**Department of Physics and Astronomy**

**Heidelberg University**

Bachelor Thesis in Physics

submitted by

**Tobias Ludwig Rieger**

born in Gelnhausen (Germany)

**2024**

# App Development for a Student Experiment about Quantum Key Distribution

This Bachelor Thesis has been carried out by Tobias Ludwig Rieger at the
Kirchhoff-Institute for Physics in Heidelberg
under the supervision of
Prof. Dr. Wolfram Pernice

## Abstract

Advances in Quantum Computation technologies lead to an increasing demand for secure encryption which extends the importance of Quantum Key Distribution (QKD) as a field of modern research. However, conveying QKD protocols to students in hands-on experiments is challenging. One approach to overcome this problem has been developed by the project *MiReQu* that has established a Mixed Reality (MR) environment to run an experiment dealing with polarisation-entangled photons and QKD using the Ekert91 protocol. In order to extract the impact of the MR environment on the students' learning experience, a comparison study with a non-MR application is needed. Within this thesis, this non-MR environment is designed and developed and this tablet-based user interface is tested on the experiment. Supplementary long-term measurements were conducted for the first time. The set coincidence window could be confirmed and it is shown that after alignment and an initial drift, the system stabilises in an alignment state close to the optimum. By using the app, the S-parameter which proves the violation of the CHSH inequality has been measured as $S = 2.34 \pm 0.03$ and confirms that the system is non-classical. Additionally, the app's capability of running the Ekert91 protocol is demonstrated.



## Zusammenfassung

Fortschritte in der Quantencomputertechnologie führen zu einer steigenden Nachfrage an sicherer Verschlüsselung, welche den Stellenwert vom Thema Quantenschlüsselaustausch in der modernen Forschung erhöht. Die Vermittlung von Verfahren zum Quantenschlüsselaustausch an StudentInnen in Experimenten stellt jedoch eine Herausforderung dar. Als möglicher Lösungsansatz wurde im Rahmen des Projekts *MiReQu* eine Mixed Reality (MR) Umgebung entwickelt, mit der StudentInnen einen Versuch zum Thema Verschränkung und Quantenverschlüsselung durchführen können. Durch eine Vergleichsstudie mit einer nicht-MR Applikation soll der Effekt der MR Umgebung auf den Lernerfolg untersucht werden. Diese Arbeit stellt die Implementierung der nicht-MR Version sowie einen Test dieses Tablet-Programms dar. Im Rahmen weiterführender Langzeitmessungen konnte das eingestellte Koinzidenzfenster bestätigt werden. Es wurde außerdem gezeigt, dass sich das System nach Ausrichtung nach einem anfänglichen Drift stabilisiert. Mithilfe des Programms wurde der S-Parameter, welcher die Verletzung der CHSH Ungleichung bestätigt, als $S = 2.34 \pm 0.03$ ermittelt. Das bestätigt, dass das System nicht-klassisch ist. Zuletzt wird veranschaulicht, dass das Programm das Ekert91 Protokoll zum Quantenschlüsselaustausch erfolgreich durchführen kann.

# Contents

# 1 Introduction

The increasing digitalisation has led to a surge in demand for secure encryption. However, as computation power and architectures evolve, encryption protocols have to adapt accordingly. Modern encryption standards such as RSA (standing for Rivest, Shamir and Adleman, the inventors of the scheme) are not intrinsically but only computationally secure [1]. This means, their security relies on mathematical operations that exceed current state-of-the-art computing power. Consequently, they could be broken faster by a universal quantum computer with Shors-Algorithm [2]. One promising approach for overcoming these problems is Quantum Key Distribution (QKD) [3]. Whilst it was developed in the late $20^{\text{th}}$ century, its applications and realisations are a field of modern research. Examples for this are the German QuNET-initiative that develops technologies for secure data transmission using QKD [4], the implementation of Decoy states into QKD protocols [5], [6] and advancements in the secret key rate [7].

The basic theory underlying QKD protocols is taught in the physics major in undergraduate lectures and can be found in standard textbooks such as Bartelmann [8] or Cohen-Tannoudji [9]. Yet, it is challenging to convey these abstract concepts in a hands-on student experiment. A novel concept has been developed by the project *MiReQu* under the guidance of Prof. Dr. Stefan Heusler and Prof. Dr. Wolfram Pernice. Their interdisciplinary team consisting of scientists from physics, didactics and design developed a Mixed Reality (MR) program for an experiment on QKD and entanglement. The program runs on Microsoft HoloLens 2 devices and projects the measurements of photon counts or illustrations of the laser beam directly into the setup [10]. The MR environment is shown in Figure 1.1.

At Heidelberg University, the experiment is part of the *Advanced Lab Course* (called FP for "Fortgeschrittenen-Praktikum"). It is usually carried out by physics undergraduate students in one of the last semesters of their bachelor studies. During the experiment, students familiarise themselves with the underlying physics of polarisation-entangled photon pairs. They measure single photon counts and coincidence counts, explore the properties of the entangled state and run a QKD protocol [12].

One aim of the developers is to study how modern quantum optics can be taught interactively to students [10]. In this context, it is necessary to compare the MR version of the experiment to a rather traditional setup using a non-MR environment. It is planned to run a comparison study in cooperation with the Department of Psychology of Heidelberg University. Therefore, it requires to develop an application to carry out the experiment

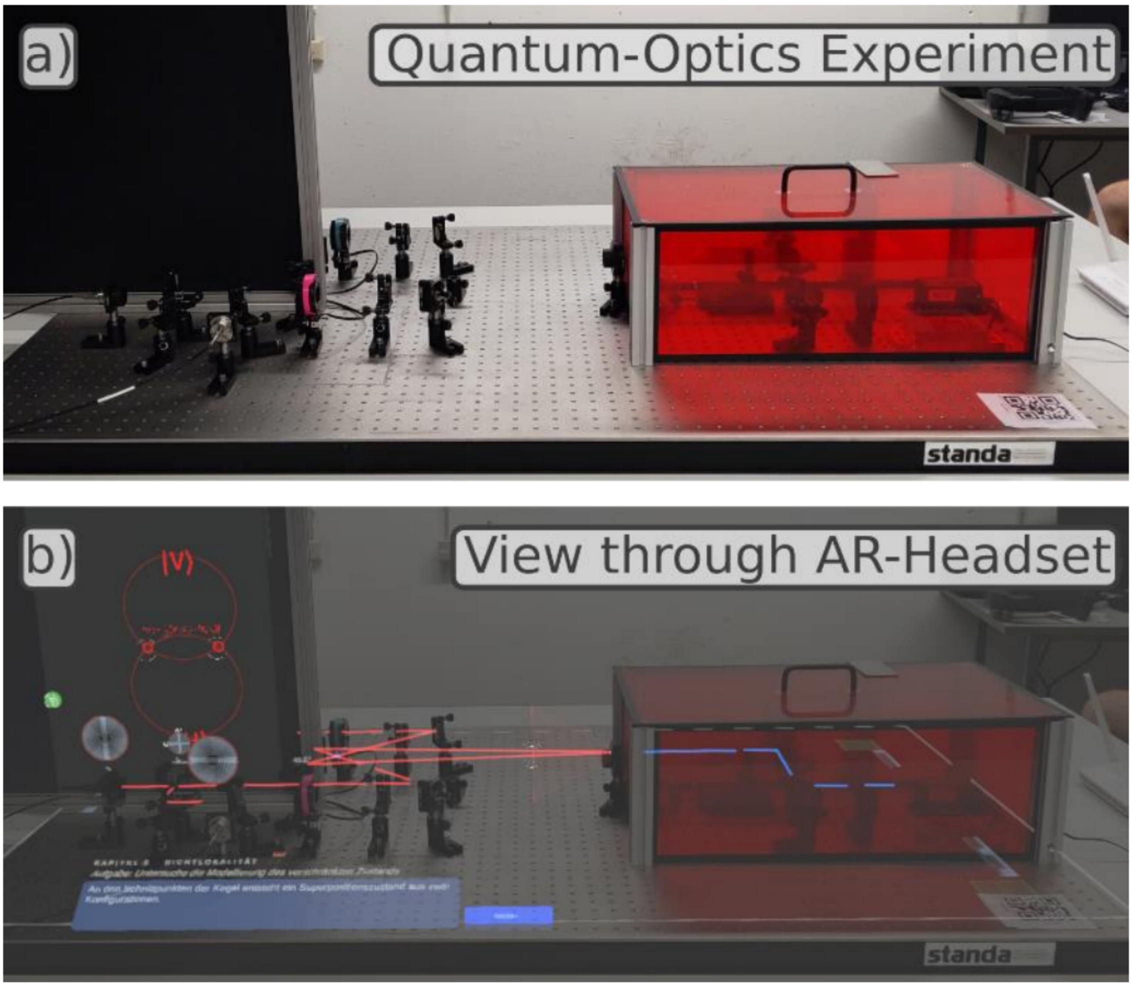



**Figure 1.1:** Comparison of the MR environment to reality. In a) the optical instruments on the experiments' table are shown. Image b) shows the MR environment, including the projected laser beam, explanations and illustrations. Figure taken from [11].

similar to the existing setup but with a conventional interface instead of AR glasses. A tablet-based environment was chosen for this purpose.

Motivated by the planned study, the main goal of this thesis is to establish the comparison setup. In this thesis, the experiment will be introduced in detail. The upcoming section two deals with the underlying theory of the experiment, particularly the QKD with the Ekert91 protocol [13]. The following third part explains the setup, especially the generation, preparation and measuring process of entangled photon pairs. In addition, this section presents the currently used MR environment. In the fourth chapter, the structure of the developed app is introduced and it is compared to the existing MR environment. Subsequently, an evaluation of the data collected during the experiment with the application and during the additional measurements is provided in section five. Finally, the contents are summarised and an outlook is given.

# 2 Theory

The experiment described in this thesis utilises the polarisation of light to represent bits. This depiction is further used for exploring and evaluating the phenomenon of entanglement and its application to QKD. First of all, the basal theory should be introduced. In the context of performing measurements on a quantum system, the two participants are commonly named Alice and Bob.

## 2.1 Quantum Information Basics

The mathematical foundation of quantum information theory is presented in [14] and [15] and should be summarised in the following. A general two-state quantum system can be described by a two-dimensional Hilbert space $\mathcal{H}$. As we deal with qubits, we can write a general state as

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{2.1}$$

In this case $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta^2| \stackrel{!}{=} 1$ because the state has to be normalised. Together with the identity matrix $\mathbb{I}$, the Pauli matrices that are defined as follows

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.2}$$

form a basis for the $2 \times 2$ matrices. The previously shown states $|0\rangle$ and $|1\rangle$ are the eigenstates of the $\sigma_z$ Pauli matrix. Thus, $|\alpha|^2$ and $|\beta|^2$ represent the likelihood of the measurement outcome when measuring the qubit's value in its eigenbasis.

By fundamental mathematics, the Pauli matrices do not commute. Therefore we cannot measure a single state in two bases such that it is an eigenstate for both bases. Every state of a two-dimensional quantum system can be illustrated on the Bloch sphere, shown in Figure 2.1. Now, we want to take a look at the $\sigma_x$ matrix and its eigenstates

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ and } |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{2.3}$$

As $\sigma_x \sigma_z \neq \sigma_z \sigma_x$, the state $|+\rangle$ is not an eigenstate of the $\sigma_z$ matrix. Therefore, if we measure $|+\rangle$ along the $\hat{z}$-axis, we cannot measure it sharply, but we can measure one of the eigenstates of $\sigma_z$, namely $|1\rangle$ or $|0\rangle$. Calculating the mean of the projection operator

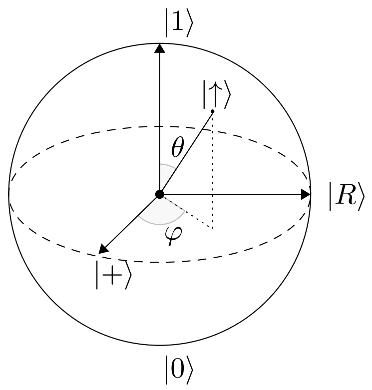



**Figure 2.1:** A Bloch sphere with the eigenstates of the Pauli matrices namely $|+\rangle$ of $\sigma_x$, $|R\rangle$ of $\sigma_y$ and $|1\rangle$ and $|0\rangle$ of $\sigma_z$. Additionally, an arbitrary state $|\uparrow\rangle$ is shown.

$P_{|0\rangle} = |0\rangle \langle 0|$ gives us the probability to measure $|0\rangle$ in the described scenario:

$$\langle P_{|0\rangle} \rangle = \langle + | P_{|0\rangle} | + \rangle = \frac{1}{\sqrt{2}} \langle + | 0 \rangle = \frac{1}{2}. \tag{2.4}$$

Now, a more complex case will be considered where the states of two photons are measured simultaneously. This can be described by a four-dimensional Hilbert space namely $\mathcal{H} \equiv \mathcal{H}_A \otimes \mathcal{H}_B$ where $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = 2$. With introducing the notation $|01\rangle \equiv |0\rangle \otimes |1\rangle$ we can write an arbitrary state

$$|\Psi\rangle = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle . \tag{2.5}$$

For general states $|\Psi\rangle \in \mathcal{H}$ we differentiate between *Separable States* that can be written as a tensor product

$$|\Psi\rangle = |\varphi\rangle_A \otimes |\eta\rangle_B \tag{2.6}$$

and on the other hand *Entangled States* that cannot be written as a product of two unique states in $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. As a consequence, measuring the state of one qubit determines the state of the other. A basis for the states in $\mathcal{H}$ is the Bell basis consisting of

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}} \left( |00\rangle \pm |11\rangle \right) \tag{2.7}$$

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}} \left( |10\rangle \pm |01\rangle \right) . \tag{2.8}$$

These states are all entangled. A special property of the entangled states is that they are entangled no matter what basis is used to describe a Hilbert space. In the following, this should be proven for $|\Psi^-\rangle$ with the limitation that the basis only rotates in the real plane. Whilst a general state is shown in Figure 2.1, assuming $|\uparrow\rangle$ is in the real plane means for the polar angle from Figure 2.1 $\varphi = 0$. So, a general state can be described as $|\uparrow\rangle = \sin(\frac{\theta}{2})\,|0\rangle + \cos(\frac{\theta}{2})\,|1\rangle$. Similarly, its complementary basis vector can be written $|\downarrow\rangle = \cos(\frac{\theta}{2})\,|0\rangle - \sin(\frac{\theta}{2})\,|1\rangle$. Starting with a modified $|(\Psi^-)'\rangle = \frac{1}{\sqrt{2}}\,(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$ we want to show $|\Psi^-\rangle = |(\Psi^-)'\rangle$.

$$\begin{aligned}
|(\Psi^-)'\rangle &= \frac{1}{\sqrt{2}}\,(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle) \\
&= \frac{1}{\sqrt{2}}\Bigg[\left(\sin\left(\frac{\theta}{2}\right)|0\rangle + \cos\left(\frac{\theta}{2}\right)|1\rangle\right)_A \otimes \left(\cos\left(\frac{\theta}{2}\right)|0\rangle - \sin\left(\frac{\theta}{2}\right)|1\rangle\right)_B \\
&- \left(\cos\left(\frac{\theta}{2}\right)|0\rangle - \sin\left(\frac{\theta}{2}\right)|1\rangle\right)_A \otimes \left(\sin\left(\frac{\theta}{2}\right)|0\rangle + \cos\left(\frac{\theta}{2}\right)|1\rangle\right)_B\Bigg] \\
&= \frac{1}{\sqrt{2}}\Big[\,|1\rangle_A \otimes |0\rangle_B - |0\rangle_A \otimes |1\rangle_B\Big] \\
&= \frac{1}{\sqrt{2}}\,(|10\rangle - |01\rangle) = |\Psi^-\rangle
\end{aligned} \tag{2.9}$$

We can see that the entanglement of $|\Psi^-\rangle$ holds even under basis transformation.

## 2.2 The No-Cloning Theorem

So far, we know that entanglement is a fundamental property of quantum mechanics. It can be used to generate intrinsically secure keys for quantum cryptography. However, this would be impossible if qubits could be copied, similar to classical bits. Nonetheless, copying qubits is prohibited by the No-Cloning-Theorem, firstly presented by [16] and further discussed in [14]. It states that an arbitrary quantum state cannot be cloned identically onto another state.

To prove this statement, let us start with any state $|\Psi\rangle$, similar to 2.1. The desired cloning operator $\hat{C}$ should clone the state $|\Psi\rangle$ onto another state, say $|0\rangle$. We want our cloning operator to behave like

$$\hat{C}\,|\Psi\rangle\,|0\rangle = |\Psi\rangle\,|\Psi\rangle = \alpha^2\,|0\rangle\,|0\rangle + \alpha\beta\,|0\rangle\,|1\rangle + \alpha\beta\,|1\rangle\,|0\rangle + \beta^2\,|1\rangle\,|1\rangle\,. \tag{2.10}$$

Nonetheless, $\hat{C}$ is an operator, so it should be linear. Therefore, the approach yields as well

$$\hat{C}\,|\Psi\rangle\,|0\rangle = \alpha\hat{C}\,|0\rangle\,|0\rangle + \beta\hat{C}\,|1\rangle\,|0\rangle = \alpha\,|0\rangle\,|0\rangle + \beta\,|1\rangle\,|1\rangle\,. \tag{2.11}$$

This leaves us with a contradiction because in general:

$$\alpha |0\rangle |0\rangle + \beta |1\rangle |1\rangle \neq \alpha^2 |0\rangle |0\rangle + \alpha\beta |0\rangle |1\rangle + \alpha\beta |1\rangle |0\rangle + \beta^2 |1\rangle |1\rangle . \tag{2.12}$$

Thus, we have to conclude, that there is no such operator $\hat{C}$ that clones any quantum state.

### 2.3 Einstein-Podolsky-Rosen Paradox

The consequences of quantum theories including entanglement were further investigated by Einstein, Podolsky and Rosen (EPR) [17]. They raised the question of whether "Quantum-Mechanical description of physical reality can be considered complete". Additionally to the original paper, their arguments are illustrated in [15].

First of all, they raised two main questions: "Is the theory correct?" and "Is the description given by the theory complete?". As quantum theory agrees well with reality, we can assume that it is correct. Their criterion for completeness is "every element of the physical reality must have a counterpart in the physical theory." In this case "real" means, that a quantity can be predicted with certainty. By looking at non-commuting quantum mechanical operators such as the Pauli-Matrices introduced in 2.2 they conclude that either quantum mechanics is incomplete or non-commuting operators do not have a simultaneous reality. This is because if $\hat{A}\hat{B} \neq \hat{B}\hat{A}$, they cannot be measured both precisely. Therefore, the assumption that quantum mechanics would be complete leaves us with the conclusion that non-commuting operators do not have a simultaneous reality.

On the other hand, starting with the assumption that quantum mechanics would be complete, we can further discuss the entanglement of spin-states. In our case, we have a system with particles prepared in the spin states $|\Psi^-\rangle$. As shown in 2.9 the states are anti-correlated regardless of the bases. This means in particular for the eigenstates of the $\sigma_z$ matrix ($|0\rangle$ and $|1\rangle$) and the $\sigma_x$ matrix (shown in 2.3)

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}} (|10\rangle - |01\rangle) = \frac{1}{\sqrt{2}} (|{+-}\rangle - |{-+}\rangle) . \tag{2.13}$$

Thus, when Alice measures the system in $\sigma_z$ direction and for example receives the result $|1\rangle$ we are left with the state

$$|\Psi_{|1\rangle_A}\rangle = \frac{\hat{P}_{|1\rangle_A} |\Psi^-\rangle}{|\hat{P}_{|1\rangle_A} |\Psi^-\rangle |} = |10\rangle \tag{2.14}$$

where $\hat{P}_{|1\rangle_A}$ is the projection operator $|1\rangle\langle 1| \otimes \mathbb{I}$ and $\mathbb{I}$ denotes the identity matrix. Otherwise, if Alice measures her spin to be $|0\rangle$, we would receive

$$|\Psi_{|0\rangle_A}\rangle = \frac{\hat{P}_{|0\rangle_A}|\Psi^-\rangle}{|\hat{P}_{|0\rangle_A}|\Psi^-\rangle|} = -|01\rangle \,. \tag{2.15}$$

Alice's measurement in $\sigma_x$ direction would leave us with similar results with the states $|+-\rangle$ or $-|-+\rangle$, respectively. As a result, Bob's spin configuration is an element of reality depending on the measurement of Alice's state. Now imagine that Alice and Bob are separated so that they cannot communicate. Bob does not have any information about Alice's measurement. So, as Bob does not know which basis Alice chooses, both elements are part of Bob's reality even though Alice cannot determine the spin state $\sigma_x$ and $\sigma_z$ jointly sharply. EPR conclude that assuming quantum mechanics is complete leads to the statement that non-commuting operators do have a simultaneous reality.

However, this is a contradiction to the statement before. As a consequence, EPR found out that the description of quantum mechanics cannot the complete. This may be explained by the fact that there are some more "hidden variables" that complete quantum theory. The effect that there is some interaction between the two systems of Alice and Bob even though they are separated in space is called *non-locality*.

## 2.4 The CHSH-Inequality

The EPR-paradox and non-locality are some major differences compared to classical mechanics. To introduce both, we have used the properties of entangled quantum states. To distinguish quantitatively between classical and non-classical correlated systems one can use the CHSH inequality (named after its inventors Clauser, Horne, Shimony and Holt) [18].

For its derivation, the expectation values of the correlated random variables $A, A', B$ and $B'$ should be determined. Each of the variables can be either $+1$ or $-1$. Thus, classically, the absolute value of the expectation values

$$S \equiv |\langle AB\rangle - \langle AB'\rangle + \langle A'B\rangle + \langle A'B'\rangle| = |\langle A(B-B') + A'(B+B')\rangle| \leq 2 \tag{2.16}$$

because either $B+B'=0$ or $B-B'=0$ and therefore the other term equals $\pm 2$. Here, the linearity of expectation values has been used. This relation is known as the CHSH inequality and the result is called the S-parameter.

Now, we move on to an entangled quantum system in the state $|\Psi^-\rangle$. The random variables $A, A', B$ and $B'$ are the spin states measured by Alice and Bob. To each variable we can assign a measurement bases with a vector (e.g. $\vec{a}$ for the variable $A$) on the Bloch sphere. The observable which belongs to the random variable is then given as

$$O_A = \vec{a} \cdot \vec{\sigma} = a_x \cdot \sigma_x + a_y \cdot \sigma_y + a_z \cdot \sigma_z \tag{2.17}$$

where $\vec{\sigma}$ is the vector containing the Pauli matrices $\sigma_x$, $\sigma_y$ and $\sigma_z$ and $a_x$, $a_y$ and $a_z$ are real numbers. The expectation value of the product of two variables can be calculated by the scalar product of the observables' vectors

$$\langle AB \rangle = -\vec{a} \cdot \vec{b} = -\cos(\phi_{\vec{a},\vec{b}}) \tag{2.18}$$

with $\phi_{\vec{a},\vec{b}}$ being the angle between the vectors $\vec{a}$ and $\vec{b}$. A full derivation for this can be found in [15]. The last equality holds as $\vec{a}$ and $\vec{b}$ are normalised. For a maximum violation of the CHSH inequality, we can choose the four observables

$$O_A = \sigma_z, \quad O_{A'} = \sigma_x \tag{2.19}$$

$$O_B = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z), \quad O_{B'} = \frac{1}{\sqrt{2}}(\sigma_x - \sigma_z). \tag{2.20}$$

In this case, the observables $O_A$ and $O_B$ can be written as a scalar product

$$O_A = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} \sigma_x \\ \sigma_y \\ \sigma_z \end{pmatrix} \text{ and } O_B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \cdot \begin{pmatrix} \sigma_x \\ \sigma_y \\ \sigma_z \end{pmatrix} \tag{2.21}$$

According to Equation 2.18, the expectation value $\langle AB \rangle$ is given as

$$\langle AB \rangle = - \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = -\frac{1}{\sqrt{2}}. \tag{2.22}$$

A similar calculation for the other expectation values from Equation 2.16 shows that all outcomes are $\pm\frac{1}{\sqrt{2}}$. Consequently, we are left with the result that for the entangled state theoretically

$$S = |\, \langle AB \rangle - \langle AB' \rangle + \langle A'B \rangle + \langle A'B' \rangle \,| = 2\sqrt{2}. \tag{2.23}$$

While this resulting S-parameter represents the theoretical outcome in an ideal system, in reality, this value will most likely not be achieved. However, even if $S > 2$, we can conclude that the system is non-classical as it violates the CHSH inequality. If $S \leq 2$, we cannot prove the entanglement of the quantum states as it does in theory not violate the inequality. A classical system could yield a value close to 2 as well. Still, if the measurements were completely random, we would expect an S-parameter value close to zero.

## 2.5 Quantum Key Distribution (QKD)

Finally, it should be pointed out how the previously explained theory, in particular the CHSH-inequality, can be used for QKD. In contrast to classical encryption which is generally used today, quantum encryption has one major advantage. It is "information-theoretically secure" [14]. The protocol that is used in the student experiment to generate an intrinsically secure key was first suggested by A. Ekert [13] and is thus named Ekert91 protocol.

In general, cryptography algorithms are well-known. So, the security of encryption depends mostly on the security of the generated key. There are other QKD protocols like BB84 [19] where one participant (Alice) sends qubits to their partner (Bob). In Ekert91, they utilise a source of entangled photons and perform simultaneous measurements. Not only is it intrinsically secure, just like BB84, but also its security is proven by the CHSH-inequality 2.16.

To run the protocol, according to Ekert, a source of spin-$\frac{1}{2}$-particles in an anti-correlated state is needed. In the setup, the particles propagate to Alice and Bob in the $\hat{y}$-direction. Both measure the spin in the $\hat{x}$-$\hat{z}$-plane along their bases in $\vec{a}_i$ and $\vec{b}_i$ direction. Each one uses three different bases where $\alpha_i$ denotes $\vec{a}_i$'s azimuth angles concerning the $\hat{z}$-axis and similarly for $\beta_i$ and $\vec{b}_i$

$$\alpha_1 = 0,\ \alpha_2 = \frac{\pi}{4},\ \alpha_3 = \frac{\pi}{2} \tag{2.24}$$

$$\beta_1 = \frac{\pi}{4},\ \beta_2 = \frac{\pi}{2},\ \beta_3 = \frac{3\pi}{4}. \tag{2.25}$$

To run the protocol, Alice and Bob measure a sequence of particle spins by choosing for each measurement one of their specified bases randomly. Afterwards, both share the bases used for each measurement. As previously shown, the expectation value can be calculated by

$$E(\vec{a_i}, \vec{b_i}) = -\vec{a_i} \cdot \vec{b_i}. \tag{2.26}$$

This holds in an ideal system if the sample size is sufficiently large. For evaluating the measurements, Alice and Bob compare their bases used for measuring the spin in each step. We differentiate between three cases:

| $\|\alpha_i - \beta_i\|$ | Usage | Possible bases pairs |
|---|---|---|
| 0 | Key generation | $\left(\vec{a_2}, \vec{b_1}\right)$, $\left(\vec{a_3}, \vec{b_2}\right)$ |
| $\frac{\pi}{2}$ | None | $\left(\vec{a_1}, \vec{b_2}\right)$, $\left(\vec{a_2}, \vec{b_3}\right)$ |
| $\frac{\pi}{4}$ or $\frac{3\pi}{4}$ | S-parameter calculation | all other combinations |

**Table 2.1:** Overview of the possible outcomes when running Ekert91 protocol.

As suggested by 2.18, if there is no difference in the bases' angles, the measurements are perfectly anti-correlated. So, Alice and Bob have information about each other's measurement outcomes. If the angle's difference is $\frac{\pi}{2}$, the measurements do not correlate at all and for a difference of $\frac{\pi}{4}$ or $\frac{3\pi}{4}$ we are left with the bases used for calculating the maximum violation of the CHSH inequality, introduced in 2.19. To calculate the S-parameter using the measurement results, a correlation function is used

$$C_{\vec{a},\vec{b}} = \left.\frac{N_{++} + N_{--} - N_{+-} - N_{-+}}{N_{++} + N_{--} + N_{+-} + N_{-+}}\right|_{\vec{a},\vec{b}} \tag{2.27}$$

with $N_{++}$ and $N_{--}$ the number of correlated measurements i.e. both, Alice and Bob measure their spin in $|\uparrow\rangle$ or $|\downarrow\rangle$ according to their used bases. Similarly, $N_{+-}$ and $N_{-+}$ are the number of anti-correlated measurements, Alice and Bob measure their spin in $|\uparrow\rangle$ and $|\downarrow\rangle$ according to their used bases or vice versa. By counting the coincidences and adding them as suggested, we should be left with a correlation coefficient close to $\pm\frac{1}{\sqrt{2}}$ while differences may occur statistically. Adding the four correlation coefficients should yield theoretically an S-parameter of $2\sqrt{2}$. Differences from this value might occur due to statistical errors as the key is not long enough to neglect them or systematic errors. The latter might originate from inhomogeneities in the setup or incorrect identification of coincidences. Similar to before, a violation of the CHSH inequality assures a quantum mechanical correlation and we can be sure that our key is secure even though it may contain some errors.

In contrast, if an eavesdropper, commonly named Eve, joins the system, a violation of the CHSH inequality cannot be measured or at least only with a vanishing probability. As previously shown, a quantum state cannot be cloned. So, let us assume the eavesdropper wants to measure Bob's bits. A measurement is nothing less than a projection onto the measuring basis, here Eve's measuring basis $\vec{e}$. In case Eve measured their bit value as $|{\downarrow_{\vec{e}}}\rangle$, the state collapses, similar to Equation 2.15 to

$$|\Psi_{|\downarrow_{\vec{e}}\rangle}\rangle = \frac{\hat{P}_{|\downarrow_{\vec{e}}\rangle}\,|\Psi^-\rangle}{|\hat{P}_{|\downarrow_{\vec{e}}\rangle}\,|\Psi^-\rangle\,|} = |{\uparrow_{\vec{e}}\downarrow_{\vec{e}}}\rangle\,. \tag{2.28}$$

Similarly, if Eve measures $|{\uparrow_{\vec{e}}}\rangle$, the state collapses to $|{\downarrow_{\vec{e}}\uparrow_{\vec{e}}}\rangle$. Both possible outcomes are product states. So, Alice's and Bob's measurements are not correlated anymore. In case Eve wants to stay undetected, they have to match Bob's measuring basis in the majority of cases. By statistics, they just match the basis in 1/3 of the cases (assuming they know the protocol). Therefore, the S-parameter becomes much smaller than 2 and the eavesdropper can be detected.

# 3 Experimental Setup

In the experiment, students study polarisation correlation and run a quantum encryption protocol. This section should not only describe the current experimental setup's hardware but also its underlying processes. The setup can be roughly divided into the light preparation, i.e. the source of entangled photons, the measuring setup itself with the optical components and the data acquisition and visualisation through the server and measuring devices.

Since its establishment more than one year ago, students run the experiment using an MR environment with Augmented Reality (AR) glasses. This modern technology allows projecting elements interactively into the real world. A study carried out by the *MiReQu* team found that a similar lab course increased the students' knowledge of the topic and was perceived as interesting and enjoyable [20]. The study presented their setup and gave an overview of the possibilities of MR in general for student education. However, the study could not draw back these results to the MR environment as they did not have a comparison to their setup.

We provide this comparison for our setup by running a study in cooperation with the Department of Psychology. To measure the effect of the MR environment on the learning outcome, an alternative setup is required to isolate the effect of the interface. Therefore, it was necessary to build an application that students could use to run the experiment on a tablet. For comparability, the tablet version should match the MR version as well as possible. Before diving deeper into the application in the upcoming section, the setup is presented in detail.

## 3.1 Optical Components

Firstly, the optical components of the setup will be briefly introduced. They are all listed in the experiment's technical description [11]. The light source in the experiment is a SureLock LM 405 laser with a wavelength of $(405 \pm 1)\,\mathrm{nm}$, an output power of $40\,\mathrm{mW}$ and a beam size of $0.6\,\mathrm{mm} \times 0.3\,\mathrm{mm}$ [21]. In the measuring setup (see Section 3.3), gold-coated mirrors are used. They have a reflectance of about $96\,\%$, while the reflectances of different polarisations differ by less than $1\,\%$. [22].

### BBO-Crystal

The entangled photon pairs are generated using a Beta-Barium-Borat (BBO)-crystal, in particular one from Newlight Photonics with a size of $5\,\mathrm{mm} \times 5\,\mathrm{mm} \times 3\,\mathrm{mm}$. The generation process is described in detail in Section 3.2. This section also further deals with the compensation of walk-off effects. For the compensation, similar crystals with 5 mm × 5 mm × 1.5 mm are used [23].

#### Half-Wave Plates

In the experiment, half-wave plates are used to set the polarisation of the laser beam. They have a fast and a slow axis and retard the phase of the polarisation on the slow axis by $\frac{\lambda}{2}$ as the name suggests. In this context, the half-wave plate's set angle $\varphi$ indicates the angle with respect to vertically polarised light. Thus, it rotates the incident light's vertical polarisation by $2\varphi$. In the setup, the model WPH05M-808 from ThorLabs is used [24]. It has a retardance accuracy of less than $\frac{\lambda}{300}$. In our case, the additional systematical error of 2.5 ‰ originating from the fact that the half-wave plate is designed for light with a wavelength of 808 nm, while in the experiment, the light's wavelength is 810 nm, is negligible.

#### Polarising Beam Splitter

In the measuring setup, for evaluating the polarisation of the photons, polarising beam splitters, PBS102 from ThorLabs, are used [25]. They have average reflection and transmission efficiencies of more than 95 % or 90 %, respectively. Their extinction ratio, the ratio between maximum and minimum transmission, is 1000:1 for "a sufficiently linearly polarized input" [25].

#### Single Photon Detectors

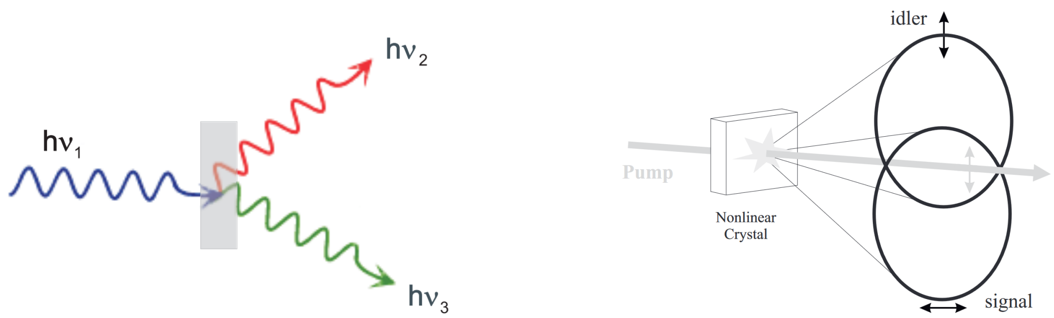
For detecting single photon events, the detectors COUNT-250N-FC from LaserComponents are used [26]. They have a dark count rate of maximum 500 counts per second, a detection efficiency of 50 % to 60 % in the used spectrum and a time resolution of 1000 ps. The light is coupled into these detectors by fiber couplers PAF2P-15B from Thorlabs [27].

## 3.2 Light Preparation

As described above, a BBO crystal is used to generate entangled photon pairs. They are needed to run the Ekert91 protocol successfully. Their generation happens due to the process of Spontaneous Parametric Down-conversion (SPDC), illustrated in Figure 3.1, and the birefringent characteristic of the crystal. During the SPDC process, one incident photon gets conversed into two outgoing photons. Birefringence means that the crystal has different refractive indices depending on the polarisation of light. These indices are $n_o$ for the ordinary axis and $n_e$ for the extraordinary axis. Both polarisation axes are perpendicular to each other. The polarisation $P$ of the non-linear crystal can be described as an expansion including higher orders [28]

$$P^i = \varepsilon_0 \left( \chi_{ij}^{(1)} E^j + \chi_{ijk}^{(2)} E^j E^k + O(E^3) \right) \tag{3.1}$$

with the dielectric constant $\varepsilon_0$, the susceptibilities $\chi$ and the electric field strengths $E$. While the first-order term explains linear effects like dispersion, the second-order term describes among other things SPDC. According to [28], the magnitude of the second-order effects is about 10 times lower compared to linear effects. Thus, a strong laser that produces much more than $10^{10}$ photons per second is needed for measuring correlated photons at an acceptable rate.




**(a)** General SPDC process, figure taken from [28]

**(b)** SPDC process of Type-II phase-matching, figure taken from [29]

**Figure 3.1:** Illustrations of the SPDC process.

In the context of SPDC, we differentiate between Type-I and Type-II phase-matching for the incoming pump photon and the outgoing signal and idler photon (in the following denoted by the indices $p$, $s$ and $i$). Type-I phase-matching means both outgoing photons are either ordinary or extraordinary polarised, depending on the incoming photon's polarisation. In contrast to that, Type-II phase-matching creates two photons with orthogonal polarisation. In general, the following two relations hold regardless of the type

$$\vec{k_p} = \vec{k_s} + \vec{k_i} \tag{3.2}$$

$$\nu_p = \nu_s + \nu_i \tag{3.3}$$

where $\vec{k}$ are the wave-vectors and $\nu$ the frequencies. Therefore, the relations can be regarded as momentum and energy conservation conditions. In our experiment, the pump laser creates light with a wavelength of 405 nm. Thus, the idler and signal photons leave the BBO crystal with a wavelength of 810 nm [28], [29].

Type-I phase-matching is unsuitable for our application as it does not easily produce entangled photon pairs. For Type-II phase-matching, due to the different polarisation and the birefringent properties of the BBO-crystal, the idler and the signal photon leave the crystal on two cones. If the angle between the incident laser beam and the crystal is adjusted correctly, these cones intersect (see Figure 3.1). A derivation of this phenomenon can be found in [29], pp. 23. Because of Equation 3.2, the photons leave the cones on opposite sites concerning the pump photons wave vector. So, if the signal photon leaves its cone on one intersecting point, the idler photons leaves on the other point. Therefore, the polarisations of the photons leaving the cones at the intersecting points are entangled in an anti-correlated manner. In general, this can be described by the state [29]

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + e^{i\phi}|01\rangle) \tag{3.4}$$

where $\phi$ is a general phase shift. In the following, we just require the state's anti-correlated characteristics. This holds for an arbitrary $\phi$.

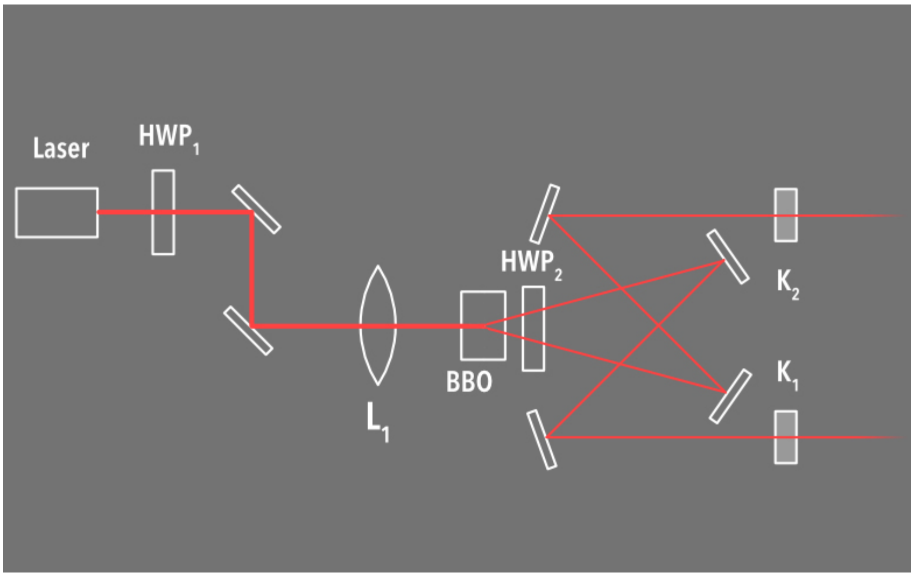



**Figure 3.2:** The light preparation setup. Figure taken from the experiment application.

The full setup for light preparation is shown in Figure 3.2. The first half-wave plate ($HWP_1$) is for setting the laser's polarisation. The two mirrors and the focusing lens ($L_1$) focus the beam into the crystal and control the incident angle of the pump beam.

#### Compensation of Walk-Off-Effects

It has to be noted, that the BBO-crystal has longitudinal and transversal walk-offs as side effects. So, they need to be compensated. Compensation for both can be achieved by the same setup. The following discussion is inspired by the work of Markus Oberparleiter [28].

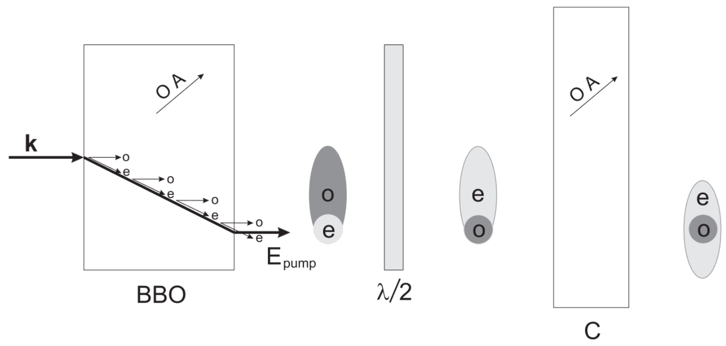



**Figure 3.3:** Transversal walk-off effect and its compensation. Figure taken from [28].

Transversal walk-off effects originate from the fact, that the optical axis of the BBO crystal is not parallel to the incoming pump photons wave-vector $\vec{k_p}$. Therefore, it is refracted and propagates in another direction compared to in free space. Depending on where the SPDC process happens, the two outgoing photons are separated in space. While the extraordinary polarised photons form a circular beam like the incoming pump photons, the ordinary polarised photons form an elliptical shape. Even if the crystal's length is only a few millimetres, the separation in space is much larger compared to the incoming beam's size.

To compensate for this effect, we flip the polarisations of the photons through a half-wave plate set at an angle of 45° (see Figure 3.2, $HWP_2$). By letting the photons propagate through another similar crystal of half the size (Figure 3.2, $K_1$ and $K_2$), we can compensate for the effect such that both beams have the same mean spatial position. Nevertheless, the after polarisation-flipping extraordinary polarised beam is still broader, see Figure 3.3.

On the other hand, longitudinal walk-off occurs because of the fundamental property of the BBO crystal of having different refractive indices regarding different wavelengths. Thus, we have one fast and one slow propagating photon, depending on their polarisation. The walk-off is maximum if the SPDC process happens at the BBO crystal's beginning (see Figure 3.4). The effect's compensation can be achieved similarly to the compensation of the transversal walk-off. Through flipping the states and compensating the differences with another crystal of half the size.

Through the compensation of longitudinal walk-off effects, we have optimised the time

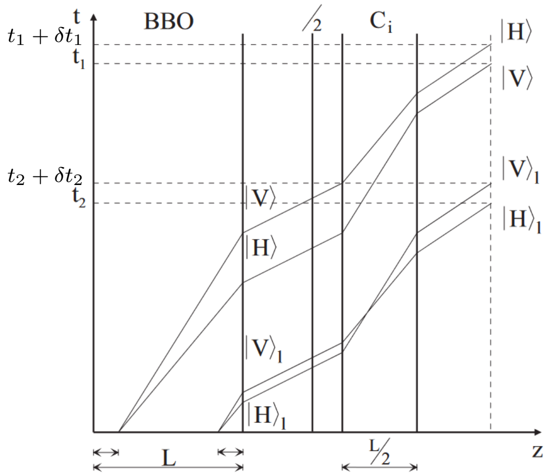



**Figure 3.4:** Space-time diagram showing the longitudinal walk-off effect of a photon pair produced by an SPDC process. Figure adapted from [28].

difference $\delta_t$ between a pair of entangled photons resulting in an indistinguishability of the photon's polarisation according to the detection time. So, now we are left with two entangled photons in an anti-correlated state and compensated walk-off effects so that we can measure them.

## 3.3 Measurement Setup

In both measuring arms for Alice and Bob, the measuring setup attaches directly to the compensation crystals. As shown below, the setups consist of a half-wave plate, followed by a polarising beam splitter and two photon detectors. A sketch of the setup is shown in Figure 3.5. As mentioned before in Section 3.1, the half-wave plate's set angle $\varphi$ indicates the angle with respect to vertically polarised light and it rotates the incident light's vertical polarisation by $2\varphi$. So, the coincidence, e.g. $\langle A_0 B_0 \rangle$ can be calculated in accordance to 2.18 and in terms of $\varphi_{a,b}$, the half-wave plates' angles of Alice and Bob, by

$$\langle A_0 B_0 \rangle = -\cos(2 \cdot (\varphi_a - \varphi_b)). \tag{3.5}$$

The photon detectors then connect to the measuring device *Time Tagger 20* by *Swabian Instruments* [30]. The half-wave plate's angles can be recorded using an *Arduino Micro* [31]. The *Arduino's* data is sent to the server and has to be decoded. For the *Time Tagger*, we can set up the measurement ourselves. The *Time Tagger* records three kinds of data: incidence counts, single-detected coincidences and coincidence counts.

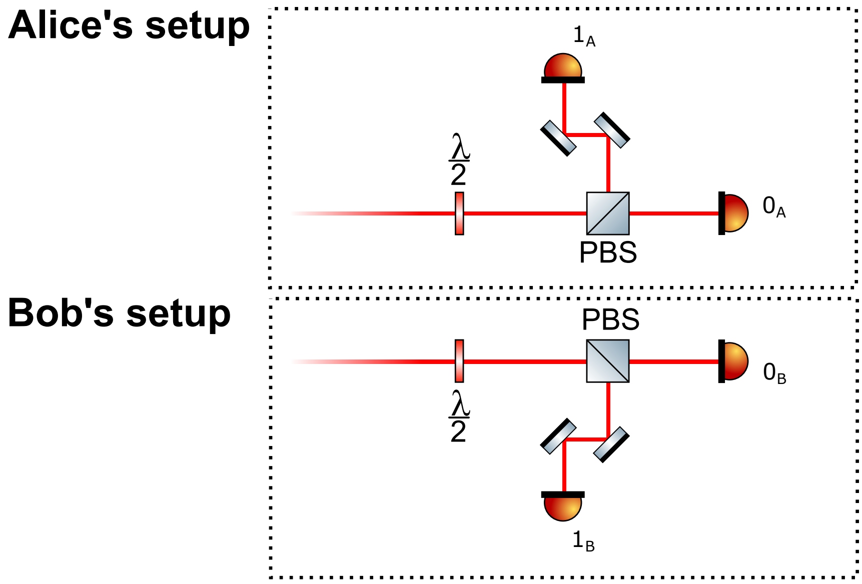



**Figure 3.5:** Measuring setup of Alice and Bob. For both, it consists of a half-wave plate a polarising beam-splitter and two photon detectors[1].

The incidences are the counts of single photons recognised by each detector in a given time frame. Single-detected coincidences are detections that happen nearly simultaneously in two detectors. We measure coincidences in each meaningful combination: $A_0$ and $B_0$, $A_0$ and $B_1$, $A_1$ and $B_0$ as well as $A_1$ and $B_1$. Here, the indices denote the measured bit, i.e. the detector that receives a signal. The coincidence time $\tau_c$ is the maximum time between two events for a coincidence [30]. This time is in the experiment set to $\tau_c = 4000\,\text{ps}$. An evaluation of this time verifying this setting as meaningful is shown in Section 5.1.

## 3.4 Data Acquisition and Visualisation

Finally, we want to have a look at how the measuring devices' data is further processed and presented to the experimenter, namely the student running the experiment. All collected data can be accessed by sending HTTP requests to the server that is connected to the *Arduino* and the *Time Tagger*. This is necessary because students wearing AR glasses need to take measurements wirelessly.

Similarly, the students send data to each other using the server. The general data flow is visualised below in Figure 3.6. The data that Alice and Bob send to each other include information on whether they want to measure counts or bits simultaneously, their current progress in the experiment or their bases used for measuring bits in the context of QKD.

In the current setup, a program on the AR glasses guides the students through the experiment, explains the tasks in each step and lets them carry out the measurement.

[1]Figure created using the Component Library (`https://www.gwoptics.org/ComponentLibrary/`).

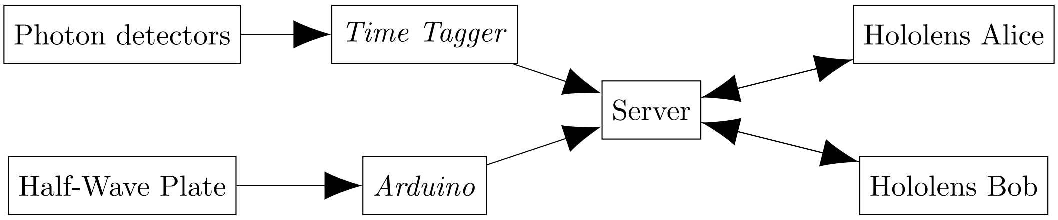



**Figure 3.6:** Data flow in the setup.

The measured data can be exported to the server so that students can further evaluate it. Figure 3.7 shows a scene from the experiment, recorded on an identical setup at Westfälische-Wilhelms-Universität (WWU) Münster where the experiment was first developed.

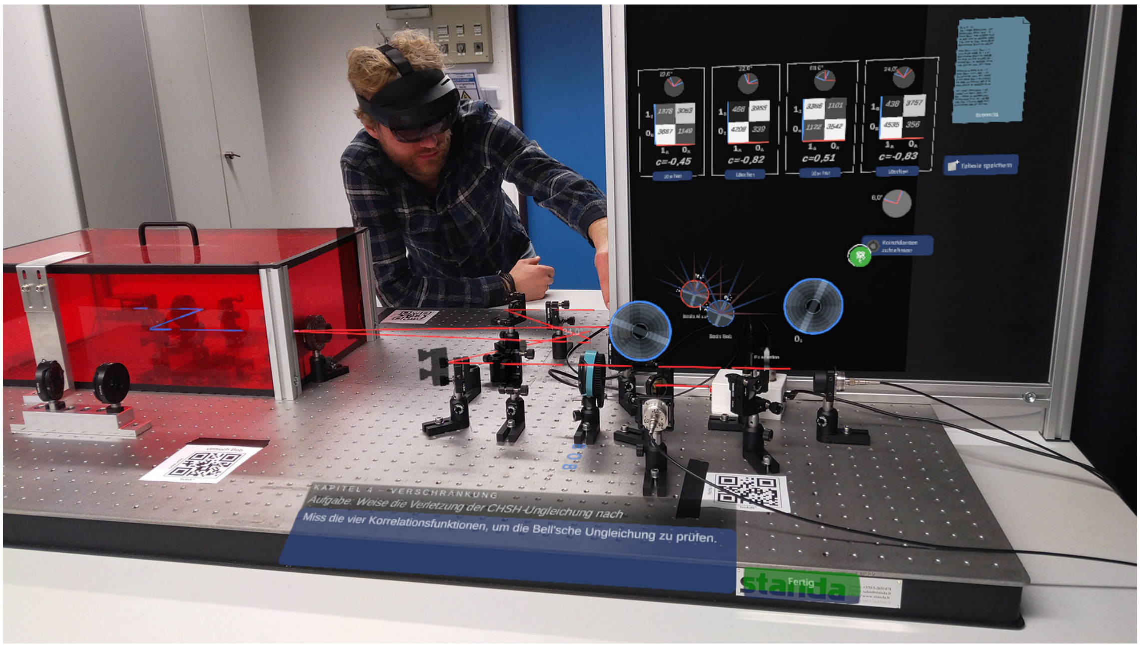



**Figure 3.7:** Image from the S-parameter measurement. At the bottom, the task is explained, further information for the experiment in projected into the setup interactively and above the measured data is visualised. Figure taken from MiReQu Website [10].

As mentioned before, the developers carried out a study for a similar experiment [20]. In their experiment, fourth-semester undergraduate students studied polarisation and Malus' Law as well as the effect of half-wave plates and polarising beam splitters. Similar to the experiment at hand, they used an MR environment to display the measurements. For their study, they evaluated the students' learning outcomes in a Pre-Post-Test. This means, the students had to answer the same questions one week before and right after experimenting. Additionally, the students' enjoyment was individually measured on a self-assessment scale. The researchers discovered that the students' knowledge could be significantly improved from a mean of four to about six out of eight correct answers and that they enjoyed the experiment. However, they were unable to investigate the extent to which these positive effects are attributable to the MR environment as they lacked a comparison to a non-MR environment. They concluded that their findings should be viewed as ”a starting point for further investigation” [20].

# 4 Application

For a comparison study, an app was developed to run the student experiment. The app and the MR version should be as similar as possible to assure comparability. Therefore the seven chapters contain identical instructions in the same order. In this section, the general structure of the application will be documented. Moreover, a comparison to the MR version is given.

The app is built in Python using the PyQt5 framework. It enables the implementation of GUI programs making use of the C++ library Qt embedded into Python. Besides its GUI opportunities, the framework introduces the powerful signal and slot mechanism [32]. It is made possible due to Qt's *meta-object-system* in the way that every class inherits the *QObject* class in which the signal and slot mechanism is implemented. Whenever certain actions are performed such as a button is clicked, a task is finished or a value is changed, signals are emitted. These signals can be connected to a desired Python function, a slot. The connection is built by the compiler when running the program and mismatches of the code are only identifiable during runtime. However, it is more intuitive compared to mechanisms other frameworks provide like callbacks (pointer to functions in C++) [32]. Signals can be either pre-designed by the library or implemented individually. In terms of performance, threading is crucial for GUI programs as the GUI should be responsive even if a task is running in the background.

The code can be divided into three sections, the backend, the frontend and the main program. The latter is the file that is needed to run when starting the app. It starts the main thread and organises the widgets on the screen. The backend and frontend are organised in packages that are imported. The backend consists of three modules, namely *Plot.py*, *ServerInterface.py* and *student.py.* The frontend contains all the measuring widgets needed to run the experiment. These three sections will be explained in the following. The full code can be found on the KIP's gitlab[2].

## 4.1 The Backend

### The Student Class

The backend is mainly implemented in *student.py.* This class handles the global data that every experimental widget has to access such as the student's name (Alice or Bob), the half-wave plate's offset and the data that is communicated to their partner. This data contains information on whether the student wants to measure a bit or counts synchronously, share

[2] Link to the gitlab: `https://git.kip.uni-heidelberg.de/riegert/mirequ-app`

their measuring base and the current step in the experiment. For sending their own and receiving their partner's information the module builds the connection to the server using the *ServerInterface.py* module.

The student class also runs the most important threads. Two permanently running threads are the *rotation thread* and the *communication thread*. Both request data from the server. The *rotation thread* acquires the current half-wave plate angles. They are needed for all measurements and should be requested permanently to display and plot them in real time in the app. The *communication thread* reads the data that the student's partner sends to the server. It compares the received data to the currently stored data and overwrites it if required. Additionally, the student class includes the *measuring thread*. It simply waits for a specified amount of time so that the *Time Tagger* can carry out the measurement. For connection handling, the student class contains a *connection thread*. When the connection to the server is lost and one tries to reconnect, this thread is started. It tries to send a dummy "Hello world" request. If this request is successful, all the other threads will start.

Furthermore, the student class contains functions to calibrate the half-wave plate, decode the *Time Tagger's* detections and compare the student's data to their partner's data. This last step is crucial for measuring synchronously. When called, it checks if the data is set for the student themself and their partner. If so, the data is set to false and a specified signal is emitted.

### The Plot Module

This module organises all different kinds of plots included in the app. There are several types of plots which can be divided into two categories, real-time updated plots and non-real-time updated plots. The latter are plots displaying measurements such as counts or bits. They are implemented in *matplotlib* as it is best suitable for plotting scientific data. However, it is not good when it comes to performance and it is therefore not feasible for real-time plotting. Yet, this is necessary for giving instant feedback on the change of the half-wave plate's angle. *Pyqtgraph* is used to plot in real-time. For increasing performance, the updating processes are outsourced to a separate thread.

### The Server Interface

As there is already a running setup of the experiment, the server is already well-established and the available requests were pre-designed. The app, namely the *server interface* can send *get-* and *post-requests* to the server through WiFi and HTTP. *Post-requests* are used to send communication data and encrypted data to the partner. The acquired data, i.e. received by sending *get-requests* include measurements by the *Time Tagger* and the *Arduino*. Depending on the desired measurement, it is necessary to get the last measured bits, the single photon counts or the correlated photon counts. There is a specific request for each case.

## 4.2 The Main Program

After running the app, namely *main.py*, the main thread has started. The experimenter is introduced by the *Welcoming window* (see Section 4.3) and after the introduction is finished, the app is built. This process includes initialising the student (implemented in the student class), the additional windows, the stack of widgets and connecting the signals.

The initialised stack consists of two parts, the stacked widget and the experimental widgets. The stacked widget contains the headings and tasks that need to be performed. Its texts are similar to the instructions from the mixed-reality version. Some version-specific descriptions needed to be adjusted. The experimental widgets are stored in an array. Each entry is either *None* or one of the widgets explained in the following part. The initialised window's structure can be seen in Figure 4.1. On top of the window is the menu bar. It consists of buttons to open the settings and calibrate the half-wave plate. The stacked widget is placed below. Next to the stacked widget are the *Next-* and the *Previous*-button. When clicked, they let the student move on with the experiment and increase the step number by one or go back to the previous step and decrease it, respectively. According to whether the widget array's entry is *None* or not, a widget is shown below or the size of the stacked widget is extended. For all widgets that are stored in the array, there is a function *setTexts*. This function is called when the app is started or the language is changed from German to English or vice versa. More languages could be supported, but there is currently no need for it.

During the initialisation process, the student's and their thread's signals are connected to slots. These connections include that the measuring thread's progress is shown by a progress bar or an experimental widget's function is called when the half-wave plate's angle is changed. Some experimental widgets make the student emit a signal, e.g. for performing a measurement. When these signals are emitted, a function of the belonging experimental widget is called. This way it is assured that the experimental widgets do not interact with each other and a non-existing function cannot be called. Finally, when certain actions are

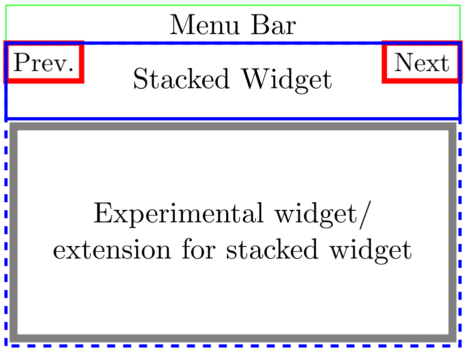



**Figure 4.1:** Main Window's screen.

performed, the signal *page finished* is emitted. This leads to an activation of the *Next*-button and the student can move on. When moving on, the *Next*-button is deactivated again.

## 4.3 The Frontend

In PyQt, widgets consist of widgets ordered in a layout. They can be everything from buttons to text boxes and labels and due to their modularity, can be created using a program called *Qt-designer*. For the app, nearly all widgets were created this way (shown in Figure 4.2). They are stored as *.ui* files loaded into Python. In the following, the different used widgets and their functionalities are introduced.

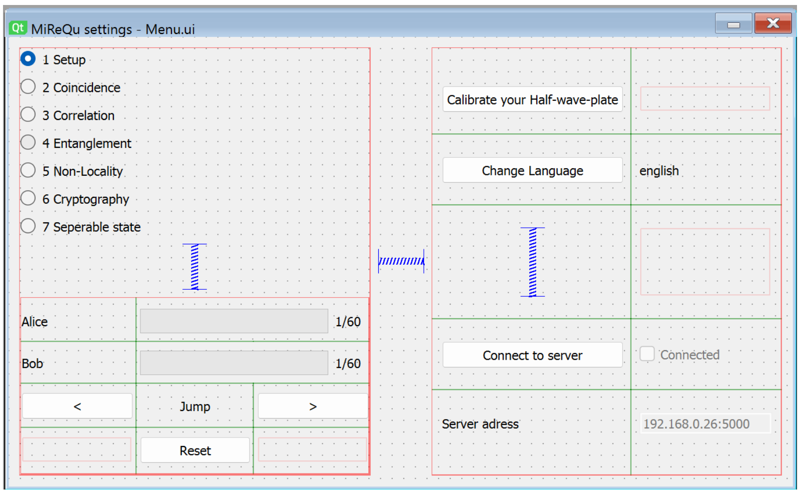



**Figure 4.2:** Screenshot of *Qt Designer*. Here, the creation of the Menu widget is shown.

### The Welcoming Window

Firstly, the user is introduced by the welcoming window. The student has to choose their preferred language, the experimental setup (in this case either the one located next to the door or next to the window) and whether they would like to run the experiment as Alice or Bob. Afterwards, the main program is built and the experiment is ready to start.

#### The Menu

In the menu, the student can jump back and forth between the chapters and steps and see their partner's progress. They can calibrate the half-wave plate, change the language and connect to the server.

#### Chapter 1 - Experimental Setup

The introduction chapter explains the experimental setup described in detail in the previous Section 3. It guides the student through each part and provides necessary information for the experiment. Therefore, the same sketches and descriptions as in the mixed reality version are used. An example of these sketches is presented in Figure 3.2.

#### Chapter 2 - Coincidence

This chapter lets the student explore the nature of randomness. They measure the counts of incoming single photons at the detectors as well as the detected single photon events. Both measurements are performed individually by the students on their setup without exchanging data. For measuring counts, students have to wait for five seconds, realised through the measuring thread. During this time, the *Time Tagger* collects data. After the time has passed, the data is acquired from the app through the server. For measuring bits, the students have to wait for one second when collecting a single bit's value or two seconds when recording a bit sequence. These numbers are chosen arbitrarily and ensure that the measurement is processed completely before new data is collected. The *Time Tagger* collects data continuously, so measuring a bit hardware-wise could be much faster. The measured counts and the bits are visualised in the app. Permanently, the half-wave plate's angle is shown in an *Angle Plot*, shown in Figure 4.3. While the angle above displays the half-wave plate's angle directly, the plot below shows the measuring basis, i.e. twice the angle from above. This plot updates in real time.

#### Chapter 3 - Correlation

For measuring correlated counts, the students have to communicate with each other. Therefore, they have to build a connection in the app over the server. In the following, they measure just as before the counts while now varying the difference between their

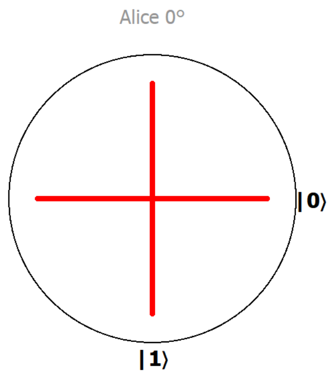



**Figure 4.3:** Angle Plot showing the HWP's angle together with the measuring bases of Alice.

half-wave plates' angles and measure correlated bits. Similar to in Chapter 2, the results are plotted in the app. Additionally, the students now see the partner's half-wave plate angle in the Angle plot. So, they should find out that their measurements are correlated.

#### Chapter 4 - Entanglement

After the introduction of photon number correlations, the nature of quantum physics will be explored in more detail. The students should prove the violation of the CHSH-inequality (see Equation 2.16). They set their measuring bases to the ones introduced before 2.25. The results are plotted here too. This measurement is of great conceptual importance as it demonstrates the non-classical nature of the system. Yet, it is very sensible and prone to errors. If the setup is not misaligned it is not possible to prove the violation.

#### Chapter 5 - Nonlocality

This chapter visualises the entangled state. Therefore, the students see their individual measuring bases and if the communication channel is activated, their partner's bases as well. The visualisations let the student explore why it is necessary to communicate with their partner to be able to measure a correlated bit.

#### Chapter 6 - Cryptography

This is the key chapter of the experiment. After having studied the entangled state in detail, the students apply it to generate a secure key as suggested in the Ekert91 protocol. Therefore, Alice and Bob have to measure the bits synchronously. As it cannot be assured that both devices send the request at the same time to the server, we use a stored measurement in the server. When one of the students presses a button to run a measurement, information is stored that they are waiting for their partner. Once the partner agrees to perform the measurement, the measurement is conducted and the server stores the measurement. The student who has initiated the measuring process then reads the stored measurement. Of course, this way, the generated key is not intrinsically secure as an eavesdropper could just get the data from the server. In terms of the experiment, it is sufficient to teach the concept to the students. Similarly, they only generate a key of 25 bits. So it would be impossible to prove the violation of the CHSH inequality as the number of bits is too low to neglect statistical errors and calculate correlations correctly. Therefore, in case they use different bases, the app uses the *Time Tagger's* measured counts to calculate the correlation.

**Chapter 7 - Separable State**

In this final chapter, the setup is modified so that a polariser is included to represent an eavesdropper. The correlated state becomes a product state and all previously measured characteristics do not hold any more. To explore the nature of the separable state, the students repeat the measurements that they carried out in chapters 3, 4 and 6, respectively. The used widgets are similar to the ones from these chapters.

**Miscellaneous Widgets**

In addition to all the previously described experimental widgets, there are some more widgets with fewer functionalities. There is a template widget for the stacked widget (see Section 4.2). The *wait* widget consists of a progress bar shown when performing a measurement. Lastly, the *Custom Button* module contains implementations for custom buttons such as the button to activate communication and the buttons to create a message for cryptography.

## 4.4 Comparison to the Current Setup

After introducing both, the currently used MR environment and the application as an additional version, they will be compared. This comparison should give some examples of the representations and the structure in general. In particular, the comparison focuses on three topics: user experience, visualisation of the half-wave plate angles and the plots of the bits and counts.

**User Experience**

The main difference between the two environments guiding the students through the experiment is the user experience of the two applications. While the MR version is highly interactively designed, the app is like regular student experiments more passively. One example of such an interactive feature is the laser beam that is shown in the MR version. When using the app, the student has to keep an eye on both, the setup and the app simultaneously while they are interconnected when working with the MR version. The study conducted on a similar experiment showed that the majority of "students had never worked with an MR headset before" [20]. It can be assumed that most students have already used a tablet.

Additionally, the environment created by the MR version does not only display the measurements and additional information in the setup. It also contains more visual effects like animations when plotting the measurements or acoustic feedback when pushing buttons. In contrast, the app is more focused on the measurements and does not contain visual effects.

### Visualisation of the Half-Wave Plate's Angle

The visualisations of the half-wave plates' angles are similar in both environments. A screenshot of the app is shown in Figure 4.3. An image of the view in the MR environment can be seen in Figure 4.4. The angle is displayed directly above the half-wave plate in the MR version, whereas in the app, it is listed above the plot. Both versions include a plot of the measurement bases and their corresponding states. In the MR version, the plot shows them individually above the fiber couplers, while in the app, they are plotted together.

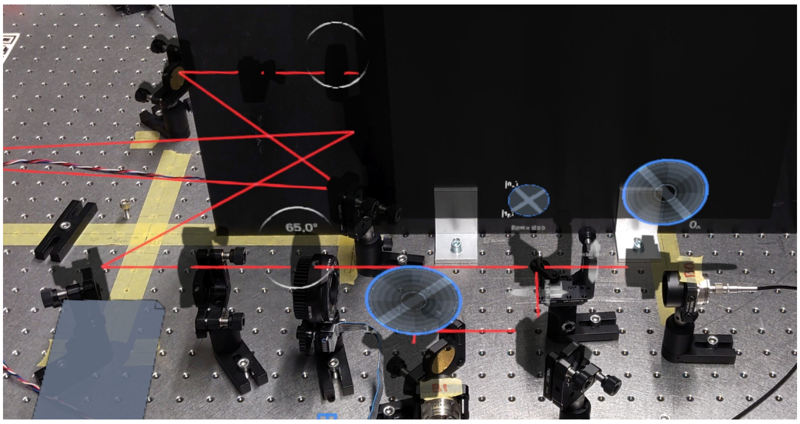
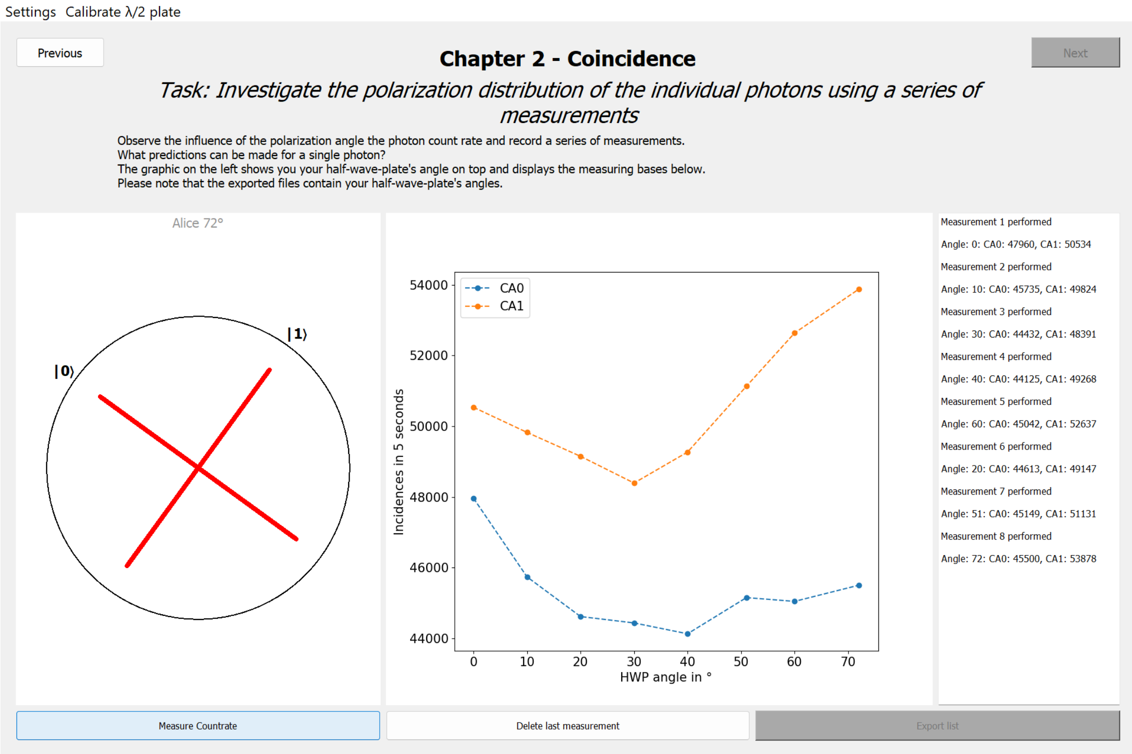



**Figure 4.4:** Visualisation of the half-wave plate's angle in the MR environment.

### Plots of the Bits and Counts

During the experiment, the students measure multiple times counts or single bits. The visualisations of both differ between the versions (see Figure 4.5). These differences originate mostly from the frameworks and programming languages in which both versions are built. The counts in the app are displayed in a scientific plot where the x-axis shows the half-wave plate's angle and the y-axis the counts. In the MR version, the counts are directly plotted as dots in the visualised state. This way, the student receives less information about the numerical values but has a direct connection between state and counts. For the subsequent evaluation, there are no differences. Both versions' values are exported to the desktop computer.

The illustration of the bit values varies throughout the versions as well. This can be seen in Figure 4.6. The MR version features both, a plot of the measuring basis and the bits. However, this plot is only completed after all 25 bits are measured. The app on the other hand contains only one plot. It shows the bits in a grid where white represents 1 and black stands for 0. In the bit, the half-wave plate's angle during the measurement is shown.



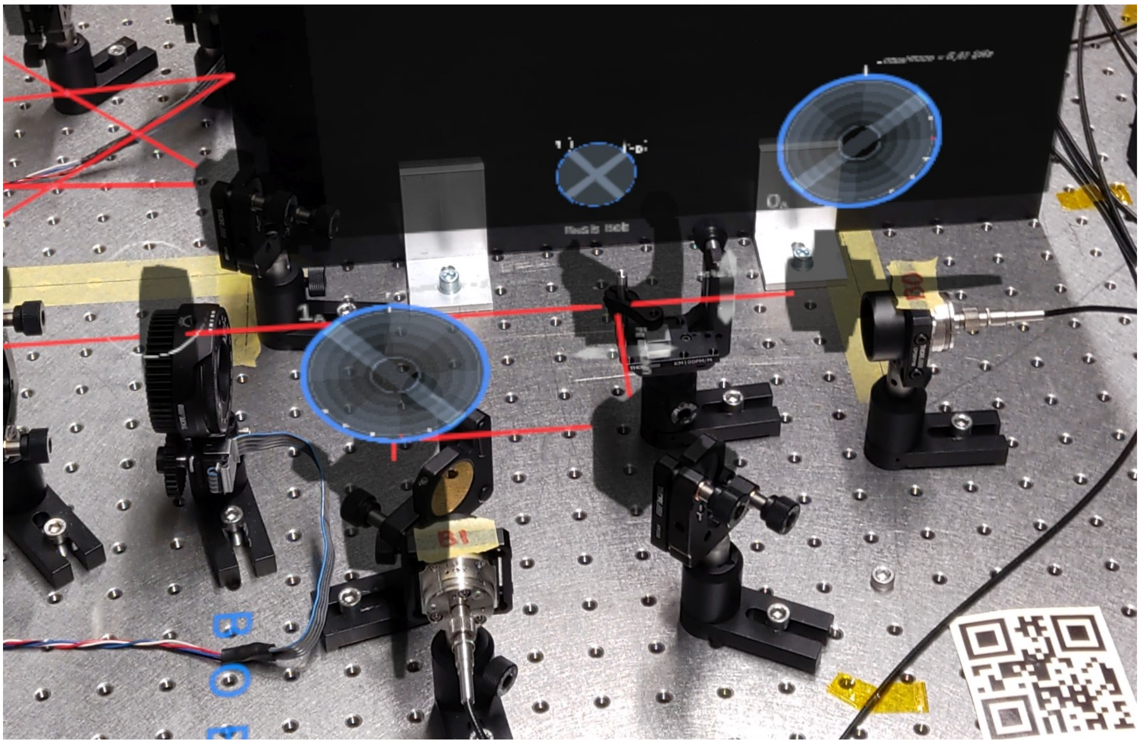



**Figure 4.5:** Visualisation of count measurements in the two versions. The screenshot on top displays the app while the capture at the bottom shows the MR version.

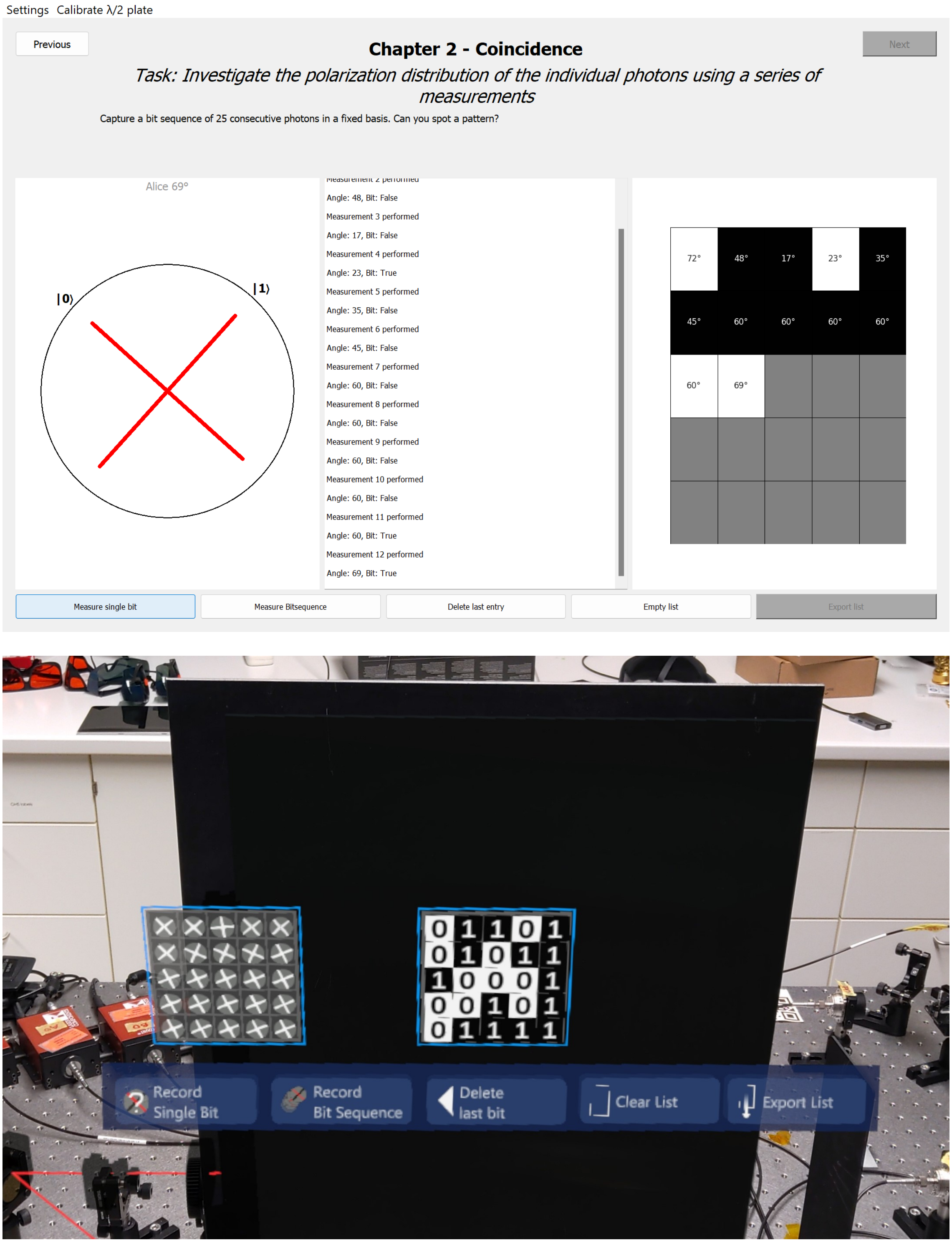



**Figure 4.6:** Visualisation of single-bit measurements in the different environments. Similar to before, the screenshot on top displays the app while the capture at the bottom shows the MR version.

# 5 Evaluation

It will be shown that the experiment can be conducted similarly to the MR environment with the tablet version. Firstly, supplementary measurements to evaluate the coincidence window, the system's alignment and its statistical errors are shown. Afterwards, the default measurements including single photon and coincidence counts are shown and the S-parameter is calculated. Finally, the app's implementation of the QKD protocol will be presented.

In general, the setup must be well-aligned to receive results that match the theory. This can only be done by instructed tutors. In case the setup is misaligned, it is not possible to measure the violation of the CHSH inequality. One important measure for the quality of the measurements is the visibility $v$ calculated by

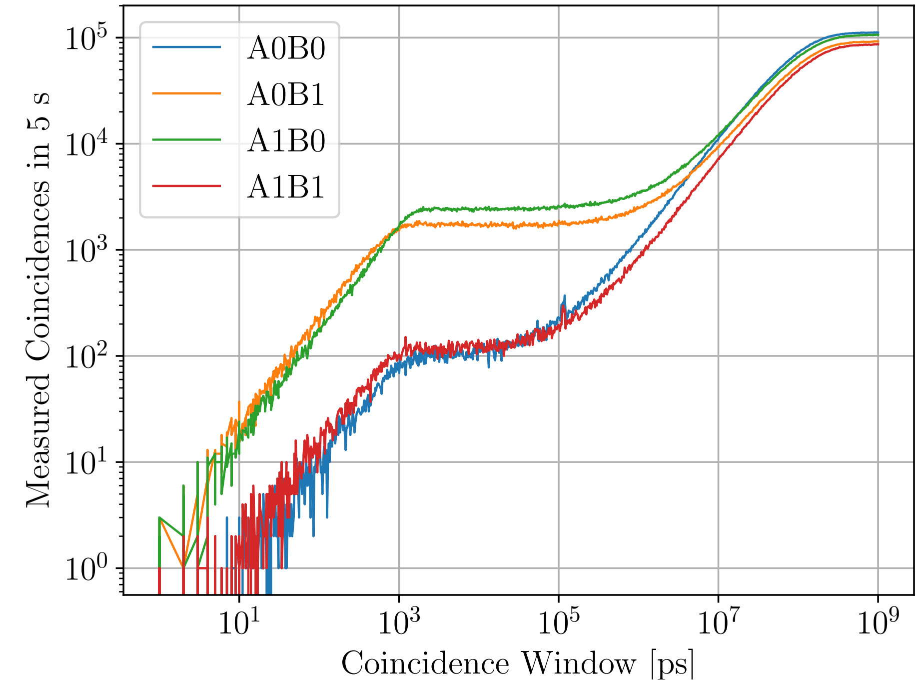
$$v = \frac{N_{\text{max}} - N_{\text{min}}}{N_{\text{max}} + N_{\text{min}}} \tag{5.1}$$

where $N_{\text{max}}$ is the maximum number of counts in the measurement while $N_{\text{min}}$ is the minimum. Indicators for bad alignment of the setup are inhomogeneous single photon counts yielding high visibilities for them and conversely low visibilities for coincidence counts. Theoretically, one would expect that for single incidences, $v = 0$ and for coincidences, $v = 1$ when measuring counts in dependence of the measuring basis or the difference between Alice's and Bob's bases, respectively.

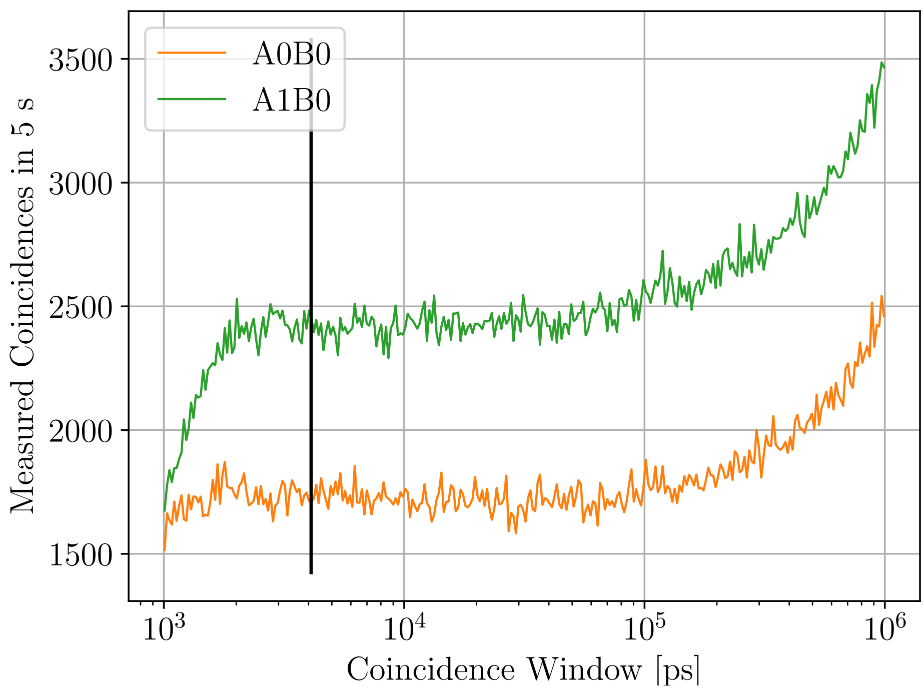
## 5.1 The Coincidence Window

Before the photon count measurements are evaluated, the set coincidence window $\tau_c$ should be analysed. The coincidence window is the maximum time between two events for a coincidence. To measure its impact on the counts, they were measured using different windows from 1 ps to 1 ms for five seconds each. The results of the measurement are shown in Figure 5.1.

In these figures, it is shown that the measured coincidences rise until roughly 1000 ps. Here, not all photon pairs are recognised as coincidences as the time resolution of the photon detectors is only 1000 ps (See Section 3.1). Afterwards, there is a plateau until about $10^5$ ps. In this region, all entangled photon pairs are identified as coincidences as they are not cut off. Thus, there are no major differences between the measurements apart from statistical errors. Afterwards, the coincidence counts increase again up to the limit at $\tau_c \simeq 10^5$ ps. Here, single photon incidences are mistaken for coincidences as




**(a)** Complete Measurement




**(b)** Zoomed into the Plateau Region

**Figure 5.1:** Sweep over coincidence Windows from 1 ps to 1 ms while measuring the coincidences over five seconds. Both half-wave plates are set to 0°, thus the state is anti-correlated. In (b), only the two lines with anti-correlation are shown. The black line indicates the currently used coincidence window of $\tau_c = 4000$ ps.

the coincidence window is too large. At very large coincidence time windows, nearly all incidences result in false-detected coincidences and the curve reaches saturation. Figure 5.1 (b) shows a zoomed view of the plateau region from $10^3$ ps to $10^5$ ps where the currently set coincidence window of $10^4$ ps is marked.

In conclusion, of the currently set coincidence time of $\tau_c = 4000\,\mathrm{ps}$ can be approved. It is ensured that all coincidences are recognised because it is well in the plateau region. As it is in the lower part of this plateau, errors of wrong detections can be minimised.

## 5.2 Alignment and Statistics

After aligning the setup, we have conducted a measurement with Alice's and Bob's measuring bases at 0° of the half-wave plate while recording the coincidences for one minute every ten minutes for roughly three full days. The results of this measurement are shown in Figure 5.2. This data was further used to calculate the correlation coefficient by using Equation 2.27. In theory, it should be equal to 1 as the state is perfectly anti-correlated. In general, we can see that the counts differ over time while the correlation coefficient tends to go down. Thus, it can be concluded, that the setup is very sensible to its environment. We were unable to find cyclic behaviours that could be attributed to day and night cycles, air conditioning or light switching.

Well before the mentioned alignment, we have carried out a long-term measurement over 14 days. No alignment took place before this measurement. Comparing the two measurements, we can see that again, the correlation counts differ over time even though we cannot see a tendency. It has to be noted that the setup was shut off at the beginning which explains the behaviour on 21 December. It seems like the correlation coefficient stabilises at around 0.91 which is roughly the same end-value of the measurement that took place after the alignment. In conclusion, it can be seen that the setup is only well aligned for a short time, while it appears to stabilise in a worse-aligned state.

However, time-dependent systematic errors are not the only ones involved in the system. Due to detection errors and errors of the whole setup's alignment, the measurements differ statistically. To analyse these errors numerically, the counts of coincidences were measured 1000 times for 5 seconds. The results are shown in Figure 5.4. The goal is to estimate a confidence interval of correlation count measurements. The data shows some systematical drift. To compensate for this drift, linear functions like

$$N(n) = m \cdot n + b \tag{5.2}$$

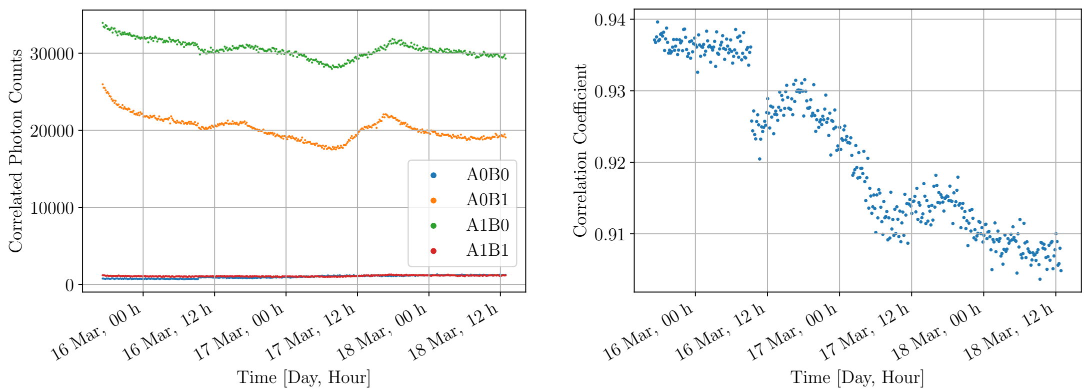



**Figure 5.2:** After aligning the setup, the correlated photon counts were measured every ten minutes over 60 seconds for nearly three full days (see on the left). Alice and Bob measured in the same basis of 0°. The figure on the right shows the belonging correlation coefficient calculated by 2.27. The measurement was conducted from 15 March to 18 March 2024.

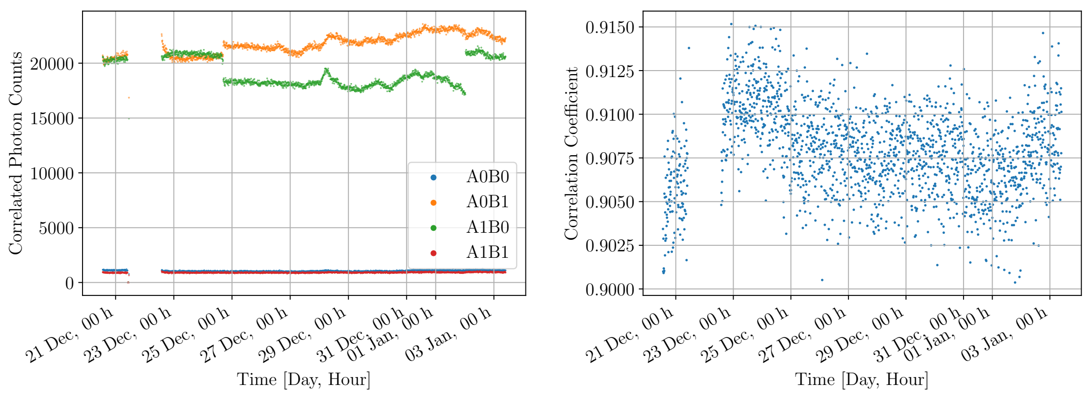



**Figure 5.3:** We have carried out a similar measurement to the one in Figure 5.2. In this case, we did not align the setup beforehand. The measurement was conducted from 20 December 2023 to 03 January 2024.

are fitted where $n$ is the number of the measurement. These fits were further used to calculate the standard deviation

$$\sigma = \sqrt{\frac{\sum_{n=1}^{1000} (N(n) - C_n)^2}{1000}} \tag{5.3}$$

where $C_n$ are the coincidence counts of the $n$-th measurement. The calculation yields

$$\sigma_{A0B0} = 10,\ \sigma_{A0B1} = 41,\ \sigma_{A1B0} = 49,\ \sigma_{A1B1} = 11. \tag{5.4}$$

As the magnitude of the counts differ, we want to analyse how to estimate the percentage

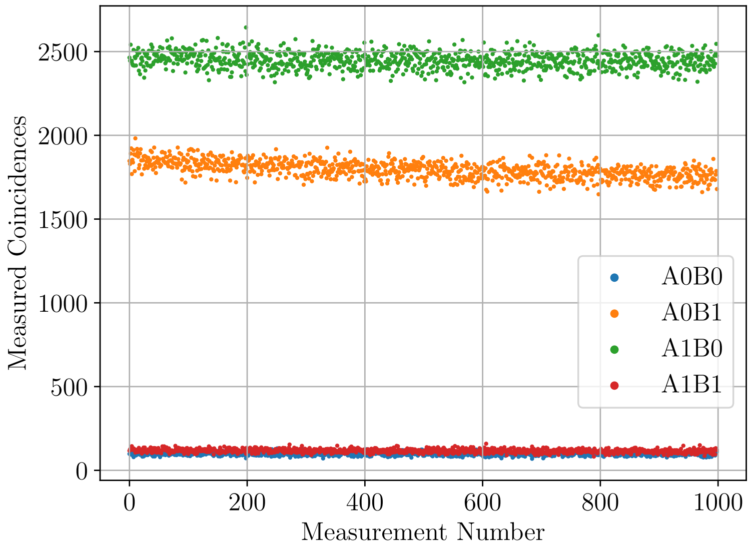



**Figure 5.4:** The coincidences were measured 1000 times for 5 s each. During the measurement both half-wave plates were set to 0°.

error which can be calculated similarly as above by

$$\sigma_p = \sqrt{\frac{\sum_{n=1}^{1000} \left(1 - \frac{C_n}{N(n)}\right)^2}{1000}}. \tag{5.5}$$

These numbers can be used to give the error of measurements without the need to run a similar error measurement each time. With this calculation, we get

$$\sigma_{p,A0B0} = 11\,\%,\ \sigma_{p,A0B1} = 2.3\,\%,\ \sigma_{p,A1B0} = 2.0\,\%,\ \sigma_{p,A1B1} = 9.7\,\%. \tag{5.6}$$

The measurement was carried out with Alice's and Bob's half-wave plate angles set to zero. So, in theory, the correlated counts should be equal to zero. Therefore, the higher relative errors of about 10 % do not represent a meaningful value. This error should in the following primarily be used for calculating the error of the S-parameter. As we do not measure a perfect correlation or anti-correlation for the S-parameter, the counts are in general higher. Nevertheless, the estimated error should in the first place give a hint about the magnitude of the error. So, we will continue the calculations with an estimated error of 5 % for each measurement. Indeed, this is only a rough estimate. The data shows a tendency that in the neighbourhood of 2000 counts, it is rather equal to 2 %. For lower counts, it is most likely higher. Therefore, the chosen 5 % should give a good estimate.

## 5.3 Single-Photon Measurements

Before diving deeper into the measurements for the violation of the CHSH inequality, the measurements of single photons and correlated photons should be evaluated. First, we have measured the number of photon incidences in dependence on the basis angle. The result of this measurement is shown in Figure 5.5. While we would estimate a straight line in theory as the incidences should not depend on the basis, reality shows a dependence on the half-wave plate's angle. We can calculate the visibilities according to Equation 5.1 and get

$$v_{A0} = 0.07,\ v_{A1} = 0.11,\ v_{B0} = 0.12,\ v_{B1} = 0.14. \tag{5.7}$$

The measurement shows that the setup is not ideal. However, it is nicely shown that $A0$

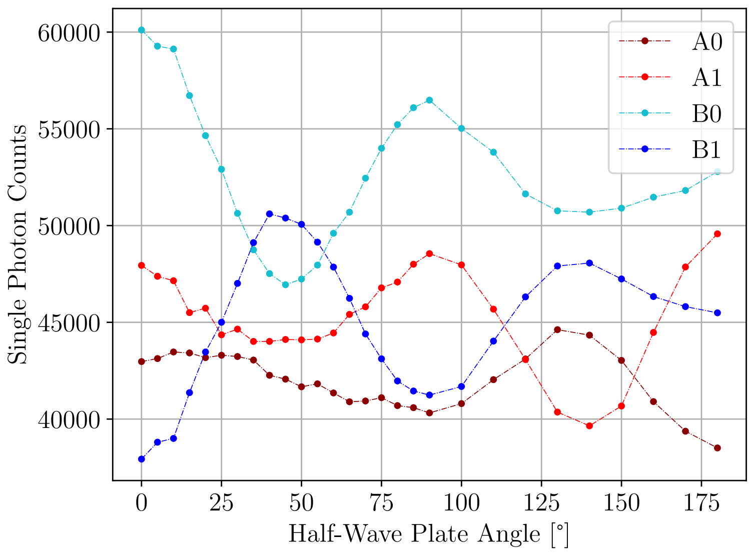



**Figure 5.5:** Measurement of single photons depending on the basis angle. The measurement was carried out on 22 March 2024.

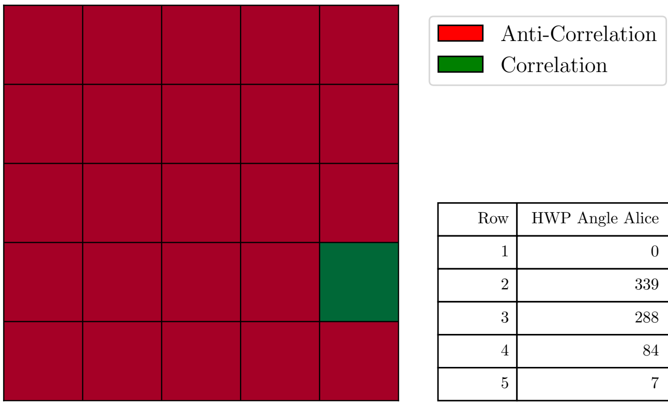
and $A1$ as well as $B0$ and $B1$ have opposite phases. It is also visible that $A0$ and $B1$ or $A1$ and $B0$, respectively are in phase. So, we can conclude that parts in the setup polarise the light because there is already some anti-correlation visible. The deviations in incidence counts most likely not originate from detection errors or lost photons. It can rather be assumed that due to polarisation not the number of photons in each detector but the total number of photons in each measuring setup is constant and not dependent on the basis' angle. This theory should be proven by calculating the visibilities in each measuring setup itself, meaning $A0$ and $A1$ or $B0$ and $B1$ together. The calculation leaves us with

$$v_A = 0.01,\ v_B = 0.04. \tag{5.8}$$

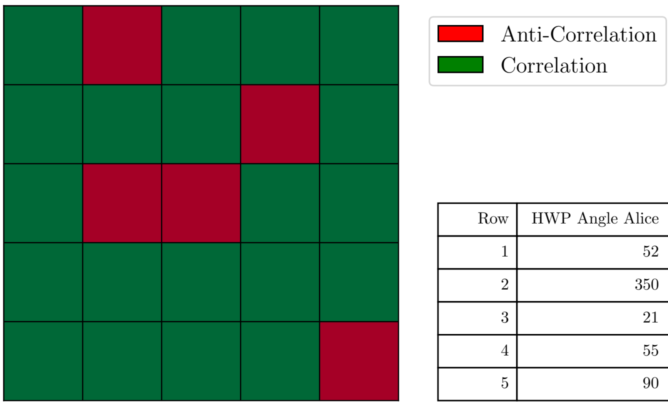
which are both close to zero. Thus, the calculation supports the aforementioned arguments.

## 5.4 Correlation Measurements

Now, the correlation of the photons in the setup should be evaluated. Therefore, three measurements were carried out. 25 bit values for each, Alice and Bob were measured when they set their measuring bases similar or complementary to each other. The results are shown in Figure 5.6. In these plots, a green bit denotes an equal measured bit value while a red bit depicts opposite measurement outcomes. The tables next to the plots show the utilised half-wave plate angles. In general, this measurement agrees with the theory.




| Row | HWP Angle Alice | HWP Angle Bob |
|---|---|---|
| 1 | 0 | 0 |
| 2 | 339 | 339 |
| 3 | 288 | 288 |
| 4 | 84 | 84 |
| 5 | 7 | 7 |




| Row | HWP Angle Alice | HWP Angle Bob |
|---|---|---|
| 1 | 52 | 7 |
| 2 | 350 | 305 |
| 3 | 21 | 336 |
| 4 | 55 | 10 |
| 5 | 90 | 45 |

**Figure 5.6:** Alice's and Bob's bit values were measured in a similar basis (top) and a complementary basis (bottom). For each grid, the basis pairs were used for the measurement of one row. The half-wave plates' angles are shown in the table right to the graphics. The measurements were conducted on 15 March 2024.

For similar bases, we estimate anti-correlation and for complementary bases correlation.

However, we can see one bit error for similar bases and five bit errors for complementary bases.

In addition, the correlation counts were measured and are shown in Figure 5.7. The predicted pattern is evident, the plot includes four periods along the 360° angle difference and the state is anti-correlated. The coincidence counts including $B0$ are in general higher compared to the others including $B1$. This result is in accordance with Figure 5.5 as we can see the same there at $\varphi_B = 0°$.

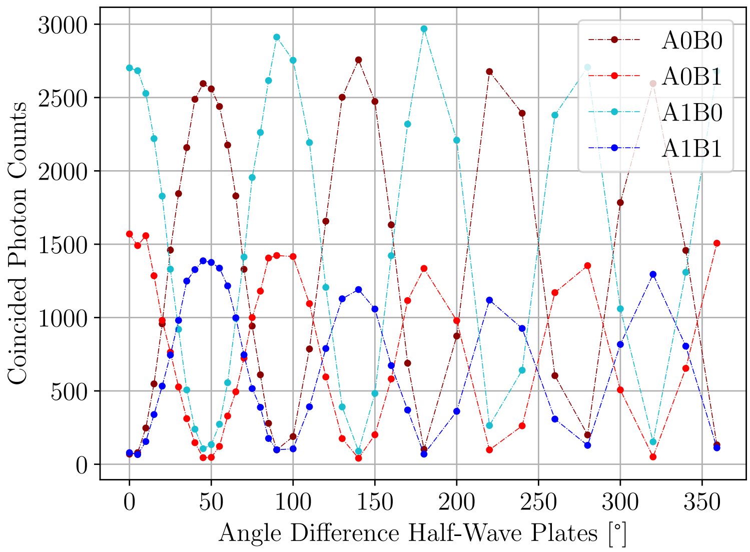



**Figure 5.7:** Correlation counts dependent on the angle difference of Alice's and Bob's half-wave plate. During the measurement, Bob's angle was set to 0° while Alice's angle was adjusted. Again, the connecting lines should just improve the clarity of the plot. The measurement was conducted on 22 March 2024.

Similar to before, we can calculate the visibilities and get

$$v_{A0B0} = 0.95, \; v_{A0B1} = 0.95, \; v_{A1B0} = 0.94, \; v_{A1B1} = 0.91. \tag{5.9}$$

These results are close to the expected value of 1, yet there are some differences. In this case, the counts at the minimum are unequal to zero resulting in differences to the theory.

The source of this systematic error could not be isolated. In Section 3.1, the used hardware has been presented. An experiment has shown the impact of the photon detector's dark current on this result is negligible. In the experiment, one beam was blocked at a time and the coincidence counts were measured. This experiment yielded repetitively zero coincidence counts even though there were some dark counts. Most likely, the combination of imperfect mirrors, errors of the half-wave plate, the beam splitter's extinction ratio and the non-ideally aligned setup cause this error.

## 5.5 The CHSH-Inequality

The central part of the evaluation is to prove the violation of the CHSH inequality 2.16. Therefore, the coincidences were measured at the given bases for maximum violation 2.19. These measurements are further used to calculate the correlation coefficients 2.27. Therefore, two measurements were carried out. The S-parameter was measured right after the alignment and additionally, one week after, same as the measurements of the counts before. The results of the measurements are shown in Table 5.1.

| Day | $C_{0°,11°}$ | $C_{0°,34°}$ | $C_{22°,11°}$ | $C_{22°,34°}$ | S-parameter |
|---|---|---|---|---|---|
| 15 Mar | -0.646 | 0.693 | -0.656 | -0.431 | $\underline{2.43}$ |
| 22 Mar | -0.513 | 0.782 | -0.676 | -0.366 | $\underline{2.34}$ |

**Table 5.1:** Correlation coefficients and resulting S-parameter of the two measurements. They were carried out right after the alignment of the setup and one week after the alignment. The given angles stand for the half-wave plate angles of Alice and Bob. The bases' angles are two times the mentioned angles.

We can see that all values except for $C_{22°,34°}$ are close to the expected $\pm\frac{1}{\sqrt{2}}$. This is most likely because it is the measurement where both angles are the furthest away from 0° which was the angle at which the setup was aligned. There are already some minor differences between the values resulting in an S-parameter difference of $\Delta S = 0.09$. Nonetheless, both results violate the CHSH inequality.

### Corrections

Despite already proving the violation of the CHSH inequality, the implementation of two correction schemes using the results from the incidence and coincidence counts is intended to align the results more closely with the values expected by theory. As previously shown, the single photon counts depend on the half-wave plate's angle and the number of coincidence counts is correlated to the number of incidence counts. Therefore, it seems natural to normalise the number of coincidence counts by the number of incidence counts at the given half-wave plate angle. The incidence counts exhibit a sinusoidal behaviour. So, we can fit a sine with an offset like

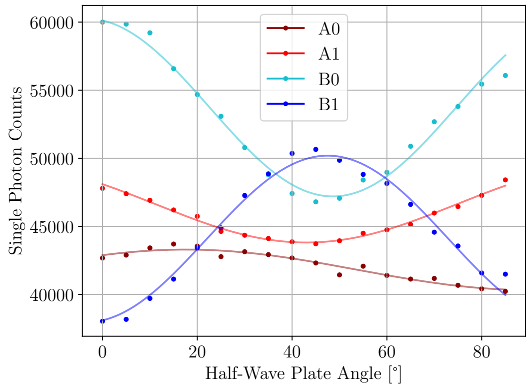
$$N(\varphi) = a \cdot \sin(b \cdot (\varphi - c)) + d \tag{5.10}$$

to the curves in the meaningful neighbourhood, i.e. from 0° to 90°, to interpolate the measurements. In the function, $N$ is the number of counts, $\varphi$ is the set angle and $a$, $b$, $c$

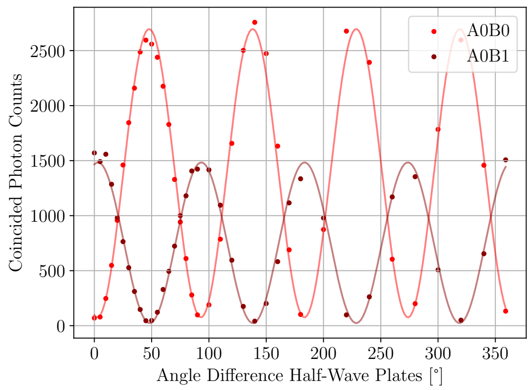
and $d$ are the fit parameters. Then, the counts $N_{\pm,\pm}$ are corrected according to

$$N'_{\pm\pm} = \frac{N_{\pm\pm}}{N_{\pm}(\varphi_a) \cdot N_{\pm}(\varphi_b)}. \tag{5.11}$$

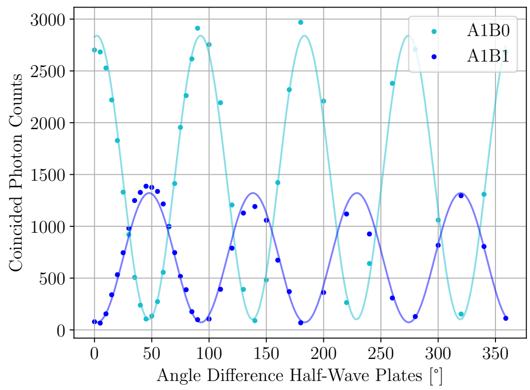
In this context, the indices + and − stand for the measured bit values 0 and 1. We have four different fit functions.




**(a)** Fit of single photon counts




**(b)** Fit of coincidence counts




**(c)** Fit of coincidence counts

**Figure 5.8:** Fits for the single photon and coincidence counts. The numerical data from these fits is further used for error correction.

Another correction that can be applied is the subtraction of the background in the measurements. As shown before, the visibilities of the coincidences are not equal to 1 as suggested by the theory. However, the cause of the difference between theory and reality could not be identified. For this second correction, it is assumed that the imperfect visibilities are caused by some background counts in the measurement which can be eliminated by fitting a similar sine to the correlation measurement. As discussed in Section 5.4, this background might originate from various errors of the equipment. For the fit, if the visibilities were equal to 1, one would arrive at $|a| = d$. Any result with $|a| > d$ would not make sense as counts cannot be negative. In contrast to the first proposed correction, for the background, the full measurement was fitted as all measurements should be in theory on the same curve. Thus, all can contribute to the fit. The fits are shown in Figure 5.8.

With the introduced schemes, three different corrections can be applied. Normalising the data by the single photon counts, subtracting the underground measurement and finally the combination of both. The results are shown in Table 5.2.

| Method | $C_{0°,11°}$ | $C_{0°,34°}$ | $C_{22°,11°}$ | $C_{22°,34°}$ | S-parameter |
|---|---|---|---|---|---|
| Uncorrected | -0.513 | 0.782 | -0.676 | -0.366 | 2.34 |
| Normalisation | -0.545 | 0.778 | -0.702 | -0.367 | 2.39 |
| Underground | -0.553 | 0.821 | -0.729 | -0.393 | 2.50 |
| Combination | -0.585 | 0.815 | -0.755 | -0.395 | 2.55 |

**Table 5.2:** Correlation coefficients and resulting S-parameter with different correction schemes. The coincidence counts were normalised by the single photon counts, the underground was subtracted and both methods were combined. The given angles stand for the half-wave plate angles of Alice and Bob.

In this table, it is visible, that all corrections could improve the S-parameter, i.e. that it is closer to its theoretical value $2\sqrt{2}$. Nonetheless, these results have to be interpreted with caution. In theory, each correlation coefficient should be equal to $\frac{1}{\sqrt{2}} = 0.707$. Here, in particular, $C_{0°,34°}$ is already in the initial measurement larger than the expected value. While the correction with the normalisation could lower it closer to $\frac{1}{\sqrt{2}}$, each method including a subtraction of the background increased it further. This pattern continues for all other values too. The normalisation brought every correlation coefficient closer to the theoretical value. On the other hand, when the subtraction of the background was included, the values just increased, even beyond the expectation.

In summary, the correction of the S-parameter with normalisation can be in this case approved as a reasonable method. However, its impact is only small. Contrarily, subtracting the background has a much larger impact on the S-parameter. Yet, in this one example, we could see some deviations from the theory as the correlation coefficients exceeded the theoretical value through the application of the scheme. Therefore, the initial assumption which motivated this scheme might be incorrect. This example showed that the imperfect visibilities of the coincidences are not primarily caused by background. The evaluation of the correctness needs further examination. For now, its incorrectness can be assumed.

**Error of the S-Parameter**

As a last step for the calculation of the S-parameter, the significance of the violation of the CHSH inequality should be calculated. As previously motivated, we estimate the statistical error of each measurement at $\delta \equiv \frac{\Delta N}{N} = 5\,\%$. We can calculate the errors of the correlation coefficients using error propagation according to

$$\Delta C_{\vec{a},\vec{b}} = \frac{\sqrt{(1 - C_{\vec{a},\vec{b}})^2 \cdot \left(\Delta N_{++}^2 + \Delta N_{--}^2\right) + (1 + C_{\vec{a},\vec{b}})^2 \cdot \left(\Delta N_{+-}^2 + \Delta N_{-+}^2\right)}}{N_{++} + N_{--} + N_{+-} + N_{-+}}. \tag{5.12}$$

These errors can be added to get the error of $S$

$$\Delta S = \sqrt{\Delta C_{\vec{a},\vec{b}}^2 + \Delta C_{\vec{a}',\vec{b}}^2 + \Delta C_{\vec{a},\vec{b}'}^2 + \Delta C_{\vec{a}',\vec{b}'}^2}. \tag{5.13}$$

This error calculation was performed for the uncorrected measurement from 22 March (see Table 5.1). It leaves us with

$$S = 2.34 \pm 0.03. \tag{5.14}$$

This result proves that the system is non-classical with a significance of more than $11\sigma$ which can be seen as a success.

As discussed before, the relative error $\delta$ is only a rough estimate. However, it is assumed to be the value for all $\Delta N = \delta \cdot N$ in Equation 5.12. Therefore, the factor can be pulled out of the root and $\Delta C_{\vec{a},\vec{b}} \propto \delta$. This holds for all $\Delta C$ in Equation 5.13 and thus $\Delta S \propto \delta$. So, even with an estimated error $\delta = 11\,\%$ which was the largest in the error calculation (see Equation 5.6), the non-classicality would be shown with a significance of more than $5\sigma$.

For the correction that includes a normalisation by the single photon counts, the error of the corrected $N'_{\pm\pm}$ can be calculated by

$$\Delta N'_{\pm\pm} = N'_{\pm\pm} \cdot \sqrt{\left(\frac{\Delta N_{\pm\pm}}{N_{\pm\pm}}\right)^2 + \left(\frac{\Delta N_{\pm}(\varphi_a)}{N_{\pm}(\varphi_a)}\right)^2 + \left(\frac{\Delta N_{\pm}(\varphi_b)}{N_{\pm}(\varphi_b)}\right)^2}. \tag{5.15}$$

To determine $\Delta N'_{\pm\pm}$, the relative error of the single counts is estimated similar to the one for the correlated counts before to $5\,\%$. This estimation yields a result of $\Delta N'_{\pm\pm} = N'_{\pm\pm} \cdot 0.05\sqrt{3}$. With this value and Equations 5.12 and 5.13, the error of the corrected S-parameter $S'$ can be calculated to

$$S' = 2.39 \pm 0.06. \tag{5.16}$$

Its error is larger than the one of the initial uncorrected $S$. It shows that the correction yields only an insignificant improvement.

## 5.6 Cryptography

Finally, it is shown how it is possible to run the Ekert91 protocol with the app. Screenshots from the app describe the process. Firstly, Alice and Bob measure their bits simultaneously. They do not have any information about the other's bit or basis value. Once they have measured a full grid of 25 bits, they share their bases and the app marks all bits for which they used different bases in red (see Figure 5.9).

After that, they accept to only keep the valid bits and all others are used to calculate the S-parameter as described in the theory. When they have measured 25 bits in the same basis, they could save the key and move on. Now, they are ready to use the generated key to send a secure message to each other (see Figure 5.10). The encryption worked well. Even though there is one bit error, the messages are still readable. The appearance of this error is in accordance with the results from Figure 5.6.

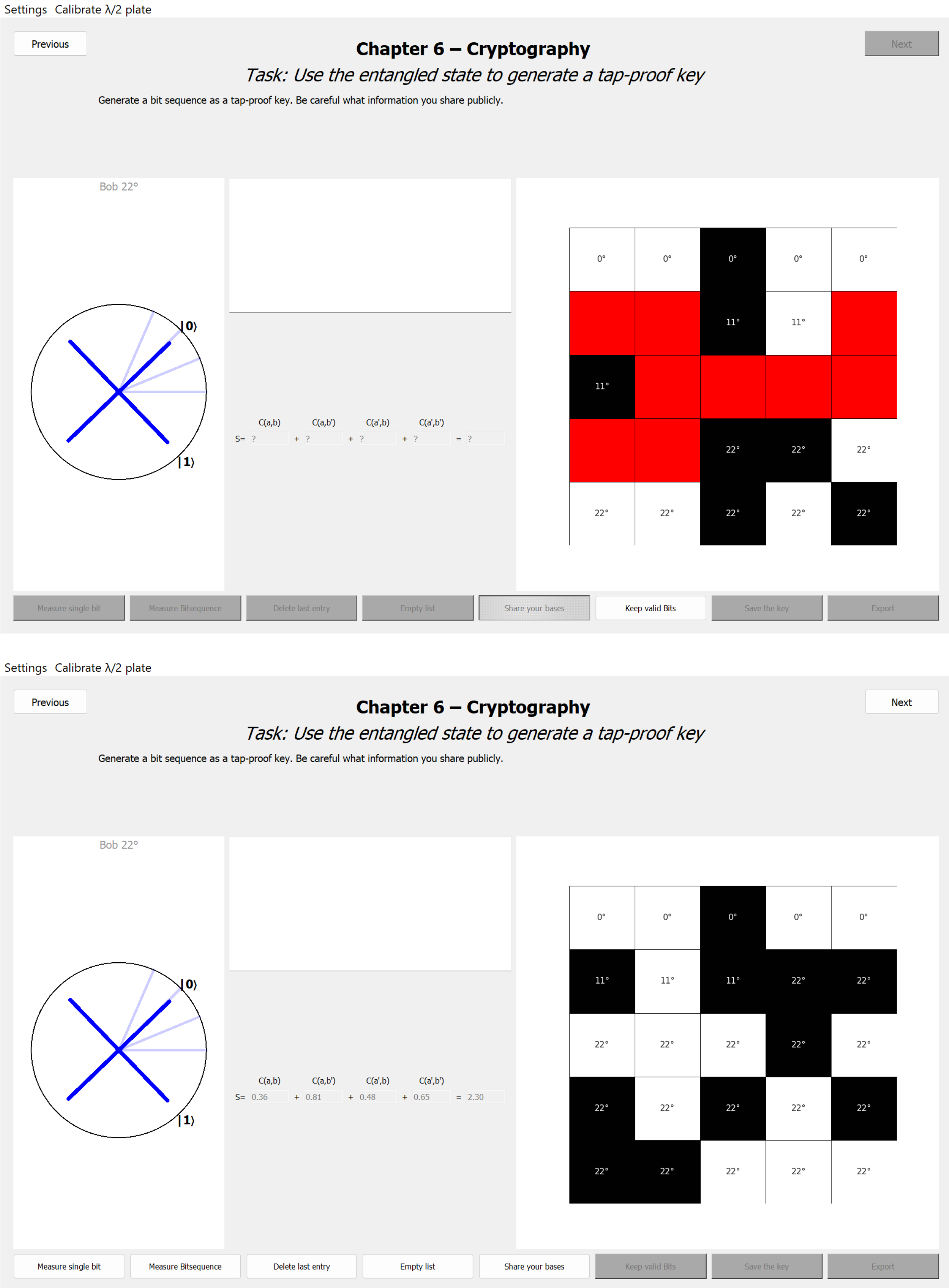



**Figure 5.9:** Bob's Key generation is shown. On top, Alice and Bob only have shared their bases, so the bits for which they used different bases are marked in red. These measurements are now used for calculating the S-parameter. The result is shown at the bottom.

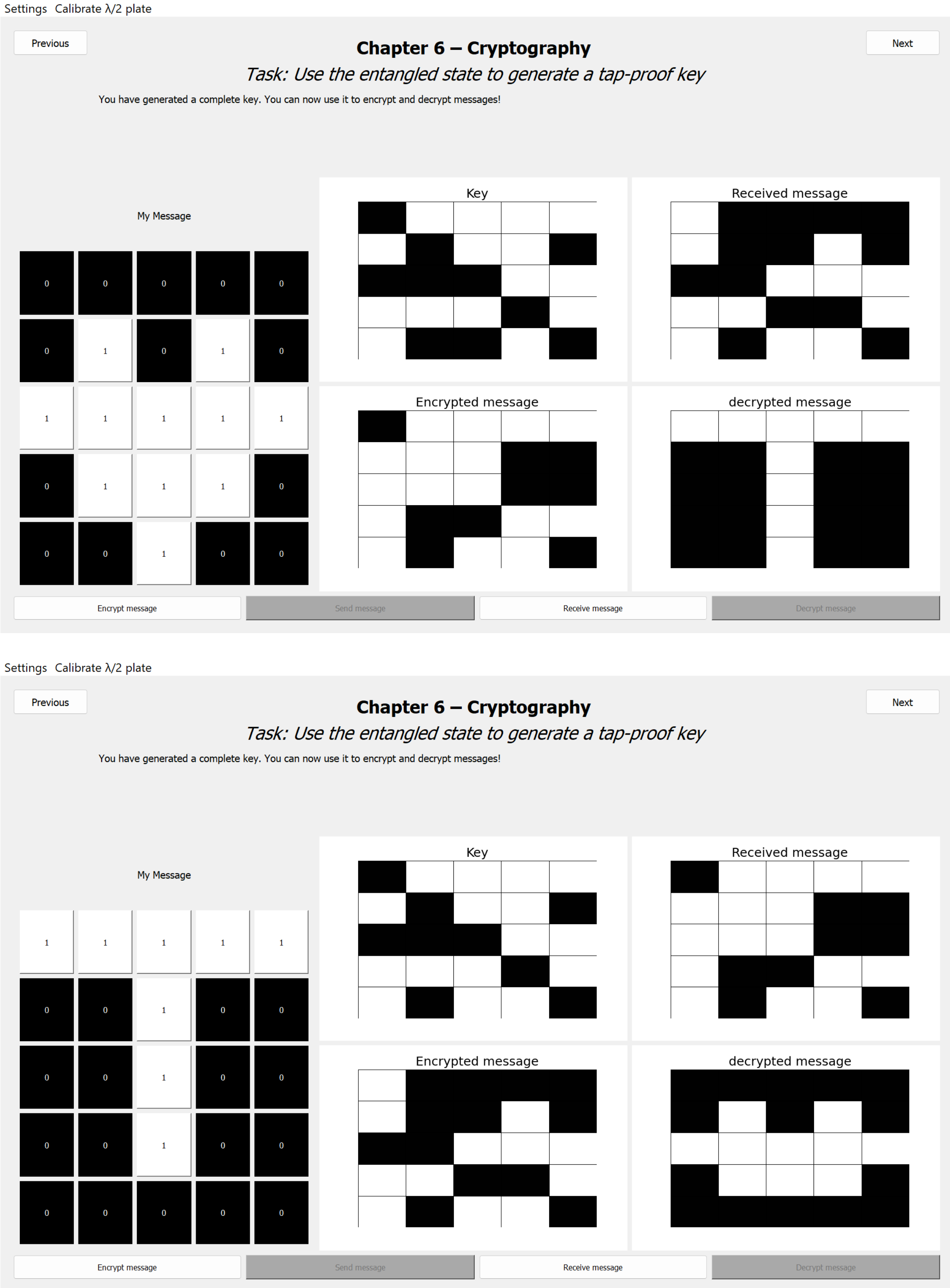



**Figure 5.10:** After they have generated a key as shown above in Figure 5.9, Alice and Bob can exchange their messages. They generate a message with the bit grid on the left side of the screen, afterwards, they can encrypt the message and send it. Once they have received the message, they can decrypt it similarly. On top, Alice's screen is shown, at the bottom Bob's screen is visible. As visible in the decrypted message, the key contains one bit error. It has to be noted, that the measurements shown in Figure 5.9 do not show the key generation process of the key that was used in this example.

# 6 Conclusion

## 6.1 Summary

In this thesis, an experiment dealing with polarisation-entangled photon pairs and QKD has been presented in detail. The experiment has been developed in the context of the project *MiReQu* and is currently carried out in an MR environment. The project aims to advance and evaluate the possibilities of using MR in hands-on student experiments. As a preparation for a comparison study, an additional non-MR application was built in the context of this thesis in Python with PyQt5. The app runs on tablets and should supplement the current setup. The experiment can be conducted with both systems similarly.

In the experiment, the entangled photon pairs are generated with a BBO-crystal making use of SPDC. Walk-off effects have to be compensated. The data is further measured with a *Time Tagger* and an *Arduino*. The former counts single photons as well as coincidences in different channels. In this context, the coincidence time of $\tau_c = 4000\,\mathrm{ps}$, the maximum time between two events for a coincidence, could be approved. It ensures that nearly all coincidences are counted while minimising incorrect detections. Long-term measurements demonstrated that a short time after alignment, the system stabilises in an alignment state close to the optimum. The statistical error of a coincidence count measurement has been roughly estimated at $5\,\%$.

All measurements that the students carry out, have been performed using the app. These measurements consist of single photon or correlated photon counts, as well as bit values. Even after aligning the setup, we saw inhomogeneous single photon counts and there were some bit errors when measuring correlated single bits. These results show the imperfection of the setup and lead to the conclusion that some parts in the setup polarise light to a small extent. Most importantly, to prove that the system is non-classical, the S-parameter that shows the violation of the CHSH inequality was measured. We could achieve an S-parameter of $S = 2.34 \pm 0.03$ which proves the the violation of the CHSH inequality with a significance of more than 11 $\sigma$. This value could be corrected to $S' = 2.39 \pm 0.06$ by normalisation through the measured single photon counts. Another scheme where the coincidence counts have been corrected by subtracting the coincidences' offsets could not be approved. In the end, the app succeeded in running the Ekert91 protocol for generating a secure key. It provides a comparable interface functionality to extract the influence of the MR environment on learning success.

## 6.2 Outlook

In cooperation with the Department of Psychology of Heidelberg University, it is planned to run a neurophysiological comparison study between the MR version of the experiment and the app as a non-MR version. In the study, the impact of the setup on brain activity should be evaluated. It is intended that one group of students uses the app for the first half of the experiment, i.e. all parts until they complete the measurement of the S-parameter, and the MR version for the final chapters. Another group runs the experiment the other way around. A questionnaire about the physics of the experiment has been created. It is planned for the students to complete the questionnaire before and after conducting the experiment. This way, the learning outcomes should be analysed and compared between the MR and the non-MR version. Additionally, the enjoyment and students' opinions of the setups should be self-assessed by the participants. Brain activity is measured using devices from the Department of Psychology.

Further measurements on the setup could evaluate the effect of temperature and vibrations in the room on the system's alignment. Moreover, the systematical errors of the optical components could be investigated individually to identify the errors' causes.

In addition, the evaluation of the measured data in this thesis showed that the S-parameter could be corrected by a normalisation depending on the measured single photon counts. The application of this scheme showed improvements that were in accordance with the theory and it can be included in the future.

# References


[1] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978, ISSN: 0001-0782. DOI: 10.1145/359340.359342. [Online]. Available: https://doi.org/10.1145/359340.359342.

[2] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring", en, in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA: IEEE Comput. Soc. Press, 1994, pp. 124–134, ISBN: 978-0-8186-6580-6. DOI: 10.1109/SFCS.1994.365700. [Online]. Available: http://ieeexplore.ieee.org/document/365700/ (visited on 04/02/2024).

[3] R. Renner and R. Wolf, "Quantum Advantage in Cryptography", en, *AIAA Journal*, vol. 61, no. 5, pp. 1895–1910, May 2023, ISSN: 0001-1452, 1533-385X. DOI: 10.2514/1.J062267. [Online]. Available: https://arc.aiaa.org/doi/10.2514/1.J062267 (visited on 03/13/2024).

[4] Fraunhofer Institut für Angewandte Optik und Feinmechanik IOF. "QuNet Initiative". (Mar. 13, 2024), [Online]. Available: https://qunet-initiative.de/.

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

[6] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states", *Phys. Rev. Lett.*, vol. 96, p. 070 502, 7 2006. DOI: 10.1103/PhysRevLett.96.070502. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.96.070502.

[7] W. Li, L. Zhang, H. Tan, *et al.*, "High-rate quantum key distribution exceeding 110 Mb s–1", *Nature Photonics*, vol. 17, no. 5, pp. 416–421, 2023, ISSN: 1749-4893. DOI: 10.1038/s41566-023-01166-4. [Online]. Available: https://doi.org/10.1038/s41566-023-01166-4.

[8] M. Bartelmann, B. Feuerbacher, T. Krüger, D. Lüst, A. Rebhan, and A. Wipf, *Theoretische Physik 3 — Quantenmechanik*. Jan. 2018, ISBN: 978-3-662-56071-6. DOI: 10.1007/978-3-662-56072-3.

[9] C. Cohen-Tannoudji, B. Diu, and F. Laloë, *Band 1*. Berlin, Boston: De Gruyter, 2019, ISBN: 9783110638738. DOI: doi:10.1515/9783110638738. [Online]. Available: https://doi.org/10.1515/9783110638738.

[10] S. Heusler. "MiReQu". (Mar. 12, 2024), [Online]. Available: https://www.mirequ.de/index.php.

[11] S. Heusler. “MiReQu Technische Beschreibung Aufbau”. (Mar. 19, 2024), [Online]. Available: https://www.mirequ.de/files/doku/technische-beschreibung_aufbau.pdf.

[12] S. Heusler. “AR-Versuch „Quantenschlüsselaustausch“ – Didaktischer Kommentar & Übersicht zu den Versuchsteilen”. (Mar. 19, 2024), [Online]. Available: https://www.mirequ.de/files/doku/versuchskonzept.pdf.

[13] A. K. Ekert, “Quantum cryptography based on bell's theorem”, *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, Aug. 5, 1991, ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.67.661. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.67.661 (visited on 02/26/2024).

[14] R. Wolf, *Quantum Key Distribution: An Introduction with Exercises* (Lecture Notes in Physics). Cham: Springer International Publishing, 2021, vol. 988, ISBN: 978-3-030-73990-4. DOI: 10.1007/978-3-030-73991-1. [Online]. Available: https://link.springer.com/10.1007/978-3-030-73991-1 (visited on 02/26/2024).

[15] W. Scherer, *Mathematics of Quantum Computing: An Introduction*. Cham: Springer International Publishing, 2019, ISBN: 978-3-030-12357-4. DOI: 10.1007/978-3-030-12358-1. [Online]. Available: http://link.springer.com/10.1007/978-3-030-12358-1 (visited on 02/26/2024).

[16] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned”, en, *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982, ISSN: 0028-0836, 1476-4687. DOI: 10.1038/299802a0. [Online]. Available: https://www.nature.com/articles/299802a0 (visited on 02/27/2024).

[17] A. Einstein, B. Podolsky, and N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?”, *Physical Review*, vol. 47, no. 10, pp. 777–780, May 15, 1935, ISSN: 0031-899X. DOI: 10.1103/PhysRev.47.777. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRev.47.777 (visited on 02/26/2024).

[18] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed Experiment to Test Local Hidden-Variable Theories”, en, *Physical Review Letters*, vol. 23, no. 15, pp. 880–884, Oct. 1969, ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.23.880. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.23.880 (visited on 03/06/2024).

[19] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014, Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84, ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2014.05.025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0304397514004241.

[20] P. Schlummer, A. Abazi, R. Borkamp, *et al.*, "Seeing the unseen—enhancing and evaluating undergraduate polarization experiments with interactive Mixed-Reality technology", en, *European Journal of Physics*, vol. 44, no. 6, p. 065 701, Nov. 2023, ISSN: 0143-0807, 1361-6404. DOI: 10.1088/1361-6404/acf0a7. [Online]. Available: https://iopscience.iop.org/article/10.1088/1361-6404/acf0a7 (visited on 03/06/2024).

[21] Coherent. "SureLock: LM Series Compact Single Frequency Laser Modules Datasheet ". (Apr. 4, 2024), [Online]. Available: https://www.coherent.com/content/dam/coherent/site/en/resources/datasheet/lasers/COHR_SureLock_LMseries_0520_7.pdf.

[22] ThorLabs. "Protected Gold Mirrors". (Apr. 4, 2024), [Online]. Available: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=744.

[23] Newlight Photonics. "BBO SPDC Crystals". (Apr. 4, 2024), [Online]. Available: https://www.newlightphotonics.com/SPDC-Components/BBO-SPDC-Crystals.

[24] ThorLabs. "Mounted Zero-Order Half-Wave Plates". (Apr. 4, 2024), [Online]. Available: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=711&pn=WPH05M-808.

[25] ThorLabs. "Broadband Polarizing Beamsplitter Cubes". (Apr. 4, 2024), [Online]. Available: https://www.thorlabs.de/newgrouppage9.cfm?objectgroup_id=739&pn=PBS102.

[26] Laser Components. "Single Photon COunting MOdule COUNT NIR Series". (Apr. 4, 2024), [Online]. Available: https://www.lasercomponents.com/de/?embedded=1&file=fileadmin/user_upload/home/Datasheets/lc-photon-counter/count-nir.pdf&no_cache=1.

[27] ThorLabs. "FiberPort Collimators / Couplers". (Apr. 4, 2024), [Online]. Available: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=2940&pn=PAF2P-15B.

[28] M. Oberparleiter, "Effiziente Erzeugung verschränkter Photonenpaare", Ph.D. dissertation, Aug. 2002. [Online]. Available: https://edoc.ub.uni-muenchen.de/350/1/Oberparleiter_Markus.pdf.

[29] Y. Nazirizadeh, "Compact source for polarization entangled photon pairs", [Online]. Available: https://xqp.physik.uni-muenchen.de/publications/files/theses_diplom/diplom_nazirizadeh.pdf.

[30] Swabian Instruments. "Time Tagger 20 manual". (Mar. 19, 2024), [Online]. Available: https://www.swabianinstruments.com/static/documentation/TimeTagger/api/VirtualChannels.html#coincidence.

[31] Arduino. "Arduino Micro documentation". (Apr. 4, 2024), [Online]. Available: https://docs.arduino.cc/hardware/micro/.

[32] The Qt Company Ltd. “Signals & Slots”. (Mar. 26, 2024), [Online]. Available: https://doc.qt.io/qtforpython-6/overviews/signalsandslots.html.

# List of Figures



# List of Tables

## Acknowledgements

First of all, I would like to express my sincere gratitude to Prof. Dr. Wolfram Pernice for the opportunity to work as a bachelor student in his research group and for providing tablets on which the application for the student experiment now runs.

Special thanks goes to Julius Römer and Philipp Schultzen for supervising my work and sharing their knowledge and experience with me. Thank you for introducing me to the experiment in the first place, helping me out with coding issues, aligning the setup and finally giving your feedback on this thesis.

I would like to extend my sincere thanks to Prof. Dr. Lauriane Chomaz for being the second examiner for this thesis. I would also like to thank Dr. Constanze Schmitt who keeps contact with the Department of Psychology and thus prepares the study that has motivated this work. Lastly, I am grateful to everyone from the Neuromorphic Quantumphotonics group for welcoming me in the group and giving me insights into their research.

## Erklärung

Ich versichere, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.
Heidelberg, den 08.04.2024,

Tobias Ludwig Rieger