into a shorter but secure key. This technique is the generalised *privacy amplification* procedure introduced by Bennett et al. [54].

2.3 Eavesdropping attacks on the ideal protocol

In order to ensure unconditional security for a QKD protocol, a security proof needs to take into account all possible classes of attacks Eve might conduct. From the theoretical point of view of quantum mechanical measurements, any eavesdropping attack can be thought of as an interaction between a probe and the quantum signals. Eve then performs measurements on the probe to obtain information about the signal states. In this framework, three main classes of attacks are possible:

Individual attacks: The adversary is supposed to apply some fixed measurement operations to each of the quantum signals, that is, Eve lets each of the signals interact

[5] This quantity is most often called "quantum bit error *rate*", but it is actually a ratio, not a rate.

with a separate probe (unentangled to the other probes) and measures the probes separately afterwards.

Collective attacks: As in the individual attack, each signal interacts with its own independent probe. In the measurement stage of an collective attack, however, the restriction for Eve to measure the probes individually is dropped: Eve is allowed to perform measurements on all probes coherently.

Coherent attacks: In the most general (also called *joint attacks*), Eve can apply the most general unitary transformation to all the qubits simultaneously. Effectively, this means that Eve has access to all signals at the same time.

A further differentiation of these attacks can be made by determining whether Eve may delay the measurement of the probes till receiving all classical data, that Alice and Bob exchange for error correction and privacy amplification.

As shown in [55], individual attacks are generally weaker than collective attacks. Hence, the security against individual attacks does not imply full security. Meanwhile, methods have been developed to prove unconditional security, that is, security against coherent attacks. However, it turns out that it is often sufficient to consider only collective attacks, since for typical protocols coherent attacks are not stronger than collective attacks [56].

2.3.1 Some specific attacks

Intercept-resend attack

The intercept-resend attack is an individual attack, where Eve performs a complete measurement on the signals, and subsequently prepares a new quantum state she sends on to Bob. By removing Alice's signal states from the quantum channel close to the transmitting unit, and reinjecting the prepared quantum state close to Bob's detection device, Eve is able to circumvent all channel imperfections. The simplest example is an intercept-resend attack in the BB84 protocol: Eve performs a measurement of each signal state in one of the signal bases and prepares a state which corresponds to her measurement result. This leads to an average error rate in the sifted key of 25%, composed of events with 0% error whenever Eve uses the same basis as Alice and Bob, and events with 50% whenever her basis differs from theirs. In this way, Eve learns 50% of the sifted key.

Optimal individual attack

A more advanced form of measuring for the adversary involves positive operator-valued measures (POVMs) which allow to increase the ratio of gathered information per induced disturbance. Lütkenhaus investigated the use of POVMs under the restriction that Eve performs her measurements before Alice reveals the basis [57]. A good indicator

for the possibility to recover a safe cryptographic key is the comparison of the mutual information I_{AB} between Alice and Bob (after eavesdropping) to the mutual informations I_{AE} and I_{BE} between Alice and Eve, and between Bob and Eve, respectively. If (whether due to eavesdropping or channel noise) $I_{AB} \leq \min\{I_{AE}, I_{BE}\}$, Alice and Bob cannot establish a secret key any more, using only one-way classical post-processing[6]. In [57], equality is reached for an error rate of $\approx 15\%$.

In [58], the use of a quantum cloning machine (restricted to a probe consisting of a single qubit) is investigated, achieving a marginal advantage over the strategy mentioned above. The optimal individual attack utilises two qubits as a probe and attains the best possible ratio between Eve's information gain and her induced disturbance [59, 60]. The threshold noise level for a potentially safe channel is therefore a QBER of $(1-1/\sqrt{2})/2 \approx 14.6\%$. The entangling-probe attack has been physically simulated recently [61] using single-photon two-qubit quantum logic. There, Eve entangles her probe qubit with the qubit that Alice sends to Bob, with the help of a controlled-NOT (CNOT) gate. Eve then makes her measurement on the probe to obtain information on the sent signal state, at the expense of imposing detectable errors between Alice and Bob. By preparing the initial state of her probe qubit, Eve can adjust the strength of her interaction, thereby determining the amount of information she can obtain and the error rate she will inadvertently create.

2.4 Other protocols

Since the invention of quantum cryptography, a large variety of alternative QKD protocols has been proposed. Some of them are optimised to be very efficient with respect to the secret-key rate, that is, the number of key bits generated per transmitted quantum state. Others are designed to cope with higher noise levels, which makes them more suitable for practical implementations [62]. The structure of the protocols that are outlined in the following, is largely very similar to the BB84 protocol.

Two-state protocol: B92

The B92 protocol [63] is conceptionally the simplest of all protocols, and shows that two non-orthogonal states are already sufficient to implement secure QKD. In the case of the qubits being realised as polarisation encoded single photons, Alice chooses randomly between the horizontal polarisation state $|H\rangle$ and the diagonal polarisation state $|+45\rangle$, which represent the bit values 0 and 1, respectively. Bob performs measurements randomly either in the rectilinear or the diagonal basis. Detection outcomes $|V\rangle$ and $|-45\rangle$ allow Bob to infer the bit value with certainty, whereas the orthogonal results are inconclusive. In the sifting step, Bob announces only on which signals he obtained

[6] That is, a post-processing scheme derived from a one-way entanglement purification protocol. See §2.4.1 for more details.

conclusive results, but not the measurement basis, since this would effectively reveal the bit value itself. The inconclusive events are discarded for key generation.

In a system with losses, such a scheme is prone to an unambiguous state discrimination attack [64,65]. Eve could perform measurements on the signal states similar to Bob, and selectively block those photons on which she obtained inconclusive measurement results, while re-sending photons she has identified with certainty on to Bob. If the latter is done avoiding the channel losses, the eavesdropper can (in a certain parameter regime) compensate the decreased transmission rate caused by the blocked signals, and stay undetected. By incorporating the non-orthogonality between the states as a continuous parameter of the scheme, the region of channel transmittance allowing for secure key generation can be optimised [65].

The two-state protocol can also be realised using interference between a bright (reference) pulse and a dim pulse containing less than one photon on average [63,66]. The qubit is encoded in the relative phase shift between the dim pulse and the reference pulse. This approach makes the protocol more resistant to eavesdropping in high loss conditions: If Eve obtains an inconclusive measurement result, she cannot simply block the strong pulse, because Bob can easily monitor its presence. Neither can Eve block the dim pulse, since the interference of the reference pulse with vacuum results in errors. Likewise, Eve would inevitably introduce detectable errors if she prepared her own dim and/or strong pulse and sent them to Bob. Although the BB92 protocol can be made unconditionally secure, Eve's information gain for a fixed disturbance of Alice's qubits is larger than for the BB84 protocol [59].

Six-state protocol

The six-state protocol [67,68] uses three conjugate bases for the encoding, but is otherwise identical to the BB84 protocol. The three bases (rectilinear, diagonal, and circular polarisation) are used with equal probability. Therefore, the probability for Alice and Bob choosing compatible bases is only 1/3. On the other hand, eavesdropping causes a higher error rate compared to a four-state protocol. This results in a higher noise threshold that can be tolerated.

Generally, the probabilities for choosing the different bases of a QKD protocol need not be equal. On the contrary, the efficiency of the protocol is increased if one of the bases is selected with probability almost one [69]. In this case, the choice of Alice and Bob will coincide with high probability, which means that the number of bits to be discarded in the sifting step is small. However, this advantage comes at the cost of a decreased tolerable error rate, because also an adversary has higher probability to guess the correct basis.

SARG protocol

The idea of the B92 protocol to use a pair of non-orthogonal states to encode the bit values 0 and 1 can be extended to more than one pair in order to enhance the robustness of the resulting protocol to photon number splitting attacks compared to BB84 (see §2.5.2). The SARG protocol [62] differs from the BB84 protocol only in the classical sifting procedure, but uses the same four quantum states. It allows to generate unconditionally secure key not only from the single photon component of a weak laser pulse source, but also from the two-photon signals [70]. This is not surprising from the viewpoint of unambiguous state discrimination: unambiguous discrimination among N states of a qubit space is only possible when at least $N-1$ identical copies of the state are available for measurement [71]. In the case of 4 states as in BB84, at least 3 copies are required for Eve to distinguish the states. Hence, it is safe to use not only one-photon signals, but also two-photon signals for key generation in the SARG protocol.

To implement the SARG protocol, Alice prepares randomly one of four quantum states and Bob performs measurements either in the rectilinear or the diagonal basis exactly as in the BB84 protocol. The classical part of the protocol, however, is modified: instead of revealing the basis, Alice announces publicly which one of the four pairs of non-orthogonal states $\{|H\rangle, |+45\rangle\}, \{|+45\rangle, |V\rangle\}, \{|V\rangle, |-45\rangle\}, \{|-45\rangle, |H\rangle\}$ she used for encoding the bit value, where $|H\rangle, |V\rangle$ represent 0, and $|+45\rangle, |-45\rangle$ represent 1. If Bob finds a state orthogonal to one of the two announced states, he learns the bit value conclusively. For example, if Bob detects $|V\rangle$, and Alice used the pair $\{|H\rangle, |+45\rangle\}$, he concludes that Alice has sent the state $|H\rangle$, corresponding to the bit value 0. Otherwise, if Bob's detection outcome is not orthogonal to the announced states, the event is discarded (analogous to the B92 protocol). In comparison with BB84, the SARG protocol allows secure key generation with attenuated laser pulses for higher channel losses. The scheme can be extended to more than 4 sets of non-orthogonal states to enable key generation from even higher multi-photon components [70].

2.4.1 Security proofs

Since the eavesdropper is allowed unlimited technological resources within the limits of the laws of physics, he may perform the most sophisticated and general attack imaginable. Hence, developing a formalism that takes into account any eavesdropping strategy is not easy, and so it took, from the invention of quantum cryptography, more than a decade to prove the unconditional security of QKD, even for an idealised system. Preferably, security should be achieved in the sense of a *universally composable* security definition: This implies that the key can safely be used in any arbitrary context, except with some small probability ϵ. The underlying idea is to characterise the security of the secret key by the maximum probability ϵ that it deviates from a perfect key (i.e., a key that is uniformly distributed and independent of the adversary's information).

The earliest ultimate, but rather complicated, security proof is due to Mayers [72, 73].

Since then, several different techniques have been applied to the problem, originating both from quantum theory and from information theory. The proofs by Lo and Chau [74] required Alice and Bob to have a quantum computer. This condition could be dropped in a subsequent important proof by Shor and Preskill [75], which unifies the ideas of Mayers and Lo and Chau. The key result of their work is that the security of QKD can be expressed in terms of an underlying entanglement purification protocol (EPP). This is based on the following observations.

Instead of preparing her system in a certain state and then sending it to Bob, Alice can equivalently prepare an entangled state, send one of the qubits to Bob, and later measure her subsystem. Thus, she effectively prepares Bob's system from a distance. If the joint system of Alice and Bob is in a pure state, then it cannot be entangled with any third party; especially it cannot be entangled with any of Eve's auxiliary systems (monogamy of entanglement). Hence, simple measurements on the entangled pair provide Alice and Bob with data totally unknown to Eve. Furthermore, if the state shared by Alice and Bob is maximally entangled, then their measurement results are maximally correlated. Therefore, Alice and Bob can obtain the desired secret bits by performing some entanglement purification protocol.

Since one is interested in the security of protocols implemented with available technology, one does not want to actually run a general entanglement distillation protocol, because this would require the storage of quantum states and quantum computation steps. The problem can be overcome by using the fact that certain entanglement distillation protocols are mathematically equivalent to quantum error correction codes. One example are the *Calderbank-Shor-Steane* (CSS) codes, which have the property that bit errors and phase errors can be corrected separately. Since the final key is classical, its value does not depend on the phase errors. Hence, Alice and Bob actually only have to correct the bit errors, which is a purely classical task. In this way, the quantum protocol becomes equivalent to the standard BB84 protocol; the decoding operation of the CSS quantum error correction turns into classical error correction and privacy amplification, and no quantum manipulation capabilities are required. With this technique, Shor and Preskill showed that BB84 is secure whenever the error rate is less than 11%. The proof has been adapted to other protocols like B92, and the six-state protocol [76, 77].

The principle exploiting the entanglement purification method uses effectively only one-way communication. This idea can be extended to two-way entanglement purification schemes, which tolerate higher noise levels in the channel than one-way EPPs. The equivalent QKD protocols require two-way classical communication between Alice and Bob in the post-processing step of classical data (i.e., in the error correction and privacy amplification stage)[7].

It turns out that the detour via entanglement purification is neither necessary nor

[7] In fact, *any* implementation of the BB84 (or six-state) protocol requires two-way classical communications anyway. For example, in the basis comparison step, it is necessary to employ two-way classical communication. Of course, the "one-way" classical post-processing requires fewer rounds of communication (and therefore less time) to complete.

	BB84		Six-state	
	one-way	two-way	one-way	two-way
Upper bound	14.6%	25%	16.7%	33.3%
Lower bound	11.0%	20.0%	12.7%	27.6%

Table 2.1: Upper and lower bounds on the tolerable bit error rate for the ideal BB84 and six-state protocols using one-way and two-way classical post-processing [81, 82].

optimal. Secret key agreement might be possible even if the state describing Alice and Bob's joint system before error correction and privacy amplification does not allow for entanglement distillation. This newer class of security proofs is based on information-theoretic arguments [78–80].

2.4.2 Bounds on performance

In QKD experiments, one is interested in maximising three quantities — the key generation rate, the tolerable error rate, and, closely related, the maximal secure distance. Concerning the robustness with respect to noise, there are a number of upper and lower bounds known for the allowable bit error rate.

Table 2.1 summarises known lower and upper bounds for the BB84 and the six-state protocol, both for one-way and two-way classical communication. The upper bounds are derived by considering some simple individual attacks, and determining when these attacks can defeat QKD. The lower bounds can be determined by the unconditional security proof assuming that Eve is performing an arbitrary attack allowed by the laws of quantum mechanics and Alice and Bob employ some special data post-processing schemes[8]. The upper bounds for one-way post-processing come from attacks based on optimal approximate cloning machines. Although one-way error correction and privacy amplification alone cannot provide Alice and Bob with a secure key beyond this QBER, the more general class of protocols utilising two-way communication can guarantee secrecy up to a higher level of QBER. The ultimate upper limit for two-way post-processing originate from the intercept-resend eavesdropping strategy. For BB84, this attack results in the known error rate of 25%. For the six-state scheme, intercept-resend leads to an error rate of 1/3. As stated before, the six-state scheme can intrinsically tolerate a higher bit error rate than BB84.

The Shor and Preskill proof of security shows that BB84 with one-way communication can be secure with a secret key rate of at least $1 - 2H_2(e)$, where e is the QBER and $H_2(x) = -x \log_2 x - (1-x) \log_2(1-x)$ is the binary Shannon entropy. The key rate reaches 0 when e is roughly 11.0%. Gottesman, Lo and Chau showed [81, 82] that it

[8] The lower bounds in the one-way classical communication case can be improved to 12.4% and 14.1% for the BB84 and the six-state protocol, respectively, if the legitimate users add some noise to the sifted key as the first classical postprocessing step [79, 80].

is possible to create prepare-and-measure QKD schemes based on two-way EPPs, and that the advantage of two-way EPPs to tolerate higher error rates can survive. The resulting QKD protocol includes a pre-processing with two-way classical communication before the conventional information reconciliation and can tolerate 20.0% error rate. Also, the key rate is increased when the error rate is higher than about 9%. Recently, this kind of two-way communication was applied to QKD protocols with weak coherent pulses [83, 84]. It should be noted that this kind of two-way preprocessing is also known in the classical key agreement context, in which it is usually called advantage distillation.

The highest key rates for the ideal BB84 and six-state protocols up to now are achieved by converting a two-way breeding EPP [85] into a QKD protocol [86] that is assisted by one-time pad encryption with a pre-shared key [87]. The improvements in distillable key are most noticeable in the regime of medium to high error rates, i.e., $\sim$ 8% to $\sim$ 13% QBER.

2.5 QKD with realistic devices

Up to now we have considered an idealised situation where Alice prepares perfect quantum states, and Bob performs ideal measurements. Real-life QKD systems, however, suffer from many types of imperfections. For instance, the detection apparatus is normally composed of so-called threshold (on/off) detectors, which just report the arrival of photons, and do not tell how many of them have arrived. Moreover, detectors often suffer false detection events due to background and intrinsic dark counts. Also, some misalignment in the detection system is inevitable. The signal states — single-photon Fock states — assumed by BB84 and its derivatives, are even more difficult to realise experimentally. It's by no means a matter of course that the unconditional security of QKD can be maintained under these circumstances, but with additional measures, this is fortunately the case [88, 89].

2.5.1 QKD with attenuated pulses

Although single photon sources may well be very useful for quantum computing, they are *not* required for QKD. Currently single photon sources are rather impractical for QKD. Instead, attenuated laser pulses are often used as signals in practical QKD devices. The electromagnetic field can be well approximated by a monochromatic coherent state, provided the spectral width of the laser pulses is much smaller than their mean wavelength. Those attenuated laser pulses, when phase randomised, follow a Poissonian distribution in the number of photons, i.e., the probability of having n photons in a signal is given by

$$P_\mu(n) = \frac{\mu^n}{n!}\, e^{-\mu}, \tag{2.1}$$

where μ is the mean number of photons, and is chosen by the sender. In order to keep the probability of emission of a multi-photon pulse low, μ is commonly set below 1. Still, there is always non-zero probability of emitting two or more photons.

2.5.2 Photon-number splitting attacks

Employing attenuated laser pulses instead of perfect single photons calls for including another attack strategy — in addition to the attacks presented so far — into the security proof: so-called *photon-number splitting (PNS) attacks* [45–47, 64]. However, the following applies not only to attenuated pulse schemes, but affects in principle all sources having a finite probability of emitting more than one photon: Provided all photons emitted in a multi-photon signal encode the same qubit, Eve can steal a copy of the information without Alice and Bob noticing it. Nevertheless, we will concentrate in the following on the combination 'BB84 protocol with attenuated pulses'.

Beam splitting attack

The concept of the beam splitting attack uses the idea that a lossy quantum channel can be described as a combination of a lossless channel and a beam splitter, which accounts for the losses of the original channel. Eve monitors the second output arm of the beam splitter, while Bob obtains the transmitted part. If a multi-photon signal is split at the beam splitter such that Bob and Eve get at least one photon of the signal, the eavesdropper can gain complete knowledge of this sifted key bit via a delayed measurement: Eve waits until Alice and Bob publicly communicate the polarisation basis and then measures her photon(s) in the correct basis. In this way, Eve learns a fraction of the sifted key deterministically, depending on the fraction of multi-photon signals emitted by Alice that enter the sifted key. One can show that the fraction f of the sifted key known to Eve is [88]

$$f_{\mathrm{BS}} = 1 - e^{-\mu(1-\eta)}, \tag{2.2}$$

where η is the transmission of the original lossy channel. The fraction f is plotted versus the channel transmission for a value of the mean photon number μ of 0.1 in Figure 2.1 (dashed red curve). It is clear that this attack cannot be excluded by Alice and Bob by any additional test of the channel, since it represents the physical model of the channel. However, the beam splitting attack is very ineffective when replacing channels with high losses, that is, large transmission distances: the known key fraction saturates at a level of order μ. In that case, for example, two-photon signals are more likely to see both photons being directed to Eve (and therefore becoming useless) rather than being split.

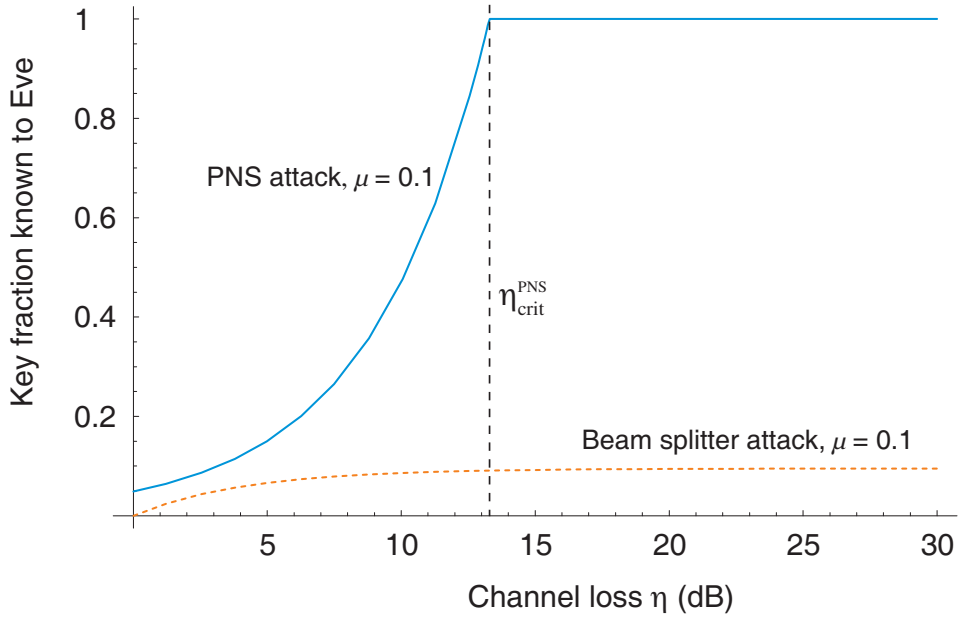

Figure 2.1: Effectiveness of different photon-number splitting attacks on Alice using attenuated pulses with mean photon number $\mu = 0.1$: fraction of sifted key bits known to Eve as a function of channel loss, if she performs a) the simple beam-splitting attack (dashed red curve), or b) the full PNS attack (solid blue curve). In the latter case, secret key generation in not possible for channel losses exceeding $\eta_{\text{crit}}^{\text{PNS}}$.

PNS attack

In the beam splitting attack, the photons of the incoming signal states are redirected statistically to Eve and Bob. In principle, Eve could arrange an improved eavesdropping method called PNS attack [45–47]: Eve can first measure the number of photons in each pulse without disturbing the degree of freedom encoding the qubits using a *quantum non-demolition measurement*. The measurement does not perturb the qubit, and in particular it does not destroy the photons (Eve actually performs a measurement in the photon number Hilbert space). Such a measurement is possible, because Eve knows in advance that Alice sends a mixture of states with well-defined photon numbers. Whenever Eve finds a multi-photon signal, she deterministically splits one photon off, and forwards the remaining photons to Bob. In order to prevent Bob from detecting a lower qubit rate, Eve can use a channel with lower losses. Ideally, Eve uses a lossless channel, which enables her, under certain conditions, to increase the probability that multi-photon pulses reach Bob's detector, while still keeping one photon for herself. Then, in order to match the original loss in the channel, Eve may block some of the single-photon signals, thereby reducing the fraction of signals that contribute to the key, but that she has not full knowledge about. On those single-photon signals that she does not block, Eve may perform any coherent eavesdropping attack. Consequently, all the errors in the sifted key

arise from eavesdropping in single-photon signals. Ignoring eavesdropping on the single photon pulses for the moment, the fraction of the sifted key known to Eve is then [46]

$$f_{\mathrm{PNS}} = \frac{p_{\mathrm{multi}}}{p_{\mathrm{exp}}} = \frac{1-(1+\mu)e^{-\mu}}{1-e^{-\eta\mu}}, \tag{2.3}$$

which is plotted as solid blue line in Figure 2.1. Equation 2.3 states that if the probability p_{multi} for a multi-photon pulse being emitted by Alice is larger than the probability p_{exp} that a non-empty pulse is detected by Bob, Eve will get full information of the sifted key without introducing any errors. Hence, there exists a critical transmission $\eta_{\mathrm{crit}}^{\mathrm{PNS}}$ below which no secure key can be generated, because Eve can afford to block *all* single-photon pulses:

$$\eta_{\mathrm{crit}}^{\mathrm{PNS}} = 1 - \frac{1}{\mu}\ln(1+\mu). \tag{2.4}$$

Lütkenhaus and Jahma investigated the possibility for Bob to detect a PNS attack by monitoring the photon number statistics, which should change under the PNS attack [90]. Although most detectors used in current experiments are not photon-number resolving, at least some information on the photon number distribution can be inferred with suitable detection schemes from the probability of coincidence events. It turns out, however, that it is possible to extend the PNS attack such that the *complete* photon number statistics, as seen by Bob, is indistinguishable from that resulting from attenuated laser pulses and a lossy channel. This can be achieved solely by introducing a photon-number dependent loss in the channel and holds in a certain parameter regime described by the implicit equation

$$\left(1+\mu+\frac{\mu^2}{2}\right)e^{-\mu} - (1+\eta\mu)\,e^{-\eta\mu} \leq 0. \tag{2.5}$$

The region in the (η, μ)-plane where this condition is fulfilled, is the area below the red curve plotted in Figure 2.2.

Evaluating the threat posed by the PNS attack, one must constitute that the PNS attack in its ideal form requires substantial technological means, and might thus be considered unrealistic, although it is certainly not unphysical. Eve needs not only to be capable of performing a quantum non-demolition measurement of the photon number [91], and of splitting the signal pulses deterministically, but also has to store her qubits for a possibly very long time[9]. The latter may be achieved either with a quantum memory (which does not exist today), or a lossless channel in a loop. Realising a lossless channel avoiding fundamental physical effects such as scattering and diffraction is also difficult.

On the other hand, approximations to the ideal PNS attack have been investigated [92], concentrating on splitting processes that are within reach of current technology and

[9] Alice and Bob may wait with the announcement of the bases until the key is actually needed for encryption.

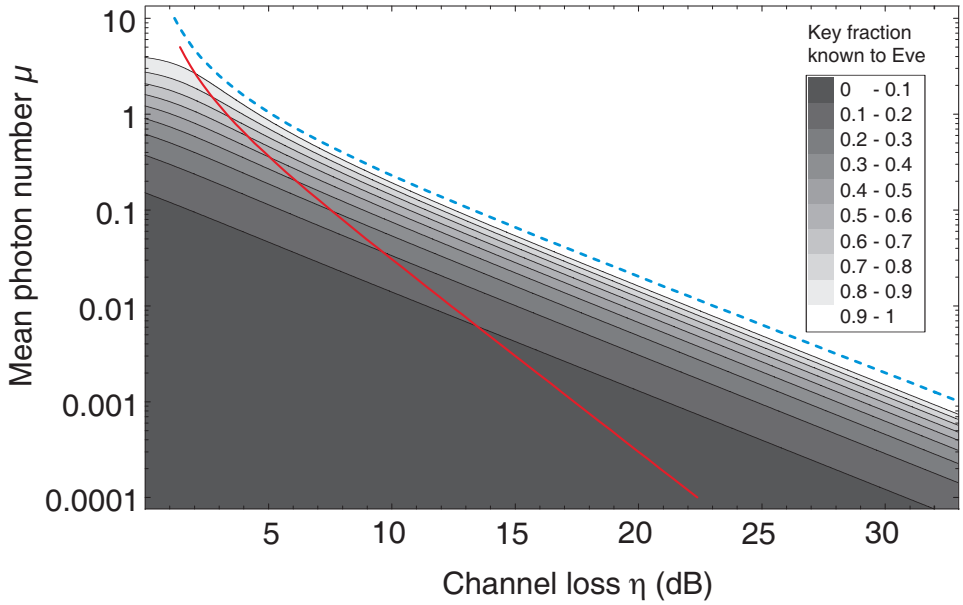

Figure 2.2: PNS attack on the BB84 protocol with attenuated laser pulses: as a function of channel loss η and the source's mean photon number μ, the fraction of sifted key bits known to Eve is coded as grey levels, with the critical (η, μ)-combination marked as a dashed blue line, where this fraction reaches 1. In the region below the red curve, Eve can additionally mimic the full photon number statistics of the original channel.

that reduce the probability of splitting off more than one photon. For example, the input state can be sent to a polarisation independent weak beam splitter. If no photons are detected in the weakly coupled output arm, the signal is sent through an identical beam splitter again. Otherwise the signal is transmitted through a perfect channel without any further processing. With this technique, the authors constructed attacks that show performance close to the full PNS attack, but with much simpler hardware.

In conclusion, it should be emphasised that multi-photon pulses do not necessarily constitute a threat to key security, but they limit the key creation rate (because more bits must be discarded during privacy amplification) and the minimum channel transmission, that is, distance, over which QKD can be made secure.

2.5.3 Security proof for attenuated pulse systems

The security of the BB84 protocol using attenuated laser pulses has been investigated by Inamori et al [88], and Gottesmann et al [89]. Their result (often abbreviated as ILM-GLLP) holds against the most general attack of Eve, the coherent attack where Eve may delay her measurements. The elementary concept there is the so-called *tagged bits*: These are signals *received by Bob* which might have leaked all of their signal information to Eve, without causing Eve to introduce errors. In the case that Alice uses

an attenuated pulse source, those raw bits caused by multi-photon pulses from Alice are regarded as tagged bits, because Eve in principle can have full information without causing any disturbance if she uses the PNS attack. The concept of tagged bits is, however, much more general, and is able to describe also other device imperfections, that leak information to Eve. The ILM-GLLP results show that, even if Alice has an imperfect source, a secure final key can be distilled if one knows an upper bound of the tagged bits. This is possible because of two important observations: Firstly, the key distillation does not need information about which raw bits are tagged. Secondly, the key distillation does not need an exact value for the fraction of tagged bits. An upper bound of the fraction of tagged bits among all initial bits is enough, albeit the tightness of the bound determines the resulting key generation efficiency. The final key rate (per pulse) in the asymptotic limit of a long key is then given by

$$R_{\mathrm{WCP}} \geq \frac{p_{\mathrm{exp}}}{2}\left[(1-\Delta) - f(e)H_2(e) - (1-\Delta)H_2\left(\frac{e}{1-\Delta}\right)\right], \tag{2.6}$$

where Δ is the fraction of the tagged bits, e is the QBER measured by Alice and Bob, $f(e)$ is the efficiency of the error correction (see §2.7.1), and H_2 is the binary entropy function given by $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$. Formula 2.6 shows that after error correction, which consumes $f(e)H_2(e)$ of raw bits, the key must be reduced by $\Delta + (1-\Delta)H_2(e/1-\Delta)$ bits in privacy amplification to guarantee security. For $\Delta = 0$, as in the case of a perfect single photon source, equation 2.6 reduces to the key generation rate of the ideal BB84 protocol,

$$R_{\mathrm{SP}} \geq \frac{p_{\mathrm{exp}}}{2}\left[1 - f(e)H_2(e) - H_2(e)\right]. \tag{2.7}$$

The central task is to find a faithful and tight estimate for the value of Δ. For security, the estimate must be faithful so that the estimated Δ is never smaller than the true fraction of tagged bits, whatever is Eve's channel. For efficiency, the estimated Δ value should be only a little larger than the true value in the normal case when there is no Eve. As a worst-case estimate for Δ, one may use the fraction f_{PNS} (equation 2.3) of the raw key bits known to Eve if she perfoms the full PNS attack, i.e., splitting all multi-photon pulses (while using a lossless channel to enhance their probability of detection by Bob) and blocking a fraction of the single-photon pulses to match the original channel transmittance,

$$\Delta = \frac{p_{\mathrm{multi}}}{p_{\mathrm{exp}}} = f_{\mathrm{PNS}}. \tag{2.8}$$

Since p_{exp} drops linearly with the channel transmittance, Δ quickly reaches unity (leaving no untagged bits to generate a secret key), unless p_{multi} is adjusted accordingly by further attenuating the pulses. This means that the mean photon number μ has to be chosen roughly proportional to η. Overall, the key generation rate R_{WCP} becomes proportional to the square of the channel transmittance η, and thus drops quickly with increasing

losses. This significant performance limitation of attenuated pulse systems has led to the belief that single photon sources would be indispensable for building efficient QKD systems. However, the decoy state method, which is described in §2.6, allows for a much tighter bound, achieving an almost linear dependency of the key generation rate on the channel transmittance. In this way, the technologically much simpler attenuated pulse systems is again on a level with systems based on single photon sources.

2.5.4 Attacks on real world systems

Obviously, a theoretical description of a protocol — even one that includes certain imperfections of the devices — is a mathematical idealisation. Any real-life quantum cryptographic system is a complex physical system with many degrees of freedom. Even a seemingly minor and subtle omission can be fatal to the security of a cryptographic system. Especially the existence of side channels [93, 94] are not covered by security proofs, because they do not depend primarily on the used protocol, but on the individual implementation of the QKD system. For instance, Eve might gain information on Alice's prepared state or Bob's measurement result by launching additional light pulses (*"Trojan horse"*) into their devices and analysing the spectral and temporal properties of the backreflected signal [95]. Another example of an attack, that does not act on the signal qubits directly, is the possibility for the eavesdropper to create an effective efficiency mismatch between Bob's detectors by tampering with the timing or wavelength of Alice's quantum signals [96–98], provided Bob's detectors use some sort of time gating.

One can hope to protect against some of these eavesdropping strategies, at least partially, with technical precautions. To ensure the security of a practical implementation of a QKD system, it has to be scrutinised with regard to any potential side-channels, and all imperfections have to be assessed quantitatively with respect to the additional information an adversary could gain from them.

2.6 Decoy-state protocol extension

Given the ILM-GLLP formula 2.6 for the secure key generation rate, and taking into account the possibility of tagged bits, one may ask, whether the fraction of tagged bits Δ can be bounded in any better way than by worst case assumptions. A rather simple — but nonetheless effective — idea to counteract the PNS attack on QKD schemes using weak laser pulses is the use of *decoy states* [48–50, 99].

2.6.1 Principle

The idea is the following: In addition to the usual signal states of average photon number μ, Alice prepares decoy states of various mean photon numbers $\mu_1, \mu_2, ...$ (but with the same wavelength, timing, etc.). Alice can achieve this, for instance, via a

variable attenuator to modulate the intensity of each signal. It is essential that each signal is chosen randomly to be either a signal state or a decoy state. Both signal states as well as decoy states consist of pulses containing $\{0, 1, 2, ...\}$ photons, just with different probabilities. Given a *single* n-photon pulse, the eavesdropper has no means to distinguish whether it originates from a signal state or a decoy state. Hence, the eavesdropper on principle cannot act differently on signal states and on decoy states. Therefore, any attempt to suppress single-photon signals in the signal states will lead also to a suppression of single-photon signals in the decoy states. After Bob's announcement of his detection events, Alice broadcasts which signals were indeed signal states and which signals were decoy states (and which types). Since the signal states and the decoy states are made up of different proportions of single-photon and multi-photon pulses, any photon-number dependent eavesdropping strategy has different effects on the signal states and on the decoy states. By computing the gain (i.e., the ratio of the number of detection events to the number of signals sent by Alice) separately for signal states and each of the decoy states, the legitimate users can with high probability[10] detect any photon-number dependent suppression of signals and thus unveil a PNS attack.

As shown by Lo et al. [50], in the limit of an infinite number of intensities μ_i of the decoy states, the only eavesdropping strategy that will produce the correct gain for all signal intensities, is the standard beam splitter attack (§2.5.2). Consequently, the resulting key generation rate with decoy states is substantially higher and grows basically like $O(\eta)$, compared to $O(\eta^2)$ in the case of non-decoy protocols. An infinite number of decoy intensities is of course impractical for an application, especially in the light of a finite number of pulses that contribute to a secret key in a real QKD system. It turns out that the number of decoy intensities can be dramatically decreased without sacrificing too much tightness of the bound for Δ [100]. Several different practical protocols have been proposed, using between two [48] and four different intensities [49, 101]. The first experimental demonstrations of decoy state QKD has been done with two different intensities [14]. In practise, it is advantageous to employ the vacuum state as an additional decoy state, since this allows a much better estimation of the background count probability. In fact, it has been shown by Ma et al. [100], that of all protocols using two decoy states, the vacuum+weak decoy state protocol, is optimal. The resulting protocol offers a good compromise between simplicity of implementation and performance and was therefore chosen for the inter-island QKD experiment presented in this thesis. In the following, the protocol is described in more detail.

2.6.2 Practical three-intensity decoy-state protocol

The security of the decoy-state method in combination with the BB84 protocol in the GLLP framework [88, 89] has been analysed by Lo et al. [50]. In particular, the final key

[10] The actual probability is a security parameter and can be chosen arbitrarily close to 1.

rate (per pulse) can be calculated by the formula

$$R \geq n_s \frac{Q_\mu}{2} \left[1 - \Delta - f(e) H_2(e) - (1-\Delta) H_2 \left(\frac{e}{1-\Delta} \right) \right]. \tag{2.9}$$

Here, Q_μ is Bob's detection probability for pulses of intensity μ, and n_s denotes the fraction of signal pulses, that is, pulses that potentially contribute to the sifted key (as opposed to decoy pulses, that only serve for parameter estimation). The goal is to find an upper bound for Δ, using only quantities that are measurable in the experiment.

In the protocol that was proposed by Wang [49] and further analysed by Ma [100], weak coherent states with mean photon numbers μ and μ' (where $\mu < \mu'$) are used for signal pulses, and the vacuum state is used as decoy pulses. Since both μ and μ' are essentially of the same order of magnitude, pulses of both types can be used to distill the final key. Alice mixes randomly the positions of all classes of pulses.

To derive an upper bound for Δ, Alice and Bob analyse the individual counting rates for the different decoy and signal states. The analysis is most conveniently expressed in terms of yield and gain: The *yield* Y_n of an n-photon state is defined as the conditional probability of a detection event at Bob, given that Alice sends out an n-photon state. The *gain* Q_n of an n-photon state is defined as the product of the probability $P_\mu(n)$ that Alice emits an n-photon state, and the yield Y_n:

$$Q_n = P_\mu(n) \cdot Y_n = \frac{\mu^n}{n!} e^{-\mu} \cdot Y_n. \tag{2.10}$$

The essence of the decoy-state method consists in the fact, that Y_n must be the same both for the signal and decoy states. After a number of pulses have been sent, Bob announces which pulses caused a detection event in his detector. Since Alice knows which pulse belongs to which class, Alice can calculate the gains of each class of pulses, that consist of the individual n-photon contributions:

$$Q_\mu = \sum_{n=0}^{\infty} P_\mu(n) Y_n = e^{-\mu} Y_0 + \mu e^{-\mu} Y_1 + M \tag{2.11}$$

$$Q_{\mu'} = \sum_{n=0}^{\infty} P_{\mu'}(n) Y_n = e^{-\mu'} Y_0 + \mu' e^{-\mu'} Y_1 + \frac{\mu'^2 e^{-\mu'}}{\mu^2 e^{-\mu}} M + r, \tag{2.12}$$

where $M := \sum_{n \leq 2} P_\mu(n) Y_n = \Delta \cdot Q_\mu$. From the vacuum decoy pulses, Alice can compute the value Q_0, that corresponds to the background probability Y_0 of Bob's detector. After eliminating Y_1 and solving for M, one can find a lower bound for the term containing r, using the inequality $\mu < \mu'$. Finally, this results in an upper bound for M, or, normalised to Q_μ, for Δ:

$$\Delta := \frac{M}{Q_\mu} \leq \frac{\mu}{\mu' - \mu} \left(\frac{\mu e^{-\mu} Q_{\mu'}}{\mu' e^{-\mu'} Q_\mu} - 1 \right) + \frac{\mu e^{-\mu} Y_0}{\mu' Q_\mu}. \tag{2.13}$$

Likewise, and given the fact that Y_1 is the same for both classes of pulses, one obtains an upper bound for the fraction of tagged pulses of the μ'-class:

$$\Delta' \leq 1 - \left(1 - \Delta - \frac{e^{-\mu} Y_0}{Q_\mu}\right) \frac{Q_\mu \mu'}{Q_{\mu'} \mu} e^{\mu - \mu'} - \frac{e^{-\mu'} Y_0}{Q_{\mu'}}. \tag{2.14}$$

Numerical values of the expected key generation rate for a linear channel model will be presented in §2.6.4.

As pointed out by Lo et al. [50, 100], a higher key generation rate can be achieved by using a stronger version [89] of equation 2.9:

$$R \geq n_s \frac{Q_\mu}{2} \left[1 - \Delta - f(e_\mu) H_2(e_\mu) - (1 - \Delta) H_2(e_1)\right], \tag{2.15}$$

where e_1 is the QBER of detection events by Bob that have originated from single-photon signals emitted by Alice. In contrast to the simpler method described above, equation (2.15) does not make the worst case assumption $e_1 = e/(1 - \Delta)$, but requires a separate estimation of e_1. Again, it is possible to find a (lower) bound on e_1 with the help of the decoy method, leading to higher key generation rates than equation (2.9). The increase is usually on the order of a few percent, but reaches much higher values close to the maximal secure channel attenuation.

If qubit losses are considerable, then Bob will receive many empty pulses, and dark counts from his detectors will induce a high error rate. A further improvement is given by the following observation (which is independent of the decoy state method). For the class of events, where Bob does not receive Alice's signal (because it was lost on the quantum channel), but records a dark count in one of his detectors, no privacy amplification is needed: The eavesdropper cannot have any a priori information about these bits, since the dark count events are independent of Alice's and Eve's actions [102–104].

$$R \geq n_s \frac{1}{2} \left[Q_0 + Q_1 - Q_\mu f(e_\mu) H_2(e_\mu) - Q_1 H_2(e_1)\right] \tag{2.16}$$

However, this is true only for erroneous events that are purely accidental and strictly not under the control of an adversary. Hence, Q_0 refers only to the intrinsic dark counts of Bob's detector, not to background counts due to stray light, since the latter could have been manipulated by Eve. It is therefore necessary to determine a lower bound on the intrinsic dark count probability, for example by blocking the detection unit and estimating Q_0 from these results.

2.6.3 Statistical fluctuations due to finite data

Any real-life experiment is done in a finite time. In particular, for a QKD system to be practical, a secret key should be provided within a reasonable time. This means that the number of exchanged qubits, and hence the data set of detection events are inevitably of

finite size. Equations (2.13) and (2.14) hold strictly only for the asymptotic case, where — thanks to an infinite amount of detection events — the values of $Q_\mu, Q_{\mu'}$ and Y_0 are precisely known. In reality, Bob can compute these values only up to a certain statistical uncertainty [49, 100, 105, 106]. In general, as the distance of QKD increases, larger and larger data sets will be needed for the reliable estimation of Δ and e, thus requiring a longer QKD experiment. Statistical fluctuations of the count rates recorded by Bob can be accounted for by Gaussian error propagation. Strictly speaking, this technique is based on normal probability distributions, whereas the count rates follow a binomial distribution. However, the normal distribution is a good approximation to the binomial distribution for reasonable count rates $\gg 1$. The uncertainties $\delta Q_\mu, \delta Q_{\mu'}, \delta Y_0$ lead to an uncertainty $\delta\Delta$ of the fraction of tagged bits according to

$$\delta\Delta = \sqrt{\left(\frac{\partial\Delta}{\partial Q_\mu}\right)^2 \delta Q_\mu^2 + \left(\frac{\partial\Delta}{\partial Q_{\mu'}}\right)^2 \delta Q_{\mu'}^2 + \left(\frac{\partial\Delta}{\partial Y_0}\right)^2 \delta Y_0^2}. \tag{2.17}$$

The behaviour of $\delta\Delta$ is mainly governed by the choice of the relative frequency of the different pulse classes. This can be assessed quantitatively if we assume some channel model, which is done in the next section.

In general, additional sources of fluctuations may exist, that were not considered here. For example, the intensity of Alice's laser pulses may be fluctuating. This problem has been investigated in [107]. The author concludes, that, given the intensity error of each pulse is random, the decoy state method can still work efficiently even with large intensity fluctuations. In addition, Eve has a non-negligibly small probability to treat, by chance, n-photon pulses from different classes a little bit differently, even they have the same state. In other words, the yields Y_n for the signal states might be slightly different from the yields Y_n' of the decoy states.

Notwithstanding the presented approach, the question of how to properly take into account the statistical effects of finite key lengths is currently still under investigation and discussion [108–113] and not yet solved conclusively.

2.6.4 Key generation rates

In order to compute expected key generation rates for different protocols, it is necessary to make assumptions on certain experimental parameters.

It is common to assume a linear *model for the quantum channel*, which means, that the absorption probabilities for different photons are statistically independent. In other words, for pulses of mean photon number μ, the probability for the detection of n photons at the end of the quantum channel with transmittance η becomes

$$P_{\mu,\eta}(n) = \frac{(\mu\eta)^n}{n!} e^{-\mu\eta}. \tag{2.18}$$

Here it should be noted, that this may not be exactly the case in reality, in particular with free-space quantum channels (see §3.4.5). However, a deviation affects only predictions

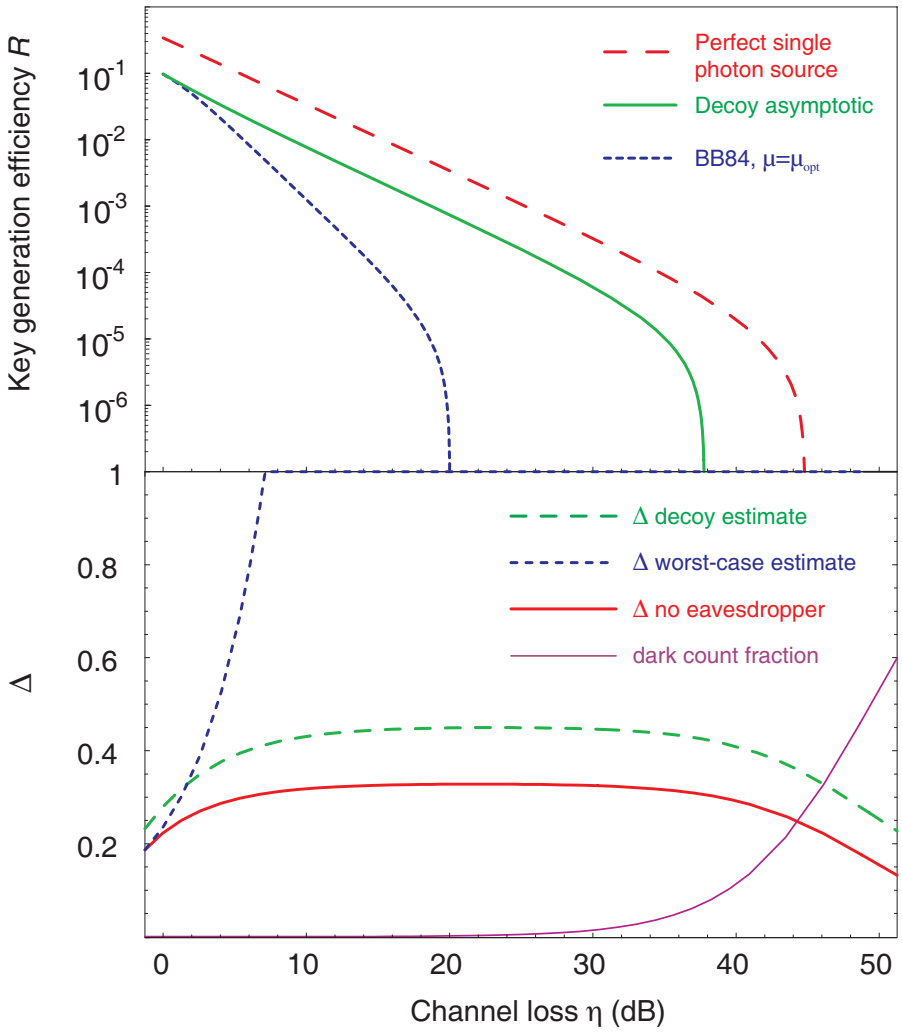

Figure 2.3: Upper graph: Asymptotic key generation rate for the BB84 protocol with ideal single photon source, BB84 with attenuated laser pulses, and the asymptotic decoy state protocol, depending on the transmission of the quantum channel. Without the decoy state extension, attenuated pulses allow secure communication only up to about 20 dB channel loss, for experimental parameters $Y_0 = 6 \cdot 10^{-6}$, $e_{\text{tech}} = 2\%$. Lower graph: Influence of multi-photon pulses in dependence of the attenuation. The actual fraction of tagged bits (solid red) is upper bounded by a worst-case estimate (dotted blue) in the case of simple BB84, and by a much tighter approximation in the decoy protocol (dashed green). The lower graph is plotted for a fixed mean photon number $\mu = 0.4$.

of the expected key generation rates and of verified values of Δ. It does not endanger the security of the decoy state method, because Eve is always assumed to possess full control over the quantum channel, which includes, in particular, to change the channel transmission at will and for each pulse, according to the result of a photon-number quantum non-demolition measurement. As a good approximation, the quantum channel

shall still be characterised in the following solely by its transmittance η.

The *dark count probability* is a property mainly of Bob's detector, but also of the level of stray light, that inevitably enters Bob's apparatus. As the dominant noise source at large transmission distances, the dark count probability governs the maximum distance over which secure QKD is possible.

The *technical error* is due to imperfections of the optical components and alignment and is accounted for by the constant e_{tech} contributing to the overall QBER.

For the following plots, realistic parameters similar to the values found in the inter-island experiment are assumed: Dark count probability $Y_0 = 6 \cdot 10^{-6}$, technical error $e_{\text{tech}} = 2\%$, efficiency of error correction $f(e) = 1.22$ (weakly dependent on the overall QBER, see §2.7.1).

The most important parameter of a real-life QKD system is, of course, the secure key rate B, measured in exchanged key bits per second, between Alice and Bob:

$$B = \nu R, \tag{2.19}$$

where ν is the repetition frequency of Alice's source and R is the secure key generation efficiency, which is normalised to the number of emitted pulses.

The upper graph of Figure 2.3 compares the asymptotic secure key generation efficiency of the decoy state method with the pure BB84 protocol, using either a true single photon source (dashed red curve), or weak coherent pulses with mean photon number $\mu = \mu_{\text{opt}}$ (dotted blue curve), according to equations 2.15, 2.7, and 2.6, respectively. The ideal single photon source constitutes an upper limit to the secure key rate taking into account the above mentioned background probability and alignment errors. The performance curve of a practical QKD system utilising attenuated pulses and the standard BB84 protocol exhibits the known $O(\eta^2)$ dependency, which puts severe limits both to key rate and achievable distance. Employing the ideal decoy state method with an infinite number of decoy states allows precise calculation of Δ and e_1, and results in a key rate that scales equally to the case of the single photon source, as well as in a much higher distance for unconditionally secure QKD. The lower graph of Figure 2.3 illustrates the role of multi-photon signals (computed for fixed $\mu = 0.4$) as a function of the channel attenuation. Plotted in red is the fraction of tagged bits arriving at Bob when no eavesdropper is present. The drop at very large attenuation is due to the increasing influence of background events, which are shown in purple for comparison. Without the decoy method, one has to assume the worst-case scenario (dotted blue curve), that is, Eve blocks as many single-photon pulses as possible, and lets the tagged photons pass. This leads to the fast drop of the secure key rate proportional to η^2. Utilising the decoy method, one obtains a much better upper bound for Δ, that reaches the true value in the limit of infinitely many decoy states. The dashed green trace represents the estimate derived from using only 3 different intensities. For a wide transmission region, this estimate is roughly constant and thus enables a key generation rate similar to the single photon case.

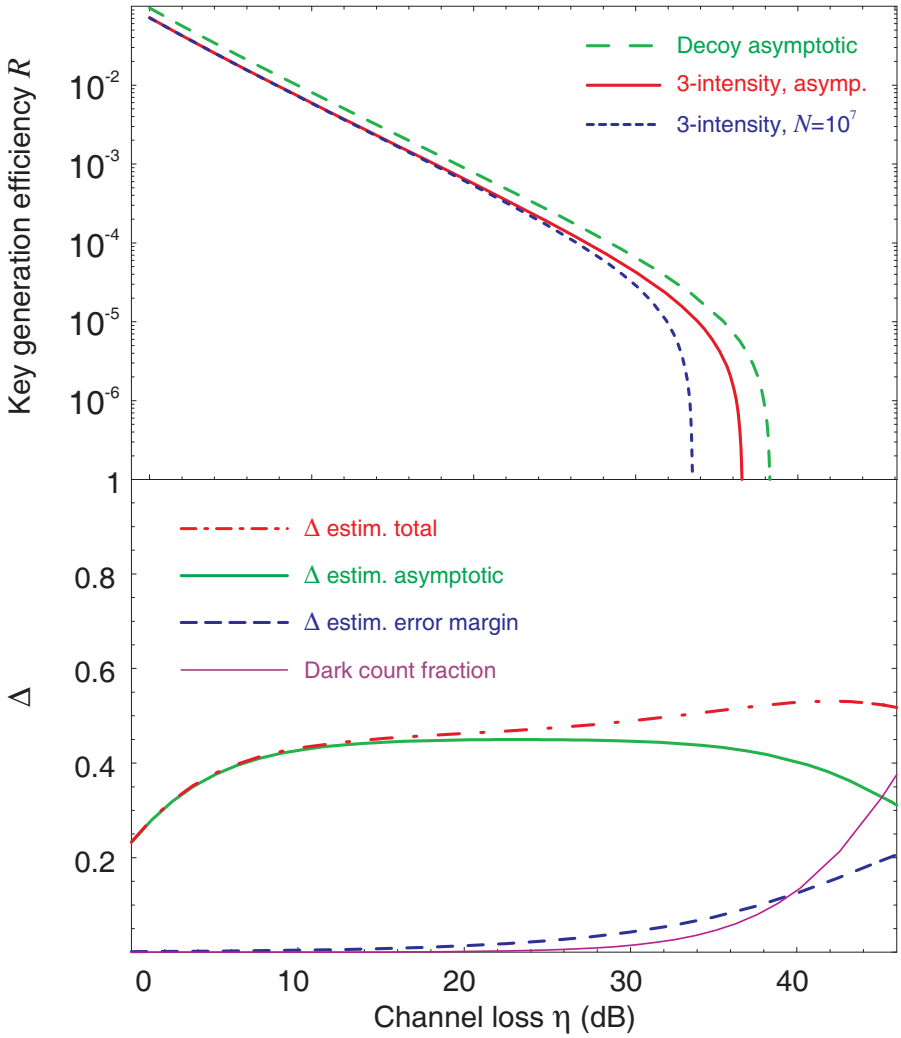

Figure 2.4: Upper graph: Key generation rates for decoy state protocols with infinitely many decoy states (dashed green), and 3 different intensities $(\mu, \mu', 0)$, if both signal and decoy states are used for key generation (solid red). For a real key exchange of limited length, the achievable key rate is decreased due to statistical effects (dotted blue, plotted for $N = 1 \cdot 10^7$). Lower graph: Estimate of the fraction of tagged bits Δ as a function of channel attenuation. To account for limited counting statistics, the asymptotic estimate is increased by an error margin of 4.4 standard deviations according to the chosen security parameters.

Figure 2.4 compares the performance of different decoy state protocols. The asymptotic limit of optimal performance for this class of protocols (dashed green line) is reached in the limit of infinitely many decoy states. However, the protocol described in §2.6.2 with just 3 different intensities (one of which is effectively the vacuum state) performs close to the optimum, if both signal and decoy states are used for key generation (solid red curve). Assuming a fixed number of transmitted pulses of $N = 1 \cdot 10^7$ in a real ex-

periment, the key rate drops especially towards high channel losses due to poor counting statistics. This is further illustrated in the lower graph of Figure 2.4. To account for the statistical uncertainty of Δ due to the limited number of recorded events, the expected value for Δ (solid green curve) has to be increased by an error margin of 4.4 standard deviations (dashed blue curve), calculated in accordance with a confidence limit of $1-10^{-5}$ (see §6.1.3). The sum of these quantities (dash-dotted red line) can then be used as a faithful upper bound in equation 2.9.

2.7 Supporting classical procedures

After the quantum transmission and the measurement of the quantum signals, Alice and Bob each possess a classical bit string. This is the raw key, from which the final secure key is extracted by applying classical procedures. First, errors in the raw key need to be corrected for the key to be useful. This is done by error correction codes, which exchange additional information over the classical channel. Since messages sent over the classical channel are not encrypted, this information is available to Eve as well. Therefore, Eve can gain knowledge of the key not only from eavesdropping on the quantum channel, but also from listening in on the classical channel. To erase Eve's information, in the second step Alice and Bob compress their corrected strings, using, for example, a hash function. After this privacy amplification, the key will be shorter, but unknown to Eve.

2.7.1 Error correction

For simplicity, one may assume that the errors in the raw key are uniformly distributed and symmetric, that is, each bit is flipped independently with some propability p. This model is called *binary symmetric channel*. The lower limit (called *Shannon limit*) for the amount of information that needs to be exchanged — and by that, disclosed — in order to correct a certain amount of errors in a string sent over a binary symmetric channel [114], is $n_{\mathrm{dis,min}} = n_{\mathrm{sif}} \cdot H_2(p)$, where $H_2(p)$ is again the binary entropy function. The probability p corresponds to the average QBER of the quantum transmission. In a real-life QKD experiment, the errors might occur in bursts, because Eve may choose to eavesdrop on a certain block of quantum signals, or because the attenuation of the quantum channel fluctuates. For this reason, Alice and Bob need to agree on a random permutation of their raw keys before starting the error correction to make the errors uniformly distributed.

A number of classical error correction codes exist, which differ, among other things, in their closeness to the Shannon limit, the level of (interactive) communication and computational resources required, the correctional probability, and their robustness to changing error rates. Different protocols may be optimal depending on the encountered error rate. Which protocol should be chosen for a specific QKD system therefore depends on a number of factors, such as availability and capacity of the classical channel, or

computational resources available at Alice and Bob. For a comparison of several error correction protocols, based on simulated data of a free-space QKD system, see [115]. CASCADE and LDPC are the most widely used schemes in connection with QKD systems.

The *CASCADE* protocol was suggested by Brassard and Salvail [116]. It works close to the theoretical Shannon limit. The protocol uses interactive communication between Alice and Bob and works by the principle of comparing parities between blocks of key bits. This enables detection of blocks with odd numbers of errors. When such a block is found, a binary search inside the block reveals the position of an error.

The *Low Density Parity Check* (LDPC) code was discovered by Gallager in 1962 [117] and recently adapted to QKD by Pearson [118]. The algorithm protects transmitted data from errors by using a large sparse matrix representing different parity checks. LDPC codes have the advantage of low interactive communication and a high correctional capability. However, the codes are sensitive to changes in the error rate. Since correctional information can be sent by Alice at the same time as Bob is decoding previous bits, LDPC codes are well suited for continuously running systems, that benefit from the fast decoding.

Any error correction code exchanges information over the public channel, thus exposing it to Eve. By listening to the correction information, she will gain n_{dis} bits of information about the key. These bits can be either specific information on the value of certain bits, or the parity of a block of bits, depending on which error correction code is used. Of course, the smaller n_{dis}, the better. However, the Shannon limit gives the lower bound for n_{dis}. The efficiency of an error correcting scheme is described by the factor $f(e)$, by which it exceeds the Shannon limit: $n_{\mathrm{dis}} = f(e) H_2(e)\, n_{\mathrm{sif}}$.

2.7.2 Privacy amplification

After the quantum transmission and key reconciliation, a proportion of the (corrected) key might have leaked to the adversary due to her eavesdropping. This amount depends on her strategy of eavesdropping on the quantum channel, and on the error correction code used. Both contributions depend on the qubit error rate e. The method of reducing Eve's information of the final secure key to an arbitrary small amount is called privacy amplification and was introduced by Bennett et al. [54, 119]. They used the concept of universal hashing, following the ideas of Carter and Wegman [53]. The hash function spreads the input in a chaotic manner; as little as a single bit-error in the input string will multiply and produce a significantly different output string. Thus, Eve, having many errors or uncertainties in her input string, will obtain an output string, that is almost uncorrelated to Alice and Bob's key.

Formally, if a function g is randomly chosen from a class of *universal*$_2$ functions $H = \{g : \{0,1\}^i \to \{0,1\}^j,\ i > j\}$, the probability that $g(x) = g(y)$, given that $x \neq y$, is upper bounded by $(\frac{1}{2})^j$ for $g : \{0,1\}^i \to \{0,1\}^j$. When using privacy amplification, the partially secure string X' is shortened by an amount depending on our estimation of

Eve's knowledge about the string, and a security factor, s. This makes Eve's information exponentially small in s. Assuming Eve gains at most k bits of information from eavesdropping on the quantum channel, and learns at most l bits from the reconciliation phase, then $r = n_{\text{sif}} - k - l - s$ is the length of the final key, and Eve's information about it is upper bounded by $2^{-s}/\ln 2$.

Since the function g has to be chosen randomly, Alice and Bob have to agree on g anew in each round of QKD. g can be represented by an $r \times n_{\text{sif}}$ matrix, but generating and exchanging $r \cdot n_{\text{sif}}$ random bits each round is not very efficient. Therefore, *Toeplitz* matrices are often used for hashing messages. The family of Toeplitz matrices are $universal_2$ functions that can be generated from only $r + n_{\text{sif}} - 1$ bits, that have to be chosen randomly and communicated between Alice and Bob.

2.7.3 Authentication

To ensure that Eve may listen but cannot modify the information sent over the classical channel, Alice and Bob need to use unconditionally secure message authentication. This is also essential to rule out a man-in-the-middle attack. One way to authenticate the classical channel is for Alice and Bob to share a short initial secret string. Using this string together with a hash function, they can create a tag from each message they wish to exchange [52]. The other party will only accept the message if he computes the same tag using the initial string. After one round of QKD, Alice and Bob use some of their generated secret key for authentication in the next round ("quantum key growing").

3 The atmosphere as a quantum channel

We know from everyday life, that rain, snow, fog, etc. affect the viewing of distant objects. The same atmospheric factors also influence the transmission of electromagnetic radiation through the atmosphere (particularly optical waves), and have to be considered when using the atmosphere as transmission channel for quantum communications. This chapter is intended to review briefly the relevant aspects of atmospheric optics, and calculate expectation values for vital experimental parameters, such as attenuation, beam spot size, etc. For this purpose, and not least to illustrate the theory with some tangible numbers, parameters from the 144 km free-space test bed will be applied. The theoretical values are compared with actually measured quantities. The last part of this chapter deals with the means of adaptive optics to compensate at least partially the effects induced by the turbulent atmosphere. The active tracking system that was implemented for the inter-island experiment is described and characterised and an outlook to the potential of higher-order adaptive optical systems is given.

3.1 Free space propagation of Gaussian-beam waves

Before presenting the description of optical waves under the influence of atmospheric turbulence, the free propagation in vacuum shall be recalled. The electric field $\mathbf{E}$ of a propagating electromagnetic wave must be a solution of the wave equation

$$\nabla^2 \mathbf{E} = \frac{1}{c^2} \frac{\partial^2 \mathbf{E}}{\partial t^2}. \tag{3.1}$$

Most often, the standard solutions, such as the unbounded plane wave or the spherical wave, are investigated. In free space optical communication, the electromagnetic field is emitted into a specific direction (typically by a laser), and one is most interested in the field close to the optical axis. Under the paraxial approximation, equation (3.1) is solved by the set of *Gaussian-beam waves* [120]. The intensity profile of the lowest order Gaussian-beam wave TEM_{00} is described by

$$I(r,z) = \frac{2P}{\pi w^2(z)} \exp\left(-\frac{2r^2}{w^2(z)}\right), \tag{3.2}$$

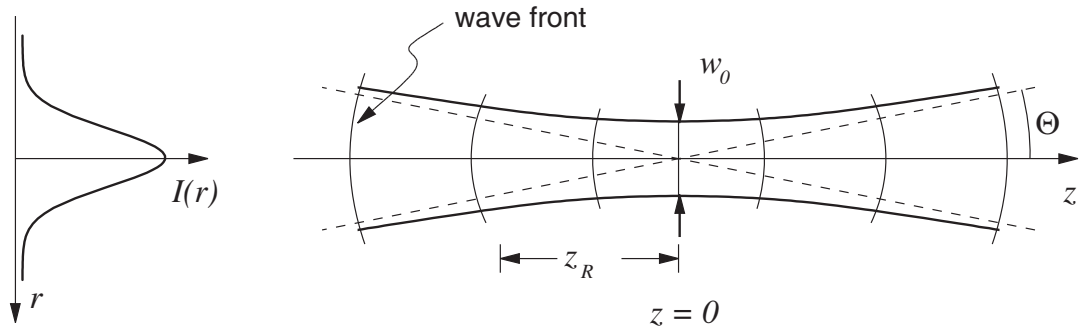

Figure 3.1: Fundamental parameters of a Gaussian beam wave: w_0 is the minimum beam waist, z_R is the Rayleigh length, and Θ is the divergence half angle in the limit $z \to \infty$. The transversal intensity profile is Gaussian shaped for all values of z.

where r denotes the distance from the optical axis, P is the power of the laser, and $w(z)$ is the local $(1/e^2)$ beam radius at the distance z in propagation direction $\hat{\mathbf{z}}$:

$$w(z) = w_0 \sqrt{1 + \frac{z^2}{z_R^2}} \tag{3.3}$$

A Gaussian beam (see Figure 3.1) is therefore characterised by its minimum beam radius, or beam waist, w_0, which is related to the characteristic beam divergence length (called *Rayleigh length*) z_R by $z_R = \pi w_0^2/\lambda$. For values $z \gg z_R$ the beam divergence half angle Θ is asymptotically equal to

$$\tan\Theta = \lim_{z\to\infty} \frac{w(z)}{|z|} = \frac{w_0}{z_R} = \frac{\lambda}{\pi w_0}, \tag{3.4}$$

and the wave front radius of curvature $R(z)$ can be expressed as

$$R(z) = z\left(1 + \frac{z_R^2}{z^2}\right). \tag{3.5}$$

At the beam waist ($z = 0$), the wave front is planar. The wave front curvature increases to a maximum at ($z = z_R$) and then decreases again towards planarity for ($z \to \infty$).

Figure 3.2a depicts the beam spreading as a function of propagation distance L for different initial beam diameters $2w_0 \in \{1\,\text{cm}, 7.5\,\text{cm}, 20\,\text{cm}\}$ in a double logarithmic plot. In an optical communication scheme, one is interested to maximise the transmittance by keeping the beam spread as low as possible, but is often limited by the diameter of the transmitting telescope. Graph 3.2b shows the beam radius w_L after propagation over different distances L (100 m, 1 km, 10 km, and 100 km) as a function of the initial beam radius w_0 at the transmitter. There's an optimal initial beam radius for each distance that results in the best combination of minimum beam radius and minimum

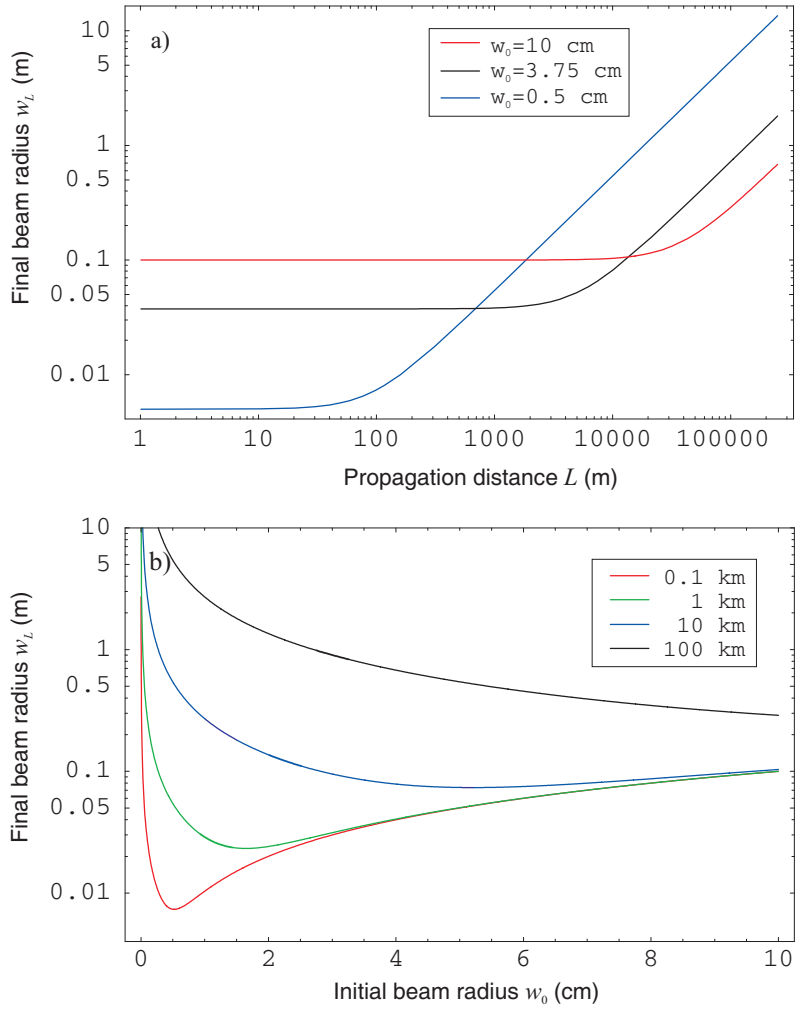

Figure 3.2: Gaussian beam propagation in vacuum at 850 nm wavelength. **(a)** Beam radius as a function of propagation distance for different beam waists. **(b)** Beam radius as a function of initial beam waist for different values of fixed propagation distance.

beam spread over the given distance. Analytically, this value is $w_0^{\text{opt}} = \sqrt{\lambda L/\pi}$ and produces a beam spread $w_L/w_0 = \sqrt{2}$.

Beam spreading in vacuum is a consequence of diffraction. In the presence of atmospheric turbulence, there is additional beam spreading, causing a larger beam spot size than diffraction alone. Generally speaking, three processes affect optical wave propagation in the atmosphere:

- Absorption,
- scattering,
- and refractive index fluctuations (*"optical turbulence"*).

Absorption and scattering are usually treated separately from optical turbulence theory, where a "*clear atmosphere*" is assumed.

3.2 Absorption and scattering

Absorption and scattering give rise to wavelength-dependent attenuation of electromagnetic radiation. Absorption and scattering can be further subdivided into two classes, according to the size of the interacting particles: molecular effects and effects caused by aerosols, that is, larger particles. The resulting attenuation, or extinction, of electromagnetic radiation is described by the *Beer-Lambert law*

$$I(\lambda, z) = I_0(\lambda) \exp(-z\, \alpha_{\text{ext}}(\lambda)), \tag{3.6}$$

where $\alpha_{\text{ext}}(\lambda) = \alpha_{\text{abs}}(\lambda) + \alpha_{\text{sca}}(\lambda)$ is the wavelength dependent extinction coefficient consisting of the sum of extinction coefficients due to absorption and scattering [121]. For our purpose, both α_{sca} and α_{abs} are assumed to be homogeneous over spatial separations on the order of λ, otherwise additional diffractive effects would have to be considered.

Absorption

Absorption is a quantum process, where atmospheric molecules absorb energy from incident photons, altering the electronic, vibrational, and/or rotational state of the molecule. The absorption spectrum of molecules therefore consists of a series of discrete absorption lines, the shape of which depends on several line-broadening effects, such as Doppler broadening, and pressure broadening. For wavelengths in the visible to near-infrared spectral range, vibrational spectra are of greatest relevance.

The extinction coefficient for a specific wavelength can be computed from detailed molecular spectra (that have been measured in laboratory experiments), and from the mixture of molecules present in the atmosphere. This can be accomplished with the major atmospheric transmission programs, such as LOWTRAN, MODTRAN, or FASCODE [122]. LOWTRAN and MODTRAN are both band models, whereas FASCODE is a line-by-line model, which provides spectra of higher resolution than the band models.

Scattering

Rayleigh scattering is elastic scattering of the optical radiation due to the displacement of the weakly bound electronic cloud surrounding the gaseous molecule, which is perturbed by the incoming electromagnetic field. Rayleigh scattering is associated with air molecules and haze, that are small in comparison with the wavelength λ of the radiation. The scattering coefficient is proportional to λ^{-4}, known as the Rayleigh law. For air molecules, scattering is negligible at $\lambda > 3\,\mu$m. At $\lambda < 1\,\mu$m, Rayleigh scattering produces the blue colour of the sky, because blue light is scattered much more than red light.

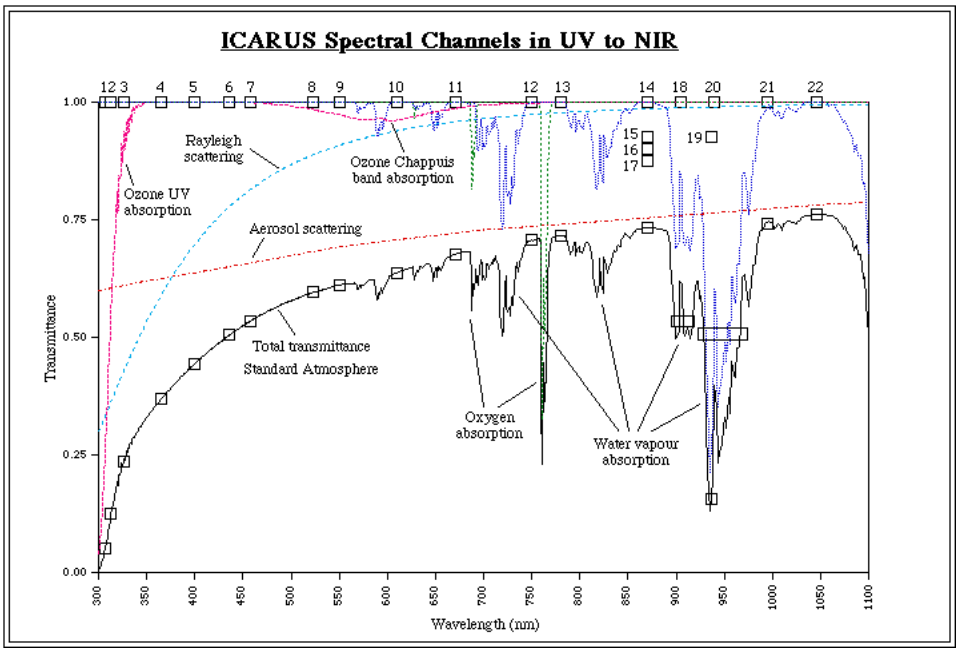

Figure 3.3: Optical transmittance of the atmosphere for a vertical propagation path between ground and space. Data from the *Natural Environment Research Council*, *http://www.soc.soton.ac.uk/RSADU/*.

Mie scattering, also known as aerosol scattering, is scattering by particles comparable in size to the radiation wavelength. Scattering losses decrease rapidly with increasing wavelength, eventually approaching the Rayleigh scattering case. An aerosol particle is larger than a molecule, but still small enough to remain suspended in the atmosphere for an extended period of time. The diameter range of atmospheric aerosols covers roughly 2 nm to 100 μm. Aerosols originate both from natural and man-made sources, among the many examples are rock and soil debris, sea salt, and particles formed from gaseous emissions. Radiation extinction caused by a single aerosol depends on the particle's size and composition. Thus, in order to evaluate aerosol-induced extinction, the aerosol composition, concentration, and particle size distribution have to be known. Since this poses considerable experimental difficulties, models have been developed describing aerosol conditions as a function of meteorological or local environmental parameters.

Figure 3.3 depicts the optical transmittance of the so-called *standard* atmosphere for a vertical propagation path, decomposed into extinction contributions from Rayleigh scattering, aerosol scattering, and molecular absorption, in the wavelength range from 300 nm to 1100 nm. Water vapour, CO_2, NO_2, CO, and ozone are the primary radiation absorbers that are present in the atmosphere. Absorption by the ozone O_2 and O_3 essentially eliminates propagation of radiation for $\lambda < 0.2\,\mu$m. Little absorption occurs at visible wavelengths (0.4 to 0.7 μm) except for H_2O absorption between 0.65 and 1.0 μm. Both CO_2 and water vapour are radiation absorbers at infrared wavelengths [123]. Ob-

viously, the actual attenuation for a specific propagation path through the atmosphere depends heavily on local humidity and environmental conditions, in particular for long horizontal paths at low altitude.

Depolarisation

Especially in the case of multiple scattering, depolarisation of the incident light can occur [121]. The depolarisation factor depends on the anisotropy of the scatterer, that is, on the deviation from the spherical form. In fact, depolarisation measurements of back-scattered light can be used to determine the physical composition of cloud constituents, such as the relative ratio of water vapour or ice crystals in a cloud. However, quantitative measurements over horizontal propagation paths in the lower clear atmosphere [124,125] indicate that the polarisation of a propagating wave is only minimally affected, often below the sensitivity of the apparatus.

3.3 Kolmogorov theory of turbulence

Turbulence of a viscous fluid is fundamentally a nonlinear process and described by the Navier-Stokes equations. Because of mathematical difficulties in solving these equations, Kolmogorov developed a statistical approach of turbulence [126], that relies on certain simplifications, but still allows to deduce important implications for wave propagation in random media. A comprehensive treatment of the topic can be found, for example, in [127].

Fluid mechanics distinguishes two types of motion in a viscous medium: laminar and turbulent flow. While the associated velocity field is continuous in laminar flow, it loses these characteristics in turbulent flow, and dynamic mixing with random subflows (called *turbulent eddies*) occurs. The state of motion is described by the dimensionless *Reynolds number* $Re = v\,l/\nu$, where v and l are a characteristic velocity and a characteristic dimension of the flow, respectively, and ν is the kinematic viscosity. The transition from laminar to turbulent conditions takes place at a *critical Reynolds number*, which depends on the exact flow configuration and must be determined empirically (common values range from 1 to 10^3). Under atmospheric conditions typically prevailing close to the ground ($l \sim 1\,\mathrm{m}$, $v \sim 1 - 5\,\mathrm{m/s}$), the Reynolds number reaches easily large values on the order $Re \sim 10^5$, which means that the motion of the air is highly turbulent. The source of energy in atmospheric turbulence is either wind shear (i.e., a wind gradient) or convection. The wind velocity increases until the critical Reynolds number is exceeded. At that point, local unstable air masses are created (large eddies), that break up into smaller eddies because of inertial forces. As the eddies become smaller and smaller, the relative energy dissipated by viscous forces increases until it matches the supplied kinetic energy: the eddies disappear, and the remaining energy is dissipated as heat. Thus, a continuum of eddies from a macroscale L_0 (*outer scale of turbulence*) to a microscale l_0

(*inner scale of turbulence*) is formed. The outer scale L_0 denotes the scale size below which turbulence properties are independent of the parent flow. In the surface layer up to 100 m, L_0 grows roughly linearly with the height above ground h and is approximately of the same order as h, whereas l_0 is typically $1 - 10\,\mathrm{mm}$ [127].

According to Kolmogorov's work [126], the turbulence on scales between l_0 and L_0 (called the *inertial subrange*) can be described by statistical means under the assumption of statistical homogeneity and isotropy of the random velocity field. This means that the mean value of wind velocity is constant over the considered region, and that correlations between random fluctuations from one point to another depend only on the absolute value of the vector connecting the two observation points. If such correlations of a property x between two different points $\mathbf{R}_1$ and $\mathbf{R}_2$ are locally homogeneous, they can be described by *structure functions* D_x, defined as

$$D_x(\mathbf{R}_1, \mathbf{R}_2) \equiv D_x(\mathbf{R}) = \langle [x(\mathbf{R}_1) - x(\mathbf{R}_1 + \mathbf{R})]^2 \rangle,$$

where the brackets $\langle\,\rangle$ denote an ensemble average and $\mathbf{R} := \mathbf{R_2} - \mathbf{R_1}$. The longitudinal structure function of wind velocity (parallel to the vector $\mathbf{R}$) is found to satisfy the power laws

$$D_{RR}(\mathbf{R}) = \langle [v(\mathbf{R}_1) - v(\mathbf{R}_2)]^2 \rangle = \begin{cases} C_v^2 R^{2/3} & : \quad l_0 \ll R \ll L_0 \\ C_v^2 l_0^{-4/3} R^2 & : \quad R \ll l_0, \end{cases} \tag{3.7}$$

Here, C_v^2 is the *velocity structure constant*, that is dependent on the average energy dissipation rate. Since only eddies of scale sizes smaller than L_0 are assumed statistically homogeneous and isotropic, by definition no general prediction of D_{RR} exists for $R > L_0$. For instance, in altidudes above $\sim 100\,\mathrm{m}$, eddies of greater size than L_0 are often much larger in horizontal dimension than in vertical dimension because of stratification. Hence, the turbulence is generally nonisotropic on that scale. Likewise, a temperature structure function $D_T(R)$ exists, that obeys the same power laws as the velocity structure function $D_{RR}(R)$, but has a different structure constant C_T^2.

Optical wave propagation in a transparent medium is governed by the index of refraction, which is sensitive to small-scale temperature fluctuations. At any point $\mathbf{R}$, the index of refraction of the atmosphere can be written as the sum of its mean value $n_0 = \langle n(\mathbf{R}) \rangle$ and the random deviation $n_1(\mathbf{R})$ from the mean value

$$\begin{aligned} n(\mathbf{R}) &= n_0 + n_1(\mathbf{R}) \\ &\simeq 1 + 7.76 \cdot 10^{-5} (1 + 7.52 \cdot 10^{-3}\, \lambda^{-2}) \frac{p(\mathbf{R})}{T(\mathbf{R})} \qquad (3.8) \\ &\simeq 1 + 8 \cdot 10^{-5}\, \frac{p(\mathbf{R})}{T(\mathbf{R})}, \qquad (3.9) \end{aligned}$$

where λ is wavelength in μm, p is pressure in mbar, and T is temperature in Kelvin. The wavelength dependence is small for optical frequencies, so expression (3.8) is a

good approximation for visible and infrared wavelengths. Since pressure fluctuations are negligible, index of refraction fluctuations are essentially due to temperature fluctuations. Applying the statistical description to the random field of fluctuations in the refractive index $D_n(R)$, one obtains again an inertial subrange $[l_0, L_0]$ and the power laws

$$D_n(R) = \langle [n(\mathbf{R}_1) - n(\mathbf{R}_2)]^2 \rangle = \begin{cases} C_n^2 R^{2/3} & : \quad l_0 \ll R \ll L_0 \\ C_n^2 l_0^{-4/3} R^2 & : \quad R \ll l_0. \end{cases} \tag{3.10}$$

C_n^2 is called refractive index structure constant or better *structure parameter*, since it is a measure of the strength of fluctuations of n. Path-averaged values of C_n^2 and inner scale l_0 can be obtained simultaneously by optical measurements over a short path length ($\sim 100\,\mathrm{m}$) using a scintillometer ([128] and references therein). Typical values of C_n^2 range from $10^{-17}\,\mathrm{m}^{-2/3}$ in weak turbulence up to $10^{-13}\,\mathrm{m}^{-2/3}$ in "strong" turbulence. While it may be reasonable to assume C_n^2 to be roughly constant (at least over short time intervals) at a certain height above a uniform terrain, it varies as a function of height for vertical or slant propagation paths, for example from ground to a satellite. In this case, C_n^2 can be described by altitude profile models (e.g., the *Hufnagel-Valley model*), that have been developed for both night and day time conditions from a series of measurements [129].

3.4 Atmospheric Propagation

Random space-time redistribution of the refractive index causes a variety of effects on an optical wave related to its temporal intensity fluctuations (scintillation) and phase fluctuations. When an electromagnetic wave propagates through a random medium like the turbulent atmosphere, both the amplitude and phase of the electric field experience random fluctuations caused by small, random changes in the refractive index. Since the wavelength λ in the visible and infrared spectral region is much smaller than the smallest scale of turbulence l_0, scattering by refractivity fluctuations is confined to a narrow cone about the progation direction. Although this observation allows some simplification, the wave equation cannot be solved analytically. Perturbative approaches using the Born approximation or Rytov approximation allow quantitative statements, at least for so-called *weak fluctuation* conditions, that is, when

$$\sigma_1^2 < 1 \quad \text{and} \quad \sigma_1^2 \Lambda^{5/6} < 1, \quad \text{with} \tag{3.11}$$

$$\sigma_1^2 = 1.23\, C_n^2 k^{7/6} L^{11/6} \quad \text{Rytov variance} \tag{3.12}$$

$$\Lambda = \frac{2L}{k w_L^2} \quad \text{Fresnel ratio at receiver.} \tag{3.13}$$

Here, $k = 2\pi/\lambda$ is the wave number, L is the propagation distance (not to be mixed with the turbulence outer scale L_0), and $w_L = w(z = L)$ is the beam spot size at the

receiver without turbulence. Strictly speaking, most of the relations given in the following are only accurate under weak fluctuation conditions. Additionally, it is assumed that the structure parameter C_n^2 is constant over the propagation path, which restricts the applicability to horizontal line-of-sight paths near ground.

3.4.1 Beam wander and beam spreading

In the absence of turbulence, a Gaussian beam is broadened by diffraction and has, in the far field, a beam radius w_L as discussed in §3.1. When analysing the beam radius in a turbulent medium, the situation is more complex, and it is usually necessary to distinguish between the short-term and the long-term beam spread. Generally speaking, when a finite optical beam interacts with refractive index inhomogeneities due to atmospheric turbulence, it is found that those turbulent eddies which are large compared to the diameter of the beam tend to deflect the beam, whereas those eddies that are small compared with the beam diameter tend to broaden the beam, but do not deflect it significantly. Consequently, if one observed the laser spot on a screen in the plane of the receiver aperture, and took a very short exposure picture, one would observe a laser spot which is broadened (due to the small eddies) to some radius w_{st}, and is deflected by some distance r_{bw} from the optical axis. Because the turbulent eddies are flowing across the propagating beam, the centroid of the short-term beam spot will be randomly deflected in different directions (Figure 3.4). This effect is called *beam wander* or *beam steering* and takes place on time scales on the order of

$$\tau_{\mathrm{bw}} = \frac{\text{beam size}}{v_{\perp}}, \tag{3.14}$$

where $v_{\perp}$ is the transverse flow velocity of the turbulent eddies. The strength of beam wander is characterised by the root-mean-square value of the beam displacement from the long-term centre, which is for a collimated Gaussian beam

$$< r_{\mathrm{bw}}^2 >^{1/2} = \sqrt{2.87 C_n^2 L^3 w_0^{-1/3}}. \tag{3.15}$$

Beam wander is, in general, smaller for divergent beams and larger for (initially convergent) beams with an intermediate focus along the propagation path. The maximum beam wander occurs for beams focused at $\sim 35\%$ of the path [130].

When taking a long-term exposure of the beam spot, averaging over time scales much longer than τ_{bw}, one sees a broadened spot with a mean-square radius w_{eff}^2 given by

$$\langle w_{\mathrm{eff}}^2 \rangle = \langle w_{\mathrm{st}}^2 \rangle + \langle r_{\mathrm{bw}}^2 \rangle. \tag{3.16}$$

The mean intensity profile at the receiver plane remains still approximately Gaussian, i.e.

$$< I(r, L) > \simeq \frac{w_0^2}{w_{\mathrm{eff}}^2} \exp\left(\frac{-2r^2}{w_{\mathrm{eff}}^2}\right), \tag{3.17}$$

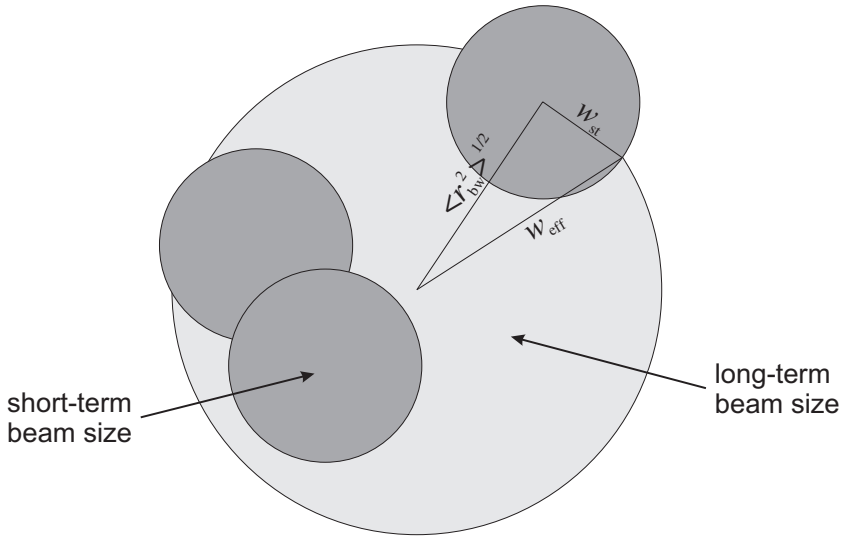

Figure 3.4: Short term and long term beam radius at the receiver for weak turbulence conditions: the dark shaded circles represent the short-term size w_{st} of the beam; additional beam wandering on a scale $\langle r_{\mathrm{bw}}^2 \rangle$ results in an effective long-term beam size w_{eff}, marked by the large, light shaded circle. (Figure adapted from [131])

where the long-term, or effective beam radius, w_{eff} is given [132] by

$$w_{\mathrm{eff}} = \frac{\lambda L}{\pi w_0} \sqrt{1 + \left(\frac{w_0}{\rho_{\mathrm{sp}}} \right)^2}. \tag{3.18}$$

Here, ρ_{sp} denotes the spherical wave transverse coherence radius defined by

$$\rho_{\mathrm{sp}} = \left[1.46 k^2 L \int_0^1 (1-\xi)^{5/3} C_n^2(\xi L)\, d\xi \right]^{-3/5}, \tag{3.19}$$

where the variable $\xi = s/L$ is the normalised distance along the path from the transmitter to the receiver. The term $(1-\xi)^{5/3}$ under the integral reflects the fact that the turbulence contained in path segments close to the transmitter has a pronounced effect on the beam wander behaviour. For a flat profile of the refractive index structure parameter $C_n^2(s)$=const, equation (3.19) reduces to

$$\rho_{\mathrm{sp}} = \left[0.55 k^2 L C_n^2 \right]^{-3/5}. \tag{3.20}$$

Note that equation (3.18) is valid under both weak and strong fluctuation conditions. The value for the short-term beam radius w_{st} can be calculated using equations (3.16) and (3.18), yielding

$$w_{\mathrm{st}} = \frac{\lambda L}{\pi w_0} \sqrt{1 + \left(\frac{w_0}{\rho_{\mathrm{sp}}} \right)^2 \left[1 - 0.62 \left(\frac{\rho_{\mathrm{sp}}}{w_0} \right)^{1/3} \right]^{6/5}}. \tag{3.21}$$

Unfortunately, the model given above only holds in the limit when turbulence is relatively weak. When turbulence is strong, the beam no longer wanders significantly, but breaks up into multiple beams. In this case a short exposure picture of the received spot would not consist of a single spot, but of a multiplicity of spots at random locations. The long-exposure picture, however, would be a blurred version of the short exposure, but with approximately the same total diameter w_{eff} [132]. For $L \gg kw_0^2$ and $w_0/\rho_{\text{sp}} \gg 1$, it is found that in homogeneous turbulence

$$\langle r_{\text{bw}}^2 \rangle \simeq C_n^{8/5} k^{-1/15} L^{37/15}, \tag{3.22}$$

which is small compared with w_{eff}. However, knowledge of $\langle r_{\text{bw}}^2 \rangle$ and w_{eff} does not yield a prediction about how many bright patches will be formed.

3.4.2 Angle-of-arrival fluctuations

The light propagating through the atmosphere from a distant transmitter is eventually collected by a lens of diameter D and focused onto some kind of detector. Atmospheric turbulence effects on the propagating beam wave thereby translate into a degradation of the image formed in the focal plane. This is of course a well known phenomenon for astronomers using ground-based telescopes [133], where the achievable angular resolution does not grow indefinitely with the telescope diameter.

The image degradation effects are associated predominantly with phase fluctuations of the incoming wave. Large scale turbulence cells induce an overall tilt of the wave front (i.e. fluctuations in the *angle-of-arrival* α), which subsequently causes the image to *jitter* or *"dance"* in the focal plane as large eddies move across the beam path, driven by the predominating atmospheric flow (Figure 3.5). Long-term *image blur* is caused by a superposition of small-scale turbulence effects and large-scale image jitter. Thus, image dancing and image blur are the image counterparts of beam wander and beam spreading.

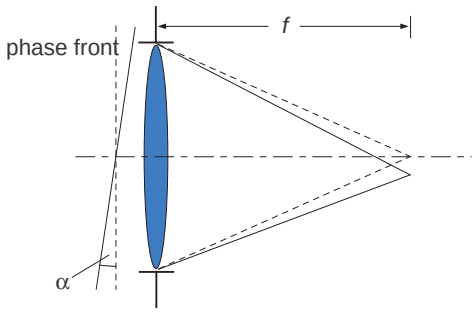

Figure 3.5: Angle-of-arrival and image jitter.

Hence, small-scale and large-scale effects have different influence on image quality, depending on the exposure time: large eddies comparable in size to the receiver aperture move across the aperture within a time $D/v_\perp$, where $v_\perp$ is the mean wind speed perpendicular to the propagation path. In contrast to this, motion of the smallest eddies is usually estimated by the inner scale size l_0. Accordingly, a long time exposure is determined by the time required to average over a number of large eddies, whereas exposure times much smaller than $D/v_\perp$ are considered *short*. Consequently, a short exposure does not include the motion of large eddies responsible for image dancing, but

is dominated by the phase front distortions arising from the small-scale turbulences on the inner scale size l_0. The resulting image exhibits a *"speckle pattern"* similar to that produced by a laser that is scattered off a rough surface.

Quantitatively, one obtains the following expression for the angle-of-arrival variance of a plane wave in nearly homogeneous turbulence [132]:

$$\langle \alpha^2 \rangle \simeq \left\{ \begin{matrix} 2.19 \\ 2.92 \end{matrix} \right\} \frac{\int_0^L C_n^2(x)\, dx}{D^{1/3}}, \qquad \begin{matrix} l_0 \ll D \ll \rho_{\mathrm{pl}} \\ \rho_{\mathrm{pl}} \ll D \ll L_0. \end{matrix} \tag{3.23}$$

Equation (3.23) is valid under strong fluctuation conditions, it represents a good estimate also for the plane wave and for a beam wave (except in the focal plane).

In §4.4 the possibility of adaptive methods to compensate for angle-of-arrival fluctuations will briefly be discussed; in this respect, the temporal spectrum of the angle-of-arrival fluctuations are of major importance because it dictates the speed of actuators and the control loop. Assuming frozen turbulence (see §3.4.5), the angle-of-arrival spectrum $W_\alpha(f)$ for a spherical wave propagating in homogeneous turbulence is given by [132]

$$W_\alpha(f) = \left\{ \begin{matrix} 0.0326 \\ 0.0652 \end{matrix} \right\} \frac{v_\perp^{5/3} C_n^2 L}{D^2} \left[1 - \frac{\sin\left(\frac{2\pi f D}{v_\perp}\right)}{\left(\frac{2\pi f D}{v_\perp}\right)} \right] \frac{f^{-8/3}}{\left[1 + \left(\frac{1.07 v_\perp}{2\pi f L_0} \right)^2 \right]^{4/3}} \qquad \begin{matrix} l_0 \ll D \ll \sqrt{\lambda L} \\ D \gg \sqrt{\lambda L} \end{matrix} \tag{3.24}$$

A plot of the angle-of-arrival spectrum (Figure 3.6), normalised to the average angle-of-arrival $\langle \alpha^2 \rangle$, shows that nearly all of the angle-of-arrival fluctuations are contained in the frequency interval

$$\frac{0.01 v_\perp}{2\pi D} \le f \le \frac{10 v_\perp}{2\pi D}, \tag{3.25}$$

provided that $D \ll L_0$.

3.4.3 Fried parameter

A quantity often used for the characterisation of the strength of atmospheric turbulence, especially in connection with astronomical imaging, is the *Fried parameter* r_0 [133]. For a known structure constant profile $C_n^2(s)$ along the propagation path, the Fried parameter is given by

$$r_0 = \left[0.423\, k^2 \int\limits_{\mathrm{Path}} C_n^2(s)\, ds \right]^{-3/5} = \left[0.423\, k^2 L C_n^2 \right]^{-3/5}, \tag{3.26}$$

where $k = 2\pi/\lambda$, and the integral is taken over the entire path from the emitter to the receiver telescope; the last expression applies for the case of constant C_n^2 along the path. The loss of spatial coherence of an electromagnetic wave propagating through

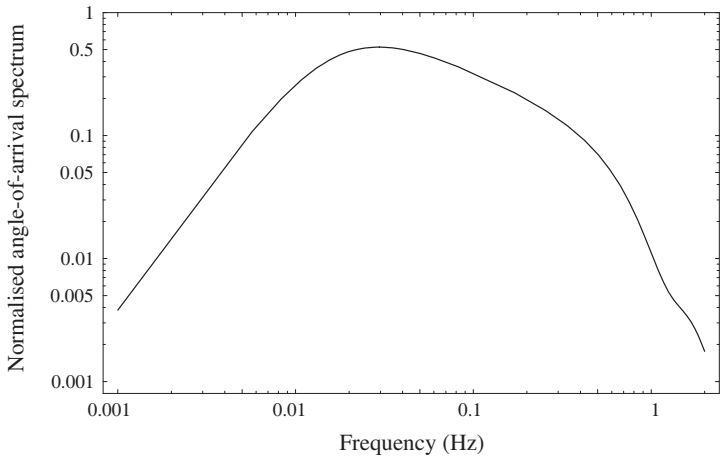

Figure 3.6: Normalised angle-of-arrival spectrum for a spherical wave received by an aperture with $D/L_0 = 0.1$.

atmospheric turbulence is characterised by the transversal coherence radius. Because r_0 is related to the transversal coherence radius ρ_{pl} of a plane wave propagating through turbulence by $r_0 = 2.1\rho_{\mathrm{pl}}$, the Fried parameter r_0 is also called *atmospheric coherence length*.

The significance of r_0 is particularly illustrative in astronomical imaging. The image of a point source, like a star, in an ideal telescope without atmosphere depends solely on diffraction and is described by an Airy function. Since the first dark ring appears at an angular distance of $1.22\lambda/D$ from the centre, the ratio λ/D equals roughly the angular extent[1] (*seeing angle* β) of the star image, and is often taken as a measure for the resolution of an ideal telescope. Under the influence of atmospheric turbulence, the seeing angle is limited by

$$\beta = 0.98\lambda/r_0. \tag{3.27}$$

Historically, the Fried parameter was initially introduced in this phenomenological way. Since the atmospheric coherence length at sea level is roughly $r_0 = 2...15\,\mathrm{cm}$ for visible and IR wavelengths, even in best conditions, a large diameter telescope without adaptive optics does not provide better resolution than a telescope with a diameter on the order of r_0. It is apparent from equation (3.26), that r_0 scales with the wavelength like $r_0 \propto \lambda^{6/5}$, therefore it is important to indicate the corresponding wavelength when specifying the Fried parameter.

3.4.4 Pulse propagation

Just as a Gaussian beam wave undergoes spatial broadening in atmospheric turbulence, a pulse of electromagnetic radiation propagating under atmospheric influence is also spread

[1] technically, the FWHM of the point spread function

in the time domain. Temporal spreading is mainly caused by two mechanisms [134]: first, the scattering process of the medium, that is, dispersive spreading due to the existence of multiple paths, and, second, the "wandering" in the time domain, meaning a time jitter of the arrival time about its mean value within the ensemble. The latter is the dominant effect in weak turbulence. Assuming an initial Gaussian temporal shape of the pulse

$$I(t) = I_0 \exp(-2t^2/T_0^2)$$

with length T_0, the combined effects from the two mechanisms result in

$$\langle I(L,t)\rangle \simeq I_0 \frac{T_0}{T_1} \exp\left[-\frac{2(t-L/c)^2}{T_1^2}\right]. \tag{3.28}$$

Thus, the centre of the pulse still arrives at the usual time delay $t = L/c$, but the shape of the pulse is broadened. Applying the usual *von Karman* spectrum for the refractive index fluctuations, the temporal broadening in weak turbulence can be estimated by

$$T_1 = \sqrt{T_0^2 + \langle \delta T^2 \rangle}, \quad \text{with} \quad \langle \delta T^2 \rangle \simeq \frac{3.127}{c^2} L_0^{5/3} \int_0^L C_n^2(x)\, dx. \tag{3.29}$$

Greenwood and Tarazano [135,136] proposed a different spectral model, that was derived empirically from actual atmospheric measurements, and that gives a more realistic value of the pulse broadening [137]:

$$\langle \delta T^2 \rangle = \frac{26.31}{c^2} L_0^{5/3} \int_0^L C_n^2(x)\, dx. \tag{3.30}$$

In the derivation of the turbulence induced quantity $\langle \delta T^2 \rangle$, the broadening originates from a pure phase effect. Consequently $\langle \delta T^2 \rangle$ is independent on the wavelength, general beam characteristics, and initial pulse width. The mean arrival time remains unchanged L/c compared to the undisturbed case. Liu and Yeh performed a calculation [138] based on the concept of temporal moments and obtained expressions that can not only be applied in the case of scattering by the continuous turbulent atmosphere, but also for discrete random scatterers, e.g., in the presence of clouds, rain, or fog. They conclude that, for optical frequencies, atmospheric turbulence does only severely affect the transient behaviour of the pulse when the pulse length is on the order of a few picoseconds or shorter. Only under very strong scattering conditions, such as in cloads, the multiple scattering of the propagating wave results in a significant extra time delay, and the pulse broadening can become substantial.

3.4.5 Fourth order statistics: Scintillation

Fluctuations in the received intensity resulting from propagation through atmospheric turbulence are commonly referred to as *scintillation*. A well known manifestation of this phenomenon is the twinkling of stars.

There is comprehensive literature about the subject of scintillation (for an introduction, see e.g. [127]), and it is beyond the scope of this chapter to summarise in some generality the many findings and cases investigated in the literature. Instead, some mechanisms associated with scintillation shall be introduced qualitatively.

The term scintillation usually includes not only the temporal variation in received intensity, but also the spatial variation within a receiver aperture (like speckle). The temporal spectrum of the intensity fluctuations is an important source of noise in classical optical communication systems. Strong scintillation can lead to temporary signal fades that have to be taken into account at signal recovery level and at communication protocol level. Scintillation characteristics can be deduced from the 4^{th} order moment of the optical field. The *scintillation index* σ_I^2 is defined as the normalised intensity variance:

$$\sigma_I^2 = \frac{< I^2 >}{< I >^2} - 1. \tag{3.31}$$

Under weak turbulence conditions, the scintillation index grows linearly with C_n^2 (or the Rytov variance $\sigma_1^2 = 1.23 C_n^2 k^{7/6} L^{11/6}$), until it reaches a maximum value greater than unity in the regime characterised by random focusing, so called, because the focusing caused by large-scale inhomogeneities achieves the strongest effect (Figure 3.7). With increasing path length (or turbulence strength) the focusing effect is weakened and the fluctuations begin to decrease, saturating at a level for which the scintillation index approaches unity from above. Saturation occurs because multiple scattering causes the optical wave to become increasingly less coherent as it propagates, eventually appearing

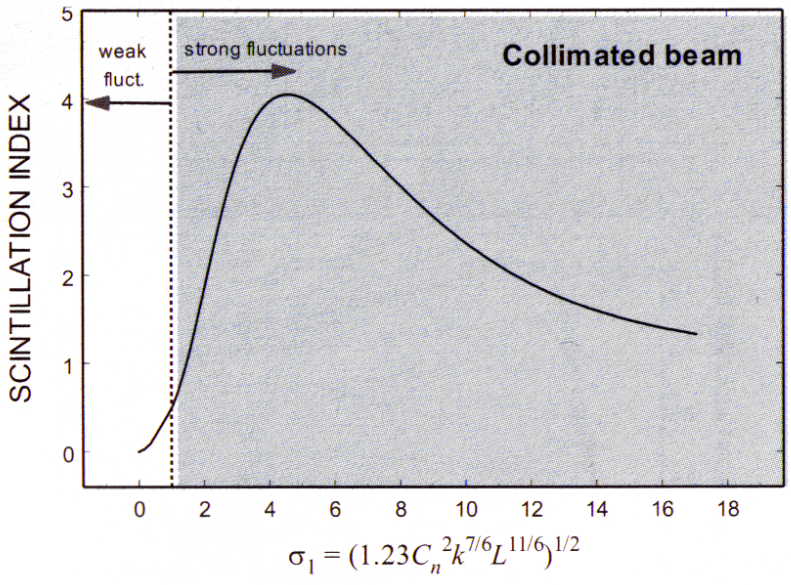

Figure 3.7: Qualitative behaviour of the scintillation index for a collimated beam as a function of the square root of the Rytov variance (Figure taken from [131]).

like extended multiple sources all scintillating with distinct random phases [131].

For weak fluctuations, there can be a significant difference between the on-axis and off-axis scintillation index: for a Gaussian beam wave, the scintillation index grows quadratically with the distance r from the optical axis. Far from the centre of the beam, beam wander actually plays a significant role for scintillation. As the strength of the turbulence increases due to long path lengths, beam wander becomes less important as the beam breaks up into a multitude of irregular shaped spots [127].

Naturally, a large receiver aperture decreases the measured scintillation strength, since the detector then averages over a certain spatial region of the beam. The characteristic scale in this respect is the lateral width (correlation length) of the intensity fluctuations, that can be estimated by the size of the Fresnel length $\sqrt{L/k}$ for weak fluctuations, and by the spatial coherence radius ρ_0 for strong turbulence.

Scintillation is usually not measured as spatial, but as temporal intensity fluctuations. Spatial and temporal statistics are connected by Taylor's *"frozen turbulence"* hypothesis: It assumes that temporal variations of an atmospheric quantity at a point are produced by *advection* of these quantities by the mean wind speed flow and not by changes in the quantities themselves. The turbulent eddies are supposed to be "frozen" over short periods of time while they are blown across the observation path, very much like clouds moving along with little change of shape. Thus, one can convert directly from spatial statistics to temporal statistics using the mean transverse wind speed $v_\perp$. By further application of a Fourier transform, one can then deduce the power spectrum of the temporal intensity fluctuations, for example. However, Taylor's hypothesis fails when $v_\perp$ is significantly less than the magnitude of turbulent fluctuations in wind velocity, which may happen when the mean wind speed is nearly parallel to the line of sight. In thas case, the temporal statistics cannot be easily inferred from the spatial fluctuations.

Change of photon statistics

In close analogy to intensity scintillations, the photon counting statistics of laser radiation are affected by propagation in the turbulent atmosphere. Under weak scintillation conditions, the Kolmogorov model predicts a log-normal photon counting distribution. For long propagation paths near ground, however, the intensity scintillations are expected to saturate because of multiple-scattering effects. In a recent (QKD) experiment [39] over a 10 km horizontal path, the counting distribution at the receiver due to the emitted highly attenuated laser pulses was found to be highly non-Poissonian and could be fitted reasonably well under the assumption of a log-normal distribution [139]. The usual assumption, that the probability for transmission of photons through the quantum channel is statistically independent, is therefore not strictly justified. The probabilities of detection for any photons propagating within a small time interval (in particular, in the same pulse) depend on the same refractive-index configuration. Hence, there are strong correlations of photon's trajectories, and thus, of detection events within a short time interval [140].

4 The inter-island link

At an early stage of the experiment, an evaluation of possible trial sites was undertaken. Key requirements for a trial site are:

- suitable infrastructure at the 'transmitter' and the 'receiver' location
- a large aperture telescope (> 0.5 m) at the receiver location capable of pointing at the transmitter location (horizon pointing)
- a line-of-sight location for the transmitter situated > 100 km from the receiver
- high altitude beam path for low attenuation and turbulence beam wander

'Suitable infrastructure' comprises requirements such as accessibility, availability of electrical power and, preferably, internet connection.

A trial site close to the ideal was identified on the Canary Islands, namely between the islands of *La Palma* and *Tenerife* (see Figure 4.1). On both islands, the *Instituto de Astrofísica de Canarias* (IAC) runs astronomical observatories which are situated at 2400 m above sea level well above the first inversion layer (clouds), and are renowned for their outstanding meteorological conditions. The sites provide seeing conditions (see §3.4.3) of sub-arcsec quality over long time periods and high atmospheric transmission. Furthermore, the site has been used for (classical) optical free-space communication experiments before [141].

The transmitter was located on a platform next to the *Nordic Optical Telescope* (NOT) on La Palma, which is one of the few places on the *Observatorio del Roque de los Muchachos* with direct line of sight to Tenerife. The transmitter telescope (consisting of a 150 mm diameter achromatic lens to collimate the light emitted from a bare single-mode fibre) was mounted on a heavy workbench to keep vibrations at a minimum. At the other end of the 144 km optical path, the Optical Ground Station (OGS) of the European Space Agency (ESA) on Tenerife served as the receiver. The 1-m telescope is located at the *Observatorio del Teide*, Izaña, and was designed for classical optical communication experiments with satellites. From the geographic coordinates of the transmitter and the receiver location

- NOT parking lot: N 28°45'26.0", W 17°53'05.8", altitude 2381 m
- OGS: N 28°17'58.3", W 16°30'36.4", altitude 2393 m

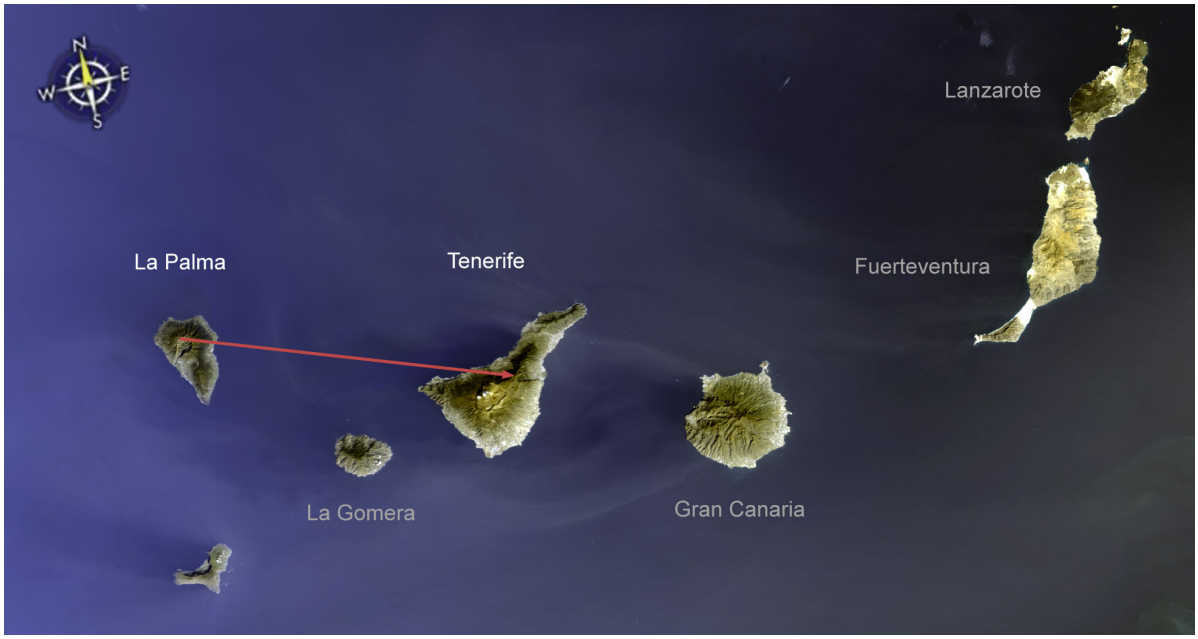

Figure 4.1: Satellite image of the Canary Islands. The arrow indicates the optical path from the transmitter on La Palma to the receiver on Tenerife. (Image by ESA/Envisat)

one calculates a cartesian distance between the two sites of 143.63 km and the course from NOT to OGS to be 110.4°.

In this chapter, properties of the free-space link between the Roque de los Muchachos and the Optical Ground Station will be presented and discussed. The data were collected during a total of five trial campaigns between May 2005 and September 2006 and can therefore be at most representative for the warmer half of the year. Besides, the collected data don't allow conclusive statements about atmospheric conditions with statistical significance, but merely characterise the conditions that were encountered at the time. The trial site and the individual parts of the experimental setup, including the transmitter and receiver telescopes, will be described in more detail in the next chapter.

4.1 Beam spreading and other losses

Applying the theory of Gaussian beam propagation in vacuum with the parameters of the inter-island link (link distance Z=143.6 km, beam radius at the transmitter w_0=3.75 cm, wavelength λ=850 nm), the beam radius at the receiver would be w_Z=1.04 m, corresponding to a divergence half angle of Θ_0=7.2 μrad. For shorter wavelengths the beam divergence would be even smaller. Using an alignment laser at 532 nm, it was possible to project the transmitted beam onto the outside wall of the OGS building. Very rough estimates of beam full widths between 3 m and 6 m were seen, corresponding to a turbulence enlarged divergence half angle Θ_T ∼10-20 μrad. The observation that turbulence

induced beam spreading was much larger than diffraction beam spreading also occurred when trying to collimate the beam by optimising the focus of the transmitter telescope: a large uncertainty in the optimal focus position was found, over which the beam spot size did not change significantly. However, the eye has logarithmic sensitivity, so a more precise method is to image the beam onto a camera and to observe the image jitter and image blur. If the camera frame rate is not fast enough to separate these two effects, one may estimate an effective long term divergence angle Θ_T under turbulence from the image spot $1/e^2$ radius of a long exposure image according to

$$\Theta_T = \frac{r_{1/e^2}}{f}, \tag{4.1}$$

where f is the focal length of the camera imaging system. Two different cameras of the OGS were used for measurements: the *wide field camera* (WFC) was mounted on a separate 300 mm aperture *Maksutov* telescope bore sighted with the OGS. The *Coudé camera* (CC) was placed at a subsidiary Coudé focus accessed by a removable mirror on the optical bench. While the CC took single pictures with various exposure times, the WFC allowed continuous recording at a rate of 25 frames/s. Estimates of the long-term effective beam radius w_{eff} at the receiver were computed from CC images with 1 s exposure time and from 1 min averages of WFC spot radii; the latter can be considered worst case values.

Since the OGS telescope aperture is smaller than the effective beam width, geometrical losses occur at the receiver. If the beam was perfectly centered around the optical axis of the receiver telescope (primary mirror diameter $D_{\text{M1}} = 1.0\,\text{m}$, central obscuration by secondary mirror $D_{\text{M2}} = 0.33\,\text{m}$), a fraction

$$\frac{P_R}{P_T} = \exp\left[-\frac{2(D_{\text{M2}}/2)^2}{w_{\text{eff}}^2}\right] - \exp\left[-\frac{2(D_{\text{M1}}/2)^2}{w_{\text{eff}}^2}\right] =: L_T \tag{4.2}$$

of the transmitted power would be collected by the receiver. This fraction is referred to as *turbulence loss* L_T in the following. End-to-end transmission losses L_{ee} were determined from comparing the intensity before the transmitter lens and after the OGS telescope optics in the Coudé focus, using identical optical power meters. Altogether, there are 4 distinct loss mechanism contributing to L_{ee}:

L_0: beam spreading loss due to diffraction, that is present even in vacuum

L_A: atmospheric losses due to scattering and absorption by air molecules

L_T: turbulent atmospheric losses, i.e., turbulence induced beam spreading

L_I: losses due to imperfections of optical components

Date	λ (nm)	Θ_T (μrad)	w_{eff} (m)	L_{ee} (dB)	L_T (dB)	L_A (dB)	camera & integration time
13/5/05	532	70	10	35.3	23.5	7.8	WFC, 1 min
16/5/05		57	8.2	34.5	21.8	8.7	CC, 1 s
		75	10.8		24.2	6.3	WFC, 1 min
18/5/05		13.6	2.0	31.7	9.8	17.9	CC, 1 s
		23.6	3.4		14.2	13.5	WFC, 1 min
14/5/05	850	39.6	5.7	41.5	18.7	18.8	WFC, 1 min
18/5/05		13.0	1.9	23.2	9.4	9.8	CC, 10 s

Table 4.1: Summary of beam propagation measurements over the inter-island link for wavelengths 532 nm and 850 nm: measured long term beam radii w_{eff}, optical end-to-end transmission losses L_{ee}, decomposed into turbulence induced losses L_T and losses due to absorption/scattering L_A. The range of values illustrates the strong dependency on weather conditions.

The transmitter and receiver telescope optics up to the Coudé focus accounted for an attenuation of $L_I \sim 4\,\text{dB}$. With these values, one can attempt to decompose the end-to-end transmission into contributions from the individual effects[1]. Table 4.1 summarises the results for wavelengths 532 nm (alignment laser) and 850 nm (quantum signal). It is apparent from the large range of obtained values, that weather conditions have a huge impact on beam spreading and overall transmittance. However, due to the limited observation time, systematic dependencies cannot be derived reliably from the data.

The absorption and scattering induced losses L_A appear to range between 6 dB and 18 dB for 532 nm, and between 10 dB and 19 dB for 850 nm light. If one concentrates on good atmospheric conditions, a value around 10 dB seems realistic for 850 nm, which implies a loss of $\sim$ 0.07 dB/km, in good agreement with values in the literature [38, 39, 142]. There, atmospheric transmission losses were found to be 0.04-0.08 dB/km at altitudes above 2000 m.

The overall transmittance values listed above are time averaged values over several minutes of measurement time. Figure 4.2 (a) shows the received power at the Coudé focus as a function of time, with measurement intervals of 250 ms, (b) depicts the corresponding propability distribution using 1 μW wide bins. Despite the aperture averaging effect of the 1-m receiver telescope, strong scintillations in the received optical power are observed. The average received power was 16 μW (equivalent to 25.9 dB link attenuation), with RMS fluctuations of 9.45 μW, which corresponds to a scintillation index of 0.35. However, this value contains only fluctuations up to a frequency of 4 Hz and is certainly too low. Still, it indicates the dominance of beam wander.

[1] More precisely, diffraction beam spreading was not subtracted from L_T, because due to the central obscuration of the OGS, the computed value for L_0 would imply a much higher effect on L_{ee} than it really has.

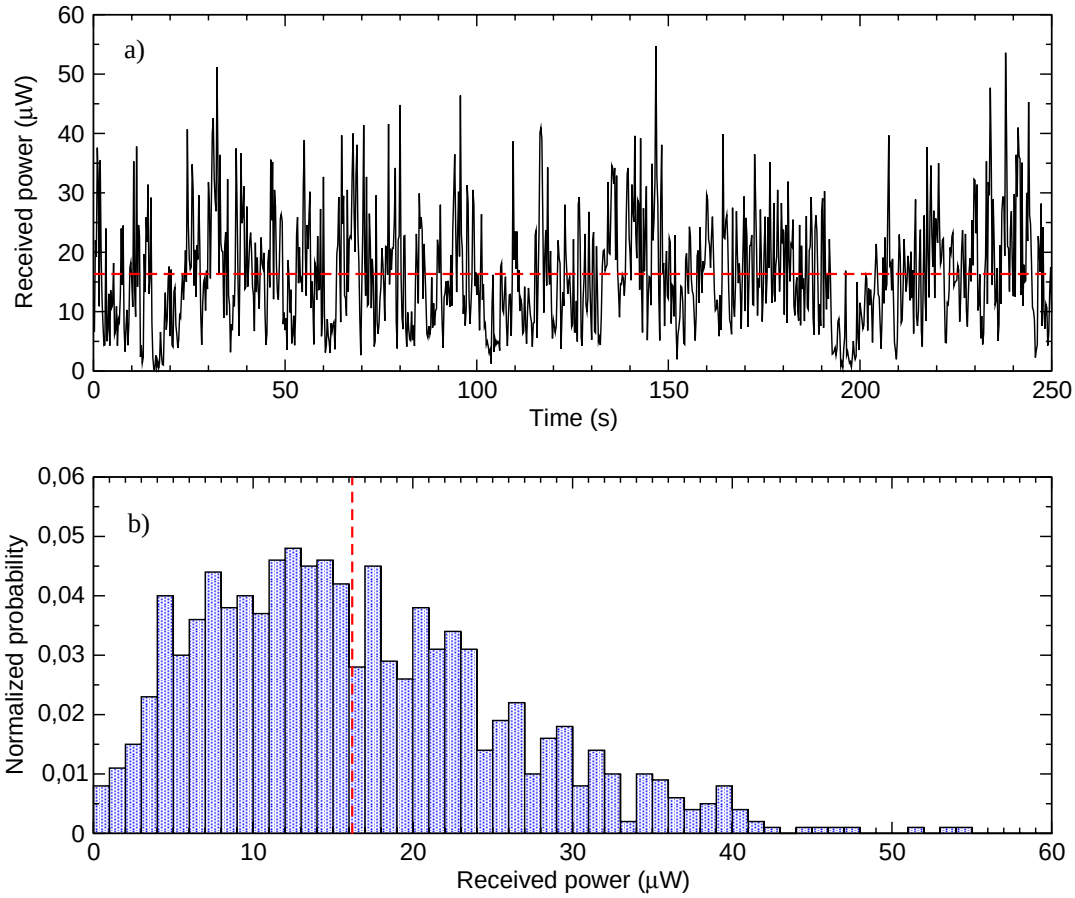

Figure 4.2: Scintillations of the optical power collected by the OGS: **(a)** received power as a function of time, measurement intervals 250 ms. The dashed line indicates the mean value of 16.2 μW. **(b)** The normalised probability distribution of the received power has asymmetric shape, extending farther to high transmittance than to low transmittance values. The transmitted power at 808 nm wavelength was 6.3 mW.

4.2 Angle-of-arrival fluctuations and long-term beam drift

The angle-of-arrival fluctuations can be deduced from the time-dependent displacement of the beam spot centroid on the WFC. One has to keep in mind, however, that the fluctuation spectrum is limited to a frequency equal to half of the WFC frame rate (25 Hz). An example of a measured spectrum is shown in Figure 4.3 as a solid blue line. In order to estimate the angle-of-arrival fluctuations over the full spectrum, a theoretical turbulence model [132] was fitted to the measured part of the spectrum by varying the atmospheric parameters L_0 and C_n^2. The resulting theoretical spectrum (green crosses in Figure 4.3) agrees well with the measured part and can therefore be

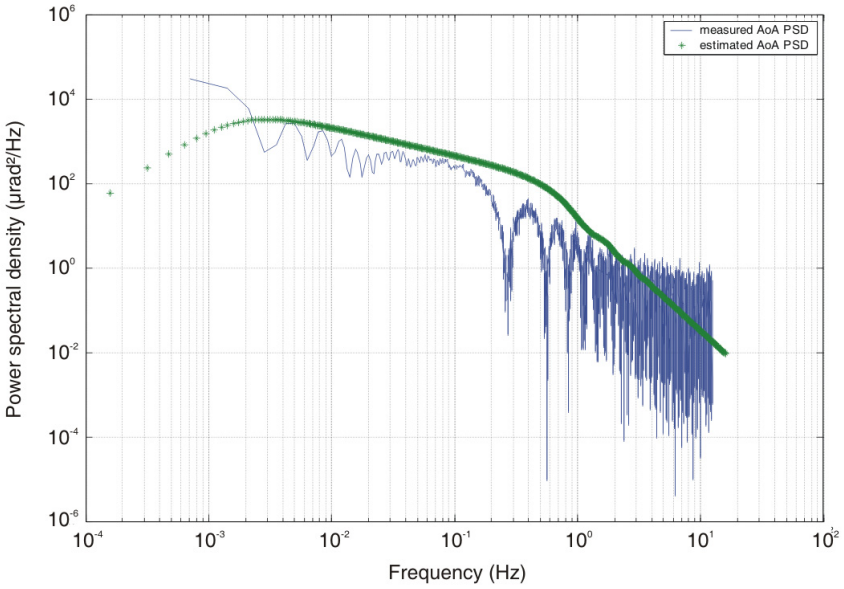

Figure 4.3: Power spectral density of angle-of-arrival fluctuations: example of calm night conditions on the inter-island link. Solid blue line: measured spectrum (up to 12.5 Hz); green crosses: theoretical prediction and extrapolation according to atmospheric turbulence model.

considered a reasonable extrapolation of the measured data. Table 4.2 summarises results collected under various atmospheric conditions. Angle-of-arrival fluctuations (full spectrum) between 15 μrad and 36 μrad were found, corresponding to a beam wander between 2.2 m and 5.2 m.

The focal length of the Coudé focus is quite long at 39.1 m and can lead to problems in connection with the given magnitude of beam wander: a wavefront tilt of some 50 μrad

Date	λ (nm)	$\langle\alpha^2\rangle^{1/2}_{\text{meas}}$ (μrad)	$\langle\alpha^2\rangle^{1/2}_{\text{full}}$ (μrad)	Comment
13/5/05	532	7.7	25.8	
16/5/05	532	6.8	28.0	
18/5/05	532	2.0	15.2	low wind $v_\perp \sim 0.1$ m/s
14/5/05	850	14.5	22.4	
15/5/05	850	7.6	(29.1)	model did not match data
16/5/05	850	7.7	36.5	
18/5/05	850	4.6	19.5	low wind $v_\perp \sim 0.1$ m/s

Table 4.2: Summary of angle-of-arrival fluctuations over the inter-island link for wavelengths 532 nm and 850 nm: the measured angle-of-arrival fluctuations $\langle\alpha^2\rangle^{1/2}_{\text{meas}}$ up to 12.5 Hz were extrapolated to the full spectrum value $\langle\alpha^2\rangle^{1/2}_{\text{full}}$ based on a Kolmogorov turbulence model.

(equals ~ 10 arcsec) causes a beam displacement of ~ 2 mm at the Coudé focus, which is much larger than the diameter of the active area of the single photon detectors (500 μm). Therefore, the received beam was not imaged directly onto the detectors, but a focal length reducer was used, bringing the receiver optics to an effective f/5 system where the beam displacement at 50 μrad wavefront tilt is 0.25 mm.

To verify the effectiveness of this optical layout, a camera was placed at the detector position, and the size and displacement of the beam spot were investigated. Figure 4.4 shows a sequence of images acquired at exposure times on the order of milliseconds, which can be considered short with regard to the time scale of large turbulences $D/v_\perp$ from §3.4.2. As expected, one observes blurred beam images exhibiting a pronounced speckle pattern, that is induced by small eddies. Comparing the images from frame to frame (temporal separation several seconds), the "dancing" of the beam centroid position because of overall wavefront tilts is apparent. The measured beam spot size was between 100 μm and 350 μm, fitting well onto the active detector area and confirming the suitability of the receiver's optical design for the turbulence conditions on the inter-island link.

A long-term measurement of the beam wander (Figure 4.5a) over 55 minutes reveals a systematic drift of the beam position as much as 600 μm. Due to the internal beam guidance optics of the OGS, the graph coordinate system is rotated by approx. 45°, that is, the beam drift takes place effectively along the vertical direction. The temporal evolution of the distance of the beam from its initial position at t=0 (Figure 4.5b) shows that random fluctuations are superimposed by a systematic drift taking place largely within 2-3 min. The explanation for this behaviour is most probably a changing temperature gradient in the atmosphere, on which the beam was diffracted. Such changes in the atmospheric layering take place on an irregular basis and pose a problem, since they can give rise to much larger beam deflections than ordinary beam wander, which is by definition isotropic. Therefore, a bidirectional active tracking system (see §4.4.2) was implemented on both transmitter and receiver telescope to compensate such effects.

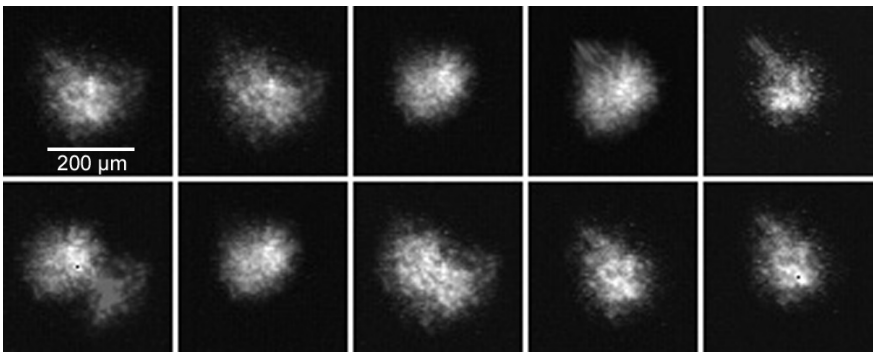

Figure 4.4: Series of beam images, recorded in the detector focal plane with short exposure times of a few milliseconds, show strong mode fluctuations. The temporal separation between the images was several seconds.

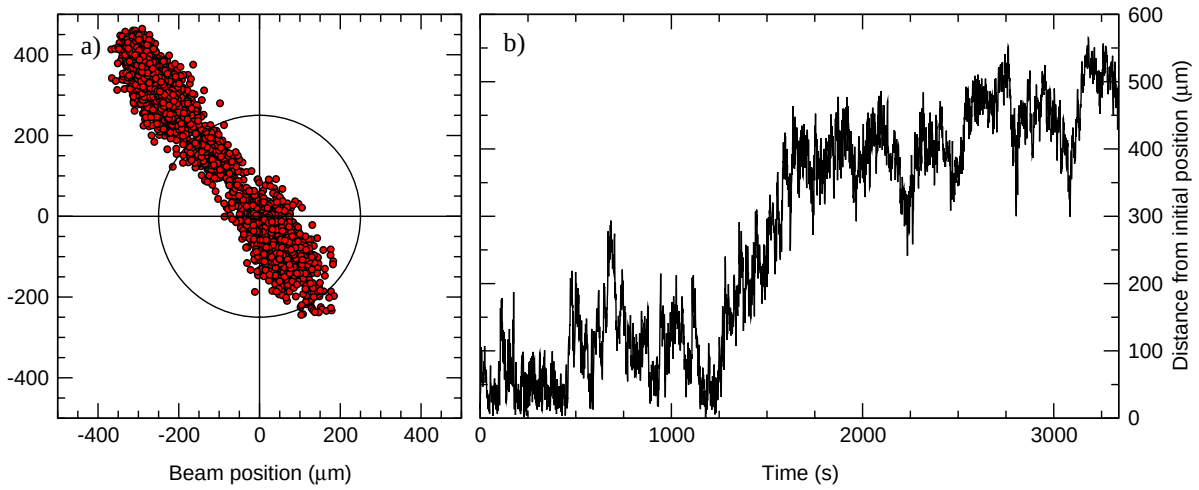

Figure 4.5: Long term measurement of beam spot position in the detector focal plane. **(a)** beam centroid positions over full measurement time of 55 min; the circle indicates the diameter of the detector active area. **(b)** Temporal evolution of the beam spot's distance from its starting position at t=0. A systematic drift due to atmospheric temperature gradients is observed on a time scale of several minutes.

4.3 Atmospheric turbulence parameters

The gathered data was used to calculate estimates of different atmospheric turbulence parameters to further characterise the inter-island link. Table 4.3 summarises some results, the respective derivations are laid out in the following.

The long time exposures taken with the Coudé camera, and accumulated frames from the wide field camera, provided measurements of the long-term spot radius of the transmitted beam, which can be considered to be approximately a point-like source. The measured FWHM of the recorded long-exposure images can be directly substituted into the definition (3.27) of the Fried parameter to obtain r_0. The measured values between 1 cm and 5 cm for 850 nm wavelength are well within the expected range for a horizontal propagation path. In a survey over the same free-space link [141], r_0 values of typically between 1.5 cm and 2.4 cm for 830 nm wavelength were obtained. It can be concluded, that — even under best conditions — the aperture of the transmitter telescope (150 mm) is sufficiently large for the beam diameter at the receiver to be turbulence limited.

Assuming homogeneous distribution of turbulence along the entire propagation path, the refractive index structure constant C_n^2 can be estimated from the measured Fried parameter using Eq. (3.26). Results range from $\sim 5{\cdot}10^{-16}\,\mathrm{m}^{-2/3}$ under moderate conditions to $\sim 4 \cdot 10^{-17}\,\mathrm{m}^{-2/3}$ under best conditions. Taking into account the orographical profile under the horizontal path, these values are in good agreement with an adjusted nighttime turbulence model for La Palma and Tenerife [141], which predicts $C_n^2 \sim 10^{-14}\mathrm{m}^{-2/3}$ near the surface and $C_n^2 \sim 5 \cdot 10^{-18}\mathrm{m}^{-2/3}$ at 2400 m altitude. The high turbulence on both path ends certainly contributed significantly to the observed mean value.

Date	λ (nm)	r_0 (cm)	C_n^2 ($m^{-2/3}$)	$\langle \delta T^2 \rangle^{1/2}$ (ps)	Camera and integration time
13/5/05	532	0.6	$5.5 \cdot 10^{-16}$	7.1	WFC, 60 s
16/5/05	532	0.8	$3.9 \cdot 10^{-16}$	6.0	CC, 1 s
	532	0.6	$6.1 \cdot 10^{-16}$	7.4	WFC, 60 s
18/5/05	532	3.2	$3.6 \cdot 10^{-17}$	1.8	CC, 1 s
14/5/05	850	1.8	$2.5 \cdot 10^{-16}$	4.8	WFC, 60 s
18/5/05	850	5.4	$3.9 \cdot 10^{-17}$	1.9	CC, 10 s

Table 4.3: Summary of measured and estimated atmospheric parameters of the inter-island link for wavelengths 532 nm and 850 nm: Fried parameter r_0, refractive index structure constant C_n^2, and estimated time-of-arrival jitter $\langle \delta T^2 \rangle^{1/2}$.

Having knowledge about the values of C_n^2 and L_0, the expected jitter in the arrival time of the weak coherent pulses can be estimated according to Eq. (3.30). Assuming a typical value for the outer scale of $L_0 \sim 100$ m, which is in good agreement with the measured angle-of-arrival spectrum, and applying the C_n^2 values inferred from the Fried parameter measurements, yields a time jitter in the range of a few picoseconds. Hence, given a weak coherent pulse duration of ~ 1 ns, atmospheric path length fluctuations should not contribute significantly to arrival time uncertainties.

Not surprisingly, with values on the order of between 10 and 100, the Rytov variance σ_1^2 falls far beyond the limit of 0.3 for weak turbulence conditions. Hence, weak turbulence theory is likely to produce inaccurate results. In fact, for fairly good conditions like on 14/5/05 ($\sigma_1^2 \approx 90$), equations (3.21), (3.15), and (3.18) yield for the short-term beam radius at the receiver $w_{\mathrm{st}} \sim 2.0\,\mathrm{m}$, for the mean centroid shift $\langle r_{\mathrm{bw}}^2 \rangle^{1/2} \sim 1.9$ m, and for the effective long-term beam radius $w_{\mathrm{eff}} \sim 2.8$ m, which is not too far from the values estimated by visual inspection of the beam on the OGS building. For the given turbulence parameters, theory actually predicts the beam rather to be broken up into multiple irregular patches exhibiting negligible beam wander. However, this does not reflect the visual impression; the discrepancy is probably due to the existence of particularly turbulent zones close to the transmitter.

4.4 Adaptive optics

Refractive index inhomogeneities of the turbulent air cause wave front distortions of optical waves propagating through the atmosphere, leading to such effects as beam spreading, beam wander, and intensity fluctuations (scintillations). Wave front distortions can be mitigated, in principle, by adaptive optics, that is, real-time wave front control. However, adaptive optics technologies, currently primarily used in astronomical imaging, need to be adapted to the requirements of free-space optical communications systems. For example, astronomical observatory sites are selected specifically in view

of low turbulences, and observations are usually made of objects at higher elevation angles. In contrast, free-space communications scenarios are typically characterised by much stronger turbulence effects near ground.

Conventional (non-adaptive) classical laser communications systems typically use a divergent beam for transmission, so that a sufficiently large beam footprint at the receiver end of the communication link eliminates the need for precision tracking. However, the wave front distortions arising from the inhomogeneities may still severely impact the performance of classical free-space optical communications systems by the deterioration of the communication link: the bit error rate depends on both electronic circuit related noise and on turbulence-induced, longer-term link disruptions known as *atmospheric signal fading*. While the short-term errors from random electronic noise can be recovered using various data encoding techniques, atmospheric signal fading is a challenging problem, which cannot be solved easily by data coding methods without sacrificing the system's data throughput rate. In contrast to classical systems, with quantum communications systems one is less concerned with occasional deep signal fades, since the establishment of the (random) quantum key does not require complete transmission of data packets. Despite this difference, free-space quantum communications system can profit significantly from adaptive optics techniques developed for classical laser communications systems, because they enhance not only signal stability but also the overall link transmittance.

4.4.1 Principle of adaptive optics

Systems that use mechanical means to sense and correct for atmospherically induced wave front deformations in real time are called *adaptive optics systems*. In order to remove the phase errors, all adaptive optics systems make use of the principle of *phase conjugation*: by applying the reverse phase to the distorted wave front, phase errors can be removed.

A conventional adaptive optics system, regardless whether it is used for imaging or for laser beam propagation, consists of three principal components (Figure 4.6): a wavefront sensor to detect the optical disturbance, an active or deformable mirror to correct for the optical disturbance, and an actuator command electronics to acquire the sensor information, compute the required corrective action, and to control the active mirror [143].

Adaptive optics can be used in different ways in free-space optical communication terminals [144]. The most straight-forward approach is the *adaptive receiver*: Here, the distortions of the received beam are compensated by the adaptive optics allowing for a better focusing of the optical beam onto a small detector area. Compensating only the lowest order abberations, that is, wave-front tip and tilt, stabilises the beam centroid location in the focal plane and may be sufficient if the detector area is large enough not to clip the focal spot. If the received beam is to be coupled into an optical fibre, high resolution phase compensation is required in addition to beam steering. The potential

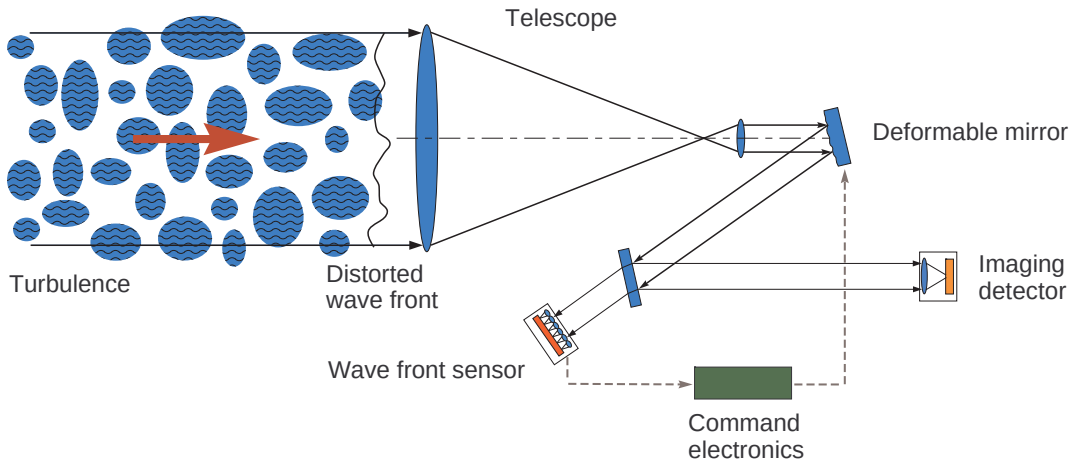

Figure 4.6: Generalised schematics of an adaptive optics system. Atmospherically induced wave front distortions on the incoming beam are sampled by a wave front sensor; based on its output the command electronics computes a corrective signal for the deformable mirror to flatten the wave front. The result is a much sharper image of the beam on the imaging detector.

of the adaptive receiver is limited though, since it allows only to compensate distortions of light waves that enter the receiver aperture. In order to increase the total power collected by the receiver telescope, an *adaptive transmitter* is required, which mitigates the turbulence induced beam spreading by precompensation of the transmitted wave. An adaptive transmitter can be realised in different ways. One approach is to use feedback from the receiver end to optimise the precompensation of the transmitted beam. In this case, data on the sensed wave front distortions have to be transmitted from the receiver terminal to the transmitter terminal. The feedback signal's inherent latency due to the propagation time represents a fundamental constraint of this approach, and limits its practicability to shorter link distances. The second way for realisation of an adaptive transmitter uses a beacon from the receiver terminal to obtain information about the wave front distortions during propagation between the terminals. Control of the adaptive optics is performed by maximisation of the beacon's beam quality, and the transmitted beam is sent in the opposite direction through the same adaptive optics elements. Because of the reciprocity of the turbulent atmosphere (at a fixed time t) [145], the wave front correction for the received beam is simultaneously the optimal precompensation for the outgoing beam [146]. However, for this scheme to work properly, the round-trip (receiver-transmitter-receiver) propagation time must be short compared to the timescale on which atmospheric fluctuations take place (typically $\sim 1\,\mathrm{ms}$, cf. §3.4.2). This condition is satisfied by near-ground paths up to $\sim 150\,\mathrm{km}$ length and space-ground-space paths, but is not satisfied by ground-space-ground paths.

By nature of quantum optical communications, the power of the transmitted signal beam is extremely low, which makes direct sensing of wave front distortions on the

quantum signal virtually impossible. Therefore, an additional beacon propagating from the transmitter terminal to the receiver terminal has to be employed for the detection of wave front distortions on the signal beam.

4.4.2 Active tracking on the inter-island link

The measurement of long-term beam wander (§4.2) gave evidence, that a stable operation of the inter-island link was impossible without employing active beam steering techniques. Changing refraction effects due to diurnal variations of the average index-of-refraction vertical gradient would have caused large beam pointing errors, degrading the link transmittance substantially, eventually beyond the limit for quantum key distribution. Therefore, a bi-directional tip-tilt correction was implemented to compensate slowly varying atmospheric influences. The realised active tracking system shall be described in the following. More details can be found in [147].

The realised tracking system (Figure 4.7) worked with two beacon lasers, one shining from the transmitter telescope towards the OGS on Tenerife, and a second one in the opposite direction. Compact diode-pumped solid-state laser modules emitting at 532 nm were attached to the transmitter telescope breadboard and to the side of the OGS telecope tube, bore sighted to the respective main telescopes. The laser modules' output beams measured roughly 1 mm in diameter and were defocused to have about 0.2 mrad divergence to ensure constant illumination of the remote wave front sensors.

On the transmitter side (Alice), the beacon laser from Tenerife was collected by a 150 mm achromatic lens (f=400 mm) and focused onto a CCD camera with 4.5 μm pixel size (see §5.1.4 for details). By calculating the centre of mass of the intensity distribution, the spatial resolution was enhanced to $\sim$ 1.5 μm, which is equivalent to a beam shift at the receiver by 0.5 m and sufficient for this application. The stepping motors acting on the pointing direction of the transmitter telescope were controlled by

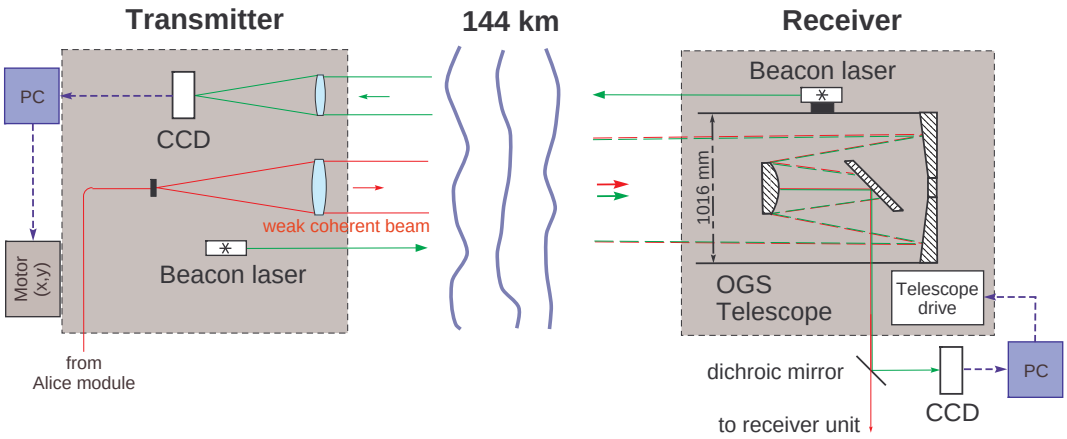

Figure 4.7: Overview of the tracking system for the inter-island link experiment.

a closed-loop, proportional control algorithm implemented in LabView. One cycle of image readout, algorithm execution, and motor movement required about 1 second on average. The reference point on the CCD camera was optimised on the basis of the measured end-to-end transmission values.

Figure 4.8 shows the difference in transmission losses with and without active tracking of the transmitter. The top viewgraph displays the attenuation of the optical link (grey: measured data; red: moving average over 50 data points). When the tracking loop was disabled (orange vertical line), the link transmission dropped within minutes from $\sim$ 30 dB to $\sim$ 45 dB. At the same time, the position of the beacon on the CCD (blue curves) moved away from the reference point by 3 pixels, corresponding to a beam wander of $\sim$4.5 m, or roughly one beam diameter, at the receiver. A comparison between horizontal and vertical perturbations shows that the observed effect is much

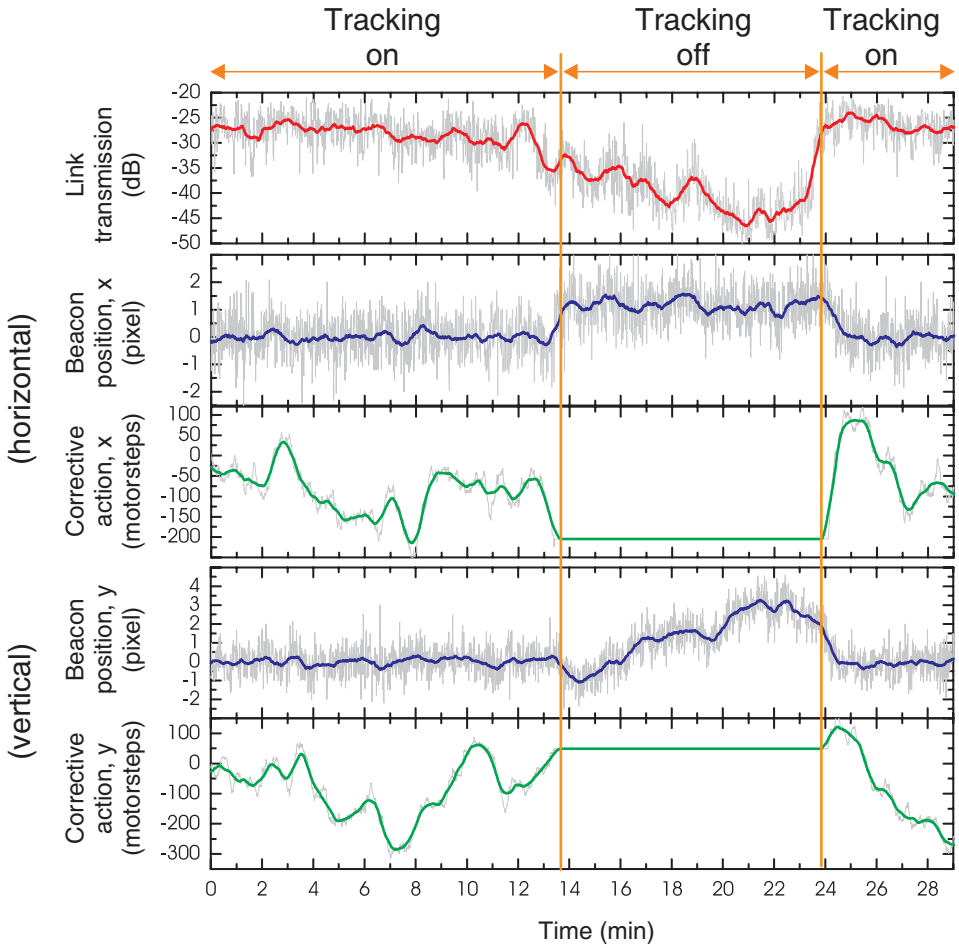

Figure 4.8: Comparison of the optical link efficiency with and without active tracking. Changes on the seconds to minutes time scale in the atmospheric temperature gradients cause the optical beam to wander. This movement is recorded with the beacon laser on the CCD.

more pronounced in the vertical direction, which is plausible because the atmospheric structure largely consists of horizontally homogeneous layers.

For the active pointing of the receiver telescope (Bob), the slow part of the tracking facilities of the OGS were used. The light of the beacon laser from La Palma was directed through the OGS telescope onto the Coudé camera, using a dichroic mirror to separate the beacon light from the weak coherent beam. Owing to the high sensitivity of the Coudé camera and long exposure times, the beacon laser on La Palma could be attenuated to about 0.1 mW output power to prevent saturation of the camera. A long integration time of 2 s was chosen to reduce errors of the spot position due to fast turbulences. The tracking/guiding software `OGSTracking` was provided by ESA and directly interfaced with the telescope drive controller. The software made use of a number of external programs to acquire images from the Coudé camera, process the image data, find the beacon image, and to display the calculated pointing corrections. Figure 4.9 shows a screenshot of the output window with the image acquired by the Coudé camera, deviation of the beacon from its target position, and the calculated corrections, expressed in the telescopes coordinate system *hour axis* (HA) and *declination angle* (Dec). One loop of the image grabbing, calculating and executing the corrections of the telescope position took ∼10 s. This speed turned out to be sufficient to ensure a stable signal beam position well within the active area of the single photon detectors.

4.4.3 Potential of higher-order adaptive optics

The active tracking system described above was designed to compensate slow beam wander and beam drifts that would have led to a loss of the optical link. Of course, the transmitted quantum signal could be used much more efficiently with a narrower beam, using fast beam-steering and higher-order wave front precompensation techniques in an adaptive transmitter configuration. Possible realisations, and the potential of such methods shall be briefly investigated in this section.

The conventional adaptive optics approach for atmospheric compensation is based on wave front sensing and reconstruction. When applied to free-space laser communications, a part of the received beam (or, alternatively, a beacon beam) is directed to a wave front sensor, for instance a Shack-Hartmann sensor, or a Shearing interferometer. The wave front is reconstructed from the measured data and used to calculate the control signals for the actuators of the wave front corrector, usually a deformable mirror of some kind. This scheme has been successfully implemented in a number of mostly astronomical systems [148, 149] before its potential for horizontal path optical communications was investigated. In [150], Levine et al. calculated the power spectral density for various Zernike polynomial modes[2] [151] to determine the degree of the expected corrections that can be accomplished by means of modal correction. There is, however,

[2]Virtually any realistic wave front $\Phi(r, \theta)$ can be decomposed into a 2-dimensional Fourier series of Zernike polynomials. Low order Zernike modes correspond to piston, tilt, focus, astigmatism, coma errors, and so on.

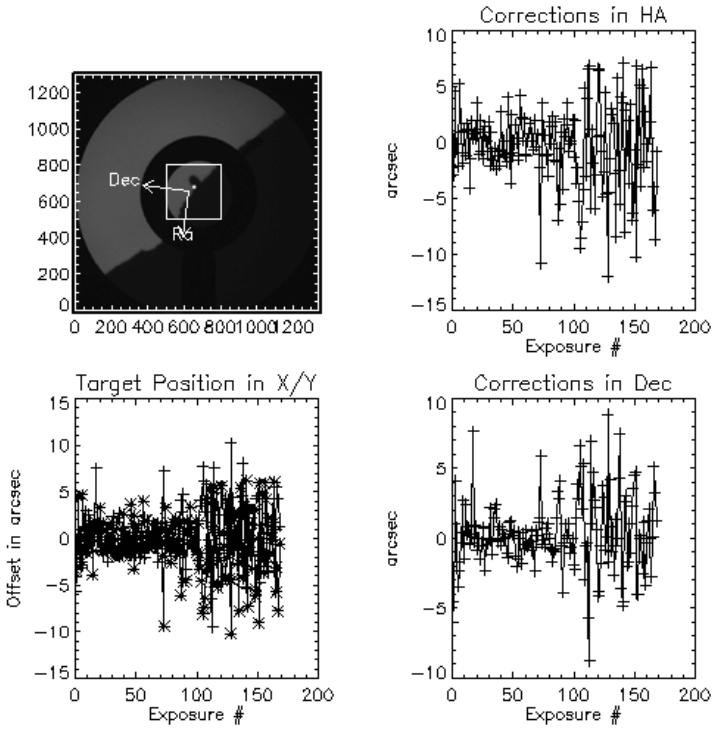

Figure 4.9: Example of the OGS tracking software output. Top left: Image acquired by the Coudé camera during twilight. Next to the bright spot of the beacon laser the silhouette of the NOT dome is visible; the dark ring around the centre is the iris in the plane of the Coudé focus. Bottum left: deviation of the beacon from its target position. Right top and bottum: calculated corrections of telescope coordinates.

a fundamental difference to astronomical systems, where the turbulence-induced wave front perturbations occur near the receiver telescope, and where intensity fluctuations are relatively weak: In laser communication applications, the beam-affecting turbulence is distributed along the entire propagation path [150, 152]. In this case, both phase and amplitude of the propagating wave get corrupted, requiring, strictly speaking, a compensation of phase as well as amplitude. Although phase-only correction of the wave front is theoretically sufficient only for a propagation distance in the near field, it has nevertheless been demonstrated to provide significant improvement in the transmitted beam quality for large distance optical communications [150]. Applied to the central figure of merit in laser communications, it was found that the bit-error rate can be improved by more than an order of magnitude even with lower-order compensation up to 40 Zernike modes [153, 154].

More recently, adaptive optical systems with more than one phase correction device have been proposed, that can compensate for both amplitude and phase abberations that result from propagation through a turbulent medium [155–157]. This class of multiconjugate adaptive optical (MCAO) systems is distinct from an earlier approach to MCAO

systems, which aimed at increasing the compensated field of view beyond the isoplanatic angle, using multiple wave-front sensing beacons and a tomographic approach based on the geometrical optics approximation.

Yet, with scintillation conditions becoming stronger, experiments showed a significant degradation in the correction achievable by conventional phase-conjugate adaptive optics systems [152]. The primary identified reason for this is that strong intensity fluctuations make wave front reconstruction in practice very difficult in zones with almost no intensity. In mathematical terms, strong scintillation leads to the occurrence of a large number of branch points in the phase of the optical field, that cause the phase reconstruction algorithm to produce results that do not adequately match the actual phase [158].

In strong scintillation conditions, it is desireable to avoid wave front measurements completely. As an alternative approach, it can be attempted to control the wave front corrector by "blind" (*model-free*) optimisation of a system performance figure of merit, called *metric*, or *cost function*. The general idea is to minimise or maximise the cost function by making small adjustments to the phase correction devices, measuring the effect on the cost function to calculate a derivative, and then following the gradient that will minimise or maximise the cost function. A common choice for the metric is the *Strehl ratio*, which denotes the ratio of the peak intensity in the far field spot to the peak intensity of the spot formed by an equivalent, diffraction limited, aberration free system. One difficulty with the model-free optimisation technique is its iterative nature to find the optimum control signal, which imposes speed requirements both on the computational speed of the control algorithm and on the control bandwidth of the phase actuator. On the other hand, a useful performance metric, like the received power level, or the coupling efficiency into an optical fibre, may readily be available in typical laser communications systems. With a microelectromechanical deformable mirror (MEMS), and a highly integrated microcontroller system implementing a stochastic parallel gradient descent algorithm, speeds up to 11.000 iterations/s have been achieved [159, 160], which seems sufficient for real-time compensation of atmospheric turbulence.

The subject of maximising the useful transmitted power in a two-telescope system was more generally addressed in a paper by Barchers and Fried [161]. They found that if one uses an adaptive optical system in each telescope, and simply uses the received beam as the wave front sensing beacon, a natural convergent iteration occurs, leading to maximum transmission of power through a turbulent medium. Any combination of means of controlling adaptive optical systems in each telescope will solve the optimal power transmission problem. Simulations indicate that for a uniform distribution of the strength of turbulence, 95% transmission of laser power is attained when both telescopes can achieve full-wave compensation, provided that the aperture diameter D of the two telescopes is greater than twice the Fresnel length $\sqrt{\lambda L}$.

In conclusion of this short overview, the use of higher-order adaptive optics could help achieve higher link efficiency in the future, even with smaller optics. This is, of course, highly attractive for any free space quantum key distribution system, and in particular for satellite-based QKD.

5 Experimental setup

The experimental setup of a QKD experiment is naturally divided into three building blocks, namely the *transmitter (Alice)*, the quantum channel, and the *receiver (Bob)*. While the linking quantum channel has been characterised in the preceding chapter, this chapter describes the individual parts of the experimental setup in detail. Alice's signal states were generated as laser diode pulses, which were strongly attenuated to an average photon number below one photon per pulse. The transmitter setup utilised a separate diode for each linear polarisation, taking advantage of the high intrinsic polarisation of the diodes. The beams were overlapped and routed to the transmitter telescope via a single-mode fibre. At the receiver end, a large diameter receiving telescope was employed to collect as many photons of the turbulence-spread beam as possible. The collected light was directed to the receiver module, where the signal pulses were detected and their polarisation was analysed. This measurement was performed with the help of polarisation optics and a set of four Silicon avalanche photodiodes for single photon detection. The exact arrival time of each pulse is recorded to allow for properly assigning the detected events to the sent signals.

5.1 The transmitter

The transmitter setup consists of the *transmitter module*, which generates the signal pulses, and the *transmitter telescope* to collimate and direct the light over the free-space optical channel to the receiver. Two different versions of the transmitter module were used during the experiments: The initial version had 4 laser diodes, and decoy pulses were created by switching on two laser diodes simultaneously. The second generation of the transmitter module was extended to 8 laser diodes to provide separate sets of laser diodes for signal pulses and brighter decoy pulses. The two versions of the transmitter module are presented and characterised separately in §5.1.2; the transmitter telescope is described in §5.1.4.

5.1.1 Location and infrastructure

The transmitter for the Canary Island experiment was located on the grounds belonging to the *Nordic Optical Telescope* (NOT) at the *Observatorio del Roque de los Muchachos* (ORM) on the island of La Palma. The place was chosen because of the direct line of sight to Tenerife, especially to the telescope of the *Optical Ground Station*. This direct

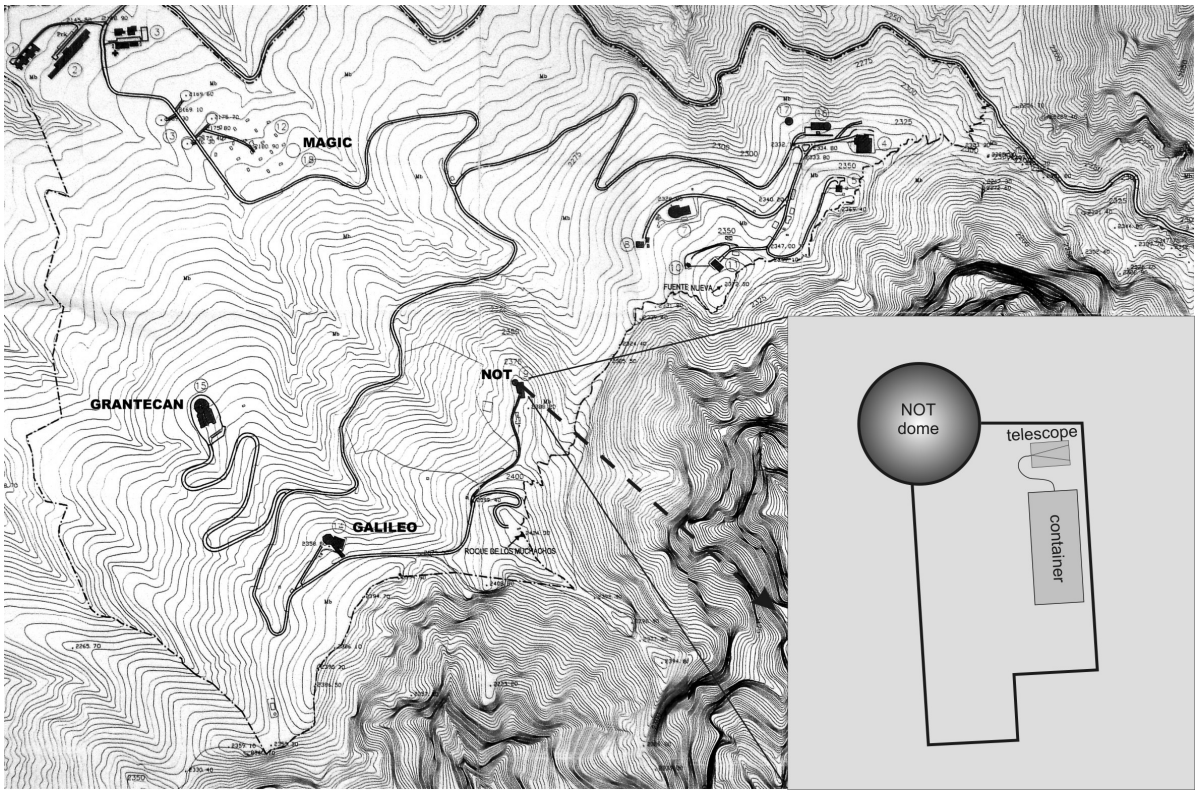

Figure 5.1: Map of the Roque de los Muchachos area on La Palma; the insert shows the location of the portacabin and the transmitter telescope on the NOT site. The dashed arrow indicates the direction to OGS.

line of sight is available only at a few locations on the ORM, and the most suitable place was chosen, which is the north-eastern corner of the driveway to the NOT telescope (see Figure 5.1).

Power and internet access was obtained from the NOT infrastructure. An open ended container ("portacabin") was installed to provide shelter from wind, rain, and dust. Sensitive components (i.e., transmitter module, lasers, electronic equipment) were set up in the container. The transmitter telescope remained outside linked to the source by fibre optics, because placing the telescope inside the container would have greatly deteriorated the beam quality at the warm-to-cold interface.

5.1.2 Alice module

The purpose of the transmitter module (in the following often called "Alice module") is to generate faint pulses of light of distinct linear polarisation. This is achieved by driving a laser diode with a short electrical pulse, and heavily attenuating the optical output. To keep the complexity of the apparatus as low as possible, a separate laser diode for each of the desired polarisation states (4 in the case of BB84) was used, and

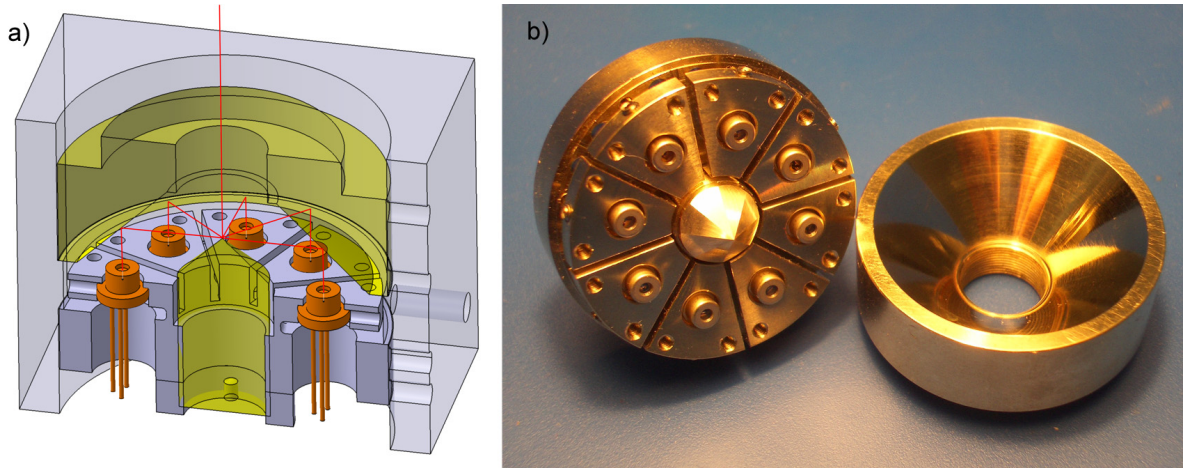

Figure 5.2: **(a)** Cut through the centre of the Alice module revealing the two conical mirrors that reflect the light from the laser diodes (orange) to the top of the housing where the single mode fibre coupler is attached. Outer dimensions are roughly 5x5x5 cm^3. **(b)** Photograph of the laser diode mounting (with convex mirror in the centre), and the concave mirror with thread for the coupling lens.

their outputs were combined into a single spatial mode defined by a single mode optical fibre. Due to the fabrication process, most laser diodes emit light of a high intrinsic linear polarisation (typically 1:1000), which means that additional polarising optics is not necessary.

Figure 5.2 shows a CAD drawing and a photograph of the mechanical structure forming the transmitter module. The mounting of the laser diodes in the chassis allows individual tip-tilt adjustment of each diode to optimise coupling efficiencies independently. Each laser diode is rotated in the mounting head by 45° with respect to the neighbouring ones. In this way, the arrangement can produce light of one of the polarisations $\{0°, 45°, 90°, 135°\}$, in the following rather denoted by the polarisation states $\{|H\rangle, |+\rangle, |V\rangle, |-\rangle\}$. The light of each diode is reflected by a concave-convex pair of conical mirrors and fed jointly into a single mode fibre (cut-off wavelength 830 nm), which is connected directly to the module. A small high-aperture lens (focal length f=11 mm, NA=0.25) is placed in front of the fibre tip. Apart from the obvious need for routing the light from the Alice module to the transmitter telescope, the single mode fibre serves an additional purpose: it is essential to ensure that the spatial intensity profile of all polarisations is identical; otherwise the eavesdropper could infer the polarisation of a photon by measuring its **k** vector. The use of a single mode fibre by definition guarantees the indistinguishability of the output beams.

The opto-mechanical design of the Alice module results in a coupling efficiency of roughly 10^{-7} from the laser diode into the single mode fibre, thus providing enough attenuation for optical output pulses on the single photon level — additional neutral density filters are not needed.

In a straightforward extension of the mechanical design from four to eight laser diodes, every two facing diodes produce identical polarisations. This configuration (see Figure 5.2b) was used to implement a second "decoy source" in addition to the "signal source" as described in §2.6.2.

Electronics

The laser diode driving electronics is integrated on a small printed circuit board that is attached directly to the Alice module in order to keep signal lines to the diodes as short as possible. This dedicated circuitry is controlled (via additional interface electronics, Figure 5.3) by a personal computer, which provides the bit pattern (i.e., random numbers with interspersed synchronisation sequences) to be sent out by the transmitter. The interface electronics buffers the parallel data provided by a digital I/O card (*NuDAQ PCI-7200*) in a *first in, first out* memory (FIFO), and translates them into serial data, that is sent synchronously to the pulse electronics. An ovenized oscillator (Trimble *Tunderbolt*), that is disciplined by the time signal of the Global Positioning System (GPS), provides the actual 10 MHz clock pulse for the laser driver electronics.

It is of paramount importance to use a "true" random number generator (i.e., a piece of dedicated hardware) for quantum cryptography, and not software-generated pseudo-random numbers. The latter are created from mathematical functions using an initial starting number called seed, and give, for every seed, a seemingly chaotic, but purely deterministic series of numbers. Due to their underlying structure, such pseudo-random sequences have reduced entropy content, which would undermine the security of the quantum key. Ideally, random numbers are therefore generated via a well-understood physical process, the quantum nature of which creates the randomness [162–164]. In our experiment, a random number generator based on thermal noise was used [165]. Because the random number generator provided random numbers at a lower rate than required by our QKD system, random numbers were created before the experiment and stored on the PC's harddrive.

In the course of the experiment, it emerged that the first generation of circuitry used in the June trial did substantially limit the performance of the key generation system and was therefore replaced by an improved design that was employed in the September trial. Due to their impact on the experimental results, these electronic drivers are briefly described and characterised in the following.

1st generation pulse electronics (4 channels)

The design of the first generation pulse driver (Figure 5.3) is based on ECL (emitter coupled logic) technology to produce a one-shot logic signal of approximately 1 ns duration on every rising edge of the 10 MHz clock pulse. This pulse form is then amplified by an RF transistor and AC coupled to the pre-biased laser diode, resulting in an voltage increase of $\approx 0.5\,\mathrm{V}$ at the diode. For the short duration of the pulse, the voltage at the

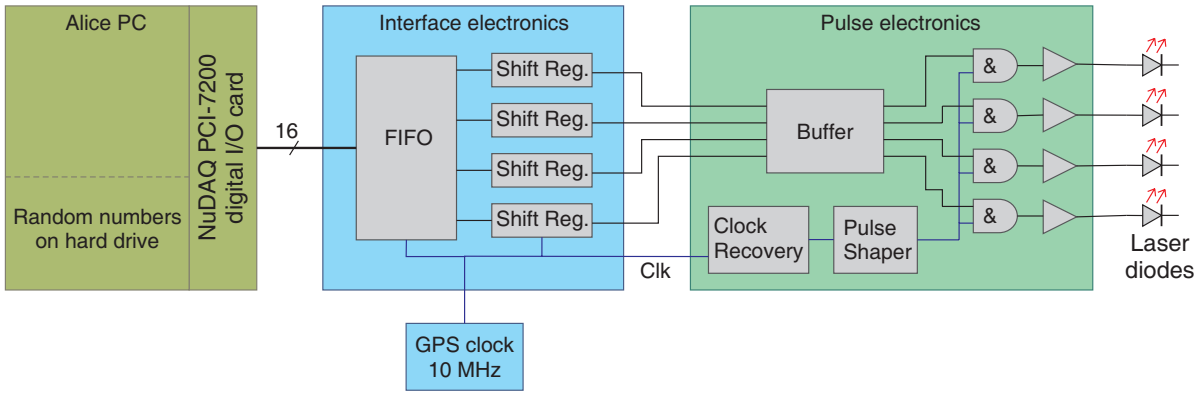

Figure 5.3: Schematic of the 1st generation transmitter electronics with 4 channels. The random bit sequence provided by the Alice PC is buffered and interfaced to the pulse electronics, that drives the laser diodes synchronously with the external clock.

laser diode is raised above the lasing threshold. To control the intensity of the optical output pulse, the bias voltage for each of the 4 channels can be adjusted with potentiometers. The duration of the electrical pulse can be tuned using a variable capacitor.

One important condition for secure QKD is the correct timing and pulse shape of the signal pulses. Figure 5.4a shows the electrical output pulses of the 4-channel pulse electronics, measured with a 20-GHz oscilloscope. The pronounced voltage ripple after the main pulse is essentially a measurement artefact due to the connection of the probe head to the circuit. The duration of the electrical pulses are very similar and around 0.9 ns FWHM. However, it is apparent that the four channels have a relative delay of up to 0.8 ns, which is a result of different signal propagation times on the printed circuit board.

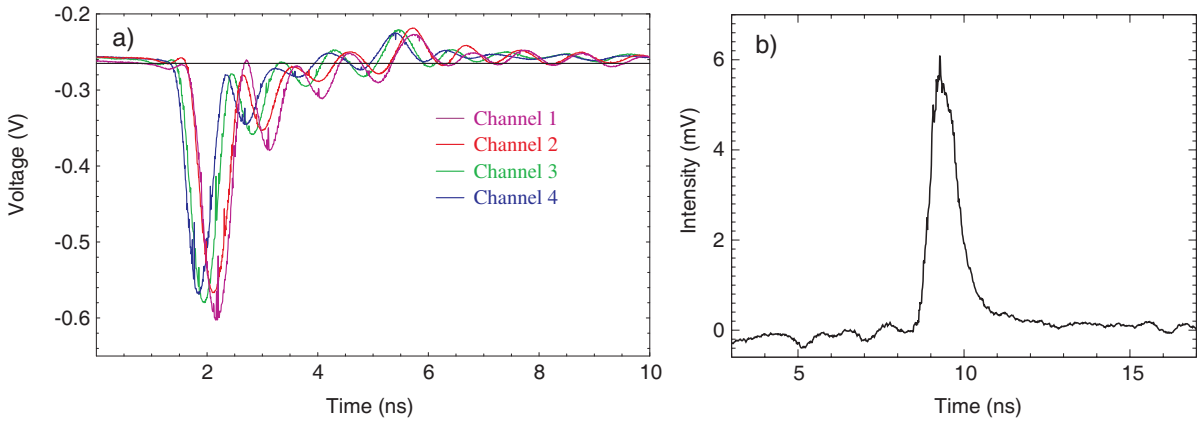

Figure 5.4: **(a)** Electrical output of the 1st generation laser diode driver. The individual channels are slightly delayed relative to each other. **(b)** Resulting typical optical pulse emitted by the laser diode.

Figure 5.4b shows the resulting time-resolved optical pulse from a 10 mW laser diode (Laser Components LCQ85010S5, slope efficiency 0.73 mW/mA), recorded with a broadband photodiode (rise time 70 ps). The full width at half maximum duration is 0.8 ns. Since the amplitude of the electrical pulse is fixed, the integrated intensity of the optical pulse can either be tuned via the pulse length, or by raising the bias voltage, which, however, results in an undesired increase of the background level.

2nd generation pulse electronics (8 channels)

The second generation pulse electronics (Figure 5.5) offers the possibility to drive 8 laser diodes to implement the decoy state protocol with two different intensities. For this purpose, the PC generates an additional *decoy flag* to switch between the two sets of laser diodes. Bias and modulation current of each laser diode can be controlled electronically by the Alice computer to match the desired mean photon number. The amplifying transistor was replaced by a commercial laser diode driver IC, which has a faster rise time and can provide a higher modulation current than the transistor-based design. Additionally, digital delay circuits have been included for channel deskewing down to a resolution of 17 ps. The laser diodes may also be run in continuous-wave mode to provide a brightness increase of around 100 to aid in the fine alignment procedure.

Figure 5.6 shows typical optical output pulses of different peak intensities and durations with a full width at half maximum of 0.27 ns, 0.54 ns, and 0.90 ns. Given a fixed

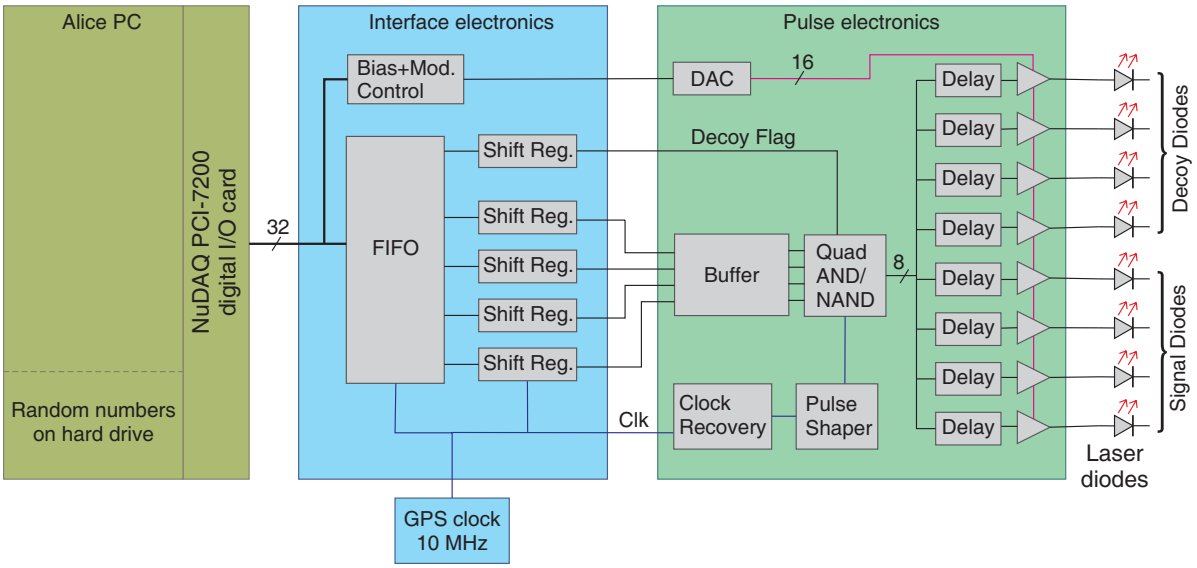

Figure 5.5: Schematic of the improved transmitter electronics with 8 channels. An additional decoy flag in the random bit stream determines which laser diode set is addressed. In this 2nd generation pulse electronics, bias and modulation current of the laser diodes are controlled remotely, and all channels are deskewed individually.

pulse attenuation, which is defined by the opto-mechanical design of the Alice module, independent tuning of the pulse length and the modulation current allows to vary the pulse intensity over a wide range of mean photon numbers. The double peak structure of the longer pulses hints at imperfect impedance matching of the driving electronics with the laser diode. Relative delays between the individual channels were matched to better than 25 ps using the digital delay stages (for clarity not shown in Figure 5.6).

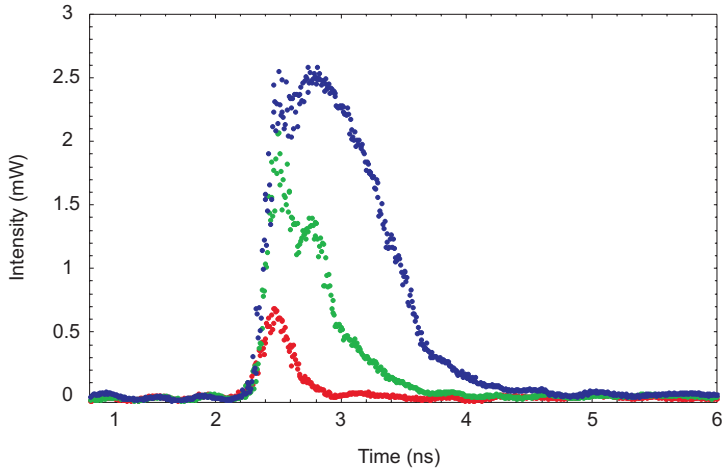

Figure 5.6: Optical pulses generated with the 2nd generation laser diode driver at different modulation currents.

5.1.3 Characterisation of the transmitter

A fundamental prerequisite for the security of the QKD system is the assumption that the information is only encoded in the polarisation degree of freedom of the signal states. Other properties, like wavelength, spatial emission profile, and timing, must be independent of the bit value and basis choice.

Wavelength

Various ways of ensuring that the laser wavelengths are indistinguishable are available. In the simplest approach, this can be achieved though the variation of laser current and operating temperature. The approach in this experiment was to select laser diodes that operate at the same wavelength and the same temperature, and to mount all laser chips on the same heat sink. Figure 5.7 compares the individual spectra of the 4 laser diodes producing the signal states in the 1st generation Alice module. The spectra are centred around 850.5 nm with an average spectral width of $\sim$ 1.5 nm. To improve indistinguishability, the lasers could be passed through a narrow-band filter ($<$ 1 nm) at the transmitter. However, laser diode emission wavelengths typically drift by about 0.12 nm/K, thus a temperature control is required to ensure the matching of the filter

and the laser wavelengths. Since a temperature control system was not yet implemented at the time, narrow-band filtering had to be abandoned.

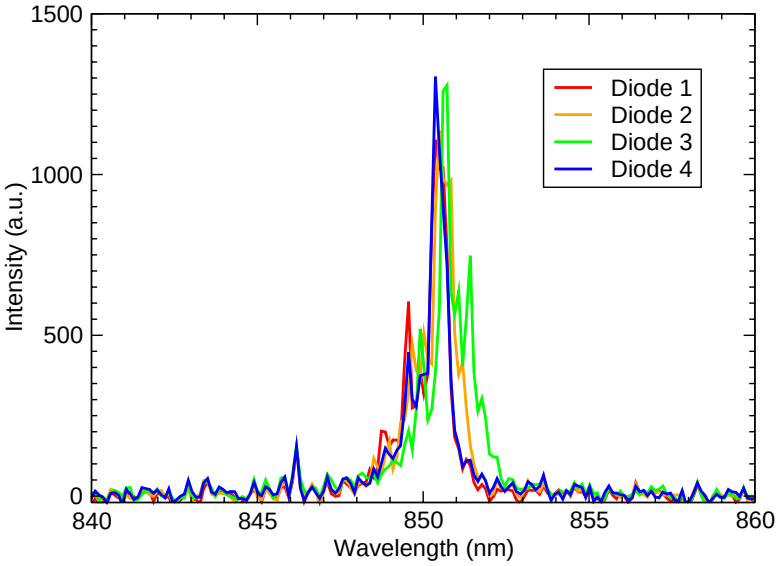

Figure 5.7: Spectra of the four transmitter laser diodes, operated in pulsed mode.

Polarisation

Figure 5.8 shows the integration of the Alice module into the transmitter setup. The mean photon number of the signal and the decoy states was adjusted and monitored with a calibrated single photon detector at one of the output ports of a 50:50 fibre beam splitter before coupling the transmitter output to the telescope. Bright alignment lasers of visible and infrared wavelengths were coupled optionally into the second input port of the beam splitter to provide a stronger signal for initial alignment of the optical link. The single-mode fibre to the transmitter telescope was firmly taped to solid material to keep polarisation fluctuations small. To measure the birefringence along the fibre, single-photon polarisation analysis was performed inside the transmitter telescope with a rotatable polarising filter and a single-photon detector. Compensation was done with a fibre polarisation controller. For the transmission of signal pulses to the receiver, the polarisation analysis setup was removed from the transmitter telescope.

Figure 5.9 shows a full polarisation analysis of the transmitter diodes after carefully compensating the fibre birefringence. The resulting visibilities of the individual laser diodes are summarised in Table 5.1. Since the polarising filter had an extinction ratio of better than 1:1000, imperfect visibility was mainly due to finite intrinsic polarisation of the laser diodes and residual errors in the fibre compensation. The orientation of the laser diodes was accurate to about $\pm 2°$. Overall, the transmitter's contribution to the quantum bit error rate is expected to be 0.3% to 0.6%.

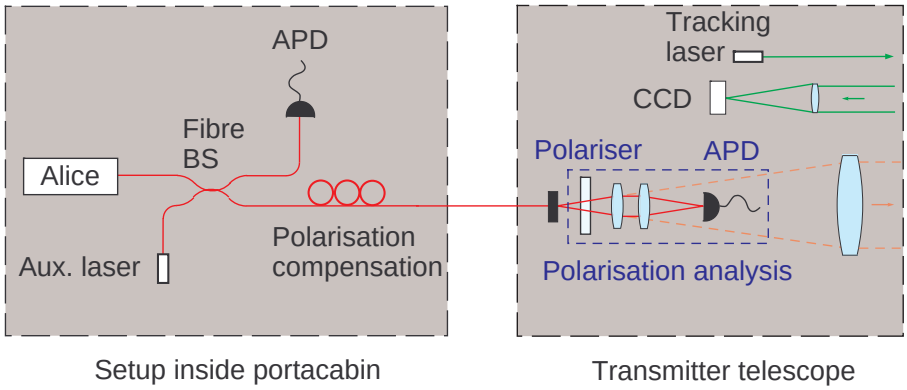

Figure 5.8: Transmitter setup in the configuration for polarisation compensation. For quantum key exchange, the polarisation analysis setup was removed.

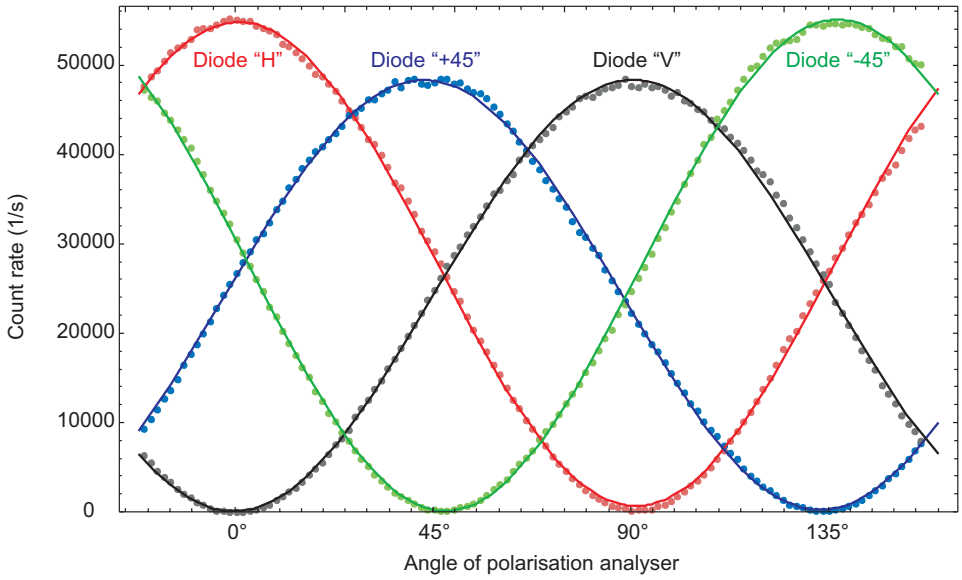

Figure 5.9: Polarisation analysis of the fibre-coupled transmitter module with 4 laser diodes.

5.1.4 Transmitter telescope

The Alice module was coupled via single-mode fibre to the transmitter telescope (Figure 5.10), which was mounted on a heavy workbench outside the portacabin, where Alice's optics and control electronics were placed. The light emitted from the bare fibre was collimated in the telescope by a 150 mm diameter f/2.7 achromatic lens. To enable focussing without touching the telescope setup, and to enhance repeatability, the fibre coupler's translation in z-direction was motorised and controlled from the user interface of the tracking software. In particular, this was necessary to compensate for residual

Diode	Visibility V_i	Angle θ_i
H	99.6%	0.0°
V	97.6%	91.5°
+45	99.5%	47.5°
−45	98.9%	-43.0°

Table 5.1: Characterisation of the transmitter module: visibilities (dark count corrected) and polarisation angles for the four laser diodes of the Alice module. The values are inferred from fitted sine functions as depicted in Figure 5.9.

chromatic abberations of the lens when switching between different wavelengths (e.g., of the different alignment lasers). In order to allow for fine adjustments of the pointing direction of the telescope, the breadboard with the optical assembly was mounted onto a stable tip-tilt stage equipped with stepper motors (PI *Stepper-Mike*) for both horizontal and vertical axis. The use of large high precision ball bearings ensured a sufficient stability of the setup. The sensitivity of the setup to local vibrations was tested by a person jumping next to the supporting workbench, which produced no noticeable effect on the beam wander at the receiver station. The influence of wind, affecting the setup more directly, however, was difficult to separate from atmospheric turbulence effects, and could not be evaluated.

The bidirectional tracking technique required two beacon beams, one of them shin-

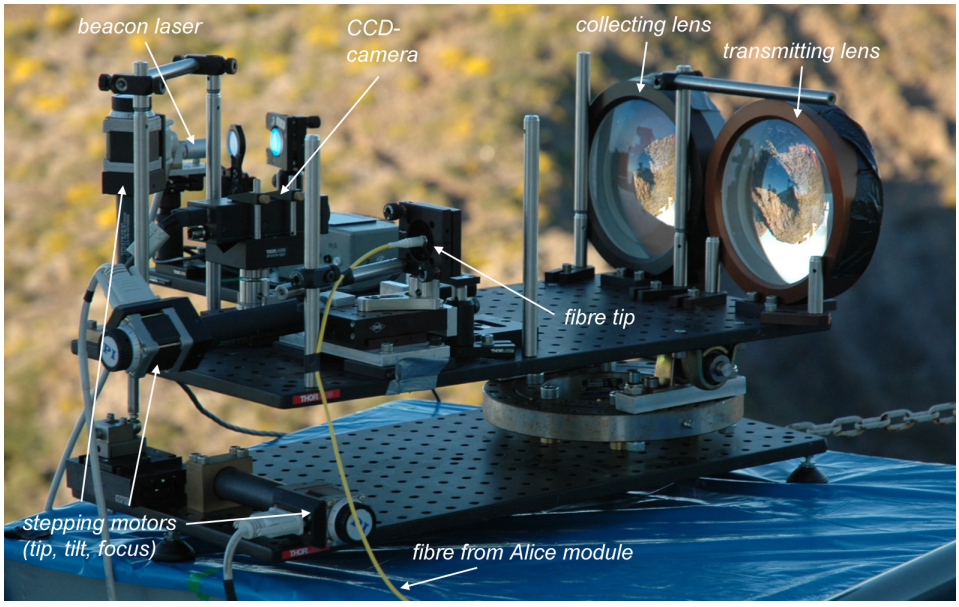

Figure 5.10: Transmitter telescope. The large lens on the right collimates the outgoing weak coherent beam, the second front lens collects the incoming light from the laser beacon. A heavy ball bearing and stepper motors allow for pointing adjustments.

ing from the quantum optical transmitter to the receiver, and the other one vice versa. Hence, a 532 nm laser module with 35 mW output power was fitted to the transmitter telescope setup. Since the 532 nm radiation was generated by internally frequency doubling, the laser had considerable output in the infrared, which was filtered out by reflecting the output beam a few times off a pair of dichroic mirrors before sending it to Tenerife. Neutral density filters were used to adjust the brightness of the beacon beam to the required level.

Likewise, an additional lens to collect and focus the light from the other beacon laser (shining from OGS to the transmitter) was required. It was of the same kind as the transmitter telescope's front lens and mounted next to it on the same breadboard. In this way, both transmitter lens and collecting lens always moved together. To record the apparent direction to the quantum optical receiver, a CCD camera was placed in the focal plane of the collecting lens, feeding its images via firewire to a personal computer for data processing. The tracking technique is explained in detail in §4.4.2.

5.2 The receiver

The light from the quantum optical transmitter was sent over 144 km optical path at a mean altitude of approx. 2400 m to the Optical Ground Station (OGS) on Tenerife, which is part of the *Observatorio del Teide* on the mountain ridge *Izaña* (Figure 5.11). An overview of the optical setup at the receiver station is given in the next section; the design of the quantum optical receiver is covered in §5.2.2.

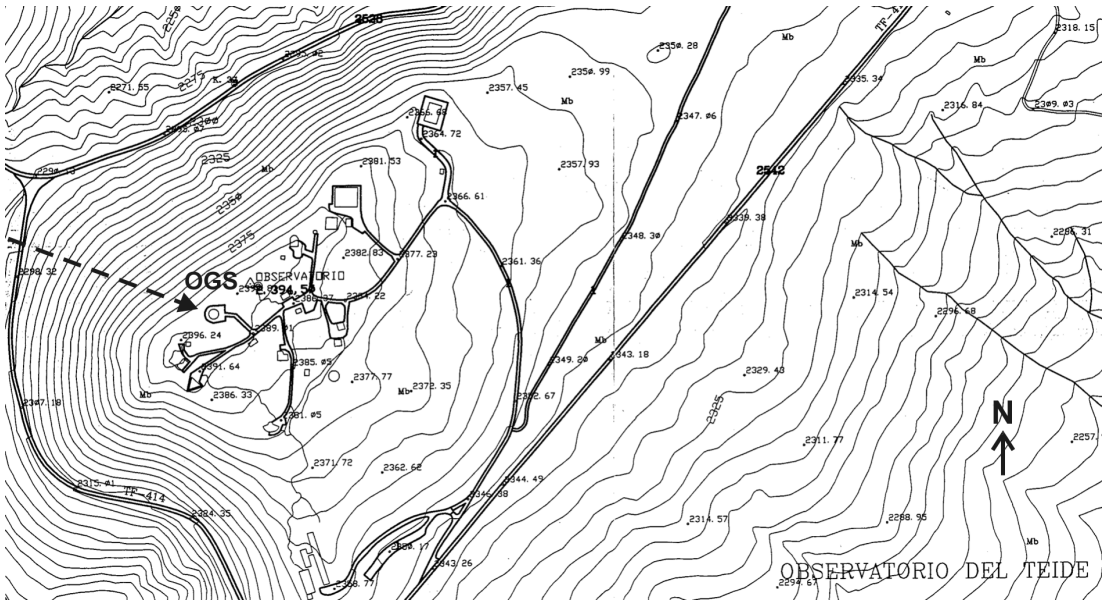

Figure 5.11: Map of the *Observatorio del Teide*. The dashed arrow indicates the direction from NOT on La Palma.

5.2.1 The Optical Ground Station

The ESA facility of the OGS consists of an observatory building with a dome and the associated infrastructure, and a reflective telescope including a control system. The telescope used in the OGS is a *Zeiss* 1-m Ritchey-Chrétien/Coudé telescope supported by an English mount. The telescope can either be used in Cassegrain focus (intended mainly for observation of space debris) or in Coudé focus configuration designed for optical communication experiments.

Figure 5.12 shows the optical arrangements of the Cassegrain and the Coudé focus of the telescope. The Coudé focus is located in a dedicated laboratory, one floor below the telescope floor. To avoid turbulence effects due to the temperature differences between the two floors, the optical path from the telescope floor to the Coudé laboratory leads via an evacuated feed-through. The Coudé laboratory provides a stabilised and well suited environment for optical experiments and accommodates a permanent setup for optical communication experiments with satellites like ARTEMIS and SMART-1.

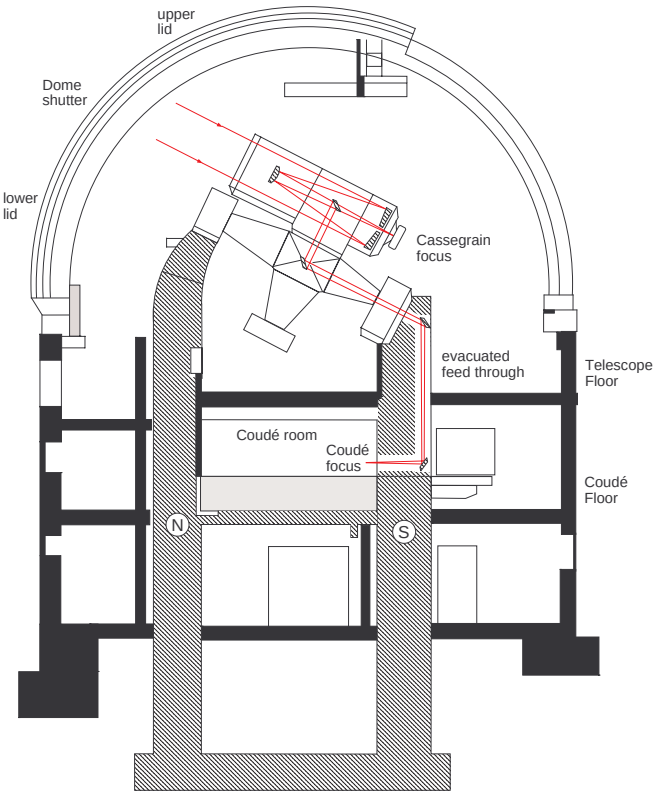

Figure 5.12: Schematic cut through the Optical Ground Station. In Coudé configuration, the light collected by the primary mirror is guided through the mount and the south pillar to the Coudé floor.

There are basically two options for placing a quantum optical receiver module: at the Cassegrain focus or at the Coudé focus. A lightweight receiver could be installed at the Cassegrain focus, attached directly to the telescope, where optical transmission losses are lowest. This option has major disadvantages, however: Access to the receiver for maintenance, adjustment and troubleshooting would be delicate since the telescope's optical axis runs about 5 m above the floor when the telescope is pointed to the horizon. Secondly, this option rules out the simultaneous use of the Coudé camera (CC) for tracking and other purposes, like monitoring angle-of-arrival fluctuations. Lastly, a major use of the telescope at the time was the observation of space debris which involves a liquid nitrogen cooled, large format CCD camera mounted at the Cassegrain focus. The removal and careful reattachment of this

heavy instrument requires the help of a crane and an experienced operator. The option to use the Cassegrain focus was therefore discarded.

The Coudé focus on the other hand is easily accessible in a well controlled, clean, and temperature stabilised environment. Moreover, the design of the Coudé beam path is such that changes to the polarisation are minimised [166]. The focus point is 30 cm above a high quality granite optical bench, that is available for temporary experimental setups. Even though the installed instrumentation includes actuators and detectors for a full Pointing, Acquisition, and Tracking (PAT) system, for practical reasons it was only possible to take advantage of the existing Coudé camera for tracking purposes. The Coudé camera is a Peltier-cooled, large-format CCD camera (1242 × 1152 pixels, pixel size 22.5 μm × 22.5 μm) located behind a collimator to observe the full Coudé field-of-view of 8 arcmin.

Background photons from stray light (especially during full moon) limit the performance of the QKD system. Therefore, a variable iris diaphragm was inserted in the Coudé focus plane to allow for adjustment of the telescope's effective field of view (Figure 5.13). A dichroic mirror, placed shortly after the focus point, was used to separate the infrared photons originating from Alice (*signal channel*, wavelength 850 nm) from the green tracking beam (wavelength 532 nm). The dichroic mirror had a reflectivity of >99.9% at 850 nm and <1% at 532 nm, providing a high isolation between the tracking light and the quantum signal. In the infrared (reflected) arm, the linear polarisation from La Palma was rotated by a halfwave plate in front of the single photon detection unit (Bob module) to match the analysing basis to the transmitted one. This was necessary because the internal reflecting optics in the optical path from the telescope to the Coudé floor give rise to a variable polarisation rotation, depending on the pointing direction of the telescope. Finally, an achromatic lens (f=400 mm) collimated the beam before it entered the single photon polarisation analyser setup.

5.2.2 Single photon polarisation analysis

The task of the single photon polarisation analyser setup (in the following called *Bob module*) is to analyse the polarisation of the incoming infrared photons. In principle, the polarisation measurement is performed by directing the incident photons — depending mainly on their polarisation state — to one of four single photon detectors. The result of the polarisation analysis consists in the information which of the four detectors produced a "click".

For secure key generation, the polarisation measurement of the incoming photons has to be performed with a random choice of the detection basis, either H/V or ±45° in the case of BB84-type protocols. One key idea to simplify the optical setup is to use a nonpolarising beam splitter to decide passively in which basis a photon will be measured [167, 168]. This avoids the need for a combination of a random number generator and a fast active polarisation control device. The polarisation detection itself is done in a straight-forward way with a pair of polarising beam splitters (Figure 5.13). Thus, a

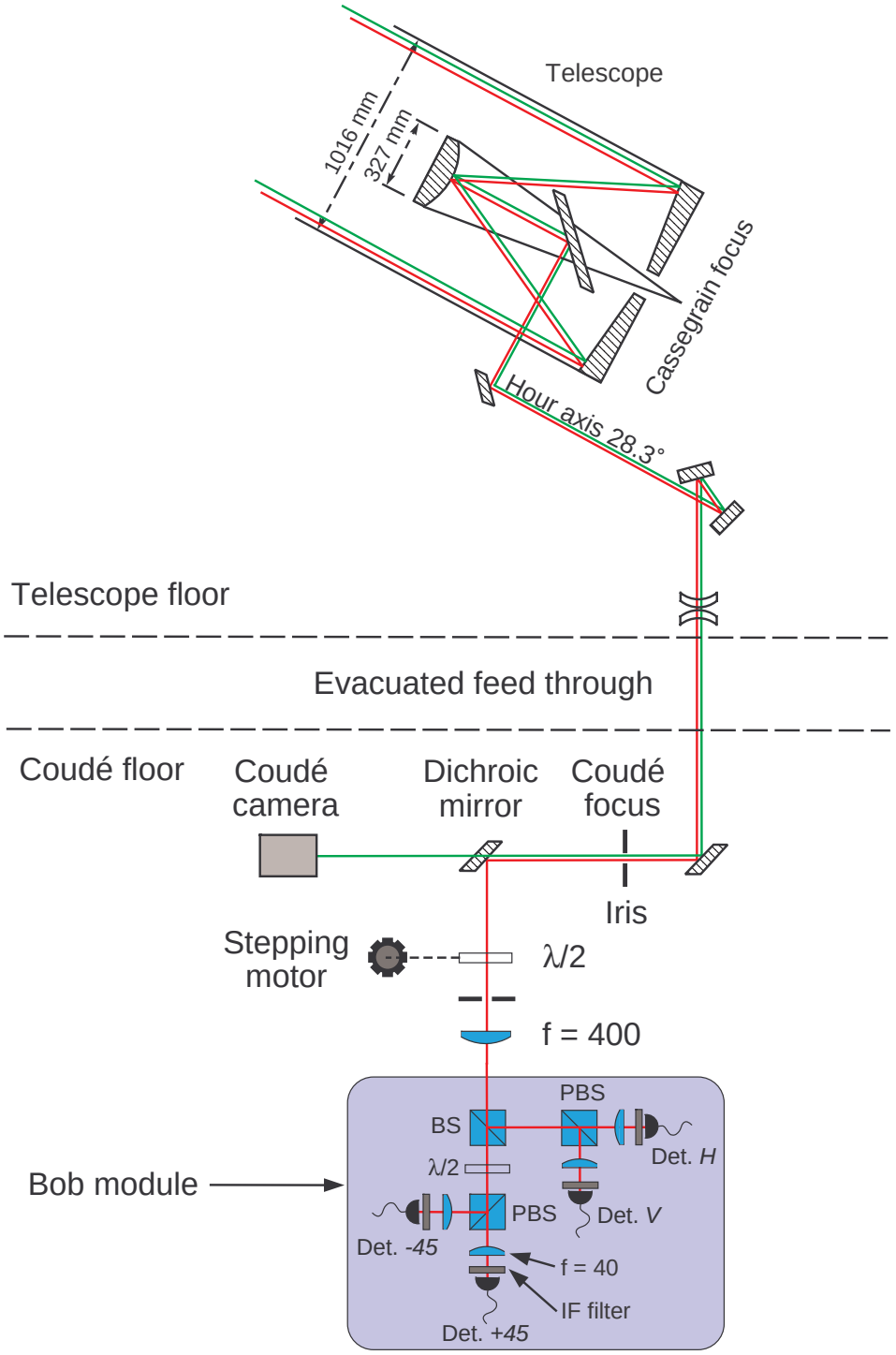

Figure 5.13: Optical setup of the receiver. Light collected by the OGS telescope is guided to the Coudé floor and split by a dichroic mirror; the quantum signal component is reflected to the single-photon polarisation analysis setup, light of the tracking beacon is transmitted to the Coudé camera.

photon behind the reflected output of the beamsplitter is analysed in the H/V basis, whereas photons in the transmitted arm pass a half wave plate at 22.5° in front of the polarising beamsplitter, and are effectively analysed along ±45°. Each analysis path contained an interference filter (centre wavelength 850 nm, FWHM 10 nm) attached to the single photon detector units, in order to suppress stray light both from the sky and from light sources in the Coudé room.

Atmospheric turbulence caused significant beam wander in the focal plane of the telescope of up to 3 mm on timescales too fast to be compensated by the active tracking system. To prevent the beam from wandering off the detectors, a focal length reducer was required to reduce the beam diameter to below 0.5 mm, the diameter of the active detector area. This was realised by collimating the beam after the Coudé focus with a 400 mm achromatic lens and refocusing with 40 mm lenses placed in front of each detector. The collimated beam had a diameter of 10.5 mm, which enabled usage of off-the-shelf 20 mm cube beam splitters. The additional optics shrunk the focus uncertainty circle by a factor of 8 and changed the effective numerical aperture from f/40 to f/5. If the Bob module had been placed directly at the Coudé focus, a considerable fraction of the photons would have missed the detectors.

Characterisation

In order to measure the contribution of the Bob module to the QBER, linearly polarised light with the same beam parameters as the light collected by the telescope was generated locally and sent to the Bob module. The emitting source, a 850 nm laser diode of the same kind as used in the Alice module, was attenuated with neutral density filters and coupled to single mode fibre for mode cleaning. After the fibre, a linear polarisation state was defined by a thin film polariser (extinction ratio better than 1:500). This fixed polarisation was then rotated by different angles by means of a half wave plate mounted in a motorised rotation stage. The polarisation angle was varied in steps of 1.5°, and, for each step, the number of detection events for each detector was recorded for a fixed integration time of 1 second. Figure 5.14 shows the number of detections as a function of the polarisation angle of the incident light. Fitting cosine functions to each data set, one obtains the visibilities of the four detectors. Table 5.2 lists the darkcount-corrected visibilities V_i and the angles γ_i defining the measurement bases.

From the visibilities V_i one can easily obtain the individual contributions to the total QBER in a quantum key distribution experiment. Since the residual error of the input polarisation has negligible impact on the measured visibilities V_i, we can calculate the contribution of the polarisation analysis setup to the QBER, for example, for horizontal polarisation from:

$$\mathrm{QBER}_{|H\rangle} = \frac{n_V(|H\rangle)}{n_V(|H\rangle) + n_H(|H\rangle)},$$

where $n_i\,|\psi\rangle$ denote the countrates of detector i for the incident polarisation state $|\psi\rangle$. This is a stricter definition than the general relation $\mathrm{QBER}_i = (1 - V_i)/2$, especially if

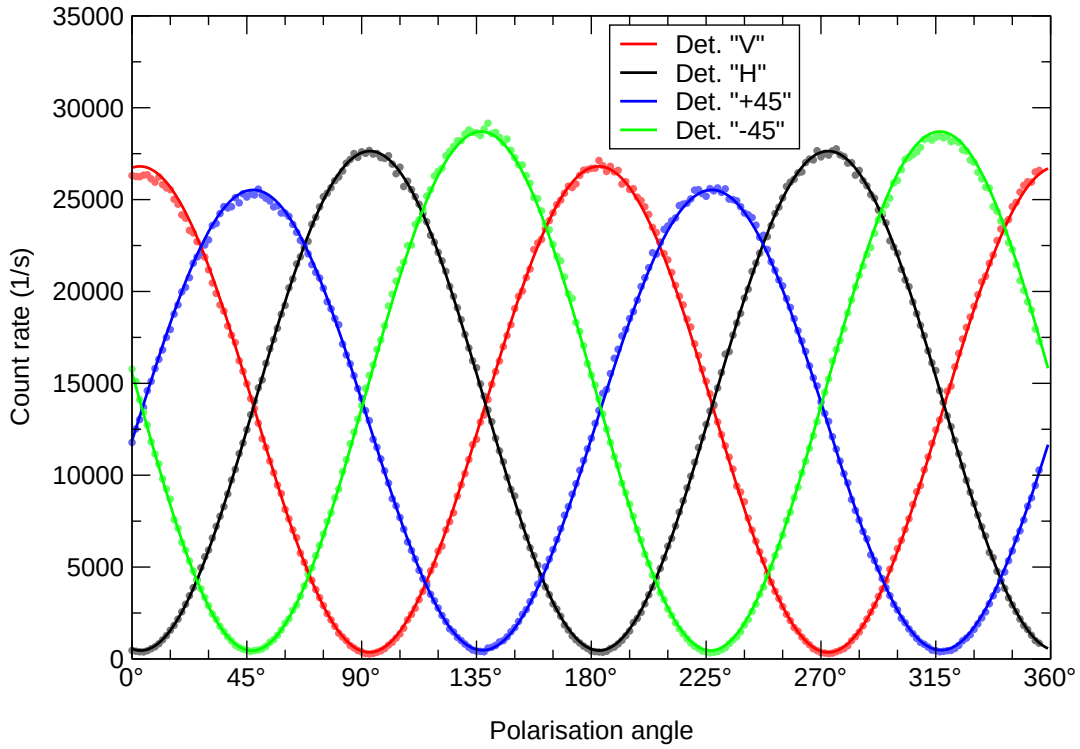

Figure 5.14: Characterisation of the polarisation analysis setup with highly linearly polarised light: Count rates of the individual single-photon detectors as a function of the polarisation angle of the incoming light.

Detector	Visibility V_i	Angle γ_i
H	98.0%	0.7°
V	98.9%	90.4°
$+45$	97.5%	44.7°
-45	98.5%	-45.7°

Table 5.2: Characterisation of the polarisation analysis setup: visibilities (dark count corrected) and bases angles for the four detectors of the Bob module. The values are inferred from fitted cosine functions to the data depicted in Figure 5.14.

the detection efficiencies of the individual detectors differ. Calculating the mean QBER of all four input polarisations $\{|H\rangle, |V\rangle, |+45\rangle, |-45\rangle\}$, one expects a contribution of the polarisation analysis of the Bob module to the total QBER of $\mathrm{QBER}_{\mathrm{Bob}} = 0.85\%$. A second source of error, that has to be attributed to the receiver optics, is the imperfect matching of the analysing basis reference frames to the transmitted one, that is, a relative rotation of the polarisation coordinate systems. Figure 5.15 shows the dependence of the contributions to the total QBER as a function of the angle mismatch. From this plot, it is apparent that a good alignment technique to keep the angle mismatch as low

as possible is crucial for operating a QKD system at the lowest QBER possible[1]. In the experiment, this was achieved by inserting a polariser into the transmitter telescope (as depicted in Figure 5.8, but without the additional lenses and detector), and optimising the rotation angle of the half wave plate in front of the Bob module (see Figure 5.13) for maximum extinction ratio in the rectilinear detection basis.

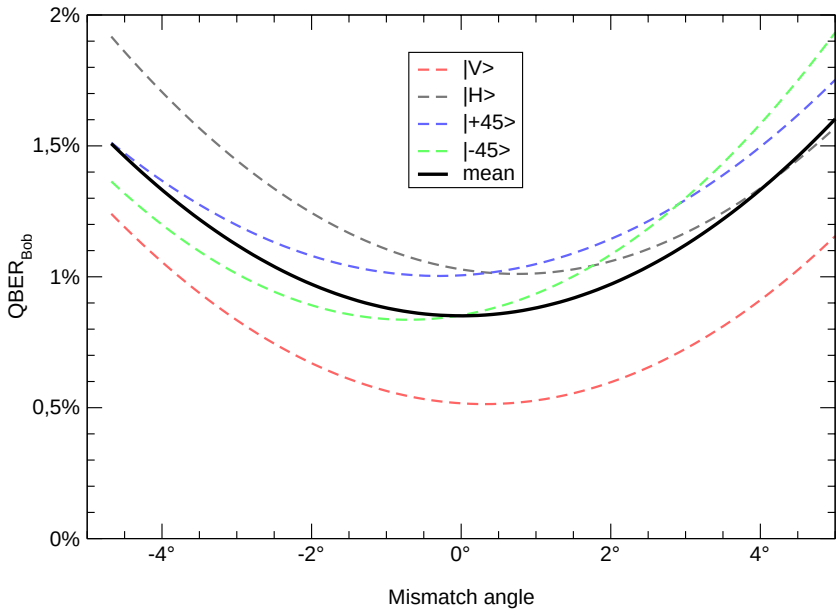

Figure 5.15: Effect of angle mismatch between transmitter bases and analyser bases on the QBER for the used polarisation analysis setup (see text). The plot shows both the individual contributions of each of the four polarisations and the mean QBER (assuming all polarisations are detected with equal probability) versus the angle mismatch.

5.2.3 Single photon detection

The detection of single photons was based on Silicon Avalanche Photodiodes (Si-APD) operated in Geiger mode, also known as *photon counting mode*. Si-APDs offer both a high detection efficiency in the visible to infrared spectral region, as well as low intrinsic dark noise.

Essentially, APDs are p-n junctions operated in reverse direction. In the Geiger mode, a bias voltage V_{bias} exceeding the breakdown voltage V_{br} by an amount called *excess bias voltage* V_{E} is applied. At this bias, the electric field across the junction is so high that a single charge carrier injected into the depletion layer can trigger a self-sustaining avalanche (*Geiger shower*). The current rises within a fraction of a nanosecond to a

[1]Especially for future satellite-based QKD systems this is a critical point, since the relative motion of transmitter and receiver demand accurate and fast adjustment of rotation angle.

macroscopic level in the milliampere range [169]. If the primary carrier is photogenerated, the leading edge of the avalanche pulse marks the arrival time of the detected photon. The current continues to flow until the avalanche is terminated by lowering the bias voltage to V_{br} or below. Then, the bias voltage is restored, in order to be able to detect another photon. This operation requires a so called *quenching circuit*. For low counting rates — as expected in this experiment — a simple passive circuit using a quenching resistor in series with the APD is sufficient [170, 171].

One of the freely available Si-APD models[2] is the diode C30902S (manufactured by *Perkin Elmer*), that was used for this experiment. The diode has a fairly large active area of 0.5 mm in diameter. For this experiment, the diodes were cooled thermoelectrically to an operating temperature around -25°C reducing the dark count rate to about $200 - 300$/s. To prevent condensation of air moisture on the diodes, they were enclosed in individual sealed housings, that also contained the necessary electronics for temperature stabilisation, biasing, and signal recovery. The APDs were thoroughly characterised in [172]; the parameters important for this experiment shall be summarised in the following.

Detection efficiency. For a photon detection event, it is necessary that the photon is absorbed in the active volume of the detector and generates a primary carrier (an electron-hole pair), as well as that the primary carrier does actually initiate an avalanche. Although conditions are such that, on the average, the number of carriers in the multiplying region increases exponentially with time, some just start a chain of ionisations that terminates before catastrophic multiplication takes place [174]. The efficiency of a photon detection increases with excess bias voltage since a higher electric field enhances the probability to trigger an avalanche [174, 175]. The photon detection efficiency η_{det} can thus be written as

$$\eta_{\mathrm{det}} = \eta_{\mathrm{q}} P_{\mathrm{br}},$$

where η_{q} is the quantum efficiency (number of generated primary electron-hole pairs per incident photon), and P_{br} is the breakdown probability, that is, the chance that a photoelectron will produce a complete discharge of the diode. It depends on the reverse bias voltage V_{bias} and is between 50-80% in the useful voltage range [176].

Accurate knowledge of η_{det} is crucial for the calibration of the mean photon number of the transmitter. However, the absolute detection efficiency η_{det} is not trivial to measure accurately without reverting to a precalibrated reference single photon detector. Therefore, η_{det} was measured with a technique utilising photon pairs, that are emitted into two spatially separated modes by a type-II spontaneous parametric downconversion source (SPDC) [177]. In this setup, the detection of a photon in the "trigger" arm guarantees with certainty the existence of a photon in the second arm (containing the detector to calibrate). Therefore, any missed detection there can only be due to nonideal efficiency of the detector under test. The measured fraction of coincidences is therefore a direct measure for the absolute detection efficiency. For more details, see, for instance [178–181].

[2] Although a large variety of APDs are offered, only very few are optimised for Geiger mode.

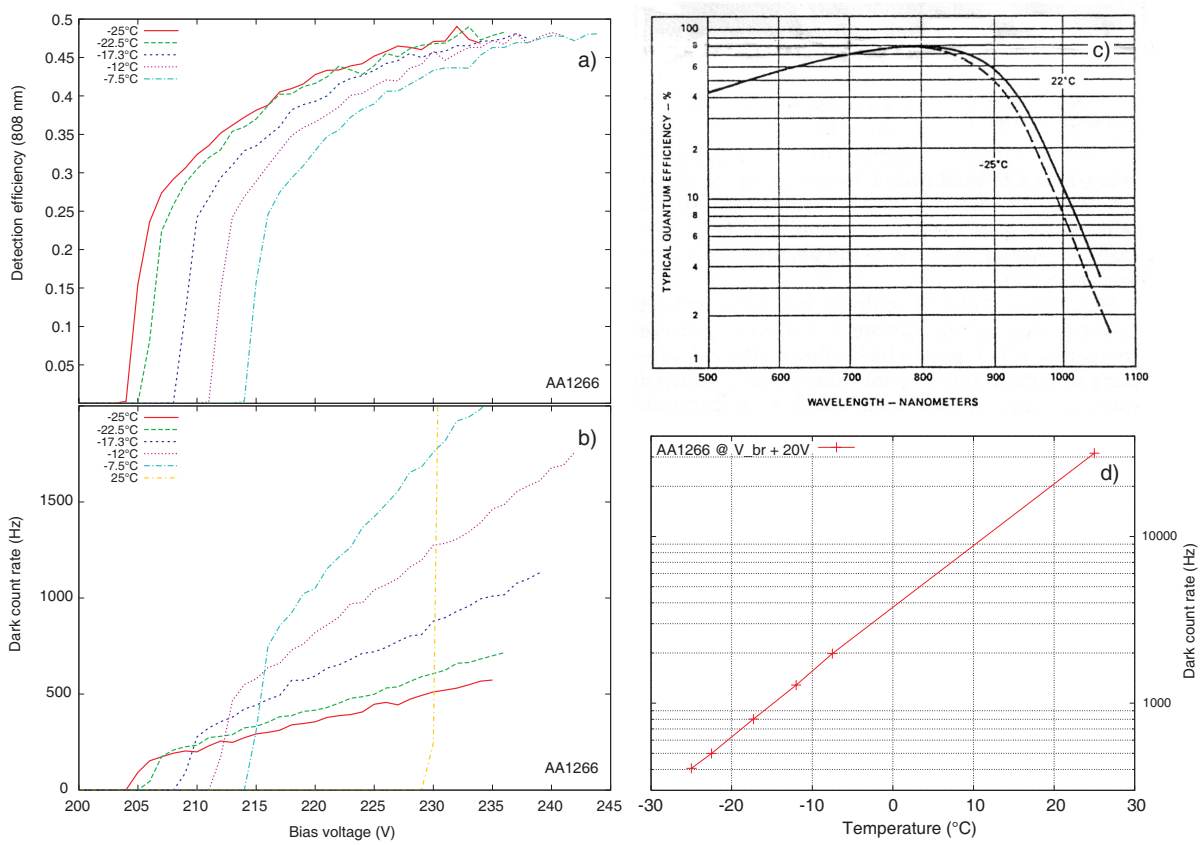

Figure 5.16: Properties of the Si-APD type C30902S. **(a)** Absolute detection efficiency at 808 nm as a function of bias voltage for different diode temperatures. At a photon flux of $\approx 3 \cdot 10^5\,\mathrm{s}^{-1}$, the detection efficiency saturates around 0.47 for bias voltages $\gtrsim 20\,\mathrm{V}$ above breakdown. **(b)** Dark count rates as a function of bias voltage for different temperatures. **(c)** Typical spectral quantum efficiency (from [173]). **(d)** Dark count rate as a function of temperature for fixed excess bias voltage, exhibiting the expected exponential behaviour.

For our APDs, the detection efficiency rises with the bias voltage (above V_{br}), and saturates around 47% efficiency for excess bias voltages of $V_{\mathrm{E}} \gtrsim 30\,\mathrm{V}$, independent of the device temperature, as can be seen in Figure 5.16a. This measurement was taken at a photon flux of approx. $3.4 \cdot 10^5\,\mathrm{s}^{-1}$ and at 808 nm wavelength. To obtain the absolute detection efficiency at the signal wavelength of 850 nm, the values of plot a) have to be rescaled using the spectral dependency of the quantum efficiency η_{q} (Figure 5.16c, [173]), whereas the breakdown probability P_{br} is essentially independent of the wavelength [176]. In this way we have to correct the values measured at 808 nm with a factor of 0.87, from which we obtain a photon detection efficiency at 850 nm of around 38% for $V_{\mathrm{E}} = 20\,\mathrm{V}$. For the five different detectors investigated, a small variation of η_{det} between 36.5% and 39.2% was found.

Dark count rate. Thermal generation of electron-hole pairs produce current pulses

even in the absence of illumination, and the Poissonian fluctuation of these dark counts represent the internal noise of the detector. According to the thermal origin, the APD dark count rate grows exponentially with temperature (Figure 5.16d). As illustrated in Figure 5.16b, the dark count rate also increases with excess bias voltage. Therefore, going to very high bias voltages does not give an advantage. As a compromise, the detectors used in this experiment were biased with 20 V above their respective breakdown voltages, giving a mean detection efficiency of $\eta_{\mathrm{det}} = 38\%$ and an average dark count rate of ~ 250/s.

Time jitter. Intrinsic darkcounts and stray light raise the error rate of the QKD system. Their impact can be reduced by choosing a narrow detection time window Δt. Therefore, the time jitter of the detector is an important parameter, as it may constitute a limitation to the minimal practical value of Δt. Both the APD itself and the pulse detection electronics contribute to the detector time jitter. The relevant parameter for the performance of the QKD system is, in this respect, the time jitter of the complete detector module, including detector electronics. It was measured using the down-conversion setup. Because in SPDC both photons are emitted within a time interval of the order 100 fs (determined solely by the bandwidth of the downconverted light [182, 183]), the relative time delay of the detector signals in the two arms of the downconversion is completely dominated by the time jitter of the two detectors. The detector under test was characterised together with a fibre-coupled detector, the time jitter of which had been determined earlier. A Gaussian function was fitted to the histogram of the recorded relative time delays, reproducing the measured data quite well (Figure 5.17). Deconvoluting the fit function with a second Gaussian (FWHM 540 ± 50 ps) of the known detector, one calculates the width (FWHM) of the time jitter $\tau_{\mathrm{Det}} = 400 \pm 50$ ps for $T = -25\,^{\circ}\mathrm{C}$ and $V_{\mathrm{E}} = 20$ V.

5.2.4 Data recording and processing

In order to enable key generation from the stream of detection events, proper mapping of detected photons to the pulses originating from Alice is essential. Furthermore, accurate synchronisation to timescales shorter than the time duration of a transmission pulse is necessary in order to maintain a narrow detection time window to curb the influence of background events. This requires to establish a common time base or synchronisation procedure between transmitter and receiver. In the experiment, this was achieved by deducing the clock rate and starting time of Alice's transmission directly from the detected photoevents. A prerequisite for the software synchronisation algorithm is, of course, the assignment of a digital timetag to each detection event. Such timetags were generated by a dedicated electronics (*timestamp unit*), transferred to Bob's PC, and later used to realise a software based synchronisation algorithm.

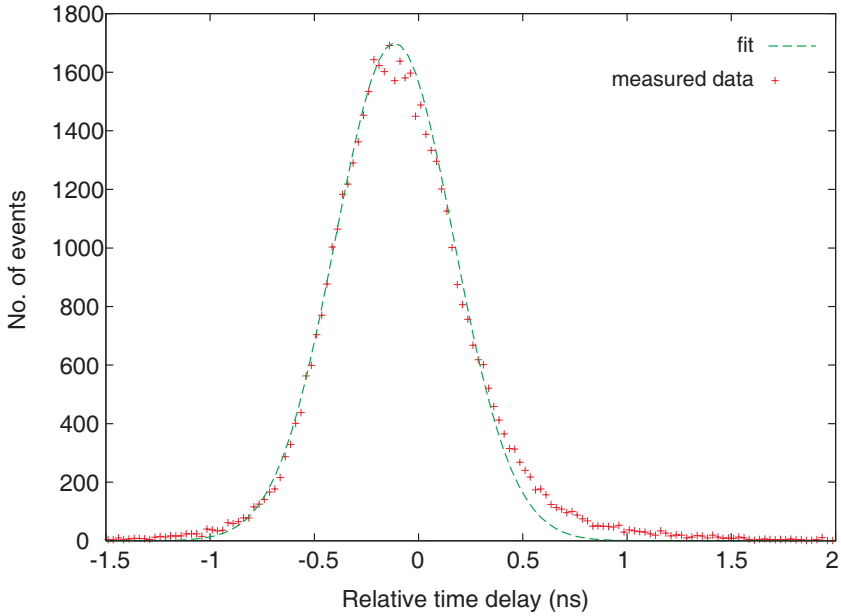

Figure 5.17: Measurement of detector time jitter: Histogram of the relative time delay between the signals of detectors placed in each arm of the downconversion setup.

Timestamp unit

The timestamp unit has four standard NIM logic inputs, that were connected to the four single-photon detectors of the receiving unit. The time base can be chosen between an internal, unstabilised crystal oscillator and an external 10 MHz reference signal. In the experiment, an ovenized oscillator, that was disciplined by a GPS receiver (*Trimble Thunderbolt*) provided a stable timebase with a mean absolute accuracy of 14 ns. The transmitter was clocked by an identical unit, in this way residual relative drifts between the two clocks were less than 10^{-11} over 100 s.

The operational principle of the timestamp unit is illustrated in Figure 5.18. A logic *high* on any of the four NIM input lines initiates a trigger, signalling to the timing control functional unit that an event has occurred. After a programmable time delay, the pattern sampler is activated and reads in parallel the four input lines. Thus, multiple events on different input lines that occur almost simultaneously can be detected and are treated as a coincidence event. The timetag associated to an event is generated by three stages of increasing timing resolution: the slowest stage consists of a cascaded array of 8-bit counters, the fastest of which is clocked by 1/32 of the 500 MHz fundamental clock rate. A faster counting module (*fast counter*, implemented in ECL logic) uses the 500 MHz fundamental clock directly and provides a resolution of 2 ns. To further increase the resolution, a *phase stage* takes a snapshot (*"phase pattern"*) of the clock waveform travelling along a sequence of delay lines at the time the event occurs. Thus, the clock phase at the moment of the event can be reconstructed by software with a

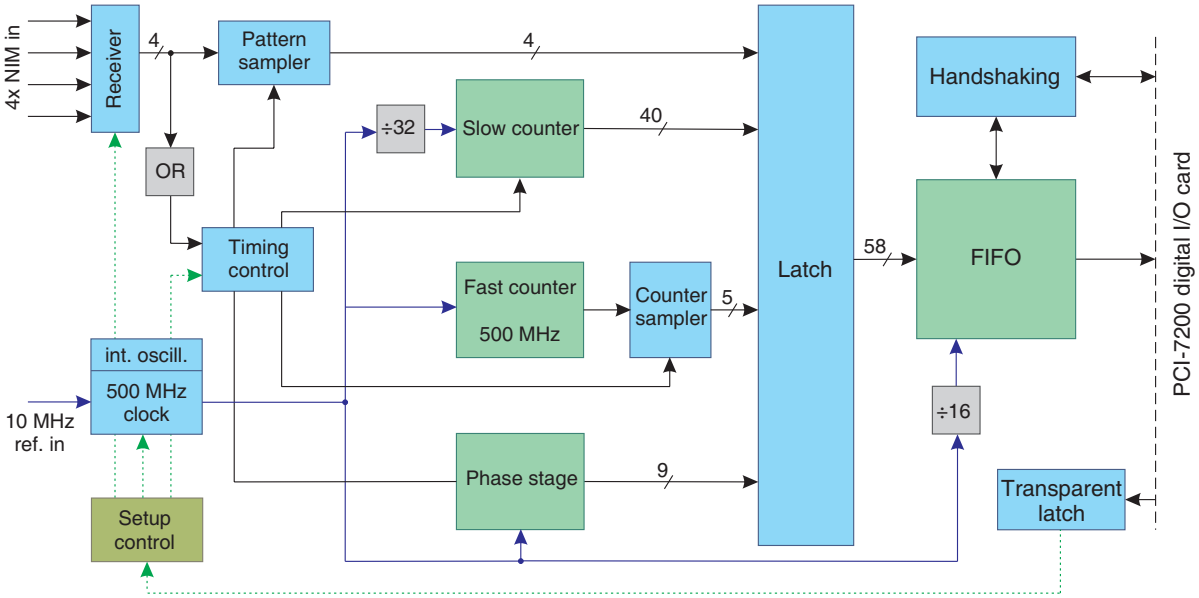

Figure 5.18: Functional block diagram of the timestamp unit: upon trigger by at least one of the four NIM input channels, a 49-bit timetag with 1/8 ns resolution is created. The timetag is buffered together with the trigger pattern in a FIFO memory, and finally transfered to a digital input/output card. See text for more details.

theoretical resolution of 1/8 ns. The timing data from all three stages together with the input pattern is collected by a latch. To minimise the deadtime after an event, and to ensure that no events are lost, the timetag is not transferred directly to the PC, but buffered in a fast, first-in, first-out memory (FIFO). A handshaking circuitry takes care of proper communication with the PC via an interfacing digital input/output card (*Adlink PCI-7200*). Several parameters of the timestamp unit, like clock source selection, or input thresholds, can be remotely controlled from the PC.

Although the theoretical resolution of the timestamp unit is 1/8 ns, imperfect implementation of the phase stage and electronic noise reduce the actual performance. Moreover, the phase stage yields a non-uniform accuracy depending on the relative phase $\Delta\varphi$ between the event and the fundamental clock. Figure 5.19a shows the colour-coded incidence probability of the different phase patterns (ordinate axis) as a function of the phase delay $\Delta\varphi$. Hence, the vertical sum of probabilities is 1 for each $\Delta\varphi$. As can be seen, not all patterns occur with equal probability. Additionally, the width of the probability distribution — and accordingly the timing accuracy — depend on the individual pattern. To obtain the average timing jitter of the timestamp unit, a stream of digital signals that were phase stable with the reference clock was fed to the inputs, and a histogram of the timing error was computed (Figure 5.19b). This procedure was repeated for different phase delays. The average standard deviation of the resulting distributions was 340 ps.

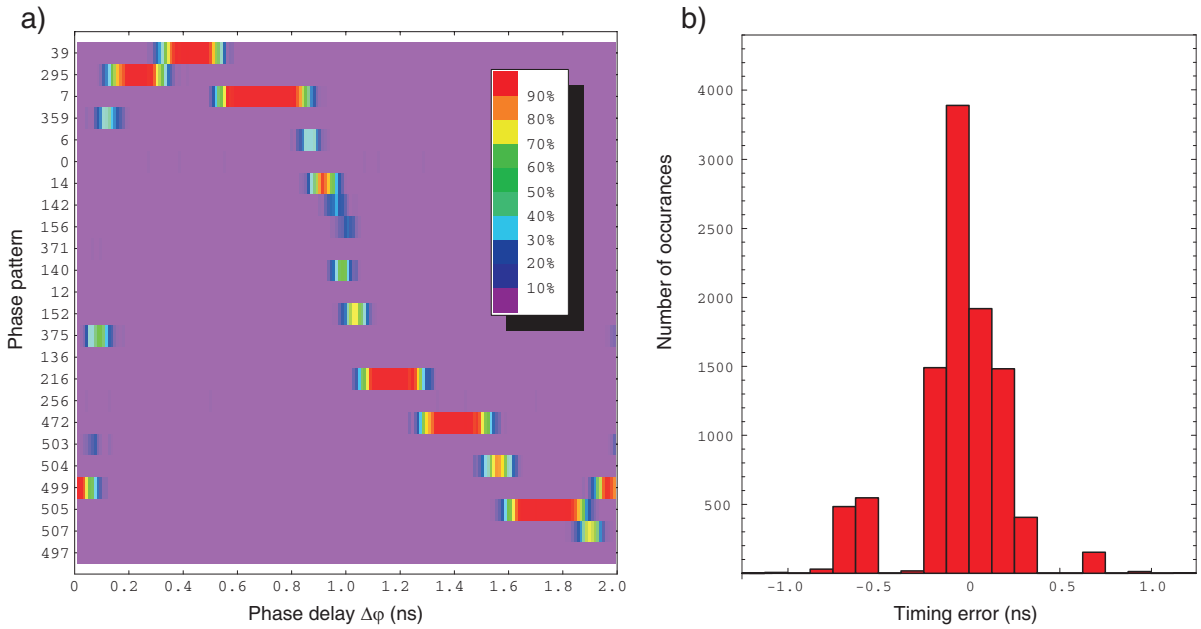

Figure 5.19: Measurement uncertainty of the timestamp unit. **(a)** Incidence probability of the individual phase patterns as a function of phase delay $\Delta\varphi$ between the event signal and the fundamental 500 MHz clock. The pattern probability distributions have unequal width, leading to non-uniform measurement uncertainty. **(b)** Example of a resulting timing error distribution for externally generated events with fixed phase delay. The standard deviation was 315 ps in this case.

Synchronisation

Based on the recorded timetags, the software-implemented synchronisation procedure was performed on Bob's PC. During this process, each photoevent has to be assigned an absolute pulse number in order to allow Alice and Bob to discuss their respective choice of basis for that pulse. The stream of digital timetags representing the detection times of the photoevents was the only timing information available for the software synchronisation algorithm. The algorithm was originally designed [184] to cope with the reduced stability of standard, unstabilised crystal oscillators serving as master clock for both Alice and Bob in an intra-city QKD experiment over distances in the km range. Facing the much higher attenuation over long distances, the number of detected pulses does not yield enough timing information to compensate large relative clock drifts. Hence, clock signals for both Alice and Bob were derived from GPS signals as explained above to mitigate the problem of fast drifting time references. However, the synchronisation algorithm still had to deal with residual drifts on the order of 10^{-11} over 100 s and the lack of an precise absolute time reference, as the PCs' system clocks were only synchronised to several hundred μs using the standard *network time protocol* (NTP). The synchronisation algorithm has to

a) ensure, that the local clocks at Alice and Bob run effectively at the same speed

b) monitor potential drifts between the local clocks

c) compute the pulse number offset ΔT_{AB} between Alice's transmissions and Bob's detections.

The situation is illustrated in Figure 5.20a: Alice transmits dim pulses with a fixed repetition rate of 10 MHz. Since not all pulses contain photons in the first place, and because of the high loss along the free-space link, only a few of these photons are actually detected by Bob. These events will, however, occur in the known 10 MHz timing cycle, forming a comb-like pattern with very few teeth. Spurious events from stray light and

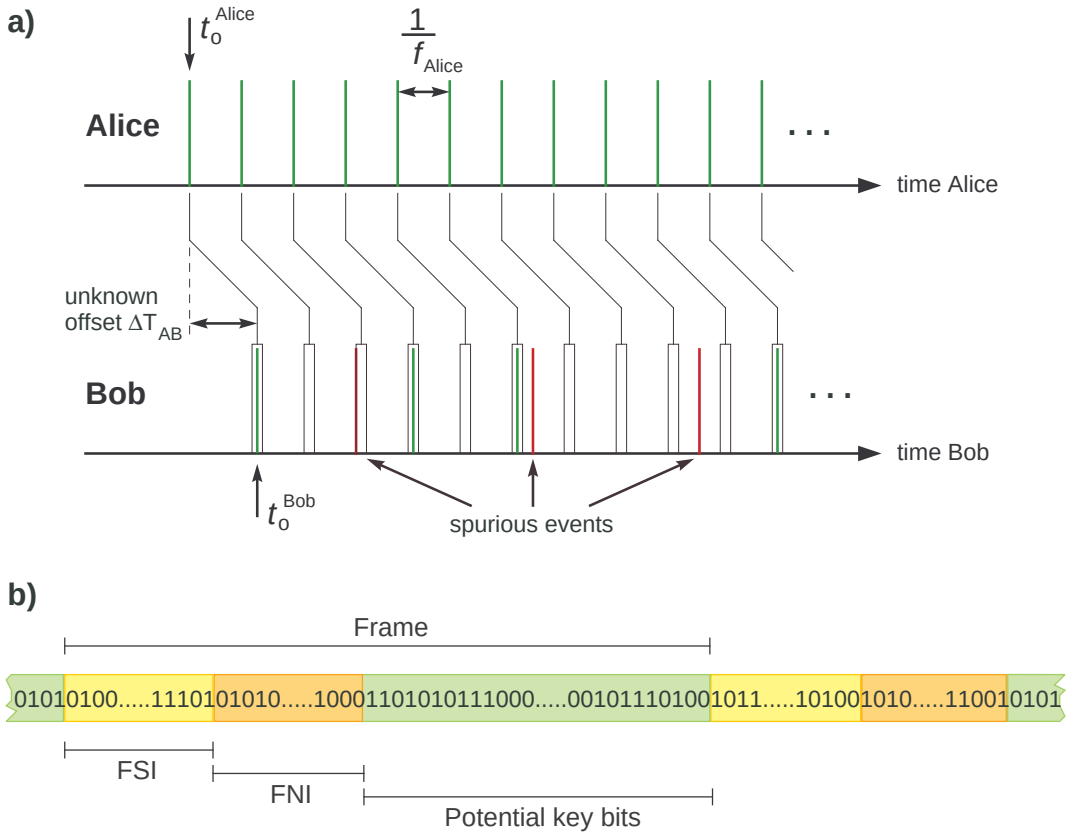

Figure 5.20: Schematic principle of the synchronisation algorithm. **(a)** The basic pulse repetition rate and the phase of Alice's transmission is deduced from the detected event timings. Spurious events are suppressed by defining a detection time window Δt. **(b)** Structure of the transmitted frame containing a header and the potential key bits. The pseudorandom bit sequences of the frame start identifier and the frame number identifier enable Bob to correctly identify the start of the respective frames and to obtain the absolute offset ΔT_{AB} between Alice and Bob.

intrinsic darkcounts are distributed evenly in time, and have only a small probability of occurring at the teeth positions of the comb.

Full synchronisation was achieved in three steps. First, a fast-Fourier-transform (FFT) algorithm was applied to the raw event timings to obtain an initial value for the basic pulse repetition rate of the transmitter with respect to the receiver clock. Owing to the limited sampling time, the accuracy of the resulting value had to be enhanced by means of a linear least square fit to the arrival times modulo the raw repetition period. Together, this provided a refined value for the repetition rate. Thanks to the GPS-disciplined clocks, only very small deviations from the theoretical value of 10 MHz occurred at this stage. Each photoevent was accepted if it was detected within a time window Δt around the expected arrival time or rejected as background otherwise. A software phase-locked-loop compensated for any slow residual drifts by analysing whether photons were arriving, on average, rather too early or too late. At the end of this stage, each accepted photoevent had been assigned a pulse number. Yet, the global pulse number offset between Alice and Bob was still unknown. To obtain this offset, the photon stream was divided into consecutive frames of fixed length, each frame starting with two headers with pseudorandom bit sequences: A *frame start identifier (FSI)*, and a *frame number identifier (FNI)*, see Figure 5.20b. The FSI was identical for all frames, whereas the bit sequence of the FNI was shifted by one bit from one frame to the next frame. Both pseudorandom bit sequences were known to Bob, and were not encoded in the polarisation of the transmitted photons, but in individual pulse brightness: For a "1", all transmitter diodes were switched on simultaneously, whereas the pulse was suppressed for a "0". To enhance the signal-to-noise ratio, it was necessary to integrate over several frames before it was possible to locate the frame start by correlating the detected events with the known FSI bit sequence. This was efficiently done with fast-Fourier-transforms. Similarly, in the last step, the absolute offset of the pulse number was determined from the shift of FNI bit sequence within the detected bit stream.

At this point, the synchronisation procedure was completed, with Bob's detection events being identified solely by their absolute pulse number. This enabled to initiate first the sifting process, and then the subsequent classical post-processing steps of error correction and privacy amplification, which will be explained together with the experimental results in the next chapter.

6 Quantum key exchange

The main goal of this experiment is the generation of a secret key shared between Alice (on La Palma) and Bob (on Tenerife). The preceeding chapters described and characterised the establishment and stabilisation of the optical link using active beam steering techniques, as well as the setup of the quantum optical transmitter and receiver. To overcome the security and performance limitations due to the photon-number splitting attack in the presence of high channel loss, a 3-intensity decoy-state extension to the BB84 protocol was employed: In addition to signal pulses with mean attenuation μ, the transmitter also emitted slightly brighter decoy pulses with a mean photon number of μ', and "pulses" with no light at all, $\mu_0 = 0$. By finally evaluating the detection probabilities at the receiver corresponding to pulses of the individual classes, one can calculate an upper bound to the fraction of tagged bits that may have leaked to the eavesdropper without thereby causing errors in the generated key.

The key exchange results presented in this chapter were obtained during two measurement campaigns. In the first campaign, the attenuated pulse transmitter was equipped with 4 laserdiodes, and decoy states were created by pulsing two laserdiodes simultaneously. However, this approach has two shortcomings: Firstly, the intensity of 2-diodes decoy pulses is firmly linked to the intensity of the (1-diode) signal pulses and therefore cannot be optimised separately. Secondly, the polarisation of 2-diodes decoy pulses is not well defined, prohibiting the use of these pulses for key generation. Both arguments lead to a decreased secret key rate compared to the ideal 3-intensity decoy protocol. For this reason, in the following campaign the transmitter module was extended to 8 laserdiodes, providing the four linear polarisation states of the BB84 protocol at two independently tunable intensities. In the following, the key exchange results are presented and discussed separately for these two transmitter configurations.

6.1 Key exchange with 4-channel Alice

In the measurement campaign of June 2006, a 4-channel Alice module was used. The four nearly identical laserdiodes each produce weak coherent pulses with distinct polarisation (horizontal, vertical, diagonal and anti-diagonal linear polarisation). Originally intended for running a pure BB84 protocol [38,185], its electronics did not allow a fast modulation of the pulse intensity from pulse to pulse. However, pulses of increased intensity μ' can easily be created by simply firing two randomly chosen laserdiodes simultaneously [105]. Although the resulting state is not identical to a signal pulse of lower attenuation μ',

an adversary has no possibility to discriminate the decoy pulses from signal pulses: The output of k lasers firing simultaneously with intensity μ is, when averaged over all k-tupels, indistinguishable from the output of one laser firing with intensity $k\mu$, because both states are described by the same density matrix.

For simplicity, in the experiment only decoy pulses (of higher μ') with $k = 2$ were used. For electronic reasons, the pulses generated by firing two randomly chosen diodes simultaneously had intensity μ' that was not twice the value of μ, but slightly lower at $\mu' = 1.43\mu$. For the additional empty decoy pulses, the electrical pulse driving the laserdiode was suppressed. Bright and empty decoy pulses were randomly interspersed in the signal sequence with probabilities n' and n_0, respectively.

6.1.1 Parameter optimisation

Generally, the 3-intensity decoy-state protocol permits both signal and decoy pulses to be used for key generation. However, a 2-diodes decoy pulse does not have a well-defined polarisation like a signal pulse, and thus cannot contribute to the sifted key. Obviously, the same is true for the empty decoy pulses that serve to determine the background from dark counts and stray light. In order to optimise the key generation rate, it is therefore desirable to use a large fraction n_s of the pulses for signal pulses, and only a small fraction n' for decoy pulses. On the other hand, too few decoy pulses lead to poor statistical significance of the derived fraction of tagged bits Δ. Hence, a larger error margin $\delta\Delta$ would have to accommodate this uncertainty. The optimal choice of the fraction of decoy pulses n' and vacuum pulses n_0, as well as the best value for μ

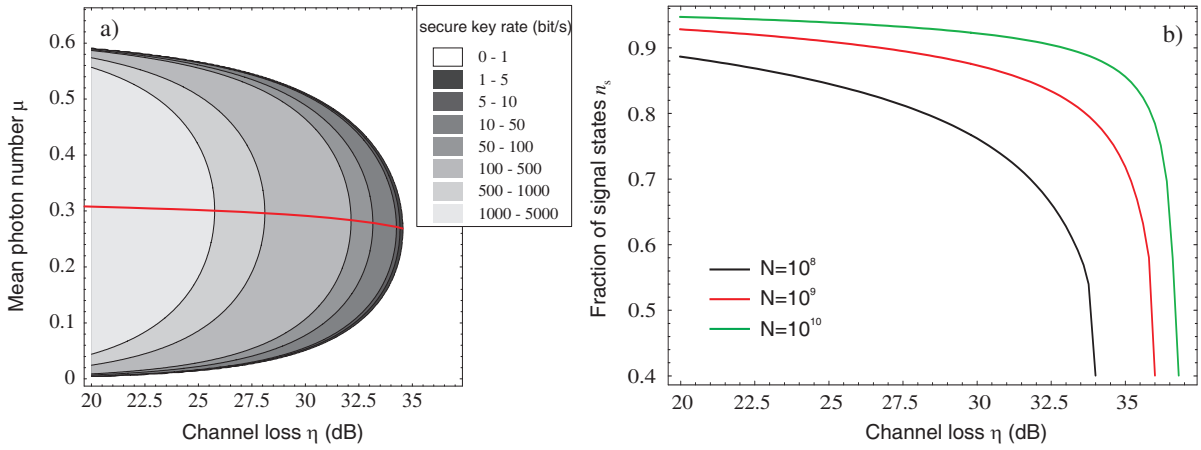

Figure 6.1: Parameter optimisation for the 4-channel Alice. **(a)** Key generation rate as a function of channel loss and mean photon number of the signal pulses for the experimental repetition rate of 10 MHz. The value of μ yielding the highest key rate (red curve) is nearly independent of the loss. **(b)** Optimum choice of the fraction of signal states n_s as a function of loss, plotted for different total numbers of emitted pulses N.

(given the fixed ratio $\mu'/\mu = 1.43$) was found by numerical optimisation of the expected key generation rate B.

Figure 6.1a shows a contour plot of the key generation rate B as a function of channel loss η and mean photon number μ of the signal states. The plot was computed for a repetition rate of the transmitter $\nu = 10^7$ Hz, a dark count probability $Y_0 = 6 \cdot 10^{-6}$, error correction efficiency $f(e) = 1.22$, and technical error $e_{\text{tech}} = 0.02$ (see §2.6.4 for definitions). The highest achieved key rate for any value of η is marked by a red curve, showing that μ is essentially independent of η. Optimising for an attenuation of the inter-island link of 30 dB and above, the average photon number of the signal pulses was set to $\mu = 0.27$. The actual pulse intensity of the Alice module was checked by measuring μ and μ' in the transmitter telescope before each QKD experiment, and additionally monitored at the second output port of the 50:50 fibre beam splitter (see Figure 5.8).

The best choice of the fractions of signal pulses n_s and decoy pulses n', n_0 strongly depends on the total number of pulses N sent during a QKD session (Figure 6.1b). Considering a practical duration of a single QKD session of ~ 100 s equivalent to $N = 1 \cdot 10^9$, the probabilities of bright decoy and vacuum pulses were chosen to be $n' = 9.4\%$ and $n_0 = 3.1\%$, respectively. This left a useful fraction of $n_s = 1 - n' - n_0 = 87.5\%$ for the signal pulses. The actual pulse sequence was generated according to random bit values, that were created beforehand by a physical random number generator and stored on Alice's hard disk.

6.1.2 Synchronisation and sifting

Under good atmospheric conditions, about 1000 photoevents per second originating from the transmitter were recorded at the receiver. A separate transmittance measurement using a bright continuous-wave laser source yielded a link efficiency L_{ee} of 28–29 dB between the transmitter telescope and the OGS Coudé focus. Taking into account the efficiency of the detector system (including the polarisation optics and interference filters) of $\sim 25\%$ equivalent to further 6 dB of loss, the observed count rate[1] is in excellent agreement with the expected value of approx. 900–1100/s. Background resulted from intrinsic detector dark counts (~ 1000/s) and stray light from the nightly sky. Stray light countrates varied between ~ 200/s at new moon and up to ~ 4000/s at full moon, when measured with 10 nm FWHM interference filters and the full field-of-view of the OGS telescope (8 arcmin). Restricting the field-of-view to about 15 arcsec (about 10 m at La Palma) by closing an adjustable iris diaphragm in the Coudé focus to 3 mm, the stray light could be reduced to 400–1000/s. Larger iris diameters were required during less favourable atmospheric conditions to allow for larger beam spot sizes due to image blurring and image dancing. Even with the bi-directional tracking running continuously, the 532 nm laser beacon from La Palma did not cause any augmentation of the background count rate. The wavelength separation of the dichroic mirror together

[1] All count rates are given as the sum of all 4 detectors unless stated otherwise.

with the high blocking ratio of the interference filters provided the required spectral isolation of the quantum channel and the tracking light.

The time tags of the raw detection events (created by the timestamp unit, see §5.2.4) were transferred to Bob's computer for further processing. First, an initial value for the transmitter's pulse repetition frequency with respect to the receiver clock was obtained by applying a fast-Fourier transform (FFT) to the the raw event timings (Figure 6.2a). Since both clock signals at Alice and Bob were derived from the GPS-disciplined oscillators, local clock drifts were smaller than 10^{-11} over 100 s. Any residual drifts were compensated by the phase-locked loop (PLL) of the synchronisation software (see §5.2.4). Figure 6.2b shows a histogram of photoevent arrival times, modulo the pulse repetition period. Atop an evenly distributed background from stray light and detector background counts, photodetections due to attenuated pulses sent by the transmitter accumulated around a specific time delay. Photoevents occurring within a time window Δt around the centre of the distribution (i.e., the expected arrival time) were accepted as originating from Alice, and rejected as background otherwise. The cumulative effect of signal pulse duration, timing jitter in the Alice electronics, reference clock and PLL noise, timing jitter of the photodetectors, and accuracy of the timestamp unit led to a temporal distribution of signal events with a FWHM of 4.3 ns. The clearly visible shoulder in the distribution indicates that the main contribution came from the duration and shape of the laserdiode pulses and probably also from an increased time jitter of the Alice electronics. Setting a value for the time window implies a trade-off between resulting raw bit rate and error rate. Due to the low signal-to-noise ratio, a rather small value of $\Delta t = 5.1\,\mathrm{ns}$ was selected, which sacrificed some raw bits, but reduced the QBER

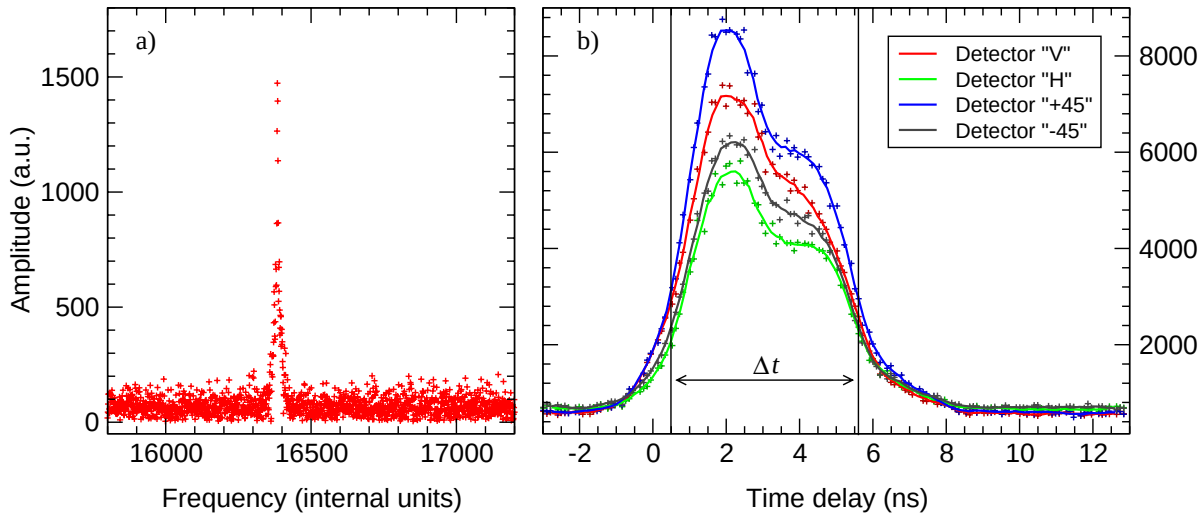

Figure 6.2: Synchronisation of the 4-channel transmitter and the receiver. **(a)** FFT of raw detection events to determine Alice's pulse repetition rate. **(b)** Histogram of photoevent arrival times. Detections within the time window Δt are accepted as received from Alice.

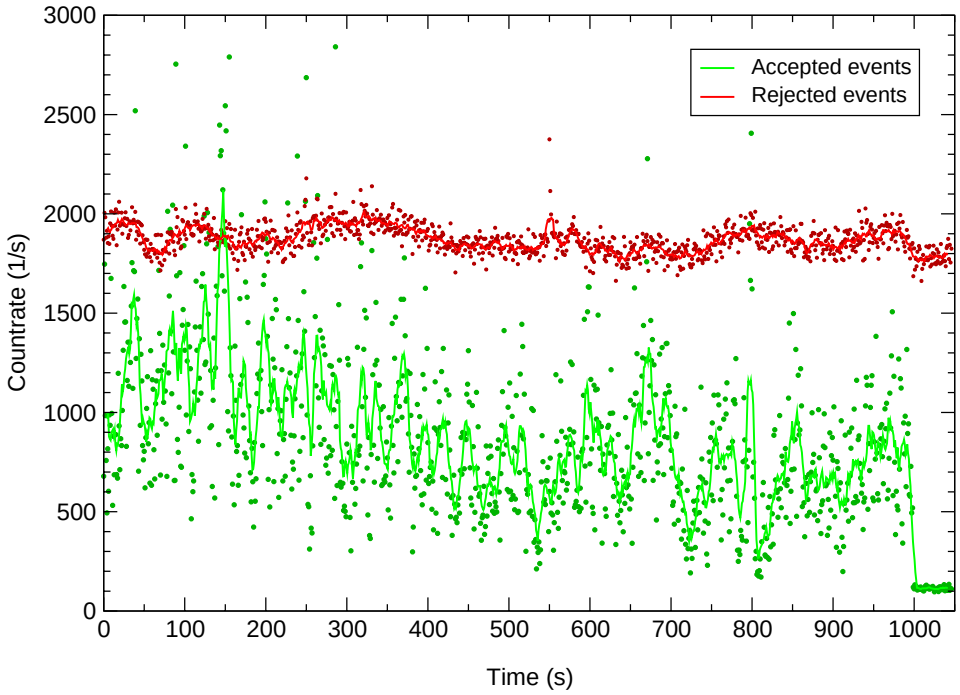

Figure 6.3: Signal (green) and background (red) countrates after synchronisation during a 1000 s QKD experimental run. The data points show 1-s averages; the full lines represent a moving average over 10 s.

to a tolerable level.

Figure 6.3 shows the resulting countrates (with 1 s wide bins) of synchronised events and background events over a full measurement run of 1000 s. The background event rate is fairly stable at ~ 2000/s, but the signal countrate exhibits large fluctuations over a timescale of seconds. The signal countrate drops to ~ 100/s spurious events when Alice stopped transmitting at $t = 1000$ s. These events, falling inadvertently into the detection time window Δt, led to an average contribution to the QBER of $\sim 5\%$. Additional contributions came from alignment errors of the Alice module including residual birefringence in the single-mode fibre ($0.3-0.6\%$) and from imperfections of the polarisation analyser (0.85%).

As a prerequisite of the sifting process, an absolute pulse number has to be assigned to each accepted photoevent, which were buffered in the PC memory until full synchronisation was achieved. As described in the preceeding chapter, the global photon number offset ΔT_{AB} was computed from pseudo-random bit sequences in the photon stream, constituting 1.2% of the pulses. Figure 6.4 shows a correlation of the detected events with the known *frame start identifier (FSI)* (a) and *frame number identifier (FNI)* (b) bit sequences. The correct position of the FSI and the correct frame number clearly stand out. Together with a basic synchronisation of the PCs' system clocks via the standard *network time protocol* (NTP), ΔT_{AB} was obtained.

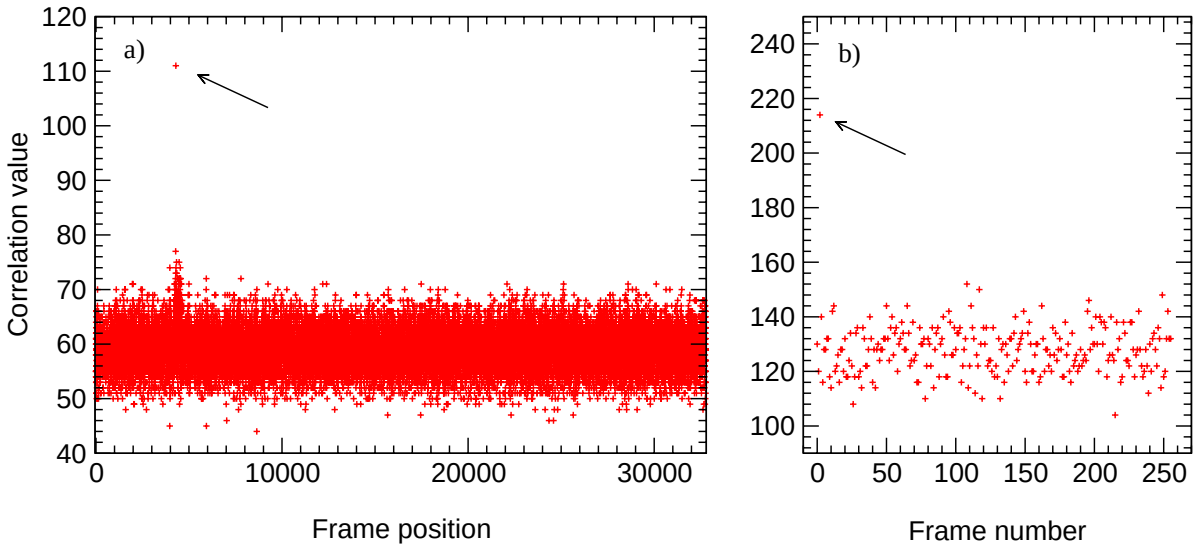

Figure 6.4: Reconstructing the absolute pulse number by correlating known pseudo-random bit sequences with detected events. **(a)** 128-bit *frame start identifier* within 32768-bit frame. **(b)** 256-bit *frame number identifier* within frame.

Because of the strong fluctuation of the link efficiency and frequent fades of the quantum signal, the signal-to-noise ratio was not constant within the measurement run. Therefore, blocks whose header was already corrupted by more than a factor of 1.1 were discarded during the synchronisation process. This led to a raw key pair of 836 kbit shared by Alice and Bob.

As soon as enough events were buffered to compute ΔT_{AB}, basis reconciliation over the classical 10 Mbit/s Ethernet channel was initiated and performed on-the-fly for the subsequent data. At the end of this process, Alice and Bob held a binary key of 278 kbit, which still contained errors due to experimental imperfections and potential eavesdropping activity.

6.1.3 Distillation of the secure key

To remove the errors from the sifted key, the classical two-way error correction protocol CASCADE [116] was applied. The algorithm works by the principle of comparing parities between blocks of key bits. This allows to detect blocks with odd numbers of errors. When such a block is found, a binary search inside the block is performed to reveal the position of an error. The protocol works in typically 4 or 5 passes, and each pass uses different block partitions, that is, different permutations of the raw bits. After each pass, each block contains an even number of errors, or no errors. If an error is found in one block in pass i (which was overlooked in passes $1, ..., i-1$), the algorithm tracks the bit back to its blocks in passes $1, ..., i-1$. By correction of the bit, there will then be blocks with odd number of errors in passes $1, ..., i-1$. Binary searches find these errors,

possibly creating more blocks with odd number of errors. This is continued until no blocks have an odd number of errors. The key to good performance in the CASCADE protocol is the choice of block sizes in the individual passes. This choice depends on the bit error rate e. Starting from values in the literature [115, 186], block sizes were optimised for the expected error rates. For an error rate around 6%, 5 passes with block sizes $\{14, 28, 64, 128, 256\}$ were used. Instead of randomly permuting the raw bits before the error correction to ensure homogeneous distribution of errors, the raw bits were grouped into *superblocks* of 1024 bits length. The CASCADE algorithm was then performed for each superblock separately, which allows for the disposal of blocks containing substantially more errors than on average. The criterion for discarding any one superblock was that the fraction of disclosed bits exceeded a value of 0.48 (corresponding to $\sim 8\%$ QBER).

With these parameters, 25% of the superblocks were discarded because of their increased error rate. The remaining 209 kbit of raw key contained $e = 5.85\%$ errors, for the correction of which a total of $n_{\text{dis}} = 79$ kbit (equivalent to 37.7% of the raw bits) were disclosed by the error correction algorithm. Hence, the CASCADE protocol exceeded the Shannon limit for perfect error correction only by a factor of $f(e) = n_{\text{dis}}/n_{\text{sif}} H_2(e) = 1.17$, which is very close to values (1.16) reported in the literature for this error rate [186].

The last important step to a secure key is the privacy amplification of the corrected key in order to limit the maximum information of the perfect eavesdropper. If the reconciled key is shortened by a fraction τ (cf. equation (2.9))

$$n_{\text{fin}} = (1-\tau)\, n_{\text{rec}}\,, \quad \text{where} \tag{6.1}$$

$$\tau := \Delta + \frac{n_{\text{dis}}}{n_{\text{rec}}} + (1-\Delta) H_2\left(\frac{e}{1-\Delta}\right), \tag{6.2}$$

then Eve's expected Shannon information is just one bit on the resulting final key [114]. In equation (6.2), the individual contributions to τ are easy to identify: apart from the fraction of tagged bits Δ, the second and the third terms account for the information revealed during error correction and for the potential information leakage due to the detected qubit error rate e, respectively. Substituting the experimental values $\Delta = 0.252$ and $n_{\text{dis}}/n_{\text{rec}} = 0.377$, and neglecting statistical uncertainties for the moment, we obtain a fraction $1 - \tau = 0.075$, resulting in a secure key of 15.7 kbit. This value corresponds to a secure key rate of $B_{\text{exp}} = 15.8\,\text{bit/s}$ and is valid in the asymptotic limit of infinitely long keys.

However, the limited statistics due to the finite run time of the experiment caused an uncertainty in the determination of the parameters Δ and e, that are relevant for the security of the final key. For example, the error rate e_{meas} observed in the specific realisation of the experiment might — with some small probability p_1 — be smaller than the expected disturbance $\bar{e}$ caused by some given eavesdropping strategy. It is therefore necessary to estimate the average error rate $\bar{e}$ from the measured quantity e_{meas}. Using

a theorem by Hoeffding, one can give a bound [114] on the expected error rate $\bar{e}$ from the observed quantity e_{meas}

$$\bar{e} < e_{\max} = e_{\text{meas}} + \delta e \tag{6.3}$$

with the confidence limit

$$(1 - p_1) > 1 - \exp\left[-2\, n_{\text{rec}} (\delta e)^2\right]. \tag{6.4}$$

Hoeffding's inequality is applicable here, because e_{meas} can be written as the sum of the random variables $e^{(i)}_{\text{meas}}$ describing the error probability for each transmitted pulse. Moreover, since we strive for security against the most general coherent attacks, correlations of the error probabilities $e^{(i)}_{\text{meas}}$ for the individual pulses are possible, which means that the assumptions of a Gaussian probability distribution of e_{meas} would not be justified. Limiting the probability for the expected disturbance $\bar{e}$ to be higher than $e_{\max}$ to $p_1 = 10^{-3}$, leads to $\delta e = 0.004$ for $n_{\text{rec}} = 209\,\text{kbit}$.

Next, we consider the uncertainty associated with the determination of the parameter Δ. Again, the measured gain values Q_0, Q_μ, and $Q_{\mu'}$ allow only the computation of the most likely value of Δ, but there is some finite probability p_2 that the expected $\bar{\Delta}$ is actually higher than Δ_{meas} for the attack chosen by Eve. In turn, this implies that the fraction of tagged bits (which are supposed to be known to the eavesdropper at no cost of induced errors), are underestimated with probability p_2. The statistical effect due to fluctuations of the count rates recorded by Bob were accounted for by Gaussian error propagation, see §2.6.3. Assuming Gaussian probability distributions is justified in this case, because an attack on the photon number degree-of-freedom is always an individual attack: The eavesdropper is assumed to learn the photon number of each transmitted pulse via quantum non-demolition measurements without disturbing the state anyway. Having full information on the photon number without the cost of induced perturbations, there is no advantage of doing this measurement coherently over many pulses.

Choosing a probability for $\bar{\Delta}$ to be larger than some $\Delta_{\max} = \Delta_{\text{meas}} + \delta\Delta$ of $p_2 = 10^{-3}$, results in a confidence interval $\delta\Delta$ of 3.3 standard deviations. For a total number of $N \sim 1 \cdot 10^{10}$ transmitted pulses, we obtained $\delta\Delta = 0.0035$. To account for the increased uncertainty for the security of the final key due to limited statistics, we substituted all occurrences of Δ by $\Delta + \delta\Delta$, and used $e_{\max}$ instead of e in the last term of the privacy amplification formula (6.2). Note that this has no impact on the error correction term of equation (6.2), since all corrected errors and disclosed bits are counted during the error correction phase. Therefore, there is no risk of underestimating the amount of bits revealed during error correction. For the specific choice of security parameters p_1, p_2, the privacy amplification parameter increased to $\tau = 1 - 0.03$, reducing the key rate to 6.3 bit/s. Figure 6.5 summarises the entire process of key generation and illustrates the individual steps, that reduce the raw key to the final secure key.

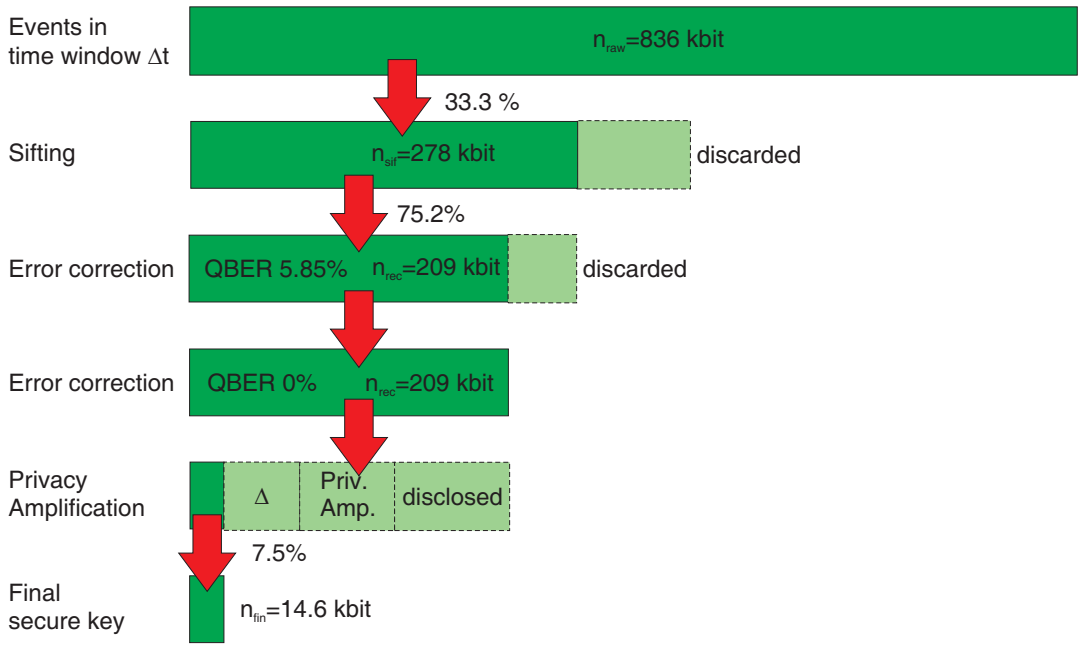

Figure 6.5: Distillation of the secure key, asymptotic values for the QKD experiment with 4-channel Alice.

6.2 Key exchange with 8-channel Alice

For the measurement campaign of September 2006, the 4-channel Alice module was replaced by an 8-channel version with improved electronics. With two laserdiodes available for each of the four distinct polarisation states of the BB84 protocol, it was possible to use separate diodes for the generation of signal pulses (intensity μ) and bright decoy pulses (increased intensity μ'). Running in principle the same decoy-state protocol (two non-zero intensities and vacuum states) as before, this allowed now to optimise the pulse intensities for signal and bright decoy pulses independently of each other. Furthermore, both pulse classes can be used for key generation.

Apart from these changes on the transmitter module, the experimental setup was identical to the one used in the previous campaign. Unless noted otherwise, experimental parameters and details were the same as described in the preceeding section.

6.2.1 Parameter optimisation

Compared to the 4-channel Alice version, the number of freely adjustable parameters increases to 4 with the 8-channel Alice: Both the signal pulse intensity μ and the bright decoy pulse intensity μ', as well as the fractions of signal, bright decoy, and vacuum pulses, (n_s, n', and n_0, respectively) need to be optimised for maximum key generation rate. As before, this was done numerically, using a linear model for the channel transmission and taking into account the statistical effects of finite key length.

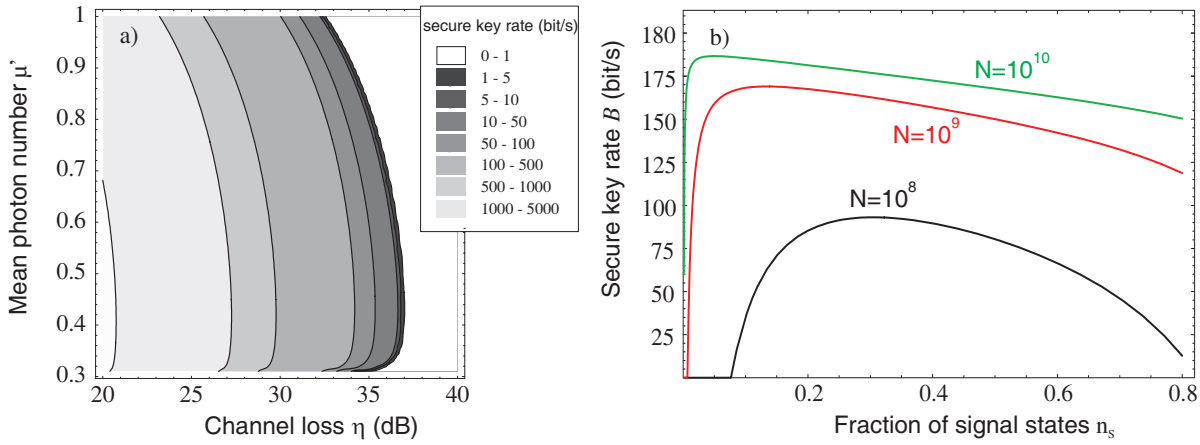

Figure 6.6: Parameter optimisation for the 8-channel Alice. **(a)** Expected secure key rate as a function of channel loss η and mean photon number of bright decoy pulses μ' for fixed $\mu = 0.3$ and $N = 10^9$. **(b)** Expected secure key rate as a function of the fraction of the signal pulses n_s for different total numbers of emitted pulses N. Plotted for $\eta = 33\,\mathrm{dB}$ and $n' = 1 - n_s - 0.016$.

A good choice for μ had already been found in the previous simulations for the 4-channel Alice with $\mu = 0.3$. Starting from this value, and substituting the additional parameters for the dark count probability $Y_0 = 6 \cdot 10^{-6}$, efficiency of the error correction algorithm $f(e) = 1.22$, pulse repetition frequency $\nu = 10\,\mathrm{MHz}$, and technical error $e_{\mathrm{tech}} = 0.02$, results in an expected key generation rate B according to Figure 6.6a. There, B was calculated as a function of channel loss η and the bright decoy pulse intensity μ'. A value of $\mu' = 0.4$ is a good choice for a wide range of channel transmittance.

As before, the best choice of the fraction of decoy pulses n', n_0 heavily depends on the total number of transmitted pulses N. Figure 6.6b shows the expected secure key rate as a function of the fraction of signal pulses n_s for QKD sessions of 10 s, 100 s, and 1000 s duration and a channel loss $\eta = 33\,\mathrm{dB}$. For the plotted curves the remaining clock cycles were assumed to be taken up by pulses of intensity μ', less a small fraction $n_0 = 0.016$ of empty pulses. Mostly for practical reasons, and since the dependency of B on n_s is relatively weak for large N, n_s and n' were equally set to 49.2%, and a fraction $n_0 = 1.6\%$ assigned to vacuum pulses.

6.2.2 Sifting and secure key generation

The QKD experiment in September was performed under slightly better atmospheric conditions than the experiment of the June campaign. A link efficiency L_{ee} between 26 and 27 dB was measured between the transmitter telescope and the Coudé focus of the receiver, resulting in a count rate of $\sim$ 1800 photoevents per second originating from Alice. Detector dark counts together with captured stray light from the sky accounted for noise of similar strength, $\sim 1800/\mathrm{s}$.

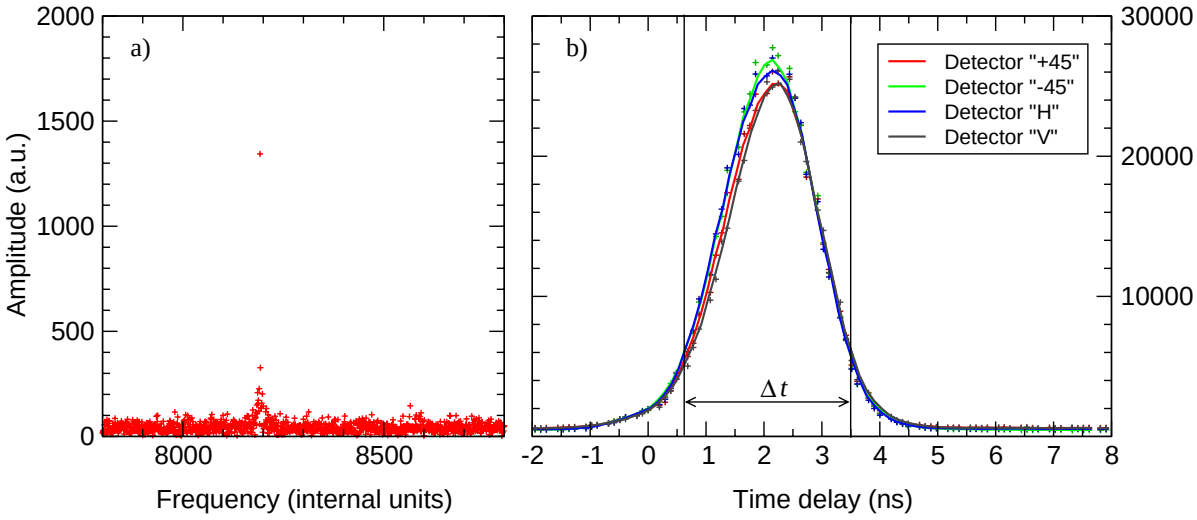

Figure 6.7: Synchronisation of the 8-channel transmitter with the receiver. **(a)** FFT of raw detection events to determine Alice's pulse repetition rate. **(b)** Histogram of photoevent arrival times. Detections within the time window Δt are accepted as originating from Alice.

Synchronisation

Figure 6.7b shows a histogram of photoevent arrival times within the 100 ns period between successive transmitter pulses. The distribution has a FWHM of 1.9 ns, more than a factor of 2 narrower compared to the measurement with the 4-channel Alice (Figure 6.2b). The FFT of the raw event timings (Figure 6.7a) exhibits a sharp peak, indicating a reduced electronic timing jitter than before. The narrow distribution of arrival times allowed the definition of a shorter time window Δt to reject a larger fraction of background events. The trade-off between stronger background suppression (leading to a lower QBER), and a reduced number of synchronised events (i.e., raw key bits) by selecting a small time window Δt is illustrated in Figure 6.8.

In this plot, Δt was varied between 2.3 ns and 5.9 ns. As the time window becomes shorter, more and more background events were rejected, resulting in a QBER as low as 2.41% (blue points). However, when Δt gets shorter than the arrival-time distribution of the transmitted photons, photoevents in the wings of the distribution are unintentionally discarded as background, reducing the number of raw key bits (red points). Together with error correction and privacy amplification (see below), these competing effects led to an optimal time window of $\Delta t = 2.9$ ns, giving the maximum secret key length (black points). With this choice of Δt, around 90% of the detected signal photons lay within the detection time window.

The resulting count rates of signal and background events are depicted in Figure 6.9 over an entire measurement run of 1000 s. The sudden increase of background events at $t = 950$ s was due to the headlights of a passing car, that illuminated the OGS telescope[2].

[2]A straight, 600 m long section of the road *TF-24* runs exactly towards the OGS building such that

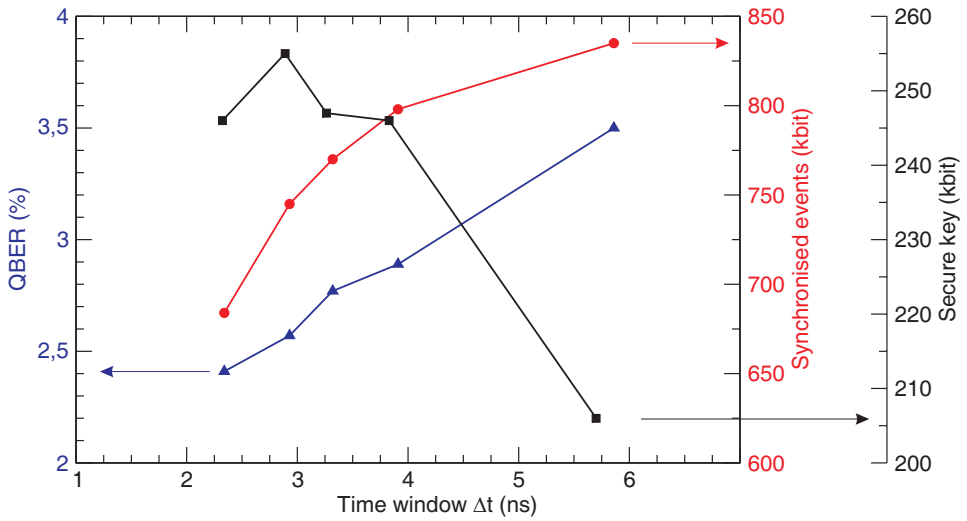

Figure 6.8: Optimisation of the detection time window Δt. The competing effects of minimising the QBER (blue triangles) and maximising the raw key length (red circles) leads to a maximum secure key length (black squares) for $\Delta t = 2.9\,\mathrm{ns}$.

The fact that the background count rate follows to some extent the fluctuations of the signal count rate, reflects the partial rejection of signal events outside the synchronisation time window. Conversely, spurious events contained within Δt contributed with $\sim 1.5\%$ to the quantum bit error rate. Additional contributions to the measured QBER of 2.6% originated from imperfections and alignment errors of the transmitter ($\sim 0.3\%$) and the receiver ($\sim 0.8\%$).

Sifting and post-processing

The synchronisation between Alice and Bob was completed by deriving the absolute photon offset ΔT_{AB} from pseudo-random bit sequences in the photon stream. Despite using the same header lengths as in the previous campaign, this time no frames were discarded because of corrupted headers. This was due to the higher signal-to-noise ratio, and using 4 times brighter synchronisation pulses compared to the June experiment.

Figure 6.10 shows the probability matrix of Bob's detections depending on the polarisation state sent by Alice, normalised to the total number of synchronised photodetections. The ideally expected probabilities for coinciding and orthogonal polarisations are 1/8, and 0, respectively, and 1/16 for complementary bases. The deviations of the measured probabilities from the theory were partly incidental, that is, caused by the limited counting statistics combined with strong fluctuations of the link efficiency. Additional errors arose from systematic effects like unequal efficiency and illumination of the individual single-photon detectors due to the fluctuating beam mode, dark counts,

the interior of the dome is illuminated by the cone of light from car headlights when the dome slit is pointed towards La Palma.

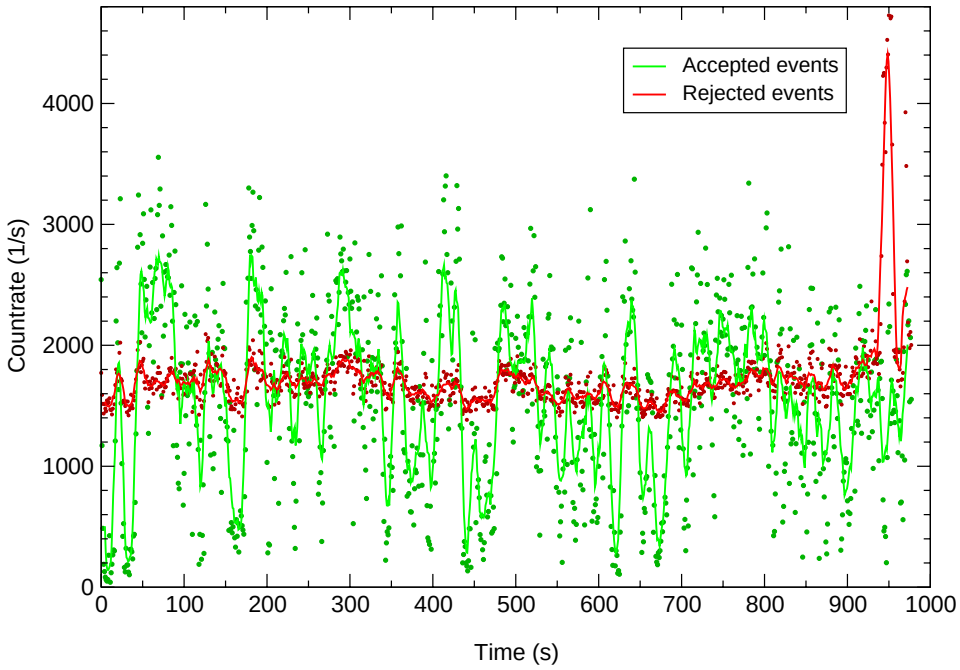

Figure 6.9: Signal (green) and background (red) count rates after applying a detection time window of $\Delta t = 2.9\,\text{ns}$ to the photoevent arrival times. The data points show 1-s averages; the full lines represent a moving average over 10 s.

and drifting signal pulse intensities. These effects led to a bias of the $|H\rangle$ polarisation in the rectilinear basis (1.13 : 1) and of the $|-45\rangle$ polarisation in the diagonal basis (1.26 : 1). It also resulted in a slight deviation of the number of events with coinciding bases (0.487) from the theoretical value of 0.5. Variation of the QBER for the individual polarisations was less pronounced with $e_{\text{H}} = 2.2\%$, $e_{\text{V}} = 3.6\%$, $e_{+45} = 2.7\%$, and $e_{-45} = 3.4\%$. Improved detector alignment and continuous monitoring of the individual signal pulse intensities should help to decrease these effects, which would otherwise have to be taken into account in the privacy amplification.

In total, 745 kbit of sifted key were generated out of $1.53 \cdot 10^6$ synchronised events. Evaluating the count rates for signal, decoy, and vacuum pulses separately, and using equations (2.13) and (2.14), Alice and Bob derived the fractions of tagged bits among the signal pulses $\Delta = 0.275$ and among the bright decoy pulses $\Delta' = 0.338$, in fair agreement with expected values 0.304 and 0.370 for a mean attenuation of 33.5 dB.

To optimise the error correction efficiency for expected error rates in the range of $2 - 3\%$, the number of passes of the CASCADE error correction was reduced to 4, and the block sizes were adapted to $\{30, 64, 128, 256\}$. With these parameters, and an average error rate $e = 2.57\%$ integrated over all superblocks of the sifted key, 19.5% of the sifted key bits were disclosed by the CASCADE algorithm. This is equivalent to an error correction efficiency of $f(e) = 1.13$. Nearly half of the errors were already

removed in pass 1, and almost the entire other half was corrected in pass 2. Although very few errors were left to be corrected in the two remaining passes, these final passes are required to ensure a high probability for an error-free reconciled string. Due to the limited amount of sifted key material, this correction probability could not be quantified precisely. However, no errors in the reconciled strings were found in the course of the experiments.

The privacy amplification step has to be slightly altered to properly take into account the two different values of Δ and Δ'. Effectively, the privacy amplification is applied separately to the key bits n_{rec} originating from signal pulses and the key bits n'_{rec} from bright decoy pulses. Together, the resulting secure key length n_{fin} can be expressed as

$$\begin{aligned} n_{\mathrm{fin}} &= n_{\mathrm{rec}}\left[1-\Delta-(1-\Delta)H_2\left(\frac{e}{1-\Delta}\right)\right] \\ &\quad + n'_{\mathrm{rec}}\left[1-\Delta'-(1-\Delta')H_2\left(\frac{e'}{1-\Delta'}\right)\right] - n_{\mathrm{dis}}. \end{aligned} \tag{6.5}$$

This shortening of the reconciled key ensures that Eve's expected Shannon information on the final key is merely one bit. In the limiting case of an infinitely long key, the measured values $e_{\mathrm{meas}} = 2.57\%$, $\Delta_{\mathrm{meas}} = 0.275$, and $\Delta'_{\mathrm{meas}} = 0.338$ were substituted directly in equation (6.5), reducing the reconciled key to 0.333 of its original length. Hence, the system yielded 253 bit/s of secure key in the asymptotic case. If we consider the statistical effects of a finite key length for the duration of the QKD session of 1000 s,

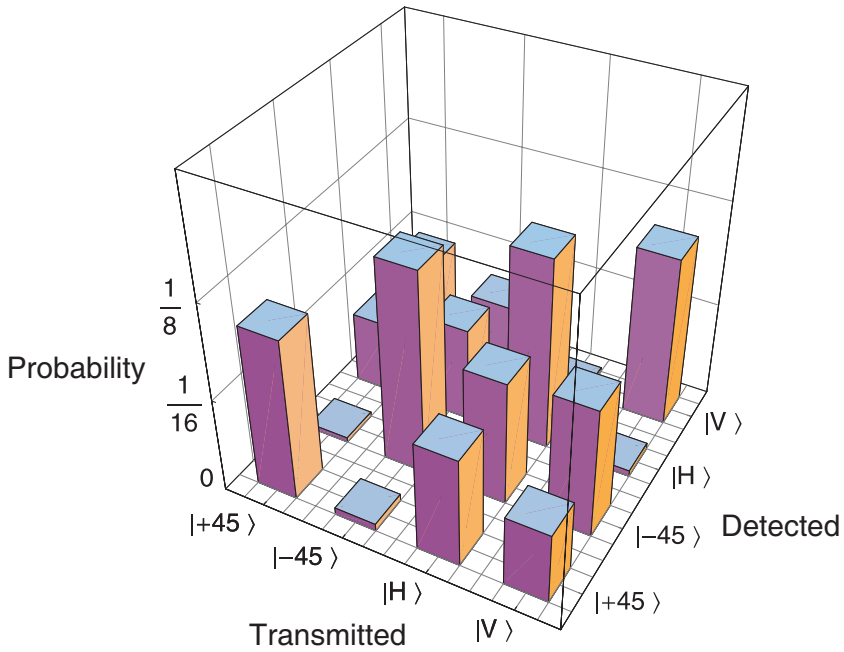

Figure 6.10: Matrix of the relative probabilities of Bob's detections depending on the polarisation transmitted by Alice.

	4-channel Alice Run #1	8-channel Alice Run #2	8-channel Alice Run #3
Channel loss η (dB)	35	33	33
Background (1/s)	2000	1700	1800
Time window Δt (ns)	5.1	2.9	2.9
Background prob. Y_0	$1 \cdot 10^{-5}$	$5 \cdot 10^{-6}$	$5 \cdot 10^{-6}$
Technical error (%)	< 1.0	< 1.0	< 1.0
Raw bits (kbit)	836	1530	1690
Sifted bits (kbit)	209	745	827
QBER (%)	5.85	2.57	2.86
Δ	0.252	0.275	0.317
Δ'	—	0.338	0.388
$n_{\mathrm{dis}}/n_{\mathrm{rec}}$	0.377	0.195	0.210
$f(e)$	1.17	1.13	1.12
$1-\tau$ (asymptotic)	0.075	0.333	0.263
Secure key rate B_{asymp} (bit/s)	15.8	253	222
$1-\tau$ (stat.)	(0.030)	0.285	0.234
Secure key rate B_{stat} (bit/s)	(6.3)	231	197

Table 6.1: Experimental parameters of QKD runs performed during the June and September campaign. The values in brackets refer to a different choice of security parameters (see text).

and choose confidence levels of $1-p_1 = 1-p_2 = 1-10^{-5}$ for underestimating the expected quantities $\bar{e}$, $\bar{\Delta}$, or $\bar{\Delta}'$, we obtained $\delta e = 0.3\%$, $\delta\Delta = 0.024$, and $\delta\Delta' = 0.017$. Replacing the corrected quantities $e_{\mathrm{meas}}+\delta e$, $\Delta_{\mathrm{meas}}+\delta\Delta$, and $\Delta'+\delta\Delta'$ in equation (6.5) results in a secret key rate of 231 bit/s. The level of security achieved with the final key is such that Eve knows less than one bit of the final key with probability smaller than 10^{-5}.

Another experimental run yielded a slightly longer sifted key (827 kbit), but had a little higher QBER of 2.86%, leading to similar secret key rates of 222 bit/s (asymptotic value) and 197 bit/s (incorporating statistics).

6.3 Discussion

Table 6.1 summarises the results of the experimental runs performed with both the 4-channel and the 8-channel Alice module. Although environmental conditions were very similar for the QKD experiments in the June campaign and in the September campaign, the realised asymptotic secure key rates differ by more than one order of magnitude. When incorporating statistical effects, this factor is even larger. The data gathered with the 4-channel transmitter did not allow the generation of a secure key for the choice of security parameters p_1, p_2 used with the 8-channel Alice. This drastic difference

becomes clear when comparing the measured results with the expected key generation rates, calculated for the respective experimental parameters (Figure 6.11).

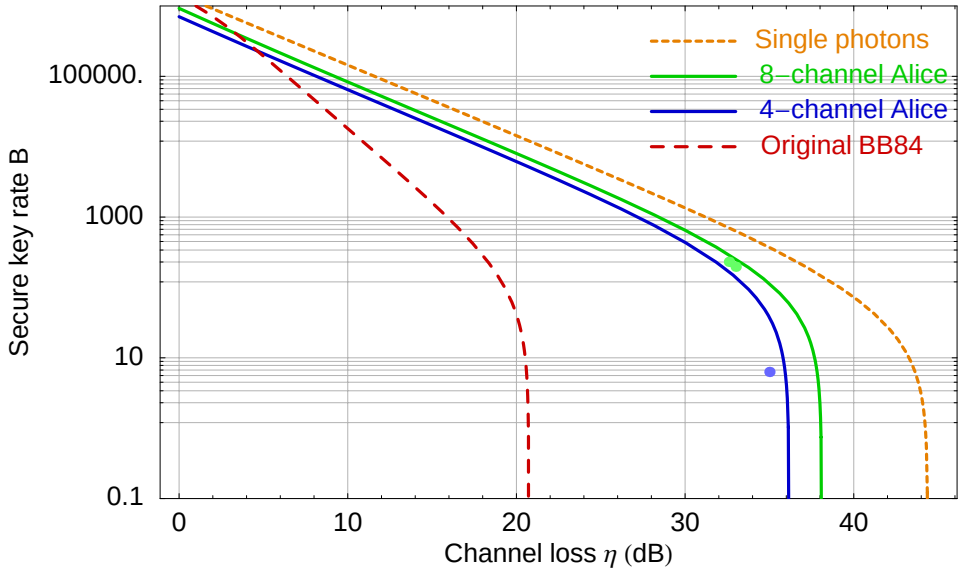

Figure 6.11: Expected secure key rate (full lines), calculated with the respective parameters of Table 6.1. The full circles represent the measured performance of successful QKD runs. With the pure BB84 protocol (long-dashed line), secure QKD is not possible for the given channel losses. The case of an ideal single photon source (short-dashed line) constitutes an upper limit to the performance of an attenuated pulse system.

For medium to low channel losses, the difference between the two transmitter versions is almost negligible. For losses exceeding $\sim$ 30 dB, however, the performance of the 8-channel Alice is substantially better. The experiment with the 4-channel transmitter lay close to the edge beyond which no secure QKD is possible. Especially the use of relatively long gate times (which was dictated by the duration of the weak coherent pulses) limited the suppression of background events. In combination with high channel losses, this led to a considerable contribution to the overall quantum bit error rate. In the privacy amplification, a high QBER has a two-fold impact on the secure key rate, firstly via the bits disclosed by the error correction, and secondly, via the privacy amplification to compensate for Eve's information gain from her error-inducing eavesdropping activity. With the QBER attaining the critical error threshold, the privacy amplification parameter τ approaches unity, and the resulting secure key rate quickly drops to zero.

The improved pulse generation of the 8-channel transmitter enabled a factor of 2 shorter gate times, curbing the influence of background events. Together with slightly lower channel losses and single-diode decoy pulses usable for key generation, the distillable secure key rate increased substantially.

Even with a narrow detection time window, an attenuated pulse system with the

original BB84 protocol does not yield any secure key under the conditions of the inter-island experiment. Without the decoy extension, and for channel losses exceeding 20 dB, the PNS attack allows the eavesdropper to obtain the full key by removing and measuring single photons from all multi-photon pulses without inducing errors. Bridging larger channel losses and distances with an attenuated pulse system is therefore only possible by employing a decoy state protocol. Thus, the decoy technique makes the technologically much simpler attenuated pulse systems again competitive with single photon QKD. Under the conditions of the inter-island experiment, a QKD system using an ideal single photon source with same brightness as our decoy state system would have an expected performance represented by the orange curve in Figure 6.11. For channel losses below $\sim 30\,\mathrm{dB}$, the key generation rates are equal up to a constant factor and scale with η, both in the single photon and the decoy state case. Yet, the maximal tolerable channel attenuation is intrinsically higher for the ideal single photon system than for any decoy state protocol, leading to significanty different key rates for higher attenuation. In practice, however, it may be difficult to realise single photon sources that offer the same brightness as attenuated pulse sources. In fact, when comparing the presented results with a related experiment over the same free-space link, but using a parametric down-conversion source [187], the secure key rate of the attenuated pulse system was a factor of 10–100 higher, depending on the link efficiency.

The presented experiment worked close to the maximal tolerable channel attenuation of our QKD system; the secure key rate is therefore very sensitive to small changes of the channel transmittance. The maximal channel attenuation is a direct consequence of the critical error threshold of the QKD protocol in combination with the fact that the influence of the background-induced QBER increases with channel attenuation. Apart from approaches to decrease the background probability Y_0 (for example by reducing the gate time, or applying narrow-band spectral and spatial filtering of the incoming light), the error tolerance of the QKD protocol can be improved (from 11% to 20%) by employing 2-way classical post-processing schemes [84, 86]. This extends the tolerable channel attenuation accordingly by about 5 dB. Depending on the actual channel transmittance, one can expect a considerable improvement of the secure key rate from 2-way post-processing protocols, and a more stable key rate in the loss regime of our experiment.

7 Conclusion and outlook

This thesis presented the successful distribution of a secret quantum key over a real distance of 144 km in free-space. The optical link was set up at a mean altitude of 2400 m between the Canary Islands of La Palma and Tenerife, taking advantage of the infrastructure of local observatories. The transmitter module was based upon a simple opto-mechanical setup using attenuated laser diode pulses, and a compact 15-cm refractive telescope. Roughly 0.1 % of the transmitted photons were collected by the 1-m mirror telescope of the Optical Ground Station on Tenerife, and directed to the polarisation analyser and single-photon detectors, that had been adapted to the optical system of the Ground Station. Active pointing mechanisms on both the transmitter and the receiver telescopes were employed to compensate for slowly changing atmospheric refraction effects. In this way, it was possible to perform a quantum key exchange with a total quantum bit error ratio (QBER) of 2.56 %. Residual birefringence of single-mode fibres together with imperfect alignment of polarisation components accounted for approximately 1.1 % of the measured error rate; the remaining 1.5 % were due to unfiltered stray light and detector-intrinsic dark count events. Despite the Poissonian nature of the emitted pulses, the secrecy of the resulting quantum key was ensured for a channel attenuation as high as 35 dB thanks to a decoy-state extension of the BB84 protocol. In this way, average secret key rates up to 250 bit/s were achieved.

The presented outdoor experiment exceeds previous distance records of free-space QKD by almost one order of magnitude. In contrast to recent laboratory demonstrations with coiled fibres [17, 20], it was performed under real-life conditions and bridged a real distance between transmitter and receiver, while attaining almost the same length of the quantum channel and achieving comparable or higher secure key rates. This was only possible by employing a decoy-state protocol to check against the disastrous photon-number-splitting attack, which normally opens a backdoor for the eavesdropper in attenuated pulse systems. The effectiveness of the decoy-state method thus restores the competitiveness of the technologically much simpler attenuated pulse systems with single photon schemes.

Still, a significant speed-up of the pulse repetition rate of more than one order of magnitude (with according increase in secret key rate) should easily be possible with state-of-the-art telecommunication technology [188–190]. Stray light still had a significant impact on the QBER in our experiment. A further reduction of the detector gate time would allow to increase the secret key rate and reduce the systems sensitivity to ambient light. This requires faster electronics on both transmitter and receiver side, as well as single-photon detectors with lower timing jitter. Such detectors are available

(or emerging), but usually have their maximum sensitivity in the visible spectral range ($500-600\,\mathrm{nm}$) and a small active area, which can be a problem in the presence of optical turbulence. Narrow-band filtering (below 1 nm FWHM) of the attenuated pulse source would not only improve the indistinguishability of the individual laser diodes, but also allow to apply the same narrow-band filtering to the received photons, thereby further reducing the influence of background. Finally, one might think about increasing the effective channel transmittance by using faster and possibly even higher-order adaptive optics.

In summary, the presented outdoor experiment implicates the feasibility of global quantum key distribution via low-earth-orbit satellites. Satellite pointing, acquisition, and tracking techniques are well established and have been demonstrated with the OGS and between the satellites *ARTEMIS* and *SPOT-4* [191], but would possibly need refinement to the required level of accuracy and speed. Most importantly, our QKD experiment was performed over a channel attenuation very similar to the expected attenuation of a LEO-to-ground link.

A series of recent studies [192–194] assessed potential experimental scenarios and associated technological challenges. The scenario involving the least risk and cost consists of one satellite in low-earth-orbit (LEO), and at least two ground stations. Downlinks tend not to suffer from turbulence induced beam spreading as much as uplinks, since the beam diameter at the top of the atmosphere will typically be larger than the beam spread due to the passage through it (lens speckle effects of the atmosphere neglected). Conversely, an uplink beam undergoes heavy turbulence-induced deflections at the very beginning of its propagation path ("shower curtain effect"). Since satellite-mounted optics is generally restricted in mass and dimension, a large spaceborne receiver telescope to compensate this effect would be just too expensive. For these reasons, a first satellite QKD experiment would comprise of a spaceborne transmitter using a relatively compact optical communication terminal (typically $10-15\,\mathrm{cm}$ diameter) with a two-axis gimbal, and a ground-based receiver capable of tracking the satellite as it passes overhead. Apart from the size of the telescope apertures, additional key factors governing the performance of the optical link are the maximum range and resulting time-of-viewing determined by the orbital height and velocity of the satellite. Assuming a 13.5-cm diameter optical head on the satellite, and a 1-m receiver telescope on ground, the calculated link loss is between 35 (30) dB and 13 dB for elevation angles of the satellite between $5°(10°)$ and $90°$ [192, 195].

The experimental results already laid a foundation for such a future satellite experiment. First steps have been taken to reduce the size, mass, and power consumption of the transmitter module, which is therefore well suitable for integration into a spaceborne quantum communication terminal. Although investigations towards space qualifyability were not attempted, the exposure to changing temperatures and vibrations during field tests and shipping already indicated a certain robustness of the opto-mechanical transmitter design. Furthermore, it was shown that the quantum receiver optics can easily

be integrated into an existing ground station to achieve single photon reception from an orbiting satellite (see also [196]).

The design and the accommodation of a quantum communication transmitter in an existing classical optical communication terminal on board a satellite has already been investigated in a recent study [192,195]. It turns out that major subunits of the classical terminals, such as those for pointing, acquisition and tracking as well as those providing the required electric, thermal, and structural backbone, can be adapted as to meet the quantum communication terminal needs. Yet, establishing and maintaining a quantum-optical link to a fast moving target holds additional challenges.

Due to the extremely low power of the quantum signal channel, additional beacon lasers (well isolated from the signal wavelength) are required to enable fast and precise pointing and tracking. Even small pointing errors lead to a dramatic decrease of link quality owing to the fast roll-off of the Gaussian intensity profile combined with large off-axis scintillations. Apart from that, the satellite motion in combination with the pointing systems results in a relative rotation of the polarisation analysis apparatus on earth and the satellite transmitter around the axis of their connecting line [197]. If a polarisation encoding scheme is employed, this rotation has to be corrected for. Conceivable solutions might be based on a polarisation reference beacon, or on a computational prediction of the rotation angle from accurate knowledge of the satellite's trajectory.

The altitude of a LEO satellite is typically between several hundred and a few thousand kilometres. The International Space Station, for example, flies in a LEO orbit at 350 km altitude. Travelling at about 7 km/s, the period of a LEO satellite is approximately 90 min. Depending on the minimum elevation angle (as seen from the ground station), at which the satellite link can be established, typical link durations are in the range of only a few minutes, with on average just one link opportunity per night [192]. This means that a QKD experiment will face limited raw key lengths, underlining the importance to further investigate the associated implications for security.

To limit the influence of stray light, short detector gate times have to be used, which requires the timing at each end to be synchronised to better than 1 ns. If using the arrival times of the photons (key bits) to drive a software phase-locked-loop (like in the inter-island experiment), a certain key rate is required to allow sufficiently frequent timing adjustments. Alternatively, periodic bright pulses of a different wavelength could be employed to lock the timing. In addition to clock drifts, varying Doppler shifts due to the satellite motion will slowly change the repetition frequency. A compensation can be calculated before the satellite pass from its telemetric data, possibly refined later by fitting the orbit to the observed time-of-flight[1].

Free-space links between earth and space have the potential to realise global-scale quantum key distribution since they allow, in principle, a much larger propagation distance of photonic qubits compared to present ground-based scenarios. Looking into the

[1] e.g., with the Geodyn II (NASA/GSFC) program, see *http://ilrs.gsfc.nasa.gov/*

future, more advanced quantum communication protocols, like quantum dense coding, or quantum secret sharing, may open up more and new applications of quantum-based telecommunications in space.

Publications

Publications related to the presented work:

- *Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km.*
  T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, Ch. Kurtsiefer, J.G. Rarity, A. Zeilinger and H. Weinfurter
  Physical Review Letters **98**, 010504 (2007).

- *Entanglement-based quantum communication over 144 km.*
  R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger
  Nature Physics **3**, 481–486 (2007).

- *Free-space quantum key distribution: Towards a real life application.*
  H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer, and H. Weinfurter
  Fortschritte der Physik **54**, 840–845 (2006).

Bibliography

[1] M. Castells. *The Information Age: Economy, Society, and Culture (3 volumes).* Blackwell, Oxford (1996–1998).

[2] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Wiley, New York (1996).

[3] M. Wiener. Efficient DES key search — an update. *RSA Laboratories' Cryptobyte* **3**, 6 (1997).

[4] R. D. Silverman. A cost-based security analysis of symmetric and asymmetric key lengths. *RSA Laboratories' Bulletin* **13** (2000).

[5] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the AIEE* **45**, 109 (1926).

[6] C. E. Shannon. Communication theory for secrecy systems. *Bell Systems Technical Journal* **28**, 656–715 (1949).

[7] S. Wiesner. Conjugate coding. *Sigact News* **15**, 78–88 (1983).

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

[9] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Reviews of Modern Physics* **74**, 145–195 (2002).

[10] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature* **299**(5886), 802–803 (1982).

[11] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New Journal of Physics* **4**, 41 (2002).

[12] A. Poppe, A. Fedrizzi, R. Ursin, H. Böhm, T. Lörunser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger. Practical quantum key distribution with polarization entangled photons. *Optics Express* **12**, 3865–3871 (2004).

[13] Z. Yuan and A. Shields. Continuous operation of a one-way quantum key distribution system over installed telecom fibre. *Optics Express* **13**, 660–665 (2005).

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

[15] Z. L. Yuan, A. W. Sharpe, and A. J. Shields. Unconditionally secure one-way quantum key distribution using decoy pulses. *Applied Physics Letters* **90**(1), 011118 (2007).

[16] C. Gobby, Z. L. Yuan, and A. J. Shields. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters* **84**(19), 3762–3764 (2004).

[17] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt. Long-distance quantum key distribution in optical fibre. *New Journal of Physics* **8**(9), 193 (2006).

[18] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Physical Review Letters* **98**(1), 010505 (2007).

[19] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt. Long-distance decoy-state quantum key distribution in optical fiber. *Physical Review Letters* **98**(1), 010503 (2007).

[20] H. Takesue, S. Nam, Q. Zhang, R. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto. Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nature Photonics* **1**, 343–348 (2007).

[21] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Physical Review Letters* **81**(26), 5932–5935 (1998).

[22] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413–418 (2001).

[23] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. Practical free-space quantum key distribution over 1 km. *Physical Review Letters* **81**(15), 3283–3286 (1998).

[24] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson. Daylight quantum key distribution over 1.6 km. *Physical Review Letters* **84**(24), 5652–5655 (2000).

[25] J. E. Nordholt, R. J. Hughes, J. R. Morgan, C. G. Peterson, and C. C. Wipf. Present and future free-space quantum key distribution. *Proceedings of SPIE* **4635**, 116–126 (2002).

[26] J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight. Ground to satellite secure key exchange using quantum cryptography. *New Journal of Physics* **4**, 82.1–82.21 (2002).

[27] M. Aspelmeyer, T. Jennewein, M.Pfennigbauer, W. Leeb, and A. Zeilinger. Long-distance quantum communication with entangled photons using satellites. *IEEE Journal of Selected Topics in Quantum Electronics* **9**, 1541–1551 (2003).

[28] A. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters* **67**, 661–663 (1991).

[29] C. Bennett, G. Brassard, and N. Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters* **68**(5), 557–559 (1992).

[30] A. K. Ekert, J. G. Rarity, P. R. Tapster, and M. G. Palma. Practical quantum cryptography based on two-photon interferometry. *Physical Review Letters* **69**(9), 1293–1295 (1992).

[31] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Physical Review Letters* **82**(12), 2594–2597 (1999).

[32] E. Waks, A. Zeevi, and Y. Yamamoto. Security of quantum key distribution with entangled photons against individual attacks. *Physical Review A* **65**, 052310 (2002).

[33] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger. Quantum cryptography with entangled photons. *Physical Review Letters* **84**(20), 4729–4732 (2000).

[34] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat. Entangled state quantum cryptography: Eavesdropping on the Ekert protocol. *Physical Review Letters* **84**(20), 4733–4736 (2000).

[35] G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden. Long-distance entanglement-based quantum key distribution. *Physical Review A* **63**(1), 012309 (2000).

[36] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time Bell states. *Physical Review Letters* **84**(20), 4737–4740 (2000).

[37] C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan. Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication. *Physical Review Letters* **94**(15), 150501 (2005).

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

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

[40] K. Resch, M. Lindenthal, B. Blauensteiner, H. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger. Distributing entanglement and single photons through an intra-city, free-space quantum channel. *Optics Express* **13**, 202–209 (2005).

[41] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer. Free-space quantum key distribution with entangled photons. *Applied Physics Letters* **89**, 101122 (2006).

[42] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier. Single photon quantum cryptography. *Physical Review Letters* **89**, 187901 (2002).

[43] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G. Solomon, and Y. Yamamoto. Secure communicationquantum cryptography with a photon turnstile. *Nature* **420**, 762 (2002).

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

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

[46] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. Limitations on practical quantum cryptography. *Physical Review Letters* **85**, 1330–1333 (2000).

[47] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A* **61**, 052304 (2000).

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

[49] X. B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters* **94**(23), 230503 (2005).

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

[51] T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters* **98**(1), 010504 (2007).

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

[53] L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences* **18**, 143–154 (1979).

[54] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory* **41**, 1915 (1995).

[55] C. H. Bennett, T. Mor, and J. A. Smolin. The parity bit in quantum cryptography. *Physical Review A* **54**, 2675–2684 (1996).

[56] R. Renner. *Security of Quantum Key Distribution.* Ph.D. thesis, Eidgenössische Technische Hochschule Zürich (2005).

[57] N. Lütkenhaus. Security against eavesdropping in quantum cryptography. *Physical Review A* **54**, 97–111 (1996).

[58] N. Gisin and B. Huttner. Quantum cloning, eavesdropping and Bell's inequality. *Physics Letters A* **228**, 13–21 (1997).

[59] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres. Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. *Physical Review A* **56**, 1163–1172 (1997).

[60] R. B. Griffiths and C.-S. Niu. Optimal eavesdropping in quantum cryptography. II. A quantum circuit. *Physical Review A* **56**, 1173–1176 (1997).

[61] T. Kim, I. Stork genannt Wersborg, F. N. C. Wong, and J. H. Shapiro. Complete physical simulation of the entangling-probe attack on the Bennett-Brassard 1984 protocol. *Physical Review A* **75**(4), 042327 (2007).

[62] V. Scarani, A. Acín, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulses implementations. *Physical Review Letters* **92**, 057901 (2004).

[63] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters* **68**, 3121–3124 (1992).

[64] M. Dusek, M. Jahma, and N. Lütkenhaus. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Physical Review A* **62**, 022306 (2000).

[65] K. Tamaki, M. Koashi, and N. Imoto. Security of the Bennett 1992 quantum-key distribution protocol against individual attack over a realistic channel. *Physical Review A* **67**, 032310 (2003).

[66] M. Koashi. Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Physical Review Letters* **93**, 120501 (2004).

[67] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters* **81**(14), 3018–3021 (1998).

[68] H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography. *Physical Review A* **59**, 4238 (1999).

[69] H.-K. Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology* **18**, 133–165 (2005).

[70] K. Tamaki and H.-K. Lo. Unconditionally secure key distillation from multiphotons. *Physical Review A* **73**, 010302(R) (2006).

[71] A. Chefles. Unambiguous discrimination between linearly dependent states with multiple copies. *arXiv e-prints* quant–ph/0105016 (2001).

[72] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In: *Advances in Cryptology — Proceedings of Crypto '96*, volume 1109 of *Lecture Notes in Computer Science*, 343–357. (Springer, Berlin) (1996).

[73] D. Mayers. Unconditional security in quantum cryptography. *J. Assn. Comput. Mac.* **48**, 351 (2001).

[74] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**(5410), 2050–2056 (1999).

[75] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters* **85**, 441–444 (2000).

[76] K. Tamaki, M. Koashi, and N. Imoto. Unconditionally secure key distribution based on two nonorthogonal states. *Physical Review Letters* **90**(16), 167904 (2003).

[77] H. K. Lo. Proof of unconditional security of sixstate quantum key distribution scheme. *Quantum Information & Computation* **1**, 81–94 (2001).

[78] M. Christandl, R. Renner, and A. Ekert. A generic security proof for quantum key distribution. *arXiv e-prints* quant–ph/0402131 (2004).

[79] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A* **72**, 012332 (2005).

[80] B. Kraus, N. Gisin, and R. Renner. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Physical Review Letters* **95**, 080501 (2005).

[81] D. Gottesman and H.-K. Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory* **49**, 457 (2003).

[82] H. F. Chau. Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate. *Physical Review A* **66**(6), 060302 (2002).

[83] B. Kraus, C. Branciard, and R. Renner. Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses. *Physical Review A* **75**(1), 012316 (2007).

[84] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo. Decoy-state quantum key distribution with two-way classical postprocessing. *Physical Review A* **74**(3), 032330 (2006).

[85] K. G. H. Vollbrecht and F. Verstraete. Interpolation of recurrence and hashing entanglement distillation protocols. *Physical Review A* **71**, 062325 (2005).

[86] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano. Key rate of quantum key distribution with hashed two-way classical communication. *Physical Review A* **76**(3), 032312 (2007).

[87] H.-K. Lo. Method for decoupling error correction from privacy amplification. *New Journal of Physics* **5**, 36.1–36.24 (2003).

[88] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *arXiv e-prints* quant–ph/0107017 (2001).

[89] D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quantum Information and Computation* **4**(5), 325–360 (2004).

[90] N. Lütkenhaus and M. Jahma. Quantum key distribution with realistic states: photon number statistics in the photon number splitting attack. *New Journal of Physics* **4**, 44 (2002).

[91] G. Nogues, A. Rauschenbeutel, S. Osnaghi, M. Brune, J. M. Raimond, and S. Haroche. Seeing a single photon without destroying it. *Nature* **400**(6741), 239–242 (1999).

[92] J. Calsamiglia, S. Barnett, and N. Lütkenhaus. Conditional beam splitting attack on quantum key distribution. *Physical Review A* **65**, 012312 (2002).

[93] C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter. The breakdown flash of silicon avalanche photodiodes — backdoor for eavesdropper attacks? *Journal of Modern Optics* **48**, 2039–2047 (2001).

[94] A. Lamas-Linares and C. Kurtsiefer. Breaking a quantum key distribution system through a timing side channel. *arXiv e-prints* quant–ph/0704.3297 (2007).

[95] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A* **73**(2), 022320 (2006).

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

[97] V. Makarov and J. Skaar. Faked states attack using detector efficiency mismatch on SARG04, phase-time, DPSK, and Ekert protocols. *arXiv e-prints* quant–ph/0702262 (2007).

[98] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo. Experimental demonstration of time-shift attack against practical quantum key distribution systems. *arXiv e-prints* quant–ph/0704.3253 (2007).

[99] X. Ma. Security of quantum key distribution with realistic devices. *arXiv e-prints* quant–ph/0503057 (2005).

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

[101] X. B. Wang. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Physical Review A* **72**(1), 012322 (2005).

[102] H.-K. Lo. Getting something out of nothing. *arXiv e-prints* quant–ph/0503004 (2005).

[103] J.-C. Boileau, J. Batuwantudawe, and R. Laflamme. Higher-security thresholds for quantum key distribution by improved analysis of dark counts. *Physical Review A* **72**(3), 032321 (2005).

[104] M. Koashi. Efficient quantum key distribution with practical sources and detectors. *arXiv e-prints* quant–ph/0609180 (2006).

[105] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt. Enhancing practical security of quantum key distribution with a few decoy states. *arXiv e-prints* quant–ph/0503002 (2005).

[106] X.-B. Wang. A review on the decoy-state method for practical quantum key distribution. *arXiv e-prints* quant–ph/0509084 (2005).

[107] X.-B. Wang. Decoy-state quantum key distribution with large random errors of light intensity. *Physical Review A* **75**, 052301 (2007).

[108] M. Hayashi. Practical evaluation of security for quantum key distribution. *Physical Review A* **74**, 022307 (2006).

[109] M. Hayashi. Upper bounds of eavesdropper's performances in finite-length code with decoy method. *arXiv e-prints* quant–ph/0702250 (2007).

[110] V. Scarani. *Private communication* (2007).

[111] J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka, and A. Tomita. Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics. *arXiv e-prints* quant–ph/0705.3081 (2007).

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

[113] V. Scarani and R. Renner. Quantum cryptography with finite resources. *arXiv e-prints* quant–ph/0708.0709 (2007).

[114] N. Lütkenhaus. Estimates for practical quantum cryptography. *Physical Review A* **59**, 3301–3319 (1999).

[115] P. Grönberg. Key reconciliation in quantum key distribution. Technical report, Sensor Technology, Swedish Defence Research Agency, Linköping (2005).

[116] G. Brassard and L. Salvail. Secret key reconciliation by public discussion. *Advances in Cryptology—EUROCRYPT'93, Lecture Notes in Computer Science* **2119**, 260–273 (1994).

[117] R. G. Gallager. Low-density parity-check codes. *IRE Transactions on Information Theory* **IT-8**, 21–28 (1962).

[118] D. Pearson. High-speed QKD reconciliation using forward error correction. In: *The 7th International Conference on Quantum Communications, Measurement, and Computing*, 299–302 (2004).

[119] C. H. Bennett, G. Brassard, and J.-M. Robert. Privacy amplification by public discussion. *SIAM J. Comput.* **17**, 210–229 (1988).

[120] A. Yariv. *Quantum electronics*. Wiley, New York (1989).

[121] D. K. Killinger, J. H. Churnside, and L. S. Rothman. *Atmospheric Optics, OSA Handbook of Optics, Chapter 44*. McGraw-Hill (1995).

[122] G. P. Anderson, F. X. Kneizys, J. H. Chetwynd, J. Wang, M. L. Hoke, L. S. Rothman, L. M. Kimball, and R. A. McClatchey. FASCODE/MODTRAN/LOWTRAN: Past/present/future. In: *18th Annual review conference on atmospheric transmission models* (1995).

[123] J. A. Curcio, L. F. Drummeter, and G. L. Knestrick. An atlas of the absorption spectrum of the lower atmosphere from 5400Å to 8520Å. *Applied Optics* **3**, 1401–1409 (1964).

[124] D. H. Höhn. Depolarization of a laser beam at 6328Å due to atmospheric transmission. *Applied Optics* **8**, 367–369 (1969).

[125] J. N. Bradford and J. W. Tucker. A sensitive system for measuring atmospheric depolarization of light. *Applied Optics* **8**, 645–647 (1969).

[126] A. N. Kolmogorov. The local structure of turbulence in an incompressible viscous fluid for very large Reynolds numbers. *C. R. (Doki) Acad. Sci. U.S.S.R.* **30**, 301–305 (1941).

[127] L. C. Andrews and R. L. Phillips. *Laser beam propagation through random media*. Bellingham, Wash.: SPIE Optical Engineering Press (1998).

[128] R. J. Hill and G. R. Ochs. Inner-scale dependence of scintillation variances measured in weak scintillation. *Journal of the Optical Society of America A* **9**, 1406–1411 (1992).

[129] R. Beland. *The Infrared and Electro-optical Systems Handbook, Vol.2 – Atmospheric Propagation of Radiation*, chapter "Propagation through Atmospheric Optical Turbulence", 212–232. SPIE Optical Engineering Press, Bellingham (1993).

[130] J. H. Churnside and R. J. Lataitis. Wander of an optical beam in the turbulent atmosphere. *Applied Optics* **29**, 926 (1990).

[131] L. C. Andrews. *Field guide to atmospheric optics*. Bellingham, Wash.: SPIE Optical Engineering Press (2004).

[132] R. L. Fante. Electromagnetic beam propagation in turbulent media. *Proceedings of the IEEE* **63**, 1669–1692 (1975).

[133] D. L. Fried. Optical resolution through a randomly inhomogeneously medium. *Journal of the Optical Society of America* **56**, 1372 (1966).

[134] C. H. Liu and K. C. Yeh. Pulse spreading and wandering in random media. *Radio Science* **14**, 925–931 (1979).

[135] D. P. Greenwood and D. O. Tarazano. A proposed form for the atmospheric microtemperature spatial spectrum in the input range. Technical report, RADC-TR-74-19 (1974).

[136] C. S. Gardner. Effects of random path fluctuations on the accuracy of laser ranging systems. *Applied Optics* **15**, 2539–2545 (1976).

[137] L. Kral, I. Prochazka, and K. Hamal. Optical signal path delay fluctuations caused by atmospheric turbulence. *Optics Letters* **30**, 1767–1769 (2005).

[138] C. H. Liu and K. C. Yeh. Propagation of pulsed beam waves through turbulence, cloud, rain, or fog. *Journal of the Optical Society of America* **67**, 1261 (1977).

[139] P. W. Millonni, J. H. Carter, C. G. Peterson, and R. J. Hughes. Effects of propagation through atmospheric turbulence on photon statistics. *Journal of Optics B* **6**, 742–745 (2004).

[140] G. P. Berman and A. A. Chumak. The effects of partial coherence on the statistics of single-photon pulses propagating in the atmoshere. *arXiv e-prints* quant–ph/0702238 (2007).

[141] A. Comerón, J. A. Rubio, and A. Belmonte. ASTC inter-island measurement campaign final report. Technical report, Technical University of Catalonia (1996).

[142] L. Eltermann. UV, visible, and IR attenuation for altitudes to 50 km. *Environmental Research Papers* **285**, AFCRL–68–0153 (1968).

[143] R. K. Tyson. *Principles of Adaptive Optics*. Academic Press, Boston (1998).

[144] T. Weyrauch and M. A. Vorontsov. Free-space laser communications with adaptive optics: Atmospheric compensation experiments. In: *Journal of Optical and Fiber Communications Reports*. Springer Science + Business Media Inc. (2004).

[145] J. Shapiro. Reciprocity of the turbulent atmosphere. *Journal of the Optical Society of America* **61**, 492–495 (1971).

[146] J. Shapiro. Optimal power transfer through atmospheric turbulence using state knowledge. *IEEE Transactions on Communications Technology* **19**, 410–414 (1971).

[147] T. Scheidl. *Methoden für Free-Space Quantenkommunikationsexperimente*. Master's thesis, Institut für Experimentalphysik der Universität Wien (2005).

[148] J. W. Hardy, J. E. Lefebvre, and C. L. Koliopoulos. Real-time atmospheric compensation. *Journal of the Optical Society of America* **67**, 360–369 (1976).

[149] F. Roddier. *Adaptive Optics in Astronomy*. Cambridge University Press, UK (1999).

[150] B. M. Levine, E. A. Martinsen, A. Wirth, A. Jankevics, M. Toledo-Quinones, F. Landers, and T. L. Bruno. Horizontal line-of-sight turbulence over near-ground paths and implications for adaptive optics corrections in laser communications. *Applied Optics* **37**, 4553–4560 (1998).

[151] R. J. Noll. Zernike polynomials and atmospheric turbulence. *Journal of the Optical Society of America* **66**, 207–211 (1976).

[152] C. A. Primmerman, T. R. Price, R. A. Humphreys, B. G. Zollars, H. T. Barclay, and J. Herrmann. Atmospheric-compensation experiments in strong-scintillation conditions. *Applied Optics* **34**, 2081–2088 (1995).

[153] R. K. Tyson. Bit-error rate for free-space adaptive optics laser communications. *Journal of the Optical Society of America A* **19**, 753–758 (2002).

[154] R. K. Tyson and D. E. Canning. Indirect measurement of a laser communications bit-error-rate reduction with low-order adaptive optics. *Applied Optics* **42**, 4239–4243 (2003).

[155] M. C. Roggemann and D. J. Lee. Two-deformable-mirror concept for correcting scintillation effects in laser beam projection through the turbulent atmosphere. *Applied Optics* **37**, 4577–4585 (1998).

[156] J. D. Barchers and B. L. Ellerbroek. Improved compensation of turbulence-induced amplitude and phase distortions by means of multiple near-field phase adjustments. *Journal of the Optical Society of America A* **18**, 399–411 (2001).

[157] J. D. Barchers. Closed-loop stable control of two deformable mirrors for compensation of amplitude and phase fluctuations. *Journal of the Optical Society of America A* **19**, 926–944 (2002).

[158] D. L. Fried. Branch point problem in adaptive optics. *Journal of the Optical Society of America A* **15**, 2759–2768 (1998).

[159] T. Weyrauch, M. A. Vorontsov, T. G. Bifano, J. A. Hammer, M. Cohen, and G. Cauwenberghs. Microscale adaptive optics: wave-front control with a μ-mirror array and a VLSI stochastic gradient descent controller. *Applied Optics* **40**, 4243–4253 (2001).

[160] T. Weyrauch and M. A. Vorontsov. Dynamic wave-front distortion compensation with a 134-control-channel submillisecond adaptive system. *Optics Letters* **27**, 751–753 (2002).

[161] J. D. Barchers. Optimal control of laser beams for propagation through a turbulent medium. *Journal of the Optical Society of America A* **19**, 1779–1793 (2002).

[162] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments* **71**, 1675–1680 (2000).

[163] M. Stipčević and B. Rogina. Quantum random number generator. *arXiv e-prints* quant–ph/0609043 (2006).

[164] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro. Secure self-calibrating quantum random-bit generator. *Physical Review A* **75**(3), 032334 (2007).

[165] kindly provided by QinetiQ (http://www.qinetiq.com).

[166] Z. Sodnik, J. Perdigues, and R. Czichy. *Design Data Summary of the ESA Optical Ground Station for In-Orbit Check-Out of Laser Communication Payloads and for the Observation and Registration of Space Debris.* ESA/ESTEC Mechanical Systems Division, xa95/267/zs edition (2000).

[167] J. Rarity and P. Tapster. "cryptographic receiver". European Patent EP 722640 B1 (1998).

[168] J. G. Rarity, P. C. R. Owens, and P. R. Tapster. Quantum random-number generation and key sharing. *Journal of Modern Optics* **41**, 2435–2444 (1994).

[169] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa. Avalanche photodiodes and quenching circuits for single-photon detection. *Applied Optics* **35**(12) (1996).

[170] R. G. W. Brown, K. D. Ridley, and J. G. Rarity. Characterization of silicon avalanche photodiodes for photon correlation measurements. 1: Passive quenching. *Applied Optics* **25**(22) (1986).

[171] R. G. W. Brown, K. D. Ridley, and J. G. Rarity. Characterization of silicon avalanche photodiodes for photon correlation measurements. 2: Active quenching. *Applied Optics* **25**(22) (1986).

[172] M. Kaminska. *Efficiency measurement and timing jitter measurement of APDs with downconverted photons.* Master's thesis, Ludwig-Maximilians-Universität München (2007).

[173] Silicon avalanche photodiodes C30902E, C30902S, C30921E, C30921S. Datasheet, PerkinElmer Optoelectronics (2001).

[174] H. Dautet, P. Deschamps, B. Dion, A. D. MacGregor, M. D., R. J. McIntyre, C. Trottier, and P. P. Webb. Photon counting techniques with silicon avalanche photodiodes. *Applied Optics* **32**(21) (1993).

[175] A. Lacaita, M. Ghioni, F. Zappa, G. Ripamonti, and S. Cova. Recent advances in the detection of photons with silicon photodiodes. *Nuclear Instruments and Methods A* **326**, 290–294 (1993).

[176] T. E. Ingerson, R. J. Kearney, and R. L. Coulter. Photon counting with photodiodes. *Applied Optics* **22**(13) (1983).

[177] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih. New high-intensity source of polarization-entangled photon pairs. *Physical Review Letters* **75**(24), 4337–4341 (1995).

[178] J. G. Rarity, K. D. Ridley, and P. R. Tapster. Absolute measurement of detector quantum efficiency using parametric downconversion. *Applied Optics* **26**(21), 4616 (1987).

[179] A. L. Migdall. Absolute quantum efficiency measurements using correlated photons: toward a measurement protocol. *IEEE Transactions on Instrumentation and Measurement* **50**(2) (2001).

[180] A. Migdall, S. Castelletto, I. P. Degiovanni, and R. M. L. Intercomparison of a correlated-photon-based method to measure detector quantum efficiency. *Applied Optics* **41**(15) (2002).

[181] M. Ware and A. Migdall. Single-photon detector characterization using correlated photons: the march from feasibility to metrology. *Journal of Modern Optics* **51** (2004).

[182] C. K. Hong and L. Mandel. Theory of parametric frequency down conversion of light. *Physical Review A* **31**, 2409 (1985).

[183] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters* **59**, 2044 (1987).

[184] H. Weier. *Experimental Quantum Cryptography*. Master's thesis, Technische Universität München (2003).

[185] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer, and H. Weinfurter. Free space quantum key distribution: Towards a real life application. *Fortschritte der Physik* **54**, 840–845 (2006).

[186] S. Liu. *Information-theoretic secret key agreement*. Ph.D. thesis, Technische Universiteit Eindhoven (2002).

[187] 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, and A. Zeilinger. Entanglement-based quantum communication over 144 km. *Nature Physics* **3**(7), 481–486 (2007).

[188] J. Bienfang, A. Gross, A. Mink, B. Hershman, A. Nakassis, X. Tang, R. Lu, D. Su, C. Clark, C. Williams, E. Hagley, and J. Wen. Quantum key distribution with 1.25 Gbps clock synchronization. *Optics Express* **12**, 2011–2016 (2004).

[189] K. Gordon, V. Fernandez, P. Townsend, and G. Buller. A short wavelength GigaHertz clocked fiber-optic quantum key distribution system. *IEEE Journal of Quantum Electronics* **40**, 900–908 (2004).

[190] K. Gordon, V. Fernandez, G. Buller, I. Rech, S. Cova, and T. P. Quantum key distribution system clocked at 2 GHz. *Optics Express* **13**, 3015–3020 (2005).

[191] T. Tolker-Nielsen and G. Oppenhauser. In-orbit test result of an operational optical intersatellite link between ARTEMIS and SPOT4, SILEX. *Proceedings of SPIE* **4635**, 1–15 (2002).

[192] M. Pfennigbauer, W. R. Leeb, G. Neckamm, M. Aspelmeyer, T. Jennewein, F. Tiefenbacher, A. Zeilinger, G. Baister, K. Kudielka, T. Dreischer, and H. Weinfurter. Accommodation of a quantum communication transceiver in an optical terminal (ACCOM): Final report. Technical report, European Space Agency Contract Report, ESTEC, Contract 17766/03/NL/PM (2005).

[193] M. Aspelmeyer, H. R. Böhm, C. Brukner, R. Kaltenbaek, M. Lindenthal, J. Petschinka, T. Jennewein, R. Ursin, P. Walther, A. Zeilinger, M. Pfennigbauer, and W. R. Leeb. Quantum communications in space ("QSpace"): Final report. Technical report, European Space Agency Contract Report, ESTEC, Contract No. 16358/02/NL/SFe (2003).

[194] H. Weinfurter, T. Schmitt-Manderbach, G. Baister, G. P. Guizzo, F. Heine, C. Barbieri, F. Tamburini, P. Villoresi, I. Capraro, T. Occhipinti, and G. Bianco. QIPS:

Quantum information and quantum physics in space. technical note 1: Preliminary design of a mid-term experiment. Technical report, European Space Agency Contract Report, ESTEC, Contract 18805/04/NL/HE (2007).

[195] M. Pfennigbauer, M. Aspelmeyer, W. Leeb, G. Baister, T. Dreischer, T. Jennewein, G. Neckamm, J. Perdigues, H. Weinfurter, and A. Zeilinger. Satellite-based quantum communication terminal employing state-of-the-art technology. *Journal of Optical Networking* **4**, 549–560 (2005).

[196] P. Villoresi, F. Tamburini, M. Aspelmeyer, T. Jennewein, R. Ursin, C. Pernechele, G. Bianco, A. Zeilinger, and C. Barbieri. Space-to-ground quantum-communication using an optical ground station: a feasibility study. In: *SPIE Proceedings on Quantum Communications and Quantum Imaging* (2004).

[197] C. Bonato, M. Aspelmeyer, T. Jennewein, C. Pernechele, P. Villoresi, and A. Zeilinger. Influence of satellite motion on polarization qubits in a space-earth quantum communication link. *Optics Express* **14**, 10050–10059 (2006).

Danksagung

Zum Schluß möchte ich mich herzlich bei den vielen Menschen bedanken, die zum Gelingen dieser Arbeit beigetragen haben:

Meinem Doktorvater Prof. Harald Weinfurter für die freundliche Aufnahme in die Arbeitsgruppe, seine stets offene Tür für Fragen und Probleme, und vor allem für die Möglichkeit, an einem so spannenden Experiment mitzuwirken.

Meinen Krypto-Kollegen Henning Weier und Martin Fürst, mit denen ich so manche bisweilen kalte Freiraum-Meßnacht verbringen durfte, und die mit ihrem Optimismus und Humor das Experimentieren ungemein gewürzt haben. Nicht zuletzt dank ihres ausdauernden Computer- und Bastelgeschicks haben sie zahlreiche Meßnächte vor dem Scheitern bewahrt. Danke für die tolle Zusammenarbeit!

Dr. Christian Kurtsiefer, der in der Anfangsphase meiner Doktorandenzeit mir unverzichtbaren Anschub gegeben hat, und von dessen reichhaltigem Physik- und Elektronikwissen nicht nur ich gerne noch länger profitiert hätte.

Den Wiener Kollegen und "Leidensgenossen" auf der Insel, allen voran Rupert Ursin, Felix Tiefenbacher und Thomas Scheidl, die für einen höchst erfrischenden österreichischen Wind gesorgt haben, und ohne die die Gemeinschaftsexperimente auf den Kanaren so nicht möglich gewesen wären.

Zoran Sodnik, Josep Perdigues und den gesamten Teams von der OGS und dem NOT für die Unterstützung vor Ort und die bereitwillige Einführung in ihr "Allerheiligstes".

Herzlicher Dank auch an die Diplomanden Ivan Ordavo, Nadja Regner, Magdalena Kaminska, Davide Marangon und Sebastian Schreiner, die eine Menge Entwicklungsarbeit in das Krypto-Projekt investiert haben.

Dr. Jürgen Volz, der nicht nur bereit war, zu jeder Tages- und Nachtzeit physikalische Fragestellungen zu diskutieren, wenn dabei ein Kuchen herausspringt, sondern auch das Manuskript sorgfältig Korrektur zu lesen. Außerdem seinem Mitschwaben Daniel Schlenk, dem ich für seine missionarische Tätigkeit in sprachlichen wie kulinarischen Angelegenheiten sehr dankbar bin.

Allen bislang unerwähnten Mitgliedern und Ex-Mitgliedern der AG Weinfurter, die für die stets gute Arbeitsatmosphäre gesorgt haben: Christian Schmid, Chunlang Wang, Markus Weber, Nikolai Kiesel, Patrick Zarda, Pavel Trojek, Wenjamin Rosenfeld, Witlef Wieczorek, und allen weiteren, insbesondere meinen Ex-Zimmergenossen Carsten

Schuck, Florian Henkel, Gerhard Huber und Juliane Bahe.

Gabriele Gschwendtner und Nicole Schmidt für kompetente Hilfe bei allen administrativen Angelegenheiten, sowie Anton Scheich für die bereitwillige Hilfestellung bei elektronischen Fragen. Ein weiterer Dank geht an Jürgen Aust und Thomas Großhauser mit ihrem Werkstatt-Team, die sich mehrfach einem knappen Zeitplan für die Verwirklichung unserer mechanischen Wünsche unterwerfen mußten.

Mein besonderer Dank gilt außerdem meinen Eltern, die durch ihre ebenso großzügige wie verläßliche Unterstützung und Ermutigung mir ein sorgenfreies Studium ermöglicht haben.

Und schließlich meiner Freundin Ruth: Danke für deine Liebe und Geduld mit mir!