Robust Polarisation Basis Alignment for Satellite-based Quantum Key Distribution

Marco Andersohn

Munich 2021

Stabile Polarisationskontrolle für satellitengestützten Quantenschlüsselaustausch

Masterarbeit

an der
Fakultät für Physik
der
Ludwig-Maximilians-Universität München

vorgelegt am
3. Mai 2021

von
Marco Andersohn
geboren am 5. August 1998 in Berlin

betreut von
Prof. Dr. Harald Weinfurter

Robust Polarisation Basis Alignment for Satellite-based Quantum Key Distribution

Master's thesis

at the
Faculty of Physics
of the
Ludwig-Maximilians-University Munich

submitted on
3rd Mai 2021

by
Marco Andersohn
born on 5th August 1998 in Berlin

supervised by
Prof. Dr. Harald Weinfurter

Contents

Abstract

Quantum key distribution (QKD) is a secure key-transmitting method based on quantum mechanics to deliver private keys for encryption. Satellite QKD is a promising technique that overcomes the limited transmission distance in optical-fibre-based systems. To enable polarisation encoded QKD, polarisation reference-frame mismatches between the satellite and a receiving optical ground station (OGS) have to be compensated. We developed and implemented a compensation method for a BB84 protocol designed QKD receiver by an additional set of three waveplates (HWP, QWP, QWP). In simulations and laboratory demonstrations, we show the robustness under conditions that we expect on our future satellite downlink mission. As a result, we expect good compensation quality for a wide range of signal to noise ratios and satellite rotation frequencies by requiring only a few signal photons of 2000 of two non-orthogonal polarisation states, respectively, to measure the reference-frame mismatch used for one compensation sequence.

Chapter 1

Introduction

Among all the methods to exchange keys, only Quantum key distribution **[1]** (QKD) has been proven to be information-theoretically secure, i.e. secure against an eavesdropper who has unbounded abilities. Even the most secure classical symmetrical encryption protocols **[2]** require safe key exchange channels, so that a shared secret key can be used to de- and encrypt a message, while channels with quantum mechanical properties using QKD protocols are theoretically protected against attacks. The classical asymmetrical encryption protocols **[3]** do not require a safe encryption-key exchange channel, as long as it can be assumed that the limited computational power of an attacker can not factorise the large numbers that are used for encryption whithin a practicable period of time. For decrypting a message which got encrypted with a publicated key, only the receiver is holder of the correct, not shared private key. However, the Shor algorithm **[4]** running on a quantum computer can break those encryptions. QKD protocols are good candidates to close security gaps, being safe from such futuristic quantum attacks **[5]**.

Recently, in March 2021, the Munich Quantum Valley (MQV) was founded with high governmental fundings with the aim of a quantum technology park. Besides other scientific fields, MQV should be used for quantum communication and quantum cryptography research, transferring the results to the economy and recruiting the new generation of quantum scientists.

Quantum communication with tap-proofed QKD and efficient communication devices will be a core component of future secure data networks and platforms against cyber attacks. In 1984, QKD was first developed by Bennett and Brassard **[6]** using BB84 protocol which is based on photon polarisation in two conjugated bases for encoding the qubits. In the past ten years, many attemps have been made from all over the world towards a secure, global quantum cryptography network **[7]** with little loss over long distances and high key rates, e.g. with the Tokyo QKD network **[8]** or the integrated space-to-ground network up to a total distance of 4600 km in China **[9]**. However, as the losses in optical fibres increase exponentially with distance, for global scale networks, satellite-based-free-space links with losses increasing only quadratically are very promising. A first step in this direction was the realisation of a downlink from an airplane to a ground station by our group in 2013, where successfully a key was exchanged **[10]**. This was followed by a successful demonstration of

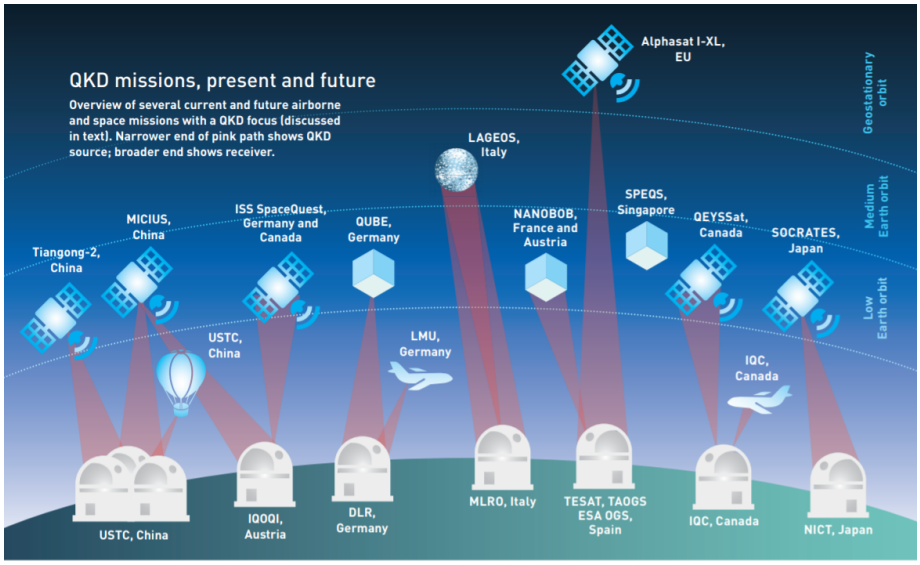


Figure 1.1: QKD missions, present and future, taken from **[13]**

an aircraft uplink in 2017 by the Jennewein group **[11]**. In 2016, a satellite has been launched by a Chinese research project in order to perform quantum experiments including QKD **[12]**. At the end of this year, our group will launch a cubesat in order to demonstrate a few months later the feasibility of satellite to ground QKD in components tests by transmitting polarisation states according to the BB84 ptotocol. Some other research groups launched satellites for QKD and many more will follow, as collated in **figure 1.1**.

To realise the exchange of polarisation states with a low quantum bit error rate (QBER), reference-frame mismatches between the receiver and the transmitter have to be compensated. As a polarisation tracking scheme, we developed and implemented a compensation method for a BB84 protocol designed QKD receiver by an additional set of three waveplates (HWP, QWP, QWP). This thesis summarises the compensation procedure in our satellite mission scenario and discusses the robustness in simulations and laboratory demonstrations.

Chapter 2 provides the mathematical foundations behind polarisation **2.1**, the description of how optical components alter polarisation states **2.2** and reports the benefits of BB84 protocol for QKD **2.3**. **Chapter 3** details the reference-frame mismatch of our satellite mission scenario **3.1**, the algorithm used for compensation **3.2** and accounts the influence of finite statistics **3.3** and noise **3.4** in compensation simulations. **Chapter 4** outlines the setups used for testing polarisation compenstion **4.1**, presents the achieved results **4.2**, compares them to state of the art implementations **4.3** and predicts similar good compenstion quality for a wide range of possible satellite mission conditions **4.4**. **Chapter 5** summarises the progress made in this thesis and indicates further research that could be carried out.

Chapter 2

Quantum Key Distribution with Polarisation Encoding

In the field of quantum information **[14]**, the science of quantum communication **[15]** is located, which contains the field of Quantum Key Distribution (QKD). QKD is characterised by using the properties of quantum mechanics, to provide two parties a sequence of random numbers. This sequence can then be used as a secret key in order to transmit messages securely using classical symmetric encryption methods **[16]**, in contrast to quantum cryptography **[17]**.

The first developed QKD scheme is the BB84 protocol, which will be explained in **section 2.3**. One practical implementation consists in the transmission of polarisation states, which are introduced in **section 2.1**. In order to describe the polarisation of light and its transformations, the Stokes formalism and the Mueller calculus, respectively, have turned out to be powerful. They will be presented in **section 2.2**.

2.1 Quantum Mechanical Foundations

Classical bits are usually represented by the binary digits 0 and 1. For example, measuring a voltage below a certain threshold corresponds to the value 0, whereas a higher voltage above a threshold is called 1. The quantum analogue of a classical bit, i.e., the smallest unit of information in the field of quantum information is the so-called quantum bit (qubit). Qubits represent 2-level quantum mechanical systems and unlike classical bits, qubit states $|\Psi\rangle$ can be in superposition of its two basis states $|\Psi_0\rangle$ and $|\Psi_1\rangle$

$$|\Psi\rangle \;=\; \alpha\,|\Psi_0\rangle + \beta\,|\Psi_1\rangle\,, \tag{2.1}$$

where α and β are complex probability amplitudes, which fulfill the normalisation condition $|\alpha|^2 + |\beta|^2 = 1$. Physical manifestations of qubits are, for example, two energy states of an atom **[18]**, spin-½ particles with spin up and spin down **[19]** or the phase **[20]** or the polarisation **[21]** of a photon.

2.1.1 Polarisation of Light

Light consists of electromagnetic waves. According to Maxwell's laws, the change of an electric field induces a magnetic field perpendicular to it, which in turn induces an electric field perpendicular then again and so on. That is how an electromagnetic wave propagates along its propagation direction $\vec{k}$. The direction of polarisation of an electromagnetic wave is given by convention by the direction of oscillation of its electric field **[22]**.

One differentiates between linearly and circularly polarised light as special cases of elliptical polarisation. For linearly polarised light, the plane in which its electric field oscillates is constant. The direction in relation to a certain plane can be specified as an angle or as a proportion of the two components parallel (p) and perpendicular (s) to it. Depending on the angle, we call light horizontally polarised, if all light is parallelly polarised to a reference frame. Accordingly, light which is polarised 90° to that reference frame is called vertically polarised. Diagonal and antidigonal polarisation refer to $+45°$ and $-45°$ polarisation direction, which corresponds to the equal superposition of horizontal and vertical polarisations with the phase 0 and π, respectively. Equal superpositions of horizontally and vertically polarised light with pase $\pi/2$ and $-\pi/2$ are called left- and right-handed circular, respectively. In general, arbitrary superpositions with a phase 0 and π are called linear polarisations, whereas other phases corresponds to elliptical polarisations.

Natural polarisation takes place through oblique reflections at interfaces, e.g. on a water surface. The reflectance and transmittance depend on the polarisation such that light polarised in the reflection plane has a larger transmittance than s-polarised light. Correspondingly, the reflected light will be rotated towards the direction perpendicular to the reflection plane. For more quantitive dependence on the angle of incidence, see Fresnel's formulas **[23]**.

2.1.2 Measuring Polarisation

For measuring the state $|\Psi\rangle$ of a qubit, the probably most simple and straightforward formulation was given by John von Neumann **[24]**, therefore called *von Neumann measurement*. It says that for a given physical property, there exists an observable A, which is described by the Hermitian operator $\hat{A}$ with the eigenvalues $\{\lambda_n\}$ and the corresponding eigenstates $\{|\lambda_n\rangle\}$. As we aim at a measurement process description for polarisation and A acts on a two-dimensional Hilbert space, we can span it with the eigenstates of the Pauli operators σ_X, σ_Y and σ_Z, building the three complementary bases $\hat{S}_X$, $\hat{S}_Y$ and $\hat{S}_Z$ **[25]**. As a two-dimensional Hilbert-space is fully described by two basis vectors, any vector can be written as a unique linear combination out of them, shown for the basis vectors in **table 2.1**, from which superposition arises. In the von Neumann measurement, the probability of measuring a quantum state $|\Psi\rangle$

	$\hat{S}_Z$	$\hat{S}_X$	$\hat{S}_Y$
$\|H\rangle$	$\|H\rangle$	$\frac{1}{\sqrt{2}}(\|P\rangle + \|M\rangle)$	$\frac{1}{\sqrt{2}}(\|R\rangle + \|L\rangle)$
$\|V\rangle$	$\|V\rangle$	$\frac{1}{\sqrt{2}}(\|P\rangle - \|M\rangle)$	$\frac{i}{\sqrt{2}}(\|R\rangle - \|L\rangle)$
$\|P\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle + \|V\rangle)$	$\|P\rangle$	$\frac{1}{2}((1+i)\|R\rangle + (1-i)\|L\rangle)$
$\|M\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle - \|V\rangle)$	$\|M\rangle$	$\frac{1}{2}((1-i)\|R\rangle + (1+i)\|L\rangle)$
$\|R\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle - i\|V\rangle)$	$\frac{1}{2}((1-i)\|P\rangle + (1+i)\|M\rangle)$	$\|R\rangle$
$\|L\rangle$	$\frac{1}{\sqrt{2}}(\|H\rangle + i\|V\rangle)$	$\frac{1}{2}((1+i)\|P\rangle + (1-i)\|M\rangle)$	$\|L\rangle$

Table 2.1: Representation of polarisation states **[26]**: horizontal $|H\rangle$, vertical $|V\rangle$, $+45°$ diagonal $|P\rangle$, $-45°$ anti-diagonal $|M\rangle$, right-circular, clockwise in right handed system, $|R\rangle$ and left-circular, clockwise in left handed system, $|L\rangle$ in $\hat{S}_Z$, $\hat{S}_X$ and $\hat{S}_Y$ basis.

in the eigenstates $\{|\lambda_n\rangle\}$ of a detector is the projection of the quantum state onto the detector eigenstates

$$P\left(|\lambda_n\rangle\right) \;=\; \left|\langle\Psi|\lambda_n\rangle\right|^2. \tag{2.2}$$

For example, measuring $|H\rangle$ in the detector frame $|P\rangle$ yields:

$$P\left(|P\rangle\right) \;=\; |\langle P|H\rangle|^2 \;\overset{\text{table 2.1}}{=}\; \left|\langle P|\,\frac{1}{\sqrt{2}}\left(|P\rangle + |M\rangle\right)\right|^2 \;\overset{\text{ortho-normality}}{=}\; \frac{1}{2} \tag{2.3}$$

The probability of $1/2$ means, that basis vectors of complementary bases are totally indistinguishable in the original basis.

2.2 Mathematical Background for Polarisation Calculations

In the beginning of this section, the Stokes formalism, for describing polarisation as well as Mueller calculus for manipulating polarisation states in the Stokes formalism are explained.

2.2.1 Stokes Formalism for Describing Polarisation

As we need a practical calculus by which we can calculate polarisation states easily by the detection intensities, we used the Stokes formalism, defined by G. Stokes in 1852 **[27]**. Therein, any state can be written as a 4-dimensional Stokes vector with its Stokes parameters:

$$\vec{S} \;=\; \begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} \;=\; \begin{pmatrix} I \\ {}^{(I_H - I_V)}/_{I} \\ {}^{(I_P - I_M)}/_{I} \\ {}^{(I_R - I_L)}/_{I} \end{pmatrix}, \tag{2.4}$$

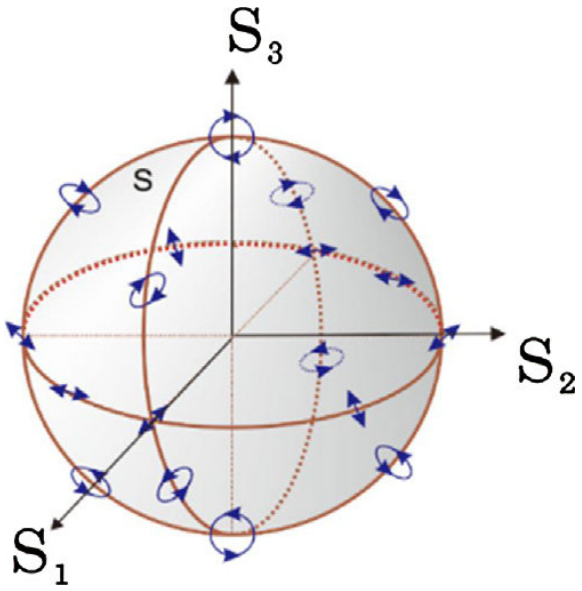


Figure 2.1: Geometrical representation of polarisation states on the Poincaré sphere **[28]**, formed by the three Stokes parameters (S_1, S_2, S_3). The equator of the Poincaré sphere represents all linear polarisation states and the poles the complete circular states. Any other point on the Poincaré sphere represents an elliptical polarisation state.

with the absolute light intensity in its "zeroth" entry and for each complementary basis, with entries of the normalised intensity difference from its conjugated basis pair. To get an overview of polarisation states, the six basis and the perfectly mixed state of light are shown:

$$\vec{S}_{H/V} = \begin{pmatrix} 1 \\ \pm 1 \\ 0 \\ 0 \end{pmatrix}, \ \vec{S}_{P/M} = \begin{pmatrix} 1 \\ 0 \\ \pm 1 \\ 0 \end{pmatrix}, \ \vec{S}_{R/L} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \pm 1 \end{pmatrix}, \ \vec{S}_{O} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \tag{2.5}$$

For example, measuring horizontally polarised light, means, observing all photons in a horizontal aligned detector $I_H = 1$, none in a vertical $I_V = 0$ and in equivalent amounts in all complementary aligned detectors $I_{other} = 0.5$, whereby its Stokes vector can get reconstructed. All possible states can get represented by the Poincaré sphere, see **figure 2.1**, in which the basis states point to, where the surface gets crossed by the axes, and the unpolarised state sits in the origin. If a state has the property of having full degree of polarisation (dop), $\text{dop} = \frac{\sqrt{S_1^2+S_2^2+S_3^2}}{S_0} = 1$, the vector representing the state points to the surface. Otherwise, if $0 \leq \text{dop} < 1$, it points inside the sphere, with the radius $r = \text{dop}$. Note that two vectors laying opposite in the sphere are perpendicular to each other, easy to check by calculating their scalar product.

Compared to the Jones formalism, light intensity can be described, but only for incoherent light. Although, the phase information of polarised light is not recorded in the Stokes parameters, interference can be described in Stokes formalism **[23]**.

2.2.2 Mueller Calculus for Manipulating Stokes Vectors

To ask, how a setup changes polarisation, is the same question as asking how the Poincaré sphere gets rotated due to the setup. For example, if any state, sent through the setup, remains the same, the coordinate system of the sphere has not changed. This is the case, for states just propagating through air, so that a matrix, which would act on incoming states, to calculate the outgoing states, would be the unit matrix. The process to measure this matrix, to characterise the effects on polarisation of optical systems, is called tomography. For describing the effects, the Mueller calculus is used. Therein, all optical components can mathematically be described by a 4×4 Mueller matrix. In **figure 2.2**, Mueller matrices of the most important components are shown. After passing a component, the outgoing polarisation state $\vec{S_1}$ can get calculated by multiplying the incoming light vector $\vec{S_0}$ on the Mueller matrix $\underline{M}$ of the component:

$$\vec{S_1} = \underline{M}\vec{S_0} \tag{2.6}$$

Although, we first have our incoming light and then our component, we took them in reversed order, to get a vector back. This mathematical intuition can get extended to the rule, that whenever light passes through one additional component, its Mueller matrix $\underline{M}_{i+1}$ has to get multiplicated from the left, to receive correct polarisation states or the total Mueller matrix $\underline{M}$ of the system:

$$\vec{S_1} = \underline{M_3}\underline{M_2}\underline{M_1}\vec{S_0} \tag{2.7}$$

$$\underline{M} = \underline{M_3}\underline{M_2}\underline{M_1} \tag{2.8}$$

2.3 Basic Concepts of Quantum Key Distribution

In order to communicate confidential, sensitive or private information secretly, humankind has developed and used a multitude of cryptography methods for thousands of years. There are some basic principles underlying any cryptographic system, from the Caesar Cipher, a bijective letter interchanger, of the ancient romans, via systems secured by primefactorisation in modern computer science, to a quantum mechanic based of tomorrow.

For such quantum mechanic based protocols, it is common that a sender, by convention called Alice, encodes the secret message, shares it with an other party, Bob, who has to decode it with a key. If sender and receiver use the same keys for encoding and decoding the message, like it is the case of the bijective Caesar Cipher, the

$$\underline{\mathrm{Pol}_V} = \frac{1}{2}\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \text{vertical transmitting polariser } (\mathrm{Pol}_V)$$

$$\underline{\mathrm{Pol}}\,(\theta) = \frac{1}{2}\begin{pmatrix} 1 & \cos(2\theta) & \sin(2\theta) & 0 \\ \cos(2\theta) & \cos^2(2\theta) & \sin(4\theta)/2 & 0 \\ \sin(2\theta) & \sin(4\theta)/2 & \sin^2(2\theta) & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad \text{any transmitting polariser (Pol)}$$

$$\underline{\mathrm{Mirror}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \qquad \text{mirror reflecting with } 45^\circ \text{ incidence direction}$$

$$\underline{\mathrm{QWP}}\,(\alpha) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos^2(2\alpha) & \sin(4\alpha)/2 & \sin(2\alpha) \\ 0 & \sin(4\alpha)/2 & \sin^2(2\alpha) & -\cos(2\alpha) \\ 0 & -\sin(2\alpha) & \cos(2\alpha) & 0 \end{pmatrix} \qquad \text{quarter-wave plate (QWP)}$$

$$\underline{\mathrm{HWP}}\,(\gamma) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(4\gamma) & \sin(4\gamma) & 0 \\ 0 & \sin(4\gamma) & -\cos(4\gamma) & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \qquad \text{half-wave plate (HWP)}$$

Figure 2.2: Mueller matrices of optical components. QWPs and HWPs are birefringing optical components with quarter or half wavelength retardance, respectively. All angles are in laboratory frame, where the fast axis of a component is tilted, so that $\vec{S}_H$ remains the same, if the angle is 0.

encryption process is called symmetric. One example for an asymmetric encryption process is the public-key-encoding process, whereby any party can encode a message with a mathematical *one-way*-function-based, public shared key and only the owner of the private key can decode the encoded ciphertext.

If an eavesdropper, usually called Eve, would spy on the message and key or would brute-force the decryption, she could become aware of the secret. Therefore, it is recommended to use qubits for transmitting a key, as measuring polarisation in non-orthogonal bases adds pure randomness in key preparation. This ensures maximum entropy, so that a transmitted bit-string contains no information, as shown by C. Shannon **[29]**. There are many reasons to use for polarisation to quantise information, for example, if the technology starts being used, infrastructure is already

Encoding **bits**	0	0	1	1	1	0	0	1
in random **bases**	1	0	0	0	1	1	0	1
gives **states** to transmit.	P	H	V	V	M	P	H	M
Measured in random **bases**,	1	1	1	0	1	0	0	0
resolves into transmitted **bits**.	0	1	0	1	1	0	0	1

Table 2.2: Procedure of key distribution ruled by BB84-protocol

there, for transmitting via fibres. As loss grows exponentially with distance in fibre and just linearly via free space, it is motivated to communicate over long distances via satellites. To examine how atmospherical turbulences affect polarisation, much research has been done **[30]**, with the result that it does not disturb polarisation up to first order.

2.3.1 QKD over long Distances with BB84-Protocol

Probably the best understood and most used protocol for QKD, due to its structural simplicity, was presented in 1984 by C. Bennett and G. Brassard **[6]**, hence it is given the name BB84 protocol. There exist reference-frame-independent QKD protocols **[31]** working with circular states. As it is experimentally not guaranteed to produce and guide photons in perfect circular states, which for security reasons is necessary in these protocols, we decided to use BB84 protocol for our satellite mission.

Therein described, Alice sends randomly linearly polarised states $\{H, V, P, M\}$ and Bob measures randomly in complementary linear bases, whose possible measuring outcome is shown in **figure 2.3**. While measuring in the same basis as Alice, Bob can be quite sure to measure the intended bits of Alice, which is shown in **table 2.2**, marked in green. If he doesn't, his results are marked in red and completely uncorrelated to Alice's bits. In a next step of the protocol, in the so called key sifting, Alice and Bob classically compare in which bases they have prepared and measured. Thereby, they can be certain, which bits got correctly transmitted, to use them as their key to de- and encrypt a classically transmitted message. In **table 2.2**, the key is Bob's green bit series 0110 – everything still without naming the sent states or the transmitting bits. The efficiency is estimated to be 50%, due to equally propable basis decisions, which halves the length of the sifted key compared to the number of sent bits. The quality of the sifted key is quantified by the quantum bit error rate (QBER), which is the ratio of false measured to sifted bits. For its determination some bits are directly compared and for security reasons, therefore discarded:

$$\text{QBER} = \frac{N_{wrong}}{N_{sifted}} \tag{2.9}$$

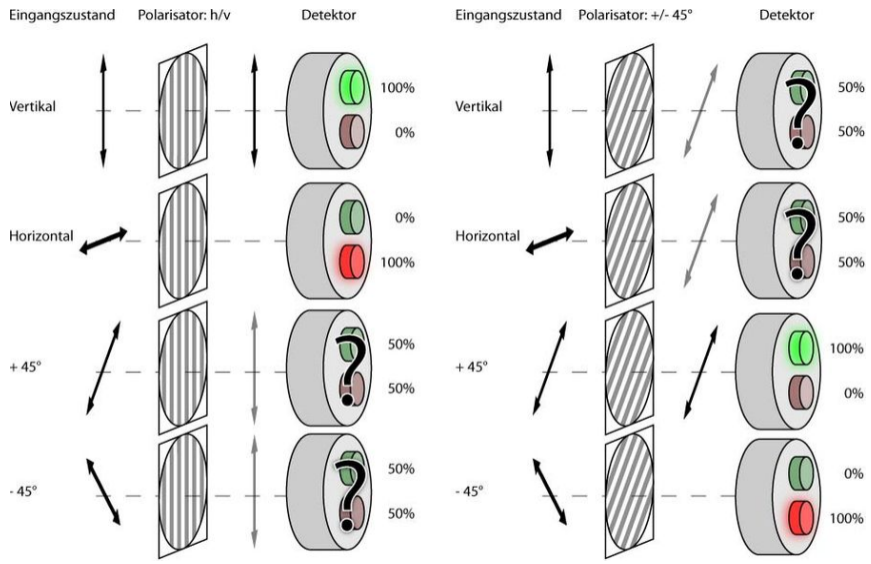


Figure 2.3: Bob's measuring outcome of Alice's states after randomly selecting H/V or P/M basis bound by BB84 protocol. In the cases marked with "?", both results occur with the same possibility, recalculatable with **table 2.1**, see **paper [32]**.

2.3.2 Security level during an Eavesdropper Attack

Errors in the exchanged bit string can either be caused by imperfections in the preparation, transmission and detection of the signals or by the presence of an eavesdropper. In the security analysis, all errors are pessimistically attributed to the attacker Eve and thus, the QBER is a measure for the amount of key information an eavesdropper may maximally have. After the key sifting, some security maximising and transmission loss minimising tools can be used, for example, "privacy amplification" **[33]** and "error-correction" **[34]**. An upper bound for the resulting secure key rate is given in **[35]**:

$$R_{sec,max} \quad = \quad R_{sift} \cdot max[1 - (f_{EC} + 1)H_2(E), 0], \tag{2.10}$$

with f_{EC} being the efficiency of the error correction algorithm, R_{sift} the sifted key rate, e.g the number of sifted bits multilied by the repetition frequency of the source and divided by the number of sent bits N, and $H_2(E)$ the binary Shannon entropy of $E \equiv$ QBER. This gives an estimate on the amount of key information was accessible to an attacker:

$$H_2(E) = -E\log_2(E) - (1-E)\log_2(1-E) \tag{2.11}$$

The maximum tolerable QBER can be found by calculating the point, where equation (2.10) drops to zero, yielding $E_{max} \approx 11\%$.

In a possible attack, the *intercept-resend attack*, Eve could take many copies of the transmitted photons and measure them in the bases Alice and Bob shared for comparing. Luckily for Alice and Bob, cloning is not possible for quantum states, at least

not lossless, due to the uncertainty principle, which enforces quantum measurements to alter quantum states, proofs in **[36]** and **appendix B.2**.

For the BB84 protocol necessary single photon sources **[37]** are practicaly realised with attenuated faint lasers, emitting so called weak coherent pulses (WCP). The *photon number splitting (PNS) attack* **[38–40]** exploits the Poissonian distributed probability being greater than zero, of sending multiple photons in a pulse. Thereby, Eve can work around the no-cloning theorem **B.2**, by determining the number of photons in each pulse, blocking all one photon pulses and storing a photon of each multiphoton pulse. One way out is the extended BB84 protocol with *decoy states*, proposed by Hwang, Wang, Lo et al. **[41–43]**. Therein explained, the protocol prescribed sending additional, non-message-contributing Poissonian distributed states with an even lower expectation value per pulse. As they are indistinguishable from the key states for Eve, due to the non-orthogonality of coherent states, she would perform the PNS attack also on them. As a consequence, Bob measures a correlation between not receiving photons and the probability that Alice would have sent one per pulse, so that Eve's PNS attack gets exposed.

Depending on which attack Eve uses, there always exists a minimum disturbance, due to her activities and the laws of quantum mechanics. One exception are the so called *side channel attacks* **[44–47]**, for example, if the degree of freedom, for encoding bits, is correlated to something not quantum-mechanical. To mention just one example, the circuits of the diodes, producing the polarised photons, could radiate electromagnetically. Therefore, Eve performs *non-demolition measurements* **[48]**, so that no error in Bob's measurements is introduced. Such loopholes need to be closed technically.

Chapter 3

Analytical Concepts and Simulations

To the end of 2021, we plan to start a satellite mission for QKD. Its scenario is explained in **section 3.1** and shown in **figure 3.1**. As polarisation states are expected to be disturbed during the satellite mission, **section 3.2** focusses on the analytical concepts for their compensation. Simulations have been made, demonstrating which QBER is to be expected after compensations which got affected by finite statistics and noise. The methods and results are presented in **section 3.3** and **section 3.4**.

3.1 Model for Polarisation Compensation

The rotation of the satellite causes a continuous change of the polarisation states, which can be described by a unitary transformation $U_{rot}(t)$. Geometricaly speaking, the polarisation states get rotated around the S_3 axis of the Poincaré sphere. By rotating a HWP of the receiver with half of the angular speed of the satellite, the time-dependency of the reference frame mismatch can be suppressed. To consider the time-independent mismatch, a polarisation tomography of the received states has to be made. Here, it is sufficient to tomograph one state each out of two complementary bases. With the data of the state tomography, a valid unitary backtransformation matrix can be calculated and performed by using a set of three waveplates (HWP, QWP, QWP).

As shown in **figure 3.1**, the cube satellite, in the role of Alice, sends photons to an optical ground station (OGS) and further to a QKD receiver, here called Bob. In the satellite, four *vertical-cavity surface-emitting lasers* (VCSEL) **[49]** produce the photons in $\{H_a, V_a, P_a, M_a\}$ polarisation states, according to the BB84-protocol. The photons are guided through optical components, e.g. waveguides **[50]** and fibres, which may change the states constant in time to $\{H', V', P', M'\}$. As the satellite rotates around an axis, which is aligned to the OGS, the reference frame changes time-dependently with the satellite's angular velocity and so do the states, resulting in $\{H''(t), V''(t), P''(t), M''(t)\}$.

The OGS focusses and collimates the photons, symbolised by the lense. In order that the OGS is aligned to the satellite, two rotational degrees of freedom are needed,

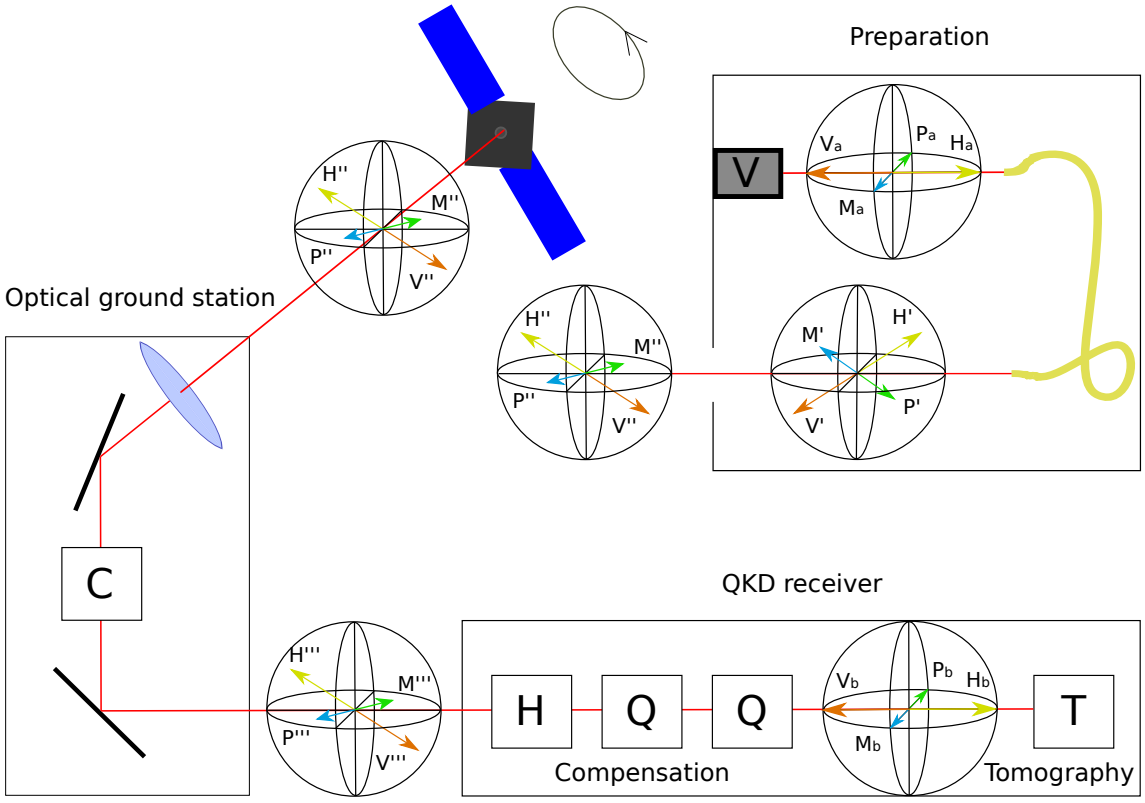


Figure 3.1: Optical downlink between a satellite and an optical ground station (OGS). Photons emitted by VCSELs (V) in the satellite get collected by the OGS and analysed by the QKD receiver, containing a compensation (H, Q, Q) and a tomography unit (T). A compensation unit C in the OGS corrects for rotational transformations due to the moving mirrors.

e.g. manifestated as a orthogonally oriented pair of rotating mirrors, one with a horizontal (azimuthal) plane of rotation and the other with a vertical (elevation) plane of rotation (**figure 4.9**), of which one reflects the beam downwards and the other to the QKD receiver. These rotating mirrors also change the polarisation states depending on the angle of incidence and their orientation in the laboratory frame. Its polarisation change is corrected by an already built-in compensation unit in the optical ground station. Therefore, the photons leave the optical ground station with the same states $\{H'''(t), V'''(t), P'''(t), M'''(t)\}$ as those they entered $\{H''(t), V''(t), P''(t), M''(t)\}$.

Arrived in the QKD receiver, the photons pass a compensation unit. To compensate for the satellite rotation, a HWP in the OGS with a rotation speed of half the satellite's rotation speed can be used. In order to not only account for the rotation along the S_3 axis, but to equalise further time-independent polarisation rotations, additional waveplates such as two QWPs are required, proof in **appendix B.1**. To figure out which rotation compensates the states $\{H'''(t), V'''(t), P'''(t), M'''(t)\}$ they have to get tomographied and analysed. Thereafter, Bob's polarisation states

$\{H_b, V_b, P_b, M_b\}$ match Alice's $\{H_a, V_a, P_a, M_a\}$. For our application, the alignment of the reference frames can be done by preparing two pure states of different bases of linear polarisation, e.g. by sending H and P polarisation states.

3.2 Analytical Solution for Compensation Settings

The most important advantage of an analytical solution, compared to a numerical one, is that the solution can be directly calculated instead of relying on a time consuming numerical method. Therefore, more time remains for the QKD procedure. Furthermore, we can perform error calculation with an analytic formula, to guarantee that we find a stable solution, disturbed by potential measuring uncertainties. We also get the extent how much the uncertainties influence the compensation angles and the QBER, see **sections 3.2.4** and **3.3**.

In this section, the essential steps for calculating the backtransformation matrix and the compensation angles will be discussed in detail. In **subsection 3.2.2**, the calculation of the Mueller matrix and its inverse are explained. How to obtain the compensation angles for a given backtransformation matrix is the topic of **subsection 3.2.3**.

3.2.1 Assumptions

To find a mathematical model, for calculating the compensation angles, which is best adapted to real conditions and does not idealise reality, we have to make practical assumptions. As the retardance plates only perform unitary rotations, polarisation can only get compensated unitarily, even if depolarising effects took place in Alice's or Bob's setup or over the transmission. Also, as long as we do not redefine the prepared polarisation states, e.g. from H to V, no anti-unitary transformation will happen. Therefore, only the unitary transformations during the communication process are relevant, by which we assume unitarity and neglecting non unitary transformations.

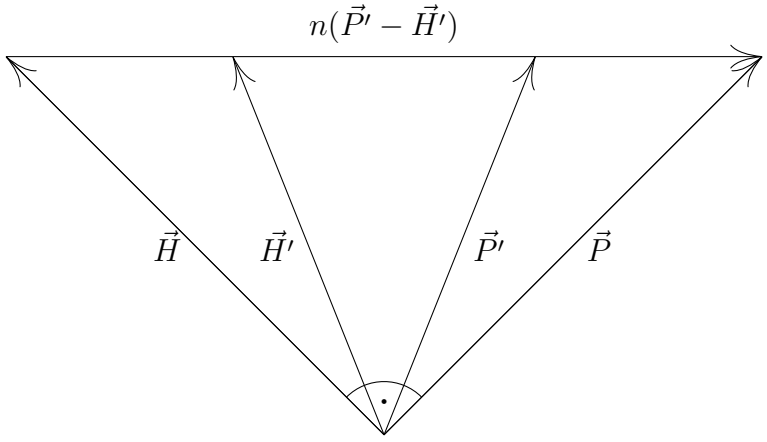
As we send states which represent vectors with 90° between them on the Poincaré-sphere with unit length, we want to normalise and orthogonalise our measured vectors as well. First we check potential harm if states are artificially normalised. Therefore, we ask if vectors with different lengths should get compensated with different priorities to Alice's states. As the atmosphere does not affect the polarisation of light up to first order **[30]**, the polarisation states do not depolarise. So, if polarisation states with seemingly smaller degree of polarisation got measured, it is because of additional background noise and dark counts, which should be unpolarised in average, and superpose the polarisation states intended for transmission. The noise affects polarised components more than already depolarised ones, so that it also

changes the direction of states. To get rid of noise, the states can be normalised and orthogonalised.

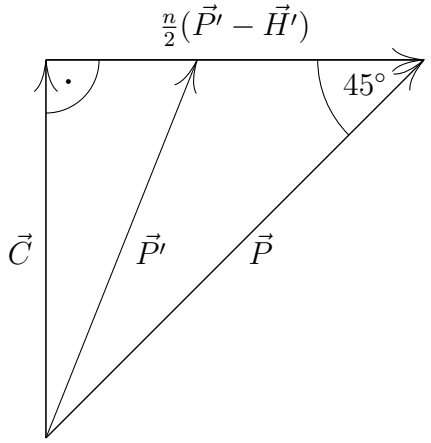
Considering orthogonality, we ask whether we should compensate for some vector components with higher priorities in the case of birefringence effects on Alice's or Bob's side. So, if both vectors got measured not perfectly orthogonal, it is not due to atmospheric turbulences, as they do not affect polarisation up to first order **[30]**. So, in this case, a birefringing component affects some polarisation more than others. If we knew the effect at Alice's or Bob's side, we could recalculate how our data would look like without the effect. If we do not know, we want to achieve an QBER which is equally distributed over all polarisation components. With orthogonalisation, all measured vectors will be compensated with the same priority into Alice's coordinate system, so that they receive the same distances after compensation to Alice's original polarisation states. Orthonormalisation also distributes statistical defects over all Stokes components and thereby smoothes some out.

It is unique in this chapter that we assume the measured degree of polarisation to be 1, due to few and low expected depolarising effects in the satellite mission and after subtracting background light and dark counts of the detectors. As the intensity component is not anymore a degree of freedom of a Stokes vector, we reduced them from four dimensions to three to gain more practicable three dimensional Stokes-like vectors with more useful properties. Note that this changes the term of orthogonality, calculated by scalar multiplication of vectors.

To gain vectors with orthonormal properties, we use the algebraic equation of a straight line, going through the normalised measured vectors $\vec{H'}$ and $\vec{P'}$. The equation, representing all points on the line, has the form $\vec{Y} = \vec{H'} + \lambda(\vec{P'} - \vec{H'})$, with $\lambda \in \mathbb{R}$. We are looking for a specific λ, called n, for which $\vec{H}$ and $\vec{P}$ enclose an angle of 90°.



Calling the small angle bisecting vector of $\vec{H'}$ and $\vec{P'}$, pointing on the straight line, $\vec{C} = \vec{H'} + 0.5(\vec{P'} - \vec{H'})$, we receive an isosceles rectangular triangle with two legs of equal length $\frac{n}{2}|\vec{P'} - \vec{H'}| = |\vec{C}| = |\vec{H'} + 0.5(\vec{P'} - \vec{H'})|$.



This resolves to $n = \frac{|2\vec{H'}+\vec{P'}-\vec{H'}|}{|\vec{P'}-\vec{H'}|} = \frac{|\vec{P'}+\vec{H'}|}{|\vec{P'}-\vec{H'}|}$. Thus, $\vec{H}$ and $\vec{P}$ are as follows:

$$\vec{H} = \vec{H'} + \frac{1-n}{2}(\vec{P'} - \vec{H'}) \tag{3.1}$$

$$\vec{P} = \vec{H'} + \frac{1+n}{2}(\vec{P'} - \vec{H'}) \tag{3.2}$$

After normalisation, $\vec{H}$ and $\vec{P}$ have the desired properties, in accordance with the assumptions. Check for orthogonality with respect to three-dimensional Stokes-like vectors:

$$\begin{aligned}
\vec{H} \cdot \vec{P} &\overset{\text{binomial formulas}}{=} \vec{H'}^2 + \frac{1-n^2}{4}(\vec{P'} - \vec{H'})^2 + \vec{H'} \cdot (\vec{P'} - \vec{H'}) \\
&\overset{\text{inserting } n}{=} \vec{H'} \cdot \vec{P'} + \frac{1}{4}(\vec{P'} - \vec{H'})^2 - \frac{1}{4}\left|\vec{P'} + \vec{H'}\right|^2 \\
&\overset{\text{binomial formulas}}{=} \vec{H'} \cdot \vec{P'} - \frac{1}{2}\vec{P'} \cdot \vec{H'} + \frac{1}{4}\vec{P'}^2 + \frac{1}{4}\vec{H'}^2 - \frac{1}{2}\vec{P'} \cdot \vec{H'} - \frac{1}{4}\vec{P'}^2 - \frac{1}{4}\vec{H'}^2 \\
&= 0
\end{aligned}$$

3.2.2 Backtransformation Matrix

Our measured and reshaped $\vec{H}_b = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix}$ and $\vec{P}_b = \begin{pmatrix} t_1 \\ t_2 \\ t_3 \end{pmatrix}$, together with their cross product $\vec{R}_b$[1] $= \vec{H}_b \times \vec{P}_b = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} s_2 t_3 - s_3 t_2 \\ s_3 t_1 - s_1 t_3 \\ s_1 t_2 - s_2 t_1 \end{pmatrix}$, form an orthonormalised basis. This basis can be easily mapped to an originally sent set of basis vectors (provided that $\vec{R}_a$ would have been sent): $\left\{ \vec{H}_a, \vec{P}_a, \vec{R}_a \right\} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$, where the polarisation vectors got relabeled by their indices from b to a, depending on if they belong to Alice's or Bob's basis, respectively. We are interested in how $\vec{H}_b$ and $\vec{P}_b$ transform back to $\vec{H}_a$ and $\vec{P}_a$. We define the backtransformation matrix:

$$\underline{\mathrm{U}} = \begin{pmatrix} s_1 & s_2 & s_3 \\ t_1 & t_2 & t_3 \\ u_1 & u_2 & u_3 \end{pmatrix} \tag{3.3}$$

Check for intended transformation:

$$\underline{\mathrm{U}} \cdot \vec{H}_b = \begin{pmatrix} s_1 & s_2 & s_3 \\ t_1 & t_2 & t_3 \\ u_1 & u_2 & u_3 \end{pmatrix} \cdot \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} \underset{\text{orthogonality}}{\overset{\text{normalisation}}{=}} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \vec{H}_a$$

$$\underline{\mathrm{U}} \cdot \vec{P}_b = \begin{pmatrix} s_1 & s_2 & s_3 \\ t_1 & t_2 & t_3 \\ u_1 & u_2 & u_3 \end{pmatrix} \cdot \begin{pmatrix} t_1 \\ t_2 \\ t_3 \end{pmatrix} \underset{\text{orthogonality}}{\overset{\text{normalisation}}{=}} \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \vec{P}_a$$

Check for unitarity:

$$\underline{\mathrm{U}} \cdot \underline{\mathrm{U}}^\dagger \underset{\text{entries}}{\overset{\text{real}}{=}} \begin{pmatrix} s_1 & s_2 & s_3 \\ t_1 & t_2 & t_3 \\ u_1 & u_2 & u_3 \end{pmatrix} \cdot \begin{pmatrix} s_1 & t_1 & u_1 \\ s_2 & t_2 & u_2 \\ s_3 & t_3 & u_3 \end{pmatrix} \underset{\text{orthogonality}}{\overset{\text{normalisation}}{=}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\Rightarrow \underline{\mathrm{U}}^\dagger = \underline{\mathrm{U}}^{-1}$$

[1] $\vec{R}_b$ is already normalised, because crossproducts of two orthonormal vectors give a third orthonormal vector. The absolute value of a crossproduct gives the area spanned by the two vectors, which are orthonormal here, so that $\left|\vec{R}_b\right| = A \underset{\text{orthogonality}}{=} \left|\vec{H}_b\right| \cdot \left|\vec{P}_b\right| \underset{\text{normality}}{=} 1$.

3.2.3 Compensation Angles

By the combination of three waveplates (2×QWPs and 1×HWP), any rotation with $\underline{\mathrm{U}}$ can be done, proof in **appendix B.1**, where $\{\alpha, \beta, \gamma\}$ are our compensation angles:

$$\underline{\mathrm{U}}\,(\alpha,\beta,\gamma) \;=\; \underline{\mathrm{QWP}}\,(\gamma)\cdot\underline{\mathrm{QWP}}\,(\beta)\cdot\underline{\mathrm{HWP}}\,(\alpha) \underset{(3.3)}{=} \begin{pmatrix} s_1 & s_2 & s_3 \\ t_1 & t_2 & t_3 \\ u_1 & u_2 & u_3 \end{pmatrix} \tag{3.4}$$

As the written out term of the Mueller matrices multiplied together is too unpracticable, to show it here, it is shown in **appendix A.2**. By considering it, we recognise, that three entries of $\underline{\mathrm{U}}$ look like a vector in spherical coordinates, but some with additional negative signs:

$$\begin{pmatrix} s_3 \\ t_3 \\ u_3 \end{pmatrix} \;=\; \begin{pmatrix} -\cos(2\gamma)\sin(2\beta-2\gamma) \\ -\sin(2\beta-2\gamma)\sin(2\gamma) \\ \cos(2\beta-2\gamma) \end{pmatrix} \tag{3.5}$$

We substitute $\theta = 2\beta - 2\gamma$ and $\phi = 2\gamma$ in equation (3.5) and obtain:

$$\begin{pmatrix} -s_3 \\ -t_3 \\ u_3 \end{pmatrix} \;=\; \begin{pmatrix} \sin(\theta)\cos(\phi) \\ \sin(\theta)\sin(\phi) \\ \cos(\theta) \end{pmatrix} \tag{3.6}$$

Due to the fact that the vector in equation (3.6) still is normalised, it resolves to:

$$\theta \;=\; \arccos(u_3) \tag{3.7}$$

$$\phi \;=\; \arctan(-s_3, -t_3) \tag{3.8}$$

Therewith, β and γ resolve, by rearranging the substitution and plugging them in (3.7) and (3.8):

$$\beta \;=\; \frac{\theta+\phi}{2} \;=\; \frac{\arccos(u_3)+\arctan(-s_3,-t_3)}{2} \tag{3.9}$$

$$\gamma \;=\; \frac{\phi}{2} \;=\; \frac{\arctan(-s_3,-t_3)}{2} \tag{3.10}$$

The same argumentation holds for:

$$\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} \;=\; \begin{pmatrix} \cos(4\alpha-2\beta)\sin(2\beta-2\gamma) \\ \sin(4\alpha-2\beta)\sin(2\beta-2\gamma) \\ \cos(2\beta-2\gamma) \end{pmatrix} \;=\; \begin{pmatrix} \sin(\theta_2)\cos(\phi_2) \\ \sin(\theta_2)\sin(\phi_2) \\ \cos(\theta_2) \end{pmatrix}, \tag{3.11}$$

so that $4\alpha - 2\beta = \phi_2 = \arctan(u_1, u_2)$ resolves with (3.9) to:

$$\alpha \;=\; \frac{\arctan(u_1,u_2)+\arccos(u_3)+\arctan(-s_3,-t_3)}{4} \tag{3.12}$$

N	200	300	400	500	600	700
$\Delta\alpha$ $[^{\text{rad}}/_{100}]$	3.8 ± 2.5	3.1 ± 2.0	2.7 ± 2.3	2.3 ± 1.5	2.1 ± 1.5	2.0 ± 1.4
$\Delta\beta$ $[^{\text{rad}}/_{100}]$	6.5 ± 5.4	5.0 ± 2.2	4.6 ± 3.2	3.9 ± 1.8	3.7 ± 2.2	3.3 ± 1.6
$\Delta\gamma$ $[^{\text{rad}}/_{100}]$	4.9 ± 4.6	3.8 ± 2.1	3.5 ± 2.9	3.0 ± 1.8	2.8 ± 2.2	2.5 ± 1.4

Table 3.1: Means of angle uncertainties over 1000 equal distributed random sets of Stokes vectors with standard deviations depending on the statistics N

Resubstituting $\{u_1, u_2, u_3\}$, the basis transformation angles of (3.12), (3.9) and (3.10) become:

$$\begin{aligned} \alpha &= \frac{\arctan(s_2t_3 - s_3t_2, s_3t_1 - s_1t_3) + \arccos(s_1t_2 - s_2t_1) + \arctan(-s_3, -t_3)}{4} \\ \beta &= \frac{\arccos(s_1t_2 - s_2t_1) + \arctan(-s_3, -t_3)}{2} \\ \gamma &= \frac{\arctan(-s_3, -t_3)}{2} \end{aligned} \tag{3.13}$$

3.2.4 Stability Analysis of Compensation Angles

An analytical solution is theoretically best suited to a known problem, but when we measure polarisation vectors with uncertainties, it is no longer precisely defined and the solution could drift. We want to know if our solution drifts away slightly, due to an uncertainty, or more rapidly. This task is called stability analysis and is usually done by calculating Gaussian error propagation.

$$\Delta s_i = \sqrt{\frac{1 - s_i^2}{n}} \tag{3.14}$$

$$\Delta t_i = \sqrt{\frac{1 - t_i^2}{n}} \tag{3.15}$$

$$\Delta\text{angle} = \sqrt{\sum_{i=1}^{3} \left[\left(\frac{\partial \text{angle}}{\partial s_i} \Delta s_i\right)^2 + \left(\frac{\partial \text{angle}}{\partial t_i} \Delta t_i\right)^2 \right]} \tag{3.16}$$

Δs_i and Δt_i are the uncertainties of the Stokes components of H_b and P_b in Bob's basis and n the number of photons measured for its Stokes component. For getting reliable values of angle uncertainties, the results in **table 3.1** are simulated over 1000 random sets of Stokes vectors. So, for 400 photons, in 1000 cases, the mean uncertainty of the calculated angle α is 0.027 radiance, due to statistical measurement uncertainties, with a standard deviation of 0.023 radiance. It is seen that the values decrease proportional to $^1/\sqrt{N}$ which is the expected phenomenon in error propagation of statistical errors. Also the standard deviations remain in the same order of magnitudes to the uncertainties, as it is expected for Poissonian distributions. Next is seen, that angle uncertainties of several hundreths of radiant are small compared to value ranges of $\alpha \in [0, ^\pi/_2]$ and $\beta, \gamma \in [0, \pi]$. So the solutions do not seem to be

unstable on average. Because of the different value ranges and extra terms in β the uncertainties are a bit higher in absolute values for the QWPs, for β than γ's. Also, the standard deviations are small, so they do not seem to vary much around being stable solutions.

In one particular case, it looks like the uncertainties diverge, if s_3 and t_3 decrease. This is the case when we measure H_b and P_b nearly linear in the equatorial plane of the Poincaré sphere, where R_b becomes more polar, of which we calculated its spherical angle ϕ_2. Also ϕ relates to a polar vector. So the more equatorial H_b and P_b become, the more uncertain ϕ and ϕ_2 gets, also, at the same time, the relevance of knowing ϕ_2 and ϕ precisely, shrinks. This is shown by the fact that the compensated polarisation vectors are just as accurate as due to any other uncertainty afflicted compensation. However, if the closeness to the equator is not a measurement uncertainty, the polarisation vectors get compensated up to machine accuracy. This is useful because $\arctan(0,0)$ is undefined if H_b and P_b approach perfectly the equator. So, with respect to the handedness of Alice's states compared to Bob's, we can redefine our compensation angles depending on if we have to turn the Poincaré sphere upside down or not:

$$\begin{array}{rcc} \alpha & = & \frac{1}{2}\arctan(\sqrt{1-t_2},\sqrt{1+t_2}) + \frac{\pi}{8} \mp \frac{\pi}{8} \\ \beta & = & \frac{\pi}{4} \pm \frac{\pi}{4} \\ \gamma & = & 0 \end{array} \tag{3.17}$$

3.2.5 Compensation Angles in circular Basis

As we will use a measurement setup that can just measure linear polarisation, it is necessary to transform the circular component into linear polarisaton. For the full tomography, we would measure each state twice. First, for the linear components and second, with compensation angles transforming to the circular component. For the basis transformation, we need the old angles of the compensation plates $\{\alpha', \beta', \gamma'\}$, to know how they already have been transformed. As we already have a mathematical tool, to rotate any arbitrary vector to $\vec{H}_a$ and $\vec{P}_a$, we should transcribe our new problem into the already solved one. The new angles $\{\alpha, \beta, \gamma\}$ have to fulfill the condition of rotating $\vec{S}_R$ to $\vec{S}_P$. As the old problem needs a second condition, we have a free degree of freedom to choose, for example $\vec{S}_H$ remains the same with the new angles. Thereby, we have all the information we need to figure out what $\vec{S}_H$ and

$\vec{S}_R$ look like, before they have passed the old compensation settings, to put them as $\vec{S'}_H$ and $\vec{S'}_R$ in the already solved problem, which rotates them to $\vec{S}_H$ and $\vec{S}_P$:

$$\underline{\mathrm{U}}^{-1}(\alpha', \beta', \gamma') \cdot \vec{S}_H = \vec{S'}_H \equiv \begin{pmatrix} s_1 \\ s_2 \\ s_3 \end{pmatrix} \tag{3.18}$$

$$\underline{\mathrm{U}}^{-1}(\alpha', \beta', \gamma') \cdot \vec{S}_R = \vec{S'}_R \equiv \begin{pmatrix} t_1 \\ t_2 \\ t_3 \end{pmatrix} \tag{3.19}$$

The resulting compensation angles are shown in **appendix A.1**, due to the large size of the formula.

3.2.6 Compensation Angles for imperfect Bob

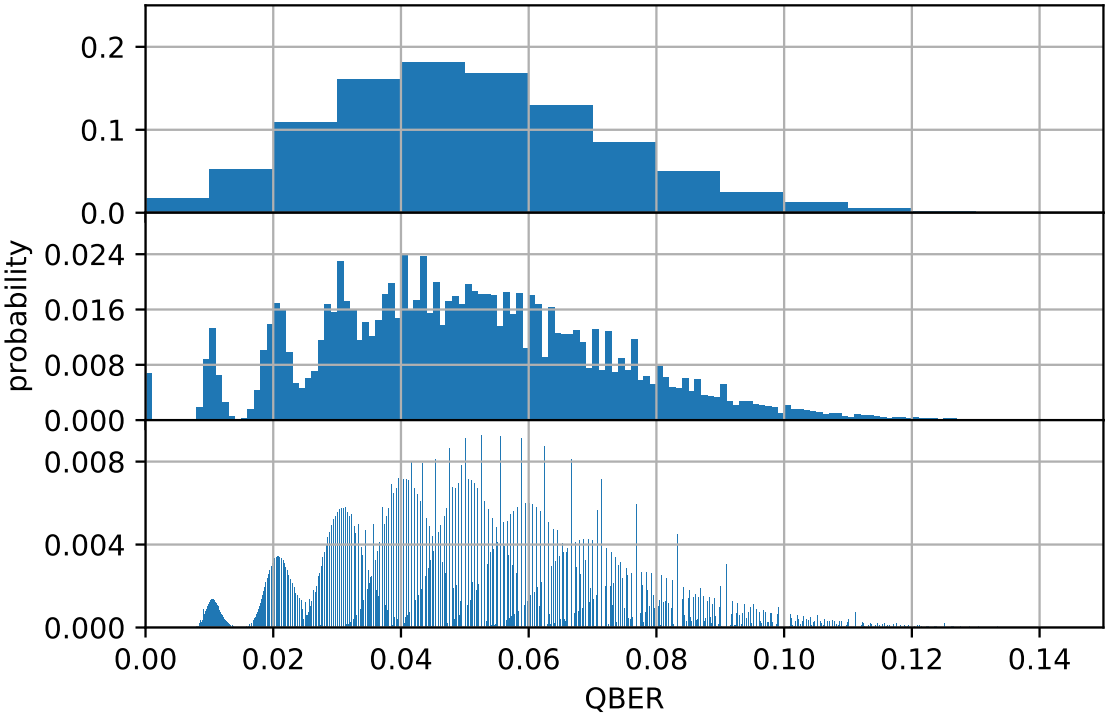
Supposing that there are polarisation-rotating components behind the compensation unit, measuring the Stokes components would be imperfect, despite good compensation. Measuring the rotation matrix of Bob after the compensation unit $\underline{\mathrm{U}}_b$ by repeating the compensation with full tomographic measurements, it iterates to compensate $\underline{\mathrm{U}}_b$, so that the compensation unit acts as its inverse $\underline{\mathrm{U}}_b^{-1}$. From now on, we can perform the inverse transformation to Bob's misalignment on every previously calculated compensation angles $\{\alpha', \beta', \gamma'\}$. To achieve compensation angles $\{\alpha, \beta, \gamma\}$, which do both transformations at once, we can transcribe the resulting transformation matrix into an already solved problem, which gives us compensation angles for any arbitrary rotation matrix.

$$\underline{\mathrm{U}}_b^{-1} \cdot \underline{\mathrm{U}}(\alpha', \beta', \gamma') \equiv \begin{pmatrix} s_1 & s_2 & s_3 \\ t_1 & t_2 & t_3 \\ u_1 & u_2 & u_3 \end{pmatrix} = \underline{\mathrm{U}}(\alpha, \beta, \gamma) \tag{3.20}$$

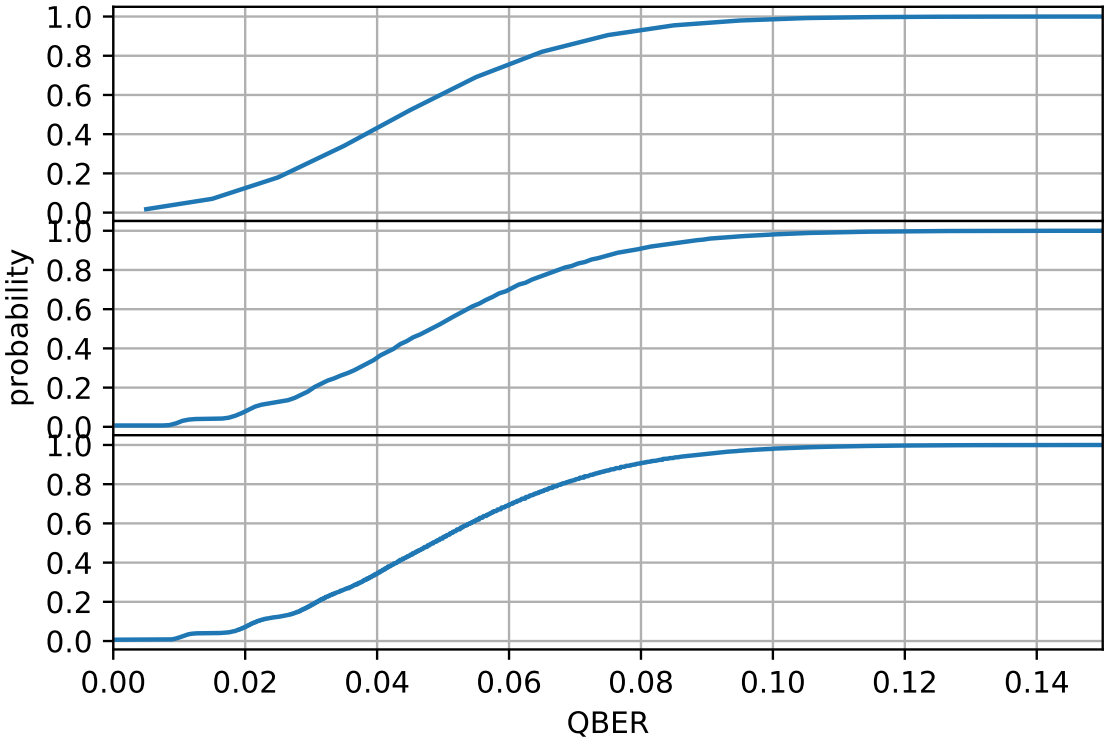
3.3 Influence of finite Statistics to QBER

In the end, we want to know which QBER of $\vec{H}$ and $\vec{P}$ is expected due to a statistics of n photons per Stokes component. Due to a descrete number of detected photons, Gaussian error propagation is not adequate. Assuming that the probability that photons hit the detectors V or M, respectively, with an expected probability of p, is binomial distributed, we can calculate how many photons k hit which detector with the probability $f(k, n, p)$.

$$f(k, n, p) = \binom{n}{k} p^k (1-p)^{n-k} \tag{3.21}$$



(a) QBER distribution



(b) cumulative QBER distribution

Figure 3.2: Simulated QBER distribution **(a)** and cumulative **(b)** of 0.05 mean QBER and 100 photons expected to measure per Stokes component and resolutions of 0.01, 0.001 and 0.0001 QBER bar width from the top to the bottom.

As we expect, measuring a certain number of photons N by a measuring time multiplied by a bandwith of photons per second, the probability $f(n, N)$ of measuring n photons is Poisson distributed:

$$f\left(n, N\right) \quad = \quad \frac{N^n \mathrm{e}^{-N}}{n!} \tag{3.22}$$

Thus, we can calculate the probability distribution of QBER $= {}^{k}/_{n}$, for example, with a mean of $p = 0.05$ QBER and $N = 100$ photons expected to measure per Stokes component:

$$P(\mathrm{QBER}) \quad = \quad P\left(\frac{k}{n}\right) \quad = \quad \sum_{n=1}^{\infty} \quad \sum_{k=n\cdot \mathrm{QBER}}^{n} f\left(k, n, p\right) \cdot f\left(n, N\right) \tag{3.23}$$

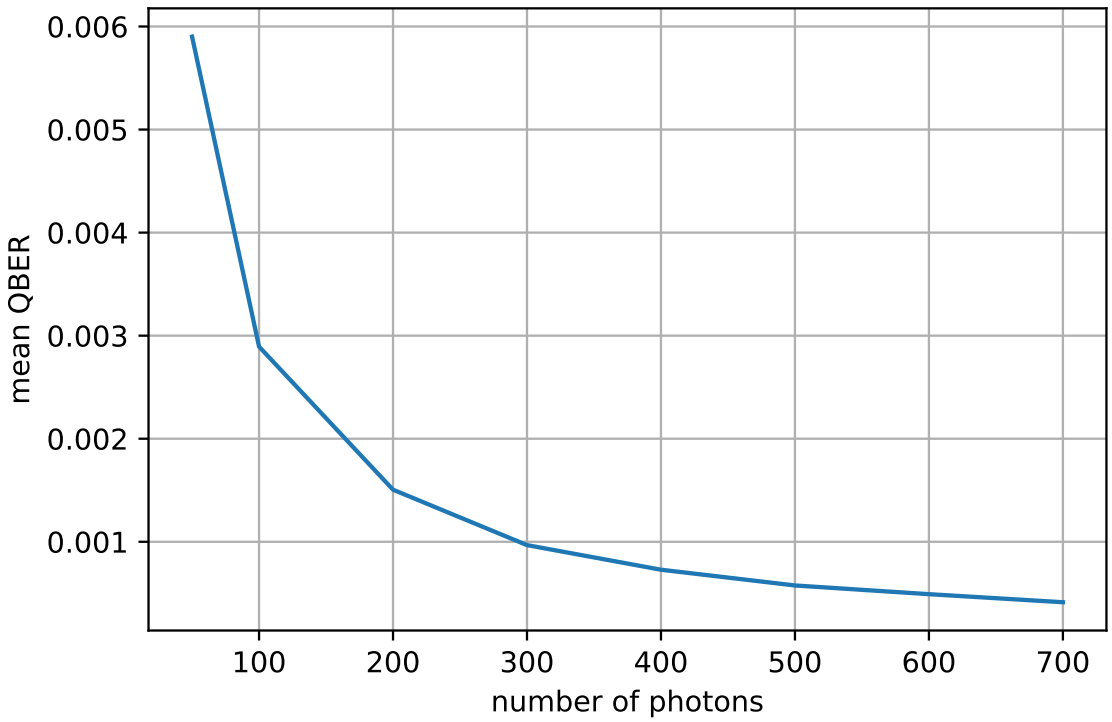
The results in **figure 3.2** show the distribution and its cumulative in different resolutions. A substructure is clearly recognisable, so that indeed, Gaussian error propagation could not be used.

To get the QBER, that occured due to finite statistics in our experiments, a simulation was made. In the simulation, two random Stokes vectors got orthonormalised $\vec{H}_b$ and $\vec{P}_b$, according to the assumptions that the atmosphere does not depolarise and does not change the polarisation up to first order. Then, their entries got discretised, due to a measurement with n photons per Stokes component, which is Poissonian distributed to N and yields the repetition of a Bernoulli experiment with the expectation value of each entry, to receive the discretised ones. Out of them, the compensation angles can be calculated, to compensate the non-discretised, originally polarised states $\vec{H}_b$ and $\vec{P}_b$, to receive $\vec{H}_a$ and $\vec{P}_a$. To measure them and to calculate their QBER, they again got discretised with the distributions. The mean QBER over an expected number of photons, is plotted in **figure 3.3 (a)** and their distribution through percentiles in **figure 3.3 (b)**, to make it comparable to measurement results.

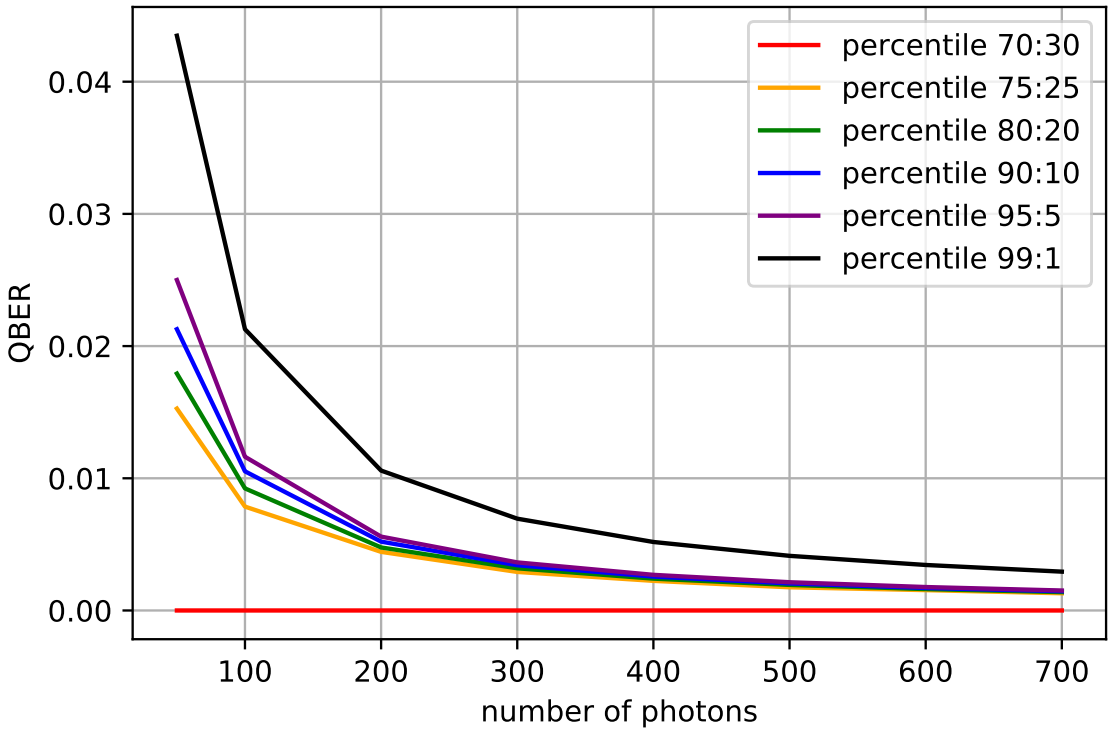
It is seen that the QBER decreases by ${}^{1}/\sqrt{N}$, as expected. Thus, the means are in a range of some promille QBER in more than 70% of all measurements, it is probable to measure no QBER up to more than 1% in one percent of the cases.

3.4 Influence of Background Radiation and Dark Counts to QBER

Apart from measuring the transmitted photons, background radiation hits the detectors as well. In addition, mostly from thermal origin, the detectors register counts without any incident light, the so-called dark counts **[51]**. For these effects, a new



(a) simulated mean QBER



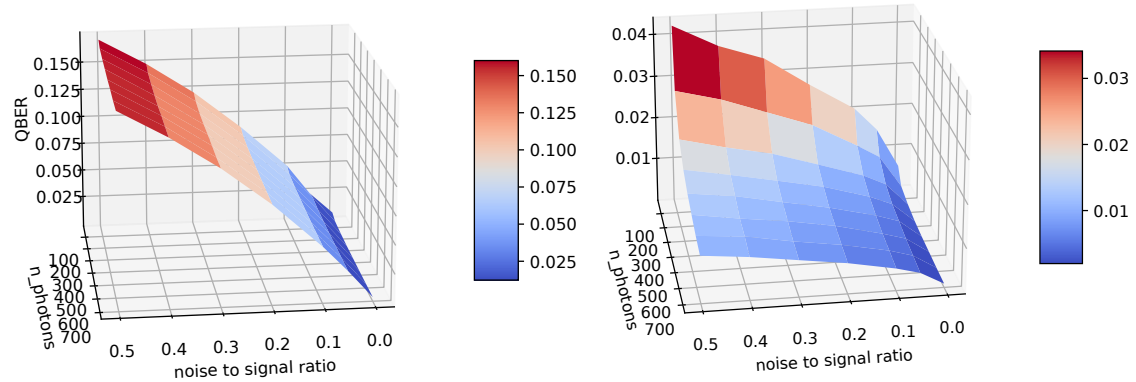
(b) with their distribution

Figure 3.3: Simulated mean QBER **(a)** and distribution **(b)** of the compensation angles due to finite statistics with 10,000 samples (plotted data tabulated in **appendix C.1**).

simulation has been conducted. It is similar to the first one of **section 3.3**, but with additional Poisson distributed photon numbers in each detector with an expected noise of half the signal times a noise to signal ratio. The results are shown in **figure 3.4a**.

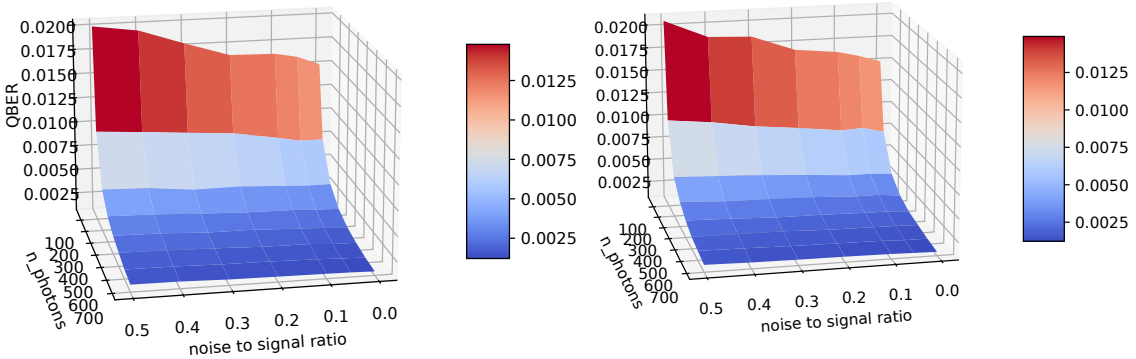
As expected, the QBER rises dominantly, if noise increases, due to minimal levels of photons in the detectors. As we want to know how the compensation was affected by the noise and not directly the QBER caused by the noise, the degree of polarisation of the states were normalised to 1, before they were evaluated in the simulation. The results in **figure 3.4c** show a strong relation between low QBER and a high number of photons.

To figure out if the compensation will work better if the expected noise will be subtracted from each detector, a simulation shows in **figure 3.4b** that the QBER would be more than quartered. There is still QBER left from the noise because not the noise was subtracted, but the expected noise, whereby the dependency on the statistics becomes more recognisable. The compensation does not improve qualitatively due to noise substraction, which is shown in **figure 3.4d**.



(a) QBER to noise and statistics

(b) noise subtraction of measurements before using for compensation



(c) QBER due to compenstion

(d) QBER due to compenstion after noise subtraction of measurements before using for compensation

Figure 3.4: Simulated dependency of mean QBER to noise and number of photons per Stokes component **(a)**. The states have been normalised to degree_of_polarisation = 1 in **(c)** and **(d)** and the mean noise was subtracted in **(b)** and **(d)** (plotted data tabulated in **appendix C.2-C.5**).

Chapter 4

Experimental Methods and Measurement Results

The previously explained compensation method is being tested experimentally for their quality and range of application in this chapter. Here, an experiment was created, which is explained in **section 4.1**. The experimental results are shown and analysed in **section 4.2**. Furthermore, achievements are compared to techniques and results of state of the art groups in **section 4.3**. Therewith, a prediction of the compensation under conditions similar those expected in the satellite mission are made **section 4.4**.

4.1 Experimental Implementation

To test the compensation method, a setup was used, as shown in **figure 4.1**, which can preparate, compensate and tomograph polarisation states. In the preparation

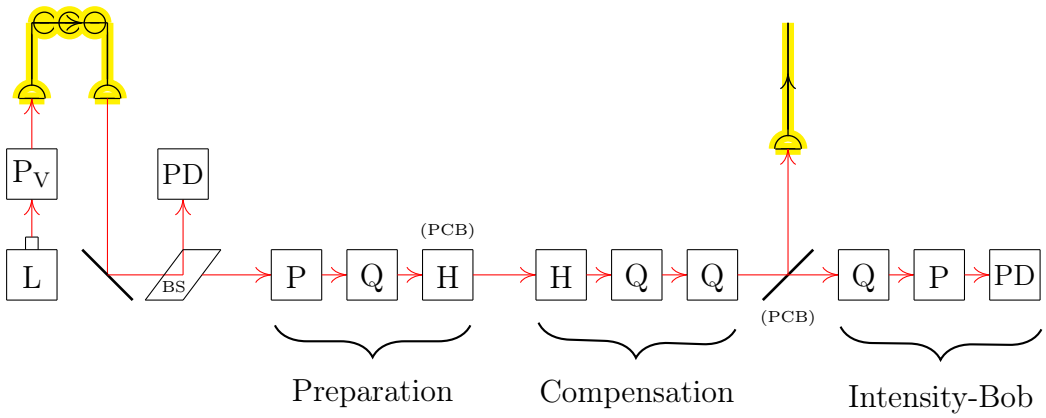


Figure 4.1: Main setup containing a laser diode (L), producing nearly vertically polarised light of $850nm$, a vertical polariser (P_V), two $850nm$ single mode fibres (yellow), two mirrors, of which the last one is addable to redirect the laser light to photon-counting-Bob (PCB), a 70/30% beam splitter (BS), two photodiodes (PD), two variable polarisers (P), four variable quarter wave plates (Q) and two variable half wave plates (H).

unit, a polariser and a QWP prepare states which are unitarily rotated. An additional HWP simulates polarisation change due to a satellite rotation. The compensation unit performs the backtransformation of the unitary distortion and the polarisation change caused by the simulated satellite rotation. We used two different tomography units, called intensity-Bob, shown in **figure 4.1** and photon-counting-Bob, shown in **figure 4.2**. With intensity-Bob, consisting of a QWP, a polariser and one photo diode, state tomography can be performed with low intrinsic QBER and high photon numbers. For the satellite mission, a setup, like photon-counting-Bob, will be used. Photon-counting-Bob performs a fast partial tomography even with low photon numbers by which extinction can be detected better.

In this paragraph, both setups are explained in a more detailed way: Monochromatic light with $850nm$ wavelength has been produced with a laser diode. A vertical polariser filters polarisation states of photons to be in the vertical state. For correcting laser intensity fluctuations, the intensity of 30% of the photons are measured with a photo diode and used as a reference. As the variable polariser in the preparation unit can be rotated, the first birefringing fibre has been adjusted such that light leaves the fibre circularly polarised, so that the light can never be extinguished by the polariser. With the variable polariser and the variable QWP, light can be prepared in states Alice would send after a unitary rotation. The HWP simulates the polarisation change of Alice's satellite rotation. The compensation unit consists of an HWP and two QWPs performing the in **section 3.2** described compensation. To direct the light to the different tomogration units, a mirror is addable. Intensity-Bob tomographes with a QWP, a polariser and a photo diode. The diode measures the light intensity of the state, which the QWP and the polariser do not filter out. Since intensity-Bob projects a state on only one basis, it is unsuitable for QKD. Photon-counting-Bob measures in $\{H, V, P, M\}$ projections simultaneously. For measuring the photons in two linear complementary bases, the beam had been split by a BS and a HWP performs a basis transformation to the second complementary basis. PBs separate the photons in a complementary basis by horizontally and vertically polarised photons, to receive conjugated states. According to the four linear basis states, the resulting four beams were coupled in four multi mode fibres, guided to four APDs, which count the photons in each beam. In order to tomograph in circular basis with photon-counting-Bob, a basis transformation had been performed with the compensation plates, described in **subsection 3.2.5**. As the birefringing single mode fibre behind the compensation unit which guides the photons to photon-counting-Bob rotates the polarisation states, their backtransformation must additionaly be perfomed by the compensation plates, as described in **subsection 3.2.6**.

To achieve that optical components, e.g. the HWP in the compensation, can rotate to a position, while performing a continuously rotation, a feedback loop was needed. The feedback loop processes the actual position of a motor and its desired velocity as an input. Thereby it adapts the number of steps, which a motor rotates in a loop, to match the position it would have had with the desired velocity over time. If the

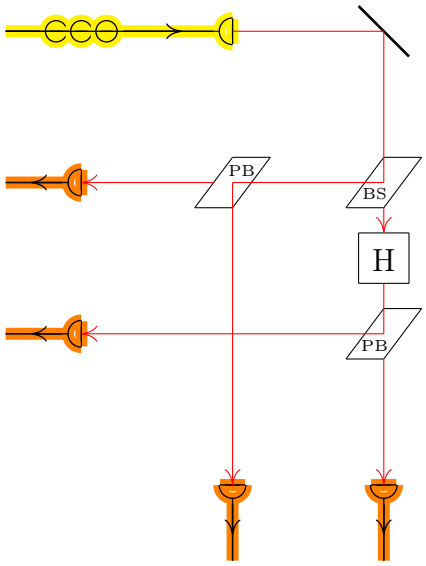


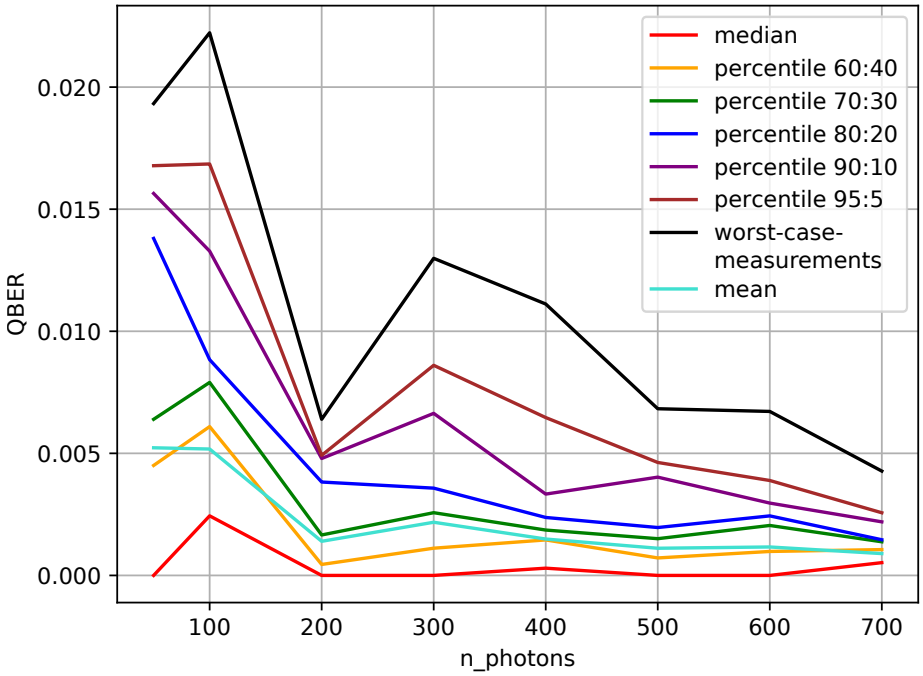
Figure 4.2: Set up of photon-counting-Bob containing one 850nm single mode fibre (yellow) in the upper left out of where the redirected laser light shines in and four multi mode fibres (orange) going out to four Avalanche photo diodes (APDs) **[52]**. Also installed is a mirror, a 60/40% beam splitter (BS), two polarising beam splitters (PB) and a fixed half wave plate (H) at 22.5°.

continuously rotating HWP of the compensation unit has to be moved by an extra amount of steps, e.g. according to a basis transformation or after a compensation, the desired position can simply be shifted by the amount of steps. In order to avoid accumulating step errors, it is necessary to maintain the underlaying rotation in the initial feedback loop. Furthermore, to achieve fast adaption without oversteering, the feedback loop stops the rotating motor and actively rotates it to the desired position once, after which its rotation continues. Thereby, the velocity can also be adapted and the position readjusted, e.g. if the angular velocity of the satellite changes over time.

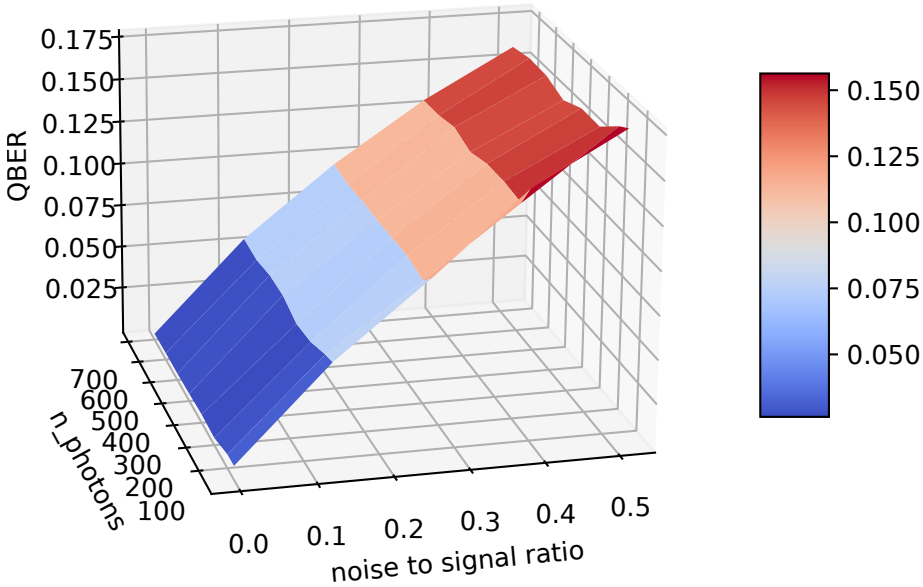
4.2 Full Compensation Sequence Test Results

With intensity-Bob, we figured out the quality of the compensation under ideal conditions, shown in **figure 4.3**. With photon-counting-Bob, we investigated the range of application of the compensation on a simulated satellite rotation, shown in **figures 4.4-4.6**. Here, the QBER of the compensated states was used as a measure of quality, because it is a limiting factor for performing QKD.

For testing the quality of compensation with intensity-Bob, two random states, which enclose an angle of 90° on the Poincaré sphere, were prepared, measured and descretised according to the procedure of **section 3.3**. The measured data was used to compensate both of the states to H and P, which finally got measured, descretised



(a) distribution of measured QBER dependent on photon number



(b) measured dependency of QBER to noise and number of photons

Figure 4.3: QBER measured with intensity-Bob include 20 samples in each data point. The distribution dependent on the photon number is shown in **(a)** and the dependency of mean QBER on noise and photon numbers in **(b)** (plotted data tabulated in **appendix C.6, C.7**).

and their QBER calculated. In a further step, background noise was artifically added to the measured data according to the procedure of **section 3.4**. For each noise and photon number grid node, the procedure was repeated 20 times, so that one data point consists of 40 QBER values, 20 of H and 20 of P polarisation states.

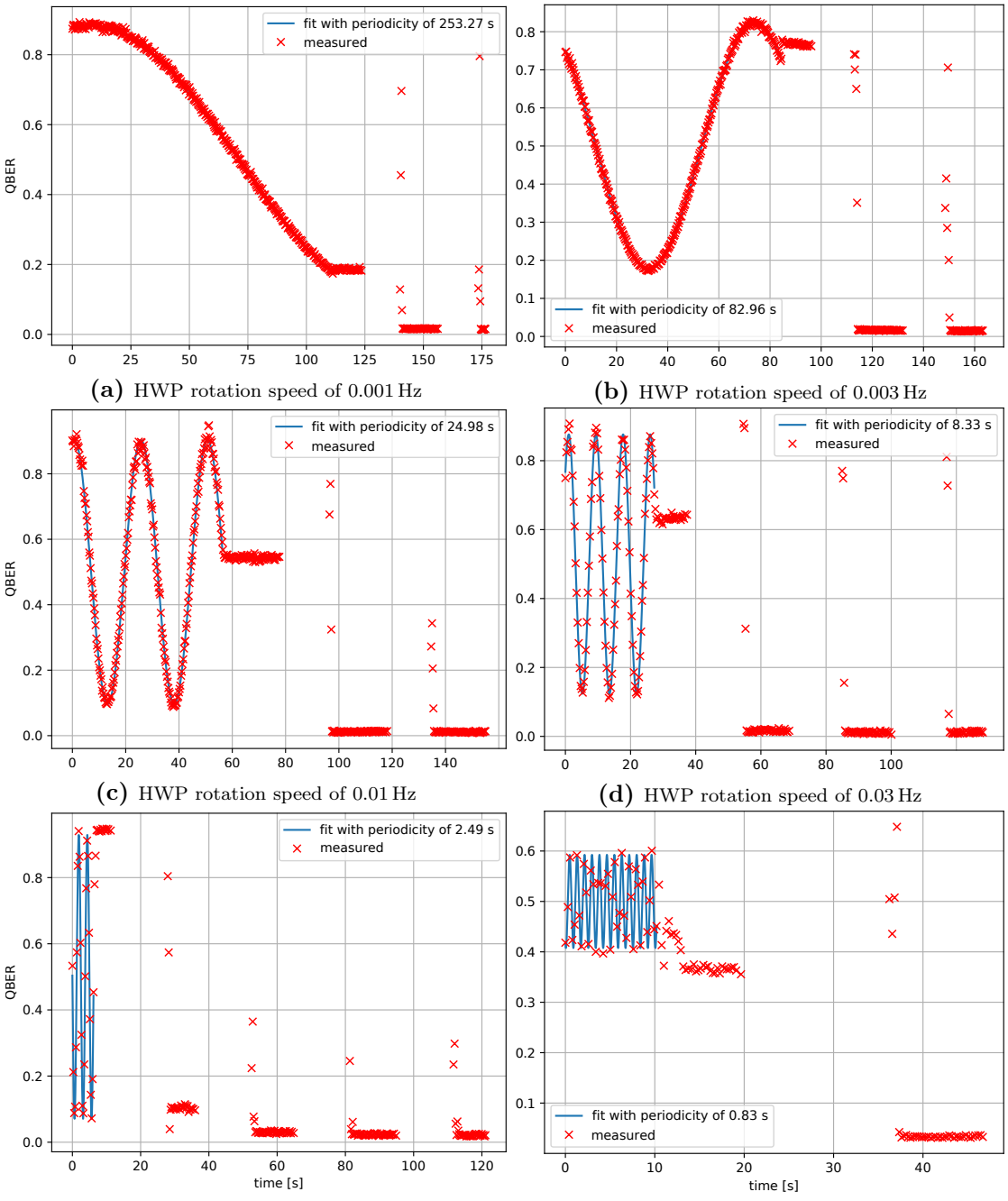
The QBER distribution over the photon numbers in **figure 4.3a** is in the same range and similar to the simulated distribution predicted in **figure 3.3**. The measurement results seem to be somewhat lower than the simulated ones, which is probably caused by the assumed distributions in **section 3.3**. As the measured mean is higher than the median, most measurements are lower than its mean, but the ones higher are more spread out. The measured graph of **figure 4.3b** is also somewhat lower with similar dependencies of QBER to noise and number of photons, compared with the simulated predictions in **figure 3.4a**. Therefore, it is likely that the QBER part, which was caused by misaligned compensation and not noise, is also in the same scale as predicted in **figure 3.4c**, which is weakly dependent on noise.

With the compensation unit in its initial position, the setup with intensity-Bob rotates polarisation with the following Mueller matrix $\underline{\mathrm{MM}}$, describing a unitary process, (4.1) (measured states in **table C.8**), which is negligible. Also the measured states show that the intrinsic QBER from intensity-Bob is lower than a promille for linear states, which is negligible for the measurement evaluations.

$$\underline{\mathrm{MM}} = \begin{pmatrix} 1.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.9999257 & 0.0121741 & -0.0006600 \\ 0.0 & -0.0121603 & 0.9997658 & 0.0178987 \\ 0.0 & 0.0008777 & -0.0178893 & 0.9998396 \end{pmatrix} \tag{4.1}$$

To test the compensation on a simulated satellite rotation, photon-counting-Bob was used, because it is a similar tomography unit to that which will be used in the satellite mission. Moreover, the reference diode for correcting laser intensity fluctuations will not be used. To show the compensation of the simulated satellite rotation, the compensating HWP rotation does not start immediately. **Figure 4.4** shows for different rotation frequencies the QBER of the H states, measured with the H and V detectors. It is recognisable that the oscillation is in a smaller range than 0 to 1 QBER, which is because the initial polarisation states are not necessarily totally linearly polarised. A fit to the oscillation, caused by the simulated satellite rotation, shows how accurate a frequency determination could be by tracking the change of polarisation. The fitted periodicities reveal that the slower the rotation speed is, the longer the measurement must take, which could already be too long during a satellite overflight. Furthermore, strong intensity fluctuations could be challenging with low photon numbers per time, so that an investigation of a high accurate frequency fit under those conditions will not be pursued.

With the start of the compensation process, the graphs show gaps in the QBER recordings. As soon as the compensation process is over, the QBER will be recorded



(a) HWP rotation speed of 0.001 Hz

(b) HWP rotation speed of 0.003 Hz

(c) HWP rotation speed of 0.01 Hz

(d) HWP rotation speed of 0.03 Hz

(e) HWP rotation speed of 0.1 Hz

(f) HWP rotation speed of 0.3 Hz

Figure 4.4: Test results with photon-counting-Bob showing QBER over time for measuring the QBER of H states for different HWP rotation velocities. A sine curve was fitted by least square method to the oscillating QBER of H states according to the simulated satellite rotation. With half of the satellites angular velocity, the HWP of the compensation starts to rotate, which compensates the oscillation (first plateau). Compensation takes place during the gaps. The lowest plateaus are of intrinsic QBER.

prepared states	H	V	P	M	R	L
intensity	1	1	1	1	1	1
H/V basis	0.9602	-0.9658	-0.0505	0.0407	0.2206	-0.2353
P/M basis	0.0748	-0.0810	0.9832	-0.9825	-0.1764	0.1592
R/L basis	-0.1059	0.0945	0.1092	-0.1080	0.9803	-0.9854
dop	0.9689	0.9738	0.9906	0.9892	1.0202	1.0256

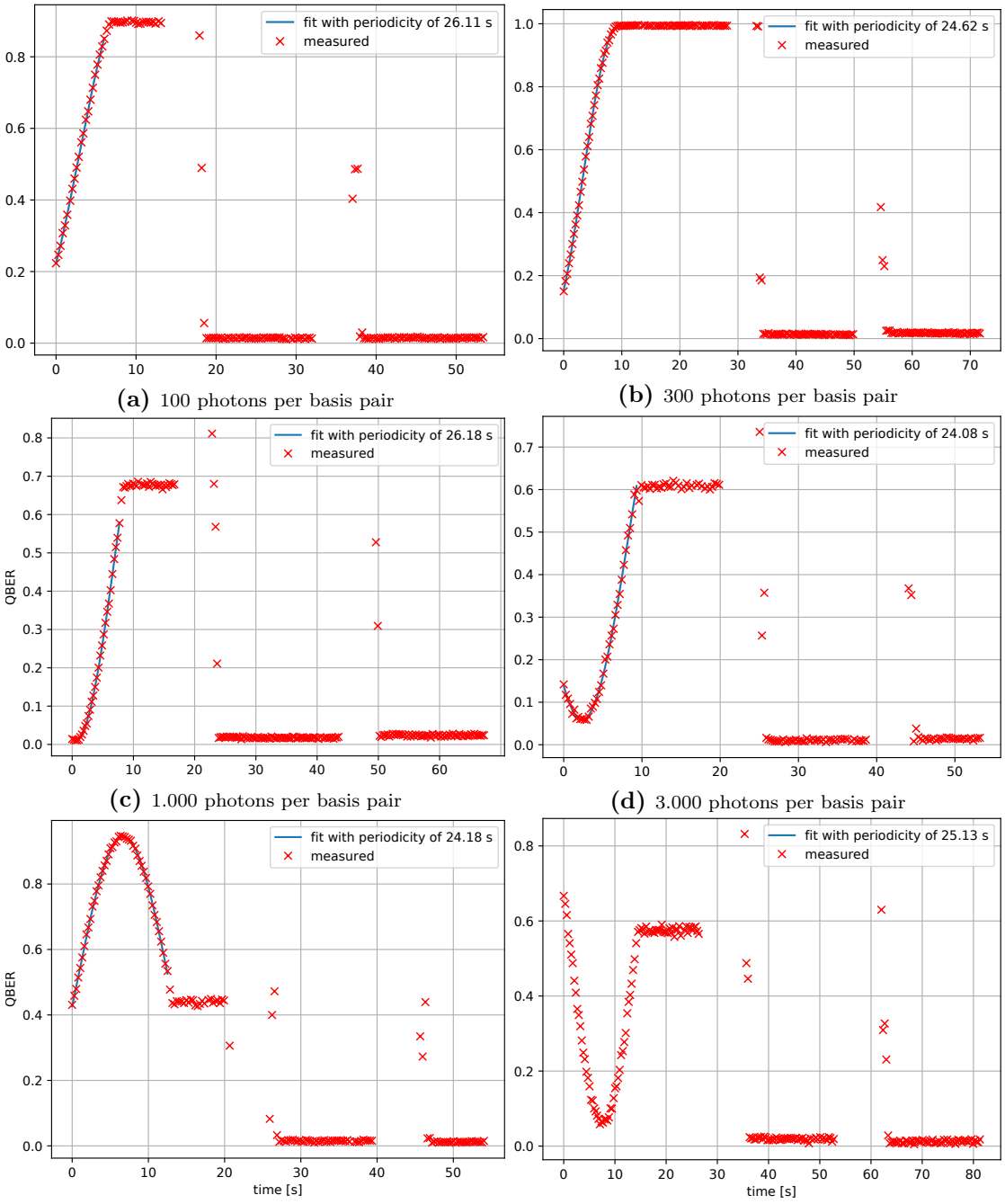
Table 4.1: Measured states with photon-counting-Bob after some compensations (their Mueller matrix, describing a unitary process, is shown in **equation** (C.1)). The degree of polarisations (dop) greater than one are unphysical and were probably caused by waveplate imperfections and different coupling efficiencies **[53]** when basis transforming.

again, even if the compensation plates are not already in their final positions, which explains the data points with higher QBER than of the compensated plateaus. For measuring both prepared states two times during the compensation, once before and once after a basis transformation, the intensities will be measured over one second, which results in 4 seconds measuring time. Also waiting times of 3 seconds were arranged after each plate rotation, consuming 12 seconds. Thereby, a compensation process takes between 15 and 20 seconds.

After some compensations, all six basis states were tomographed with photon-counting-Bob, which are shown in **table 4.1**. The measured states demonstrate the intrinsic QBER of photon-counting-Bob being between $1 - 2\%$, possibly caused by polarisation losses in the beam splitter, the two polarisation beam splitters and the fibre couplers. The states also shows the conservation of orthogonality, whereby it is likely that orthogonal states behave similarly in the setup.

Also measurements have been made with different measuring times of tenths to thousandths of a second, corresponding to different measured photon numbers per basis. Typically good results are shown in **figure 4.5** and typically bad (in which more than one compensation had to be done to reach intrinsic QBER), shown in **figure 4.6**. It seems that more bad cases appear, if the photon number gets smaller, e.g. up to every second case with 300 photons and lower and seemingly none for photon numbers with at least 3.000 after half a dozen of tries.

Here, only 3 waiting times are remained and further reduced to 1.5 seconds between a rotation and a mesurement. The plate rotations are the second biggest time consumers after the waiting times. For each compensation, two basis transformations, one compensation adjustment and one change in preparation had to be done, which causes up to 3 seconds rotation time, as one 360° rotation would consume about a second. Thereby, a compensation process takes between $6 - 8$ seconds.



(a) 100 photons per basis pair

(b) 300 photons per basis pair

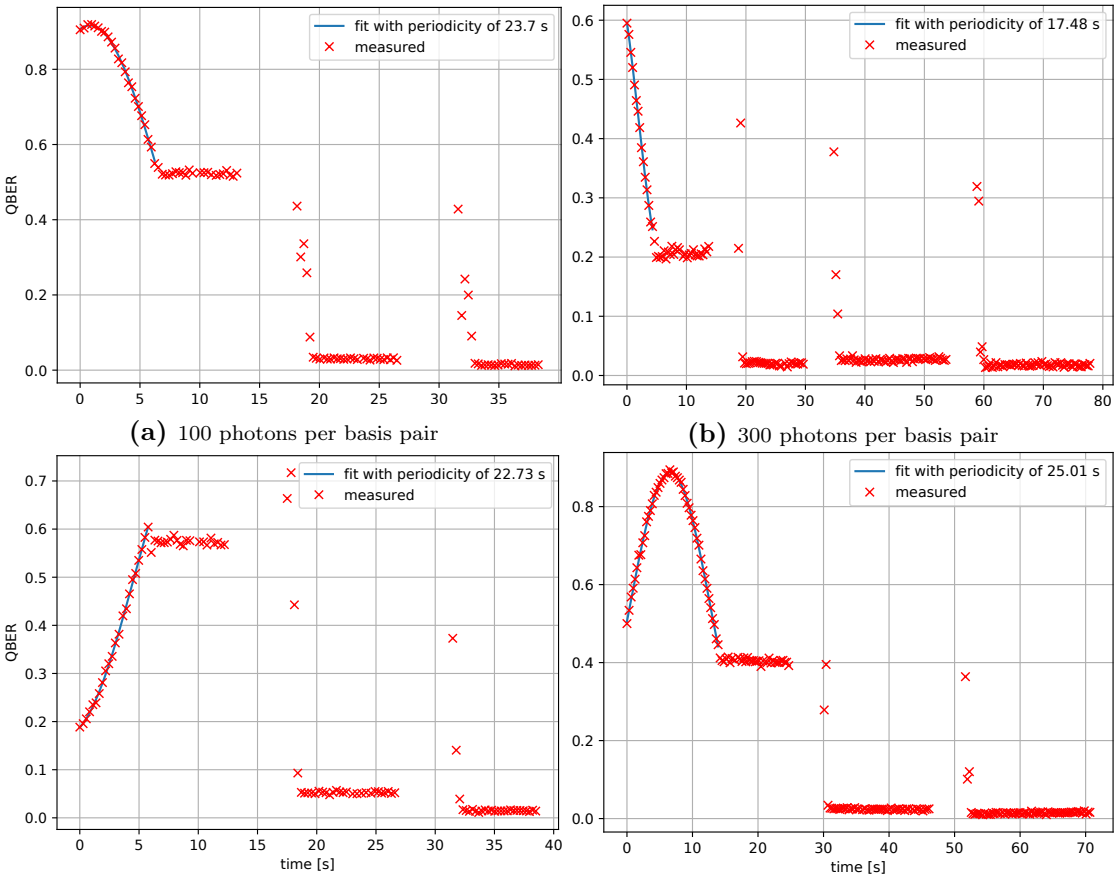
(c) 1.000 photons per basis pair

(d) 3.000 photons per basis pair

(e) 10.000 photons per basis pair

(f) 30.000 photons per basis pair

Figure 4.5: Best test results with photon-counting-Bob of rotating the HWPs with 0.01 Hz, showing QBER over time for measuring the intensities of detectors H and V for different measurement times corresponding to different photon numbers per basis pair.



(a) 100 photons per basis pair

(b) 300 photons per basis pair

(c) 1.000 photons per basis pair

(d) 3.000 photons per basis pair

Figure 4.6: Bad test results with photon-counting-Bob of rotating the HWPs with 0.01 Hz, showing QBER over time for measuring the intensities of detectors H and V for different measurement times corresponding to different photon numbers per basis pair.

4.3 Comparison with State of the Art Implementations

As they made similar progress, we want to compare the techniques and results of the Jennewein group to ours in **subsection 4.3.1**. Therein, it is compared to their simulations **[54]** of their compensation method and two field trials that implemented it. There, BB84 decoy-state quantum signals were exchanged in simulated satellite uplinks to receivers, traveling at angular speeds consistent with a LEO satellite. They demonstrated QKD transmissions from the ground to a moving truck **[55]** and an aircraft in flight **[11]**, which our group performed first, 4 years earlier **[10]**. Since there are several approaches to implement QKD, **subsection 4.3.2** is about alternative realisations.

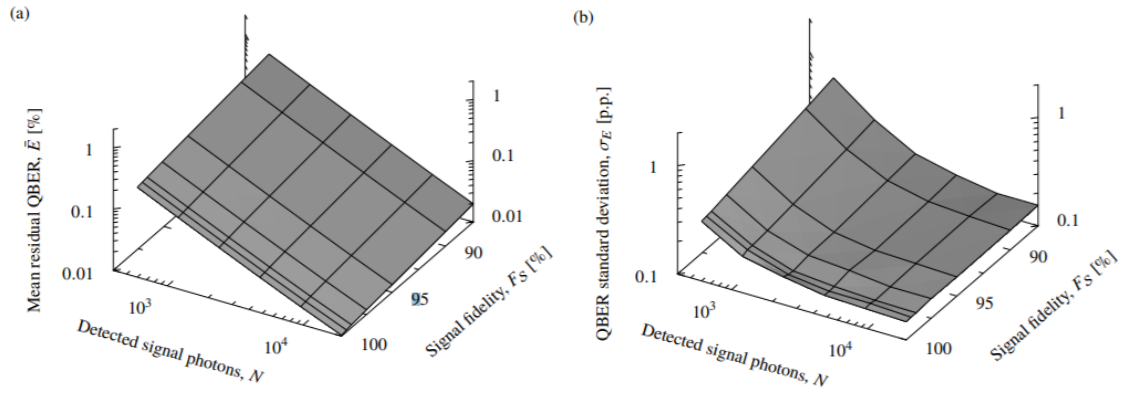


Figure 4.7: Performance of the reversed polarization alignment protocol. (a) Mean residual QBER of nominal signal states after optimized compensation based on characterization analysis of N detected signal photons with intrinsic signal fidelity F_S at the receiver. Only a few hundred photons are required to achieve low mean QBER. (b) Standard deviation of the QBER. Low photon counts and low intrinsic signal fidelities significantly increase the variation of performance between applications of the protocol.

4.3.1 Methods and Results of the Jennewein Group

In their simulations, they distinguished between compensating at Bob's receiver, which they called the "forward protocol" **[54]** and at Alice's transmitter, the "reversed protocol" **[54]**, which both gave similar results, shown in **figure 4.7**. For compensating, they used a QWP, a HWP and a second QWP with backtransformation-matrix $\hat{V}(\theta_1, \theta_2, \theta_3) = \hat{Q}(\theta_3)\hat{H}(\theta_2)\hat{Q}(\theta_1)$. This is similar to our compensation unit, though the order is different. Also they used the second QWP as a basis-changer, so that they measured in $\hat{Z}$ and $\hat{X}$ basis when the last used QWP is at 0°-position and in $-\hat{Y}$ and $\hat{X}$ basis when the QWP is at 45°-position. We use all plates for the basis transformation depending on the angles set. For characterising their measurements, they calculated its density matrix $\hat{\rho}_n = (2F_S - 1)\left|\Psi_{b,n}\right\rangle\left\langle\Psi_{b,n}\right| + (1 - F_S)\hat{I}$, where F_S is the signal fidelity, using maximum likelihood estimation for each n. We, however, use formulas of **subsections 2.2.1** and **3.2.2** to approximate a backtransformation, describing a unitary process. For calculating their compensation angles, they minimised by least-square method the cost-function $C = -\sum_n \left\langle\Psi_{a,n}\right| \hat{V}(\vec{\theta})\hat{\rho}_n\hat{V}^\dagger(\vec{\theta})\left|\Psi_{a,n}\right\rangle$, which is "the negative sum of fidelities between each predicted state, after applying the compensation operation, and the corresponding initial state" **[54]**. Our group instead used a direct, much faster analytical formula.

For classifying their compensation method, they did Monte-Carlo-simulations, which investigate the dependencies of QBER to signal fidelity and the number of detected photons. They found out that the overall performance and variability of the reversed protocol is very similar to the forward protocol. In their simulations, they achieved a QBER of 0.39% with an intrinsic fidelity of 95% and overall 600 photons, which

are 100 per input state. If we use 100 photons per Stokes component determination, our protocol would use also 600 photons for compensation, resulting in 0.3% QBER, which is a slightly better result.

Also, they simulated Poissonian background noise and tried a removal strategy, in which they subtracted the mean of a pre-calibrated background level, "while guarding against unphysical negative counts" **[54]**. Their results "indicate that background subtraction is not better, and in many conditions clearly worse, than leaving the counts with background unaltered" **[54]**. Our simulations confirm that background subtraction does not yield better compensation results.

They implemented their polarisation alignment protocol in two laboratory experiments and a field trial. There, they used "up-conversion of a mode-locked $810nm$ Ti:sapphire laser (featuring a high clock rate of 76 MHz) with a 1550 nm polarization-modulated continuous-wave telecom laser" **[56]**, a weak coherent pulsed 532 nm QKD signal source and a fiber-based balanced Mach-Zehnder interferometer **[57]** as a polarisation modulator. As they used "85 m of single-mode optical fiber, guiding QKD states from the source in a temperature-controlled laboratory, through the core of the building, to the transmitter on the pointing stages located in an open-air dome on the building's roof" **[56]**, they had to improve their alignment protocol by an active, automated, every-second polarisation correction, because with "such a long fiber, continuous movement and temperature fluctuations dominated contributions to the QBER" **[56]**. Tested in a preliminary laboratory test, by using the first 10 000 detection events every second, resulted in $6 - 7\%$ intrinsic QBER, see **figure 4.8**. Within circa 5 seconds of inducing polarisation disturbances by manipulating the fiber, the compensation was mostly delayed "by the limited rotation speed of the compensation wave plate mounts (up to 2.25 seconds for the longest trip), combined with settling of the manipulated fiber, and the up-to 1-second delay inherent to the data collection" **[56]**. Our compensation, however, takes a similar amount of time to compensate to the intrinsic QBER level of its measuring apparatus.

In their first field-trial, they put Alice in the back of a truck and compensated only at Alice's side to correct rotations from the source up to the free-space link to Bob. In this setup "with about 4300 detections each second, it maintained a received QBER of approximately 6%, very close to the intrinsic QBER of the source, and allowing positive key distillation" **[55]**.

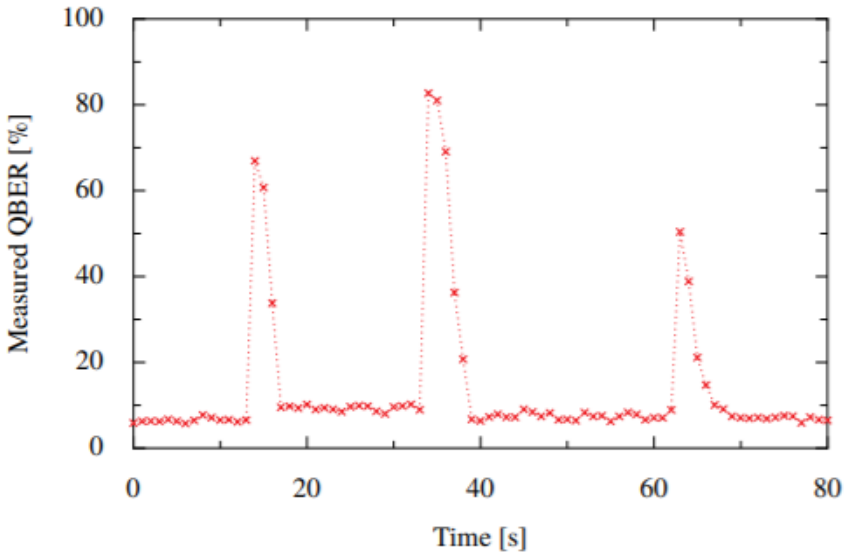


Figure 4.8: Experimentally measured QBER (points) with automated application of the polarization alignment protocol, based on analysis of 10 000 detections each second. Dotted lines act as visual guides. Sudden increases in the QBER were caused by rapidly moving fiber polarization controller plates by hand, and were almost immediately corrected by the protocol—limited, primarily, by the speed of the rotating motors, taken from **[56]**

In their next field trial, "a similar on-line compensation approach has also most recently been utilized in next-generation apperatures - which include larger telescopes, integrated receiver optics, and a 400 MHz QKD-state source at 785 nm with intrinsic QBER of only approximately 1% - to support a demonstration of QKD transmitted from the ground to an aircraft in flight" **[11]**. 4 years earlier, our group was the first proving the feasibility of BB84 QKD between an aeroplane and a OGS **[10]**. There, a motorised polarisation controller was developed, also using three waveplates to compensate for arbitrary polarisation rotations. It also compensated the polarisation change of the rotating OGS mirrors, whose angular positions were modelled and transcripted in angular functions for the compensation setting. After 38 dB loss, a dead count and a stray light rate of $500\,s^{-1}$ each, we achieved a receiving signal count rate of $800\,s^{-1}$ with an average QBER of 4.8%.

Also, they developed a method to distinguish if high measured QBER came from bad basis alignment or time synchronisation **[56]**. Therein is explained that in case of bad time synchronisation, tagged measurement outcomes do not correspond to source events, whereby the probability to measure the intended states decreases to 25%, which makes the measurement outcome equivalent to a completely incoherent mixture. By collecting sufficient detection statistics in the four linear measurement bases, it is still probable to measure at least $^3/_8$ of the states correctly, whereby it is possible to differentiate between misaligned timing and misaligned polarisation regimes.

4.3.2 Different Approaches for QKD Implementations

In 2011, a group in Tokyo, Japan, M. Toyoshima et al. **[58]**, performed QKD with a $\lambda = 0.86\,\mu m$ quantum channel using B92 protocol **[59]** over 1 km free-space between two Tokyo skyscrapers. They compensated polarisation rotations with a rotating HWP, optimising a minimum intensity after a fixed polariser with a reference beam of $\lambda = 1.5\,\mu m$ wavelength. With a pulse rate of 100 MHz and a loss of 10.3 dB, they received in average 0.0962 photons per pulse, a QBER of 0.57% and a sifted key rate of 240.21 kbps.

In 2013, a group from China in Harbin, G. Zhang et al. **[60]**, proposed a method, where the beacon of a satellite can be used twofold, for pointing of satellite and OGS and for polarisation determination, which can be used for compensation, e.g. by a proposed HWP. A group in Beijing, Li et al. **[61]**, proposed in the same year that for compensation, a beacon signal should not be transmitted utilising wavelength division multiplexing but rather time division multiplexing. The recommendation is based on simulations of polarisation state evolutions under different orbits with different results depending on the wavelength of the used photons. They also discussed the possibility of calculating the polarisation rotations of all the trajectories in advance of which the compensation settings could be determined.

4.4 Expected Behaviour under Satellite Mission Conditions

For the purpose of a satellite mission, we developed and tested a concept for compensation under as many realistic conditions as possible. Based on internal simulations, we expect a satellite rotation frequency of less than a Hertz, a background noise rate after time filtering **[10]** of $BNR = 200\ {}^{\text{photons}}/_{\text{second}}$, a dark count rate of $DCR = 100\ {}^{\text{photons}}/_{\text{second}}$ and a signal loss, including margins, of $45 - 55$ dB, depending on the beam propagation ratio or beam quality, which is expected to be between $1 < M^2 < 3$. Our satellite will be in $z = 500\,\text{km}$[1] low earth orbit (LEO). We will send on average $\mu = 0.5$ photons per pulse with a pulse repetition frequency of $PRF = 100\,\text{MHz}$ and a wavelength of $\lambda = 850nm$. The beam can be approximately Gaussian with a smallest radial beam waist width of $\omega_0 = 7.07\,\text{mm}$, so that at a distance from the optical ground station, the beam will be widened to at least $38m$ in diameter (4.4). With aperture diameters of $M_1 = 825\,\text{mm}$ and $M_2 = 288\,\text{mm}$, see **figure 4.9**, we will collect 3.26‰ of the photons[2], due to Gaussian widening and the dimensioning of the optical ground station, which causes the main loss[3]of

[1] possibly just in an altitude of $400km$, when the planning stage is over

[2] The ratio of the area integral (power) of the intensity (4.3) at $z = 500\,\text{km}$ from $x = 0$ to $x = M_1$ minus the power from $x = 0$ to $x = M_2$ over the power from $x = 0$ to $x = \infty$.

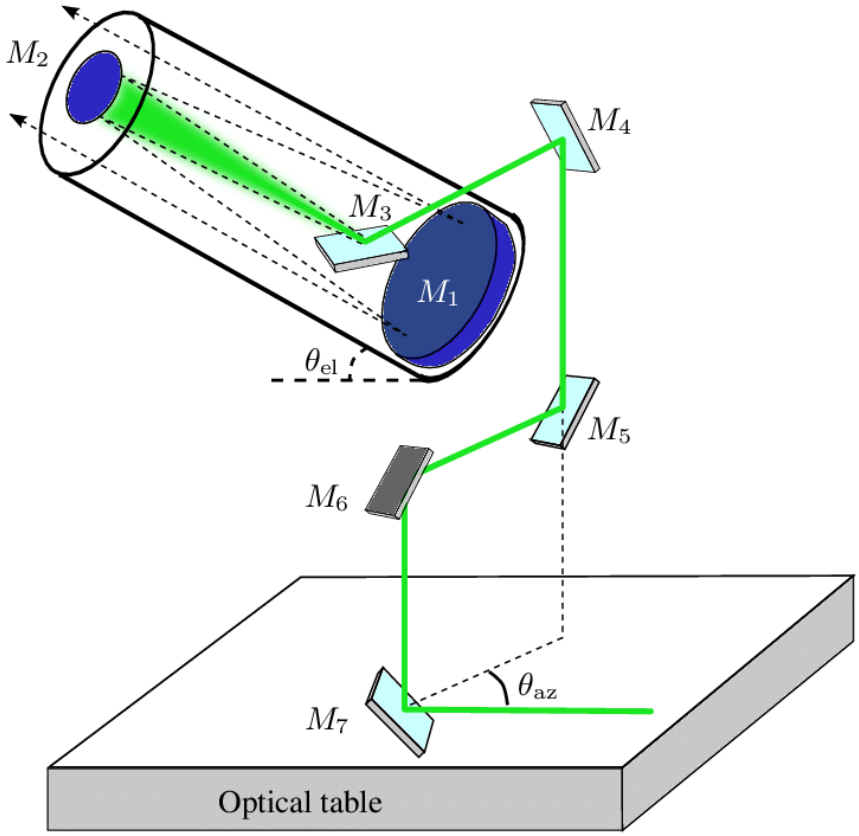


Figure 4.9: Coudé path of an optical ground station **[62]** with our M_3 being eliptical

25 dB. Other loss effects are due to atmospheric attenuation, mirror efficiencies and satellite to telescope focus inaccuracy. With a signal loss rate (SLR) in a range of $[10^{-5.5}, 10^{-4.5}]$, the transmission rate (TR) will be:

$$TR \in PRF \cdot \mu \cdot SLR \approx [158, 1581] \,{}^{\text{photons}}/_{\text{second}} \tag{4.2}$$

With an overall noise rate of $NR = BNR + DCR = 300 \,{}^{\text{photons}}/_{\text{second}}$, we will expect a range of noise to signal of ${}^{NR}/_{TR} = [0.2, 1.9]$. For measuring at least 500 signal photons for an accurate Stokes component determination, we will therefore measure at least between $0.3 - 3.2$ s. As we determine two Stokes components per measurement and as we measure two times two polarisation states each, we will require a total time of measurement of $2.5 - 25.3$ s. For comparison, according to a rough estimation, see **appendix B.3**, the OGS can track the satellite for at most 11 min.

[3] loss $= 10 \log_{10}$ (power_ratio) dB

$$I(x,z) = I_0 \left(\frac{\omega_0}{\omega(z)} \right)^2 \exp\left(-\frac{2x^2}{\omega^2(z)} \right) \tag{4.3}$$

$$\omega(z) = \omega_0 \sqrt{1 + \left(\frac{z\lambda}{\pi\omega_0^2} \right)^2} \tag{4.4}$$

Figure 4.10: Intensity of a Gaussian beam with its radial transversal coordinate x, its axial coordinate z in propagation direction, I_0 as a normalisation intensity constant and its radial beam waist width $\omega(z)$, containing $1 - 1/e^2 \approx 86.5\%$ of the intensity, taken from **[63]**.

The compensation method, which was first described in this thesis, was tested under noise conditions, which only have a negligible effect on the compensation, as shown in **figure 3.4c**. The quality of continuous wave plate rotations was tested for different satellite angular velocities for the expectable range of $0.002 - 0.6\,\mathrm{Hz}$ without discontinuous fluctuations, presented in **figure 4.4**. Measurements with intensity-Bob, depending on different photon numbers, were well compatible to the theory, to see in **figure 4.3a**, resulting in low QBER with at least 300 photons for determining one Stokes component of a state. Measurements with photon-counting-Bob reveal higher average QBER (after removing intrinsic QBER), clearly seen in **figure 4.5**, which is probably caused by setup imperfections and cancels out by increasing the photon number to 500.

As this compensation method compensates as quickly and robustly down to the intrinsic QBER as other methods in preliminary laboratory tests, which later succeed in proof-of-principle experiments in up- and downlinks to an aeroplane, separately performed by our and the Jennewein group, it is likely that this compensation method will succeed in field-tests as well.

Chapter 5

Conclusion and Outlook

In this thesis, a compensation method was developed, implemented in simulations and experiments and analysed for its quality. It was investigated up to which QBER can be compensated under satellite mission conditions such as background noise, photon statistics and satellite rotation frequency. With intensity-Bob, the same results as those from the simulations could be achieved: background noise is negligible for the compensation and with at least 300 photons per Stokes component determination, the compensation reaches intrinsic QBER levels.

For a more precise working partial tomography unit, called photon-counting-Bob, of which a similar one will be used in our satellite mission, full tomography was achieved by basis transformation through the compensation plates. However, the QBER was only reliably compensated to intrinsic level with at least 500 photons per Stokes component determination, probably due to setup imperfections. As a rotating HWP compensates the simulated satellite rotation, the results did not depend on the satellite rotation frequency.

Summarised, this paper offers a robust compensation method for reference-frame mismatches between a receiver and a transmitter. This method enables the exchange of polarisation states with a low quantum bit error rate (QBER) by using only a few signal photons of 4000, especially appropriately designed for our satellite mission scenario.

One question remains if the transmission rate fluctuates between two measurements of one polarisation state, the orientation of the state on the Poincaré sphere could have changed which would lead to incorrect compensation. One suggested solution could be that because the H/V-basis gets measured twice of each polarisation state, the second measurement could be used as calibration to adjust all measurements to the same transmission rate. In a test without noise, transmission rate adjusting turned out to be counterproductive probably due to setup imperfections which should definetely be investigated further.

To make the compensation procedure even faster, more efficient motor drivers are needed to avoid waiting times between rotatations and measurements. The tomography could also be accelerated and made more reliable if a reference beam with higher intensities will be used, as proposed in **[60]**, especially because the VCSELs need time to switch back to the intensity-weak QKD operation after turning up.

Appendix A

Long Formulas

A.1 Transforming circular Basis to linear

$$
\begin{aligned}
\alpha &= \tfrac{1}{4}(\arccos(\sin(2(\beta'-\gamma'))\sin(2\gamma')) + \arctan(\cos(2\gamma')\sin(2(\beta'-\gamma')),\\
&\quad -\cos(2(\beta'-\gamma'))) + \arctan(-\sin(4\alpha') + 4\cos(2\gamma')\sin(4\alpha'-2\beta') + ...\\
&\quad ... + \sin(4(\alpha'-\beta')) + 2\cos(4\alpha-2\beta)\sin(2(\beta'-2\gamma')),\\
&\quad \cos(4\alpha') - \cos(4(\alpha'-\beta')) - \cos(4(\alpha'-\gamma')) - ...\\
&\quad ... - 4\cos(4\alpha'-2\beta')\cos(2\gamma') + \cos(4(\alpha'-\beta'+\gamma'))))\\
\beta &= \tfrac{1}{2}(\arctan(\cos(2\gamma')\sin(2(\beta'-\gamma')), -\cos(2(\beta'-\gamma'))) + ...\\
&\quad ... + \arccos(\sin(2(\beta'-\gamma'))\sin(2\gamma')))\\
\gamma &= \tfrac{1}{2}\arctan(\cos(2\gamma')\sin(2(\beta'-\gamma')), -\cos(2(\beta'-\gamma')))
\end{aligned}
\tag{A.1}
$$

Figure A.1: Compensation angles to transform the circular Stokes component to the diagonal while maintaining the first Stokes component. Calculation done in **subsection 3.2.5**

A.2 Backtransformation Matrix $\underline{\mathrm{U}}$

$$\underline{\mathrm{U}} = \underline{\mathrm{QWP}}\,(\gamma) \cdot \underline{\mathrm{QWP}}\,(\beta) \cdot \underline{\mathrm{HWP}}\,(\alpha) =$$

$$\begin{pmatrix}
\frac{1}{4}(\cos(4\alpha) + \cos(4(\alpha-\beta)) + \cos(4(\alpha-\gamma)) + \cos(4(\alpha-\beta+\gamma)) + 4\sin(4\alpha-2\beta)) \\
\frac{1}{4}(\sin(4\alpha) - 4\cos(2\gamma)\sin(4\alpha-2\beta) - \sin(4(\alpha-\beta)) - 2\cos(4\alpha-2\beta)\sin(2(\beta-2\gamma))) \\
\cos(4\alpha-2\beta)\sin(2(\beta-\gamma))
\end{pmatrix}^{\top},$$

$$\begin{pmatrix}
\frac{1}{4}(\sin(4\alpha) + \sin(4(\alpha-\beta)) + \sin(4(\alpha-\gamma)) - 4\cos(4\alpha-2\beta)\cos(2\gamma) + \sin(4(\alpha-\beta+\gamma))) \\
\frac{1}{4}(-\cos(4\alpha) + \cos(4(\alpha-\beta)) + \cos(4(\alpha-\gamma)) + 4\cos(4\alpha-2\beta)\cos(2\gamma) - \cos(4(\alpha-\beta+\gamma))) \\
\sin(4\alpha-2\beta)\sin(2(\beta-\gamma))
\end{pmatrix}^{\top},$$

$$\begin{pmatrix}
-\cos(2\gamma)\sin(2(\beta-\gamma)) \\
-\sin(2(\beta-\gamma))\sin(2\gamma) \\
\cos(2(\beta-\gamma))
\end{pmatrix}^{\top} \tag{A.2}$$

Figure A.2: Backtransformation matrix calculated and simplified with `Mathematica` **[64]**

Appendix B

Proofs and Derivations

B.1 Performing all Poincaré Rotations by $\underline{\mathrm{U}}$

As an arbitrary rotation matrix $\underline{R}(\theta, \phi, \omega)$ can get represented as $\underline{R}(\theta, \phi, \omega) = \underline{R_z}(\theta)\underline{R_y}(\phi)\underline{R_x}(\omega)$ (property taken from **website [65]**) with:

$$\underline{R_x}(\alpha) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\alpha) & -\sin(\alpha) \\ 0 & \sin(\alpha) & \cos(\alpha) \end{pmatrix} \tag{B.1}$$

$$\underline{R_y}(\alpha) = \begin{pmatrix} \cos(\alpha) & 0 & \sin(\alpha) \\ 0 & 1 & 0 \\ -\sin(\alpha) & 0 & \cos(\alpha) \end{pmatrix} \tag{B.2}$$

$$\underline{R_z}(\alpha) = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) & 0 \\ \sin(\alpha) & \cos(\alpha) & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{B.3}$$

$$\underline{R_z}(\theta)\underline{R_y}(\phi)\underline{R_x}(\omega) = \begin{pmatrix} \cos(\theta)\cos(\phi) & \cos(\theta)\sin(\phi)\sin(\omega) - \sin(\theta)\cos(\omega) & \cos(\theta)\sin(\phi)\cos(\omega) + \sin(\theta)\sin(\omega) \\ \sin(\theta)\cos(\phi) & \sin(\theta)\sin(\phi)\sin(\omega) + \cos(\theta)\cos(\omega) & \sin(\theta)\sin(\phi)\cos(\omega) - \cos(\theta)\sin(\omega) \\ -\sin(\phi) & \cos(\phi)\sin(\omega) & \cos(\phi)\cos(\omega) \end{pmatrix} \tag{B.4}$$

Considering the wave plate matrices without their first row and column, $\underline{\mathrm{QWP}}(\alpha) = \underline{R_z}(2\alpha)\underline{R_y}(2\alpha)\underline{R_x}(\frac{\pi}{2})$ and $\underline{\mathrm{HWP}}(\gamma) = \underline{R_z}(4\gamma)\underline{R_y}(0)\underline{R_x}(\pi)$ are rotation matrices and because the product of rotation matrices is again a rotation matrix, $\underline{\mathrm{U}} = \underline{\mathrm{QWP}}(\alpha)\underline{\mathrm{QWP}}(\beta)\underline{\mathrm{HWP}}(\gamma)$ is a rotation matrix, which must fulfill the property above. Element-wise comparison of $\underline{R}$ with $\underline{\mathrm{U}}$ shows that (out of **appendix A.2**):

$$\theta = 2(2\gamma - \beta) \tag{B.5}$$

$$\phi = 2(\alpha - \beta) \tag{B.6}$$

$$\omega = -2\alpha \tag{B.7}$$

Because the angles characterising $\underline{U}$ can be substituted to the angles of $\underline{R}(\theta, \phi, \omega)$, which performs any arbitrary rotation, $\underline{U}$ can perform any arbitrary rotation.

B.2 No-Cloning Theorem

Imagine a cloning device (a "quantum Xerox machine") that takes an input particle in state $|\Psi_1\rangle$ and copies it on a "blank sheet of paper", the state $|X\rangle$:

$$|\Psi_1\rangle |X\rangle \rightarrow |\Psi_1\rangle |\Psi_1\rangle \tag{B.8}$$

If the device is able to clone an arbitrary state, it can e.g. clone $|\Psi_2\rangle$ as well:

$$|\Psi_2\rangle |X\rangle \rightarrow |\Psi_2\rangle |\Psi_2\rangle \tag{B.9}$$

What about e.g. the state $|\Psi_3\rangle$ as a linear combination of $|\Psi_1\rangle$ and $|\Psi_2\rangle$?

$$|\Psi_3\rangle = \alpha |\Psi_1\rangle + \beta |\Psi_2\rangle \tag{B.10}$$

$$|\Psi_3\rangle |X\rangle \rightarrow |\Psi_3\rangle |\Psi_3\rangle \tag{B.11}$$

$$\begin{aligned} |\Psi_3\rangle |X\rangle \underset{\text{(B.10)}}{=} (\alpha |\Psi_1\rangle + \beta |\Psi_2\rangle) |X\rangle &= \alpha |\Psi_1\rangle |X\rangle + \beta |\Psi_2\rangle |X\rangle \\ &\rightarrow \alpha |\Psi_1\rangle |\Psi_1\rangle + \beta |\Psi_2\rangle |\Psi_2\rangle \end{aligned} \tag{B.12}$$

$$\begin{aligned} |\Psi_3\rangle |X\rangle \rightarrow |\Psi_3\rangle |\Psi_3\rangle &\underset{\text{(B.10)}}{=} (\alpha |\Psi_1\rangle + \beta |\Psi_2\rangle)(\alpha |\Psi_1\rangle + \beta |\Psi_2\rangle) \\ &= \alpha^2 |\Psi_1\rangle |\Psi_1\rangle + \beta^2 |\Psi_2\rangle |\Psi_2\rangle + ... \\ &\quad ... + \alpha\beta(|\Psi_1\rangle |\Psi_2\rangle + |\Psi_2\rangle |\Psi_1\rangle) \end{aligned} \tag{B.13}$$

Because equation (B.12) contradicts (B.13) (even if $|\Psi_1\rangle$ and $|\Psi_2\rangle$ would be orthogonal $\Rightarrow |\Psi_1\rangle |\Psi_2\rangle = 0$, which in general can not be the case for any two arbitrary states, so that the assumption that a cloning device can clone any arbitrary states, is wrong. The proof is copied from **Griffiths [66]**. The original, more complex proof was made by Wooters and Zurek **[36]**.

B.3 Estimation of Duration of Vision during a LEO Satellite Overflight

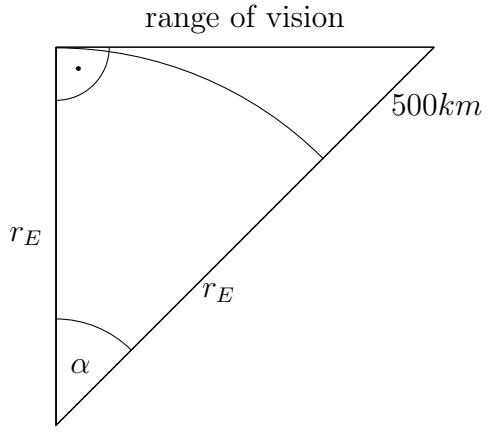


Figure B.1: Sketch of a sphere section of the earth with OGS in the upper left corner and a satellite with an orbit of 500km in the upper right at the time of the first visual contact.

The round-trip time T of a satellite with 500 km distance to earth, with radius r_E and mass m_E, can be calculated like a two-body problem **[67]**. With the estimation of a circular orbit, T resolves to:

$$T = \sqrt{\frac{4\pi^2 \left(r_E + 500\,\mathrm{km}\right)^3}{G m_E}} \approx 94.47\,\mathrm{min} \tag{B.14}$$

At the time of the first visual contact, the satellite, the center of earth and the OGS enclose the angle α, as shown in **figure B.1**.

$$\alpha = \arccos\left(\frac{r_E}{r_E + 500\,\mathrm{km}}\right) \approx 21.99^\circ \tag{B.15}$$

$$\tag{B.16}$$

The angle of the whole overflight is twice the angle of the section. Also, the ratio of the duration of vision (DoV) to the round-trip time is the same as the ratio of twice the angle to the angle of a circle.

$$\Rightarrow \quad DoV = T\frac{2\alpha}{360^\circ} \approx 11.54\,\mathrm{min} \tag{B.17}$$

Appendix C

Measurement Data

number of photons N	50	100	200	300	400	500	600	700
mean values [‰ QBER]	5.9	2.9	1.5	0.97	0.73	0.58	0.49	0.41
70% percentile [‰ QBER]	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
75% percentile [‰ QBER]	15.3	7.8	4.4	2.9	2.2	1.8	1.5	1.3
80% percentile [‰ QBER]	17.9	9.2	4.8	3.2	2.4	1.9	1.6	1.4
90% percentile [‰ QBER]	21.3	10.5	5.2	3.4	2.6	2.0	1.7	1.4
95% percentile [‰ QBER]	25.0	11.6	5.6	3.6	2.7	2.1	1.8	1.5
99% percentile [‰ QBER]	43.5	21.3	10.6	6.9	5.2	4.1	3.4	2.9

Table C.1: Results of simulated mean QBER and distribution of the compensation angles due to finite statistics with 10,000 samples (plotted in **figure 3.3**).

number of photons N	50	100	200	300	400	500	600	700
0.0 SNR^{-1} [‰QBER]	0.6	0.3	0.2	0.1	0.1	0.1	0.0	0.0
0.05 SNR^{-1} [‰QBER]	2.5	2.7	2.5	2.5	2.5	2.4	2.4	2.4
0.1 SNR^{-1} [‰QBER]	5.1	4.8	4.7	4.7	4.6	4.7	4.6	4.6
0.2 SNR^{-1} [‰QBER]	9.0	8.7	8.5	8.4	8.4	8.4	8.4	8.4
0.3 SNR^{-1} [‰QBER]	12.1	11.9	11.7	11.7	11.6	11.6	11.6	11.6
0.4 SNR^{-1} [‰QBER]	14.9	14.7	14.5	14.4	14.4	14.4	14.4	14.4
0.5 SNR^{-1} [‰QBER]	17.4	17.0	16.8	16.7	16.7	16.8	16.7	16.7

Table C.2: Mean QBER measured with intensity-Bob of 20 samples per data point dependent on number of photons and noise to signal ratio (SNR^{-1}), plotted in **figure 3.4a**.

number of photons N	50	100	200	300	400	500	600	700
0.0 SNR^{-1} [‰QBER]	5.8	3.1	1.4	0.9	0.7	0.6	0.5	0.4
0.05 SNR^{-1} [‰QBER]	15.2	11.2	6.7	5.5	4.6	4.2	3.8	3.4
0.1 SNR^{-1} [‰QBER]	20.6	13.6	9.2	7.5	6.7	5.7	5.1	4.8
0.2 SNR^{-1} [‰QBER]	28.4	18.6	12.7	10.7	9.0	8.0	7.3	6.8
0.3 SNR^{-1} [‰QBER]	34.4	22.5	16.1	12.9	10.9	10.0	9.2	8.1
0.4 SNR^{-1} [‰QBER]	38.2	26.2	18.7	15.0	12.9	11.7	10.6	9.5
0.5 SNR^{-1} [‰QBER]	42.3	28.3	20.6	16.7	14.3	12.8	11.7	10.8

Table C.3: Mean QBER measured with intensity-Bob of 20 samples per data point dependent on number of photons and noise to signal ratio (SNR^{-1}), plotted in **figure 3.4b**.

number of photons N	50	100	200	300	400	500	600	700
0.0 SNR^{-1} [‰QBER]	15.5	7.8	3.8	2.6	2.0	1.5	1.3	1.1
0.05 SNR^{-1} [‰QBER]	15.5	7.8	4.1	2.7	2.0	1.6	1.4	1.2
0.1 SNR^{-1} [‰QBER]	15.9	7.9	4.1	2.7	2.1	1.7	1.4	1.2
0.2 SNR^{-1} [‰QBER]	16.6	8.3	4.5	2.8	2.3	1.8	1.4	1.3
0.3 SNR^{-1} [‰QBER]	17.8	9.1	4.6	3.2	2.3	1.9	1.6	1.3
0.4 SNR^{-1} [‰QBER]	18.3	9.7	4.8	3.2	2.4	1.9	1.5	1.4
0.5 SNR^{-1} [‰QBER]	20.1	10.0	5.0	3.5	2.5	2.1	1.7	1.4

Table C.4: Mean QBER measured with intensity-Bob of 20 samples per data point dependent on number of photons and noise to signal ratio (SNR^{-1}), plotted in **figure 3.4c**.

number of photons N	50	100	200	300	400	500	600	700
0.0 SNR^{-1} [‰QBER]	15.7	7.9	4.0	2.6	1.9	1.5	1.3	1.2
0.05 SNR^{-1} [‰QBER]	15.5	9.2	3.9	2.7	2.0	1.6	1.4	1.2
0.1 SNR^{-1} [‰QBER]	15.4	8.1	4.1	2.7	2.1	1.6	1.4	1.2
0.2 SNR^{-1} [‰QBER]	17.7	8.7	4.3	2.9	2.2	1.8	1.5	1.3
0.3 SNR^{-1} [‰QBER]	18.8	9.2	4.7	3.1	2.4	1.9	1.5	1.3
0.4 SNR^{-1} [‰QBER]	18.4	9.7	5.0	3.2	2.5	2.0	1.6	1.3
0.5 SNR^{-1} [‰QBER]	19.6	10.1	5.0	3.4	2.6	2.0	1.7	1.5

Table C.5: Mean QBER measured with intensity-Bob of 20 samples per data point dependent on number of photons and noise to signal ratio (SNR^{-1}), plotted in **figure 3.4d**.

number of photons N	50	100	200	300	400	500	600	700
median [‰ QBER]	0.0	2.4	0.0	0.0	0.3	0.0	0.0	0.5
60% percentile [‰ QBER]	4.5	6.1	0.4	1.1	1.5	0.7	1.0	1.1
70% percentile [‰ QBER]	6.4	7.9	1.7	2.6	1.9	1.5	2.0	1.4
80% percentile [‰ QBER]	13.8	8.8	3.8	3.6	2.4	2.0	2.4	1.5
90% percentile [‰ QBER]	15.6	13.3	4.8	6.6	3.3	4.0	3.0	2.2
95% percentile [‰ QBER]	16.8	16.9	4.9	8.6	6.5	4.6	3.9	2.6
worst-case [‰ QBER]	19.3	22.2	6.4	13.0	11.1	6.8	6.7	4.3
mean values [‰ QBER]	5.2	5.2	1.4	2.2	1.5	1.1	1.2	0.9

Table C.6: QBER distribution measured with intensity-Bob of 20 samples per data point dependent to number of photons (plotted in **figure 4.3a**).

number of photons N	50	100	200	300	400	500	600	700
0.0 SNR^{-1} [% QBER]	0.5	0.5	0.1	0.2	0.1	0.1	0.1	0.1
0.13 SNR^{-1} [% QBER]	5.9	5.7	5.2	5.0	5.5	5.5	5.3	5.4
0.26 SNR^{-1} [% QBER]	10.1	9.4	9.6	9.6	9.5	9.5	9.4	9.6
0.38 SNR^{-1} [% QBER]	14.6	13.3	13.4	13.4	13.0	13.4	13.1	13.0
0.51 SNR^{-1} [% QBER]	17.5	17.1	16.1	16.1	15.6	16.1	16.1	15.9

Table C.7: Mean QBER measured with intensity-Bob of 20 samples per data point dependent on noise to signal ratio (SNR^{-1}) and number of photons (plotted in **figure 4.3b**).

prepared states	H	V	P	M	R	L
intensity	1	1	1	1	1	1
H/V basis	0.9998	-0.9998	-0.0096	0.0168	-0.0046	0.0070
P/M basis	0.0078	-0.0147	0.9999	-0.9998	-0.0019	0.0208
R/L basis	0.0004	0.0152	0.0233	-0.0083	0.9953	-0.9953
dop	0.9999	1.0001	1.0003	1.0000	0.9955	0.9955

Table C.8: Measured states of intensity-Bob for the Mueller matrix in **equation** (4.1). The degree of polarisations (dop) greater than one are unphysical and were probably caused by waveplate imperfections and different coupling efficiencies **[53]** when basis transforming.

$$\underline{\mathrm{MM}} = \begin{pmatrix} 1.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.9863458 & 0.0114927 & -0.1642861 \\ 0.0 & 0.0114927 & 0.9903266 & 0.1382794 \\ 0.0 & 0.1642861 & -0.1382794 & 0.9766724 \end{pmatrix} \tag{C.1}$$

Figure C.1: Unitary Mueller matrix after compensating with measurements of photon-counting-Bob, see **table 4.1**

Bibliography

[1] Valerio Scarani et al. "The security of practical quantum key distribution". In: *Reviews of Modern Physics* 81.3 (2009), pp. 1301–1350. ISSN: 0034-6861. DOI: 10.1103/RevModPhys.81.1301.

[2] Mihir Bellare et al. "A concrete security treatment of symmetric encryption". In: *Proceedings 38th Annual Symposium on Foundations of Computer Science*. IEEE. 1997, pp. 394–403. ISBN: 0-8186-8197-7. DOI: 10.1109/SFCS.1997.646128.

[3] Mihir Bellare and Phillip Rogaway. "Optimal asymmetric encryption". In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer. 1994, pp. 92–111. ISBN: 978-3-540-44717-7. DOI: 10.1007/BFb0053428.

[4] Peter W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509. ISSN: 0097-5397. DOI: 10.1137/S0097539795293172.

[5] Michele Mosca. "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" In: *IEEE Security & Privacy* 16.5 (2018), pp. 38–41. ISSN: 1540-7993. DOI: 10.1109/MSP.2018.3761723.

[6] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Theoretical Computer Science* 560 (Dec. 2014), pp. 7–11. ISSN: 0304-3975. DOI: 10.1016/j.tcs.2014.05.025.

[7] Miralem Mehic et al. "Quantum Key Distribution". In: *ACM Computing Surveys* 53.5 (2020), pp. 1–41. ISSN: 0360-0300. DOI: 10.1145/3402192.

[8] M. Sasaki et al. "Field test of quantum key distribution in the Tokyo QKD Network". In: *Optics express* 19.11 (2011), pp. 10387–10409. ISSN: 1094-4087. DOI: 10.1364/OE.19.010387.

[9] Yu-Ao Chen et al. *An integrated space-to-ground quantum communication network over 4,600 kilometres*. 2021. URL: https://www.nature.com/articles/s41586-020-03093-8#citeas.

[10] Sebastian Nauerth et al. "Air-to-ground quantum communication". In: *Nature Photonics* 7.5 (2013), pp. 382–386. ISSN: 1749-4885. DOI: 10.1038/NPHOTON.2013.46.

[11] Christopher J. Pugh et al. "Airborne demonstration of a quantum key distribution receiver payload". In: *Quantum Science and Technology* 2.2 (2017), p. 024009. DOI: 10.1088/2058-9565/aa701f.

[12] Elizabeth Gibney. "Chinese satellite is one giant step for the quantum internet". In: *Nature* 535.7613 (2016), pp. 478–479. ISSN: 0028-0836. DOI: 10.1038/535478a.

[13] Imran Khan et al. "Satellite-based QKD". In: *Optics and Photonics News* 29.2 (2018), pp. 26–33.

[14] "Quantum information". In: *Quantum Information*. New York, NY: Springer New York, 2007, pp. 81–89. ISBN: 978-0-387-35725-6. DOI: 10.1007/978-0-387-36944-0_5.

[15] Nicolas Gisin and Rob Thew. "Quantum communication". In: *Nature Photonics* 1.3 (2007), pp. 165–171. ISSN: 1749-4885. DOI: 10.1038/nphoton.2007.22.

[16] M. Bellare et al. "A concrete security treatment of symmetric encryption". In: *Proceedings 38th Annual Symposium on Foundations of Computer Science*. 1997, pp. 394–403. DOI: 10.1109/SFCS.1997.646128.

[17] S. Pirandola et al. "Advances in quantum cryptography". In: *Adv. Opt. Photon.* 12.4 (2020), pp. 1012–1236. DOI: 10.1364/AOP.361502.

[18] John M. Martinis et al. "Rabi oscillations in a large Josephson-junction qubit". In: *Physical review letters* 89.11 (2002), p. 117901. DOI: 10.1103/PhysRevLett.89.117901.

[19] Jarryd J. Pla et al. "A single-atom electron spin qubit in silicon". In: *Nature* 489.7417 (2012), pp. 541–545. ISSN: 0028-0836. DOI: 10.1038/nature11449.

[20] Jin-Xuan Han et al. "Multi-qubit phase gate on multiple resonators mediated by a superconducting bus". In: *Optics express* 28.2 (2020), pp. 1954–1969. DOI: 10.1364/OE.384352.

[21] Berthold-Georg Englert, Christian Kurtsiefer, and Harald Weinfurter. "Universal unitary gate for single-photon two-qubit states". In: *Physical Review A* 63.3 (2001). ISSN: 1050-2947. DOI: 10.1103/PhysRevA.63.032303.

[22] Serge Huard. *Polarization of Light*. 1997.

[23] Edward Collett. "Mathematical Formulation of the Interference Laws of Fresnel and Arago". In: *American Journal of Physics* 39.12 (1971), pp. 1483–1495. ISSN: 0002-9505. DOI: 10.1119/1.1976702.

[24] John Von Neumann. *Mathematical foundations of quantum mechanics: New edition*. Princeton university press, 2018.

[25] William K. Wootters and Brian D. Fields. "Optimal state-determination by mutually unbiased measurements". In: *Annals of Physics* 191.2 (1989), pp. 363–381. ISSN: 00034916. DOI: 10.1016/0003-4916%2889%2990322-9.

[26] Jacob Birkmann. "Towards Compact High-Altitude-Platform Based Quantum Key Distribution". Master's Thesis. Ludwig-Maximilians-University, Apr. 1, 2019.

[27] George Gabriel Stokes, ed. *Mathematical and Physical Papers*. Cambridge: Cambridge University Press, 2009. ISBN: 9780511702266. DOI: 10.1017/CBO9780511702266.

[28] Binjie Qian et al. "Generation of vector beams using a Wollaston prism and a spatial light modulator". In: *Optik* 148 (2017), pp. 312–318. ISSN: 0030-4026. DOI: https://doi.org/10.1016/j.ijleo.2017.09.015.

[29] C. E. Shannon. "Communication theory of secrecy systems". In: *The Bell System Technical Journal* 28.4 (1949), pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

[30] Morio Toyoshima et al. "Polarization measurements through space-to-ground atmospheric propagation paths by using a highly polarized laser source in space". In: *Optics express* 17.25 (2009), pp. 22333–22340. DOI: 10.1364/OE.17.022333.

[31] Hongwei Liu et al. "Reference-Frame-Independent Quantum Key Distribution Using Fewer States". In: *Physical Review Applied* 12.3 (2019). DOI: 10.1103/PhysRevApplied.12.034039.

[32] QuaNTH project. *The BB84 cryptography protocol*. 2014. URL: https://qig.itp.uni-hannover.de/quanth/index.php/A3/Das_BB84_Kryptographie_Protokoll (visited on 01/10/2021).

[33] et al. Tang Bang-Ying. *High-speed and Large-scale Privacy Amplification Scheme for Quantum Key Distribution*. 2019. URL: https://www.nature.com/articles/s41598-019-50290-1 (visited on 01/15/2021).

[34] et al. Buttler W. T. *Fast, Efficient Error Reconcilation for Quantum Cryptography*. 2003. URL: https://arxiv.org/abs/quant-ph/0203096 (visited on 01/15/2021).

[35] Daniel Gottesman et al. "Security of quantum key distribution with imperfect devices". In: (2004). URL: http://arxiv.org/pdf/quant-ph/0212066v3.

[36] W. K. Wootters and W. H. Zurek. "A single quantum cannot be cloned". In: *Nature* 299.5886 (1982), pp. 802–803. ISSN: 0028-0836. DOI: 10.1038/299802a0.

[37] Alexios Beveratos et al. "Single Photon Quantum Cryptography". In: *Physical Review Letters* 89.18 (Oct. 2002). ISSN: 1079-7114. DOI: 10.1103/physrevlett.89.187901.

[38] B. Huttner et al. "Quantum cryptography with coherent states". In: *Physical Review A* 51.3 (Mar. 1995), pp. 1863–1869. ISSN: 1094-1622. DOI: 10.1103/physreva.51.1863.

[39] Miloslav Dušek, Ondřej Haderka, and Martin Hendrych. "Generalized beam-splitting attack in quantum cryptography with dim coherent states". In: *Optics Communications* 169.1-6 (1999), pp. 103–108. ISSN: 00304018. DOI: 10.1016/S0030-4018(99)00419-8.

[40] Brassard et al. "Limitations on practical quantum cryptography". In: *Physical review letters* 85.6 (2000), pp. 1330–1333. DOI: 10.1103/PhysRevLett.85.1330.

[41] Won-Young Hwang. "Quantum Key Distribution with High Loss: Toward Global Secure Communication". In: *Physical Review Letters* 91.5 (Aug. 2003). ISSN: 1079-7114. DOI: 10.1103/physrevlett.91.057901.

[42] Xiang-Bin Wang. "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography". In: *Physical Review Letters* 94.23 (June 2005). ISSN: 1079-7114. DOI: 10.1103/physrevlett.94.230503.

[43] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. "Decoy State Quantum Key Distribution". In: *Physical Review Letters* 94.23 (June 2005). ISSN: 1079-7114. DOI: 10.1103/physrevlett.94.230504.

[44] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. "Effects of detector efficiency mismatch on security of quantum cryptosystems". In: *Physical Review A* 74.2 (Aug. 2006). ISSN: 1094-1622. DOI: 10.1103/physreva.74.022313.

[45] Henning Weier et al. "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors". In: *New Journal of Physics* 13.7 (July 2011), p. 073024. ISSN: 1367-2630. DOI: 10.1088/1367-2630/13/7/073024.

[46] Markus Rau et al. "Spatial Mode Side Channels in Free-Space QKD Implementations". In: *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (2015), pp. 187–191. ISSN: 1077-260X. DOI: 10.1109/JSTQE.2014.2372008.

[47] Lars Lydersen et al. "Hacking commercial quantum cryptography systems by tailored bright illumination". In: *Nature Photonics* 4.10 (Aug. 2010), pp. 686–689. ISSN: 1749-4893. DOI: 10.1038/nphoton.2010.214.

[48] W. G. Unruh. "Analysis of quantum-nondemolition measurement". In: *Physical Review D* 18.6 (1978), pp. 1764–1772. ISSN: 0556-2821. DOI: 10.1103/PhysRevD.18.1764.

[49] Takeshi Kamiya et al., eds. *Vertical-Cavity Surface-Emitting Laser Devices*. Springer Series in Photonics. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003. ISBN: 978-3-642-08743-1. DOI: 10.1007/978-3-662-05263-1.

[50] Konstantinos Poulios et al. "Quantum walks of correlated photon pairs in two-dimensional waveguide arrays". In: *Physical review letters* 112.14 (2014), p. 143604. DOI: 10.1103/PhysRevLett.112.143604.

[51] Mark A. Itzler et al. "Statistical analysis of dark count rate in Geiger-mode APD FPAs". In: *Electro-Optical Remote Sensing, Photonic Technologies, and Applications VIII; and Military Applications in Hyperspectral Imaging and High Spatial Resolution Sensing II*. Ed. by Gary Kamerman et al. SPIE Proceedings. SPIE, 2014, p. 925003. DOI: 10.1117/12.2068744.

[52] Naser Faramarzpour et al. "Fully Integrated Single Photon Avalanche Diode Detector in Standard CMOS 0.18- μm Technology". In: *IEEE Transactions on Electron Devices* 55.3 (2008), pp. 760–767. ISSN: 0018-9383. DOI: 10.1109/TED.2007.914839.

[53] Peter Freiwang. "Towards Hand-held Quantum Key Distribution". Master thesis. LUDWIG-MAXIMILIAN-UNIVERSITY.

[54] Brendon L. Higgins, Jean-Philippe Bourgoin, and Thomas Jennewein. "Numeric estimation of resource requirements for a practical polarization-frame alignment scheme for quantum key distribution (QKD)". In: *Advanced Optical Technologies* 9.5 (2020), pp. 253–261. ISSN: 2192-8576. DOI: 10.1515/aot-2020-0016.

[55] Jean-Philippe Bourgoin et al. "Free-space quantum key distribution to a moving receiver". In: *Optics express* 23.26 (2015), p. 33437. ISSN: 1094-4087. DOI: 10.1364/OE.23.033437.

[56] Brendon L. Higgins, Jean-Philippe Bourgoin, and Thomas Jennewein. *Practical polarization-frame alignment for quantum key distribution with single-photon-level resources; peer-reviewed in [54]*. 2018.

[57] Zhizhong Yan et al. "Novel High-Speed Polarization Source for Decoy-State BB84 Quantum Key Distribution Over Free Space and Satellite Links". In: *Journal of Lightwave Technology* 31.9 (May 2013), pp. 1399–1408. ISSN: 1558-2213. DOI: 10.1109/jlt.2013.2249040.

[58] Morio Toyoshima et al. "Polarization-Basis Tracking Scheme in Satellite Quantum Key Distribution". In: *International Journal of Optics* 2011 (2011), pp. 1–8. ISSN: 1687-9384. DOI: 10.1155/2011/254154.

[59] Bennett. "Quantum cryptography using any two nonorthogonal states". In: *Physical review letters* 68.21 (1992), pp. 3121–3124. DOI: 10.1103/PhysRevLett.68.3121.

[60] Zhang Guangyu et al. "Dynamic polarization-basis compensation for free-space quantum communications". In: *China Communications* 10.2 (2013), pp. 27–32. ISSN: 1673-5447. DOI: 10.1109/CC.2013.6472856.

[61] Ming Li et al. "General model on polarization compensation in satellite-to-ground quantum communication". In: *Optical Engineering* 52.4 (2013), p. 045001. ISSN: 0091-3286. DOI: 10.1117/1.OE.52.4.045001.

[62] Giuseppe Vallone et al. "Experimental Satellite Quantum Communications". In: *Physical review letters* 115.4 (2015), p. 040502. DOI: 10.1103/Physrevlett.115.040502.

[63] "Laser and Gaussian Beam Propagation and Transformation". In: *Encyclopedia of Optical and Photonic Engineering, Second Edition*. Ed. by Craig Hoffman and Ronald Driggers. CRC Press, 2015, pp. 1–15. ISBN: 9781439850992. DOI: 10.1081/E-EOE2-120009751.

[64] WolframAlpha. *Mathematica-Computing meets Knowledge*. https://www.wolfram.com/mathematica/. Version 12.1. Dec. 31, 2020. (Visited on 01/05/2021).

[65] Wikipedia articel Rotation matrix. *Rotation matrix — Wikipedia, The Free Encyclopedia*. 2021. URL: https://en.wikipedia.org/wiki/Rotation_matrix#General_rotations (visited on 01/10/2021).

[66] David Griffiths. *Introduction of Quantum Mechanics*. Prentice Hall, Inc., 1995. ISBN: 0-13-191175-9.

[67] Dino Boccaletti and Giuseppe Pucacco. "The Two-Body Problem". In: *Theory of Orbits*. Ed. by I. Appenzeller et al. Astronomy and Astrophysics Library. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 125–175. ISBN: 978-3-642-08210-8. DOI: 10.1007/978-3-662-03319-7_3.

Acknowledgement

At this point I would like to thank everyone who supported and motivated me while writing this Master thesis.

First of all, I would like to thank Prof. Weinfurter, who supervised and assessed my thesis.

I would like to thank my supervisors Dr. Lukas Knips and Peter Freiwang for the helpful suggestions and constructive criticism in the preparation of this thesis.

I would also like to thank my fellow students for proofreading my Master thesis.

Finally, I would like to thank my parents, who made my studies possible with their support and who always had an open ear for me.

Marco Andersohn

München, 3. Mai 2021

Declaration of Honour

I hereby certify and declare on my honour that I have written the present Master's thesis independently and that I have not used any sources and resources other than those specified in this thesis.

Munich, 3. Mai 2021

Marco Andersohn