universität wien

# MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Quantum key distribution against extreme noise effect using high dimensional entanglement with MUB“


verfasst von / submitted by

Thomas Unglaub BSc


angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Science (MSc)

Wien, 2023 / Vienna, 2023

| | |
|---|---|
| Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet: | UA 066 876 |
| Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet: | Masterstudium Physics |
| Betreut von / Supervisor: | Mag. Dr. Marcus Huber, Privatdoz. |

# 1 Acknowledgements

A huge thank you goes to Mateus Araújo and Flavien Hirsch! Without their help, their patience, kindness, cleverness and more positive characteristics, I would not have done this thesis. No words, written or oral could represent how much I am thankful to have both of them as my supervisors and I hope I did not stress their patience too much.
Another huge thanks goes to Marcus Huber the group leader. Even if he was very busy quite a few times, he tried to support me. He also had the best ideas for some proofs.
In this context, I also want to give a huge thanks to Anna Novak and Sarah Grüner. Even if they were busy they did read through my thesis and corrected most spelling and grammar mistakes.
And also a thanks goes to my friends who already did motivate me to finish this thesis.

## 2 Abstract

There are thousands of published papers dealing with QKD protocols and how to extend the distance of a quantum channel in order to use it for quantum communication. In the high number of published papers, one can see how this topic is getting more relevant to society, even now when quantum communication is still at its beginning stage. One paper introducing a new approach to quantum key distribution and how to overcome large distances was published by Mirdit Doda Doda et al. "Quantum Key Distribution Overcoming Extreme Noise: Simultaneous Subspace Coding Using High-Dimensional Entanglement" [1]. During his research, he used high dimensional entanglement to create subspaces where Alice and Bob could prepare, send and measure quantum states. In this master thesis, Doda's results will be recapitulated and a deeper understanding of why his protocol works will be given. Secondly and most importantly, a focus will be laid on improving the QKD protocol. Two methods came up which could be applied to the theoretical construct of the high dimensional entanglement protocol. First, the well-known self-test scenario will be undertaken. In contrast to Mirdit Doda's paper, it will be shown that the self-test scenario does not improve the QKD protocol. Therefore, a mutually unbiased basis will be utilised for the measurement which has demonstrated an improvement of the QKD protocol against extreme noise.

Es gibt tausende von publizierten wissenschaftlichen Arbeiten die sich mit QKD Protokolle beschäftigen und wie man im Zusammenhang mit der Verwendung von Quanten Kommunikation die Entfernung von Quantenkanälen erweitert. Anhand dieser Unzahl an veröffentlichten Arbeiten kann man sehen, wie dieser Themenbereich mehr und mehr an Relevanz in unserem Alltag gewinnt. Dabei steht dieses, noch relativ junge Themenbereich, erst an den Anfängen. Eine wissenschaftliche Arbeit welches einen neuen Weg von Quantenschlüsselaustausch geht und wie man große Entfernungen überbrücken kann wurde von Mirdit Doda et al in seiner Arbeit "Quantum Key Distribution Overcoming Extreme Noise: Simultaneous Subspace Coding Using High-Dimensional Entanglement" [1] eröffentlicht. In seiner Arbeit verwendet er höher dimensionale Verschränkung um Unterräume zu schaffen in welche Alice und Bob einen Quantenzustand bearbeiten, senden und messen können. In dieser Masterarbeit werden die Ergebnisse von dem Paper von Mirdit Doda et al. [1] rekapituliert und ein tieferes Verständnis warum dieses Protokoll funktioniert wird gegeben. Zum zweiten und der Hauptteil dieser Masterarbeit, eine Verbesserung des QKD Protokolls wird vorgestellt und mathematisch hergeleitet. Dabei werden zwei Methoden für das theoretische Konstrukt des QKD Protokolls verwendet. Zuerst das sehr bekannte 'self-test scenario'. Im Gegensatz zu Mirdit Dodas et al. Arbeit führt diese Methode jedoch zu einer Verschlechterung des Protokolls. Deswegen werden 'mutual unbiased bases' als Messungen eingeführt, welches eine Verbesserung des Protokolls mit extremen Quantenrauschen zeigt.

# Contents

# 1 Introduction

There is a pretty broad understanding that communication is just an act of "social affairs". Contrary, communication is more than just some human evolved system that is simplified through human speech and language [2]. The whole evolution of the world is built upon communication and the basics are found in every form of it. We can see it in the entire nature. Communication is based on three parts, namely *communicator-stimulus-receiver* [3]. This includes the symbiosis between mushrooms [4], ants making scent trails in order to send specific information to their colony [5] or wolves communicating with each other via facial expressions [6] and many more. In general, communication is sharing information between two parties which these parties could be any on earth living being. Humans play a special role in the evolution of communication. In the beginning, the communication of humans was based only on sounds. It is not clear how and when humans were able to create and form formants that form our speech. Humans were able to share complex information and socialise which resulted in a higher probability to survive. Since then, speech and languages undergo continuous change over the course of time. Over 5000 years ago, the first humans expressed words with signs that they carved in stone [7]. By doing this, they were able to share information over time and over distances as well as to lay the basis for the development of future societies. Our own evolution distinguished us completely from being an animal. Sharing information often comes with a huge responsibility. History taught us many times that in every piece of communication, there can be someone who uses the shared information to their own benefit. It does not matter if someone communicates with a friend or with our bank via online banking. In the wrong hands, each extracted piece of information can be used by an unwanted third party. Cryptography protocols were invented to overcome this issue. Some famous examples are the Enigma machine in World War II or the Caesar cipher which will be treated in the next chapter. On the other hand, the Enigma machine as a second example teaches us that no matter how complex our cryptography protocol is, even complex protocols are not secure. The question is if there is the possibility to find a completely secure way to share information without the possibility of a third unwanted party hacking or extracting information from an encrypted message.

> *"Any key which is produced by humans, can be hacked by humans."*
>
> *Unkown*

The goal of this thesis is, to introduce a possibility of a secure protocol. For a better understanding, some examples will be given first. These are all more or less related to the protocol which was introduced in the paper of Mirdit Doda (2020) [1] and which will be improved in this thesis.

## 1.1 Classical Cryptography

The word cryptography did expand in the past few decades. Hundreds of years ago cryptography was just the "transmission of secret messages" [8]. Nowadays, communication is not based just on two persons who want to send secret messages. Sharing information includes sending our personal data to a server who can identify you as the right person. In this view, sharing information can also be used wrongly. Mainly all social media platforms use your data to have a better picture of their users. Other platforms even do not hide their will to get information. Some online newspapers ask if someone agrees to send data such that this person can use their website for free. It is hard to use cryptography for this example because the person which uses such websites/social media platforms agrees in a more or less way to work with their personal data. Therefore we only consider the communication part between the two parties.

### 1.1.1 Caesar Cipher

Let us start with a basic concept of cryptography, namely *Caesar Cipher*. Although it is not the oldest form of securing a message, it can nevertheless be seen as a suitable introduction to the topic of this thesis.
Caesar cipher is based on the Roman alphabet and was used to send messages in the form of a letter so that the enemies could not read the text [9]. It contributed to the power of the Roman Empire. The military orders by Caesar could only be read by the commander himself.
Using the Roman alphabet, each letter is assigned to a number

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| S | T | U | V | W | X | Y | Z | | | | | | | | | | |
| 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | | | | | | | | | | |

If person A wants to send a message to person B with Caesar cipher, they just define a number $N$ by which they want to shift their plain text. They find the encrypted letter $E$ of their plain text $M$

$$E(M) = (M + N)(\mathrm{mod}\, 26) \tag{1.1}$$

The modulo *mod* is used here just in case that $M + N > 26$ in order to begin from the letter *'A'* again.
To decipher this message one just have to invert the formula

$$D(C) = (C + (26 - N))(\mathrm{mod}\, 26) \tag{1.2}$$

Here $C$ is dedicated to the numeric version of the cipher text.
Surely, this method is simple and can be easily decrypted by a third party nowadays, however, in Caesar's time, this method was largely secure.
Note, in this chapter the expression of person A and person B as two persons who want

to share information was used. Equivalent, it is common to call both sides *parties* in consideration that in modern cryptography one side has not to be human.

### 1.1.2 One-time-pad

Another example of an encryption technique is *One-time-pad* (OTP). The main concept of shifting letters stays the same as in Caesar's cipher. But in contrast, the key is used which shifts each letter of the plain text with each letter of the cipher text. The key or in other words, the cipher text is as long as the plain text itself which makes this protocol so strong secure. Each symbol of the cipher text is random. For a text which is 56 symbols long one gets a cipher text which is $(26)^{56} \approx 10^{79}$ [9]. Additionally, if one sends a message from a technical device, it uses bytes and bits to send a message and also to encrypt the message. Therefore it differs between lower and upper cases as well as special characters [10]. Based on Shannon's consideration [11] that this protocol is "optimal" which means that "there is no encryption method that requires less key" [12]. Furthermore, if both parties always use different, random keys this method should be safe in principle.
It is possible to claim that OTP is secure, so what is the issue with this concept? The problem lies in the cryptographic key. Person A uses this key, but person B needs to decipher the decrypted text. In the classical world, it can be easy for a third party to get this key and decipher the decrypted text. Therefore, a protocol is needed in which one can use OTP encryption with sending the key in a secure way, but this seems impossible in the classical context.

## 1.2 Quantum cryptography

The life of many scientists would be much easier if they could find a simple *'yes'* or *'no'* answer to the question if there is a way to find a cryptography protocol which gives 100% security for every sent message. The most promising way for secure communication lies in the physics of quantum mechanics. Phenomena of a world which are not describable by classical, already-known physics were detected in the end of the 19th century, but it took a few years until a valid theory was formed. A milestone was Schrödinger's equation which tries to show the evolution of a state with quantification operators that correspond to energy, momentum and position.
Since, the theory of quantum mechanics was formed and experimentalists tried to prove some logical consequences out of this theory. But until this day, quantum physics could not be disproved. On the contrary, each prediction which follows from the theory could be proven to be right, even if someone does not understand why. This theory is the foundation of quantum cryptography and very soon, first ideas came up to share secure information between two parties using photons which were prepared in a quantum state. Even if the initial intention behind the experiment was to find a way of securing banknotes in order to make them impossible to counterfeit [13]. Charles Bennet and Gilles Brassard invented the first quantum cryptography protocol [14]. Soon, other protocols came up

which used entanglement [15], the Decoy state protocol [16], the six state protocol [17] and many more.
The purpose of this master thesis is to introduce the concept of a new protocol which uses high dimensional entanglement. In fact, high dimensionality is already well-known in quantum physics. Nowadays, it is already possible to create high dimensional quantum states and also high dimensional entanglement but in experiments, it was only possible to achieve dimension in high one-digit, lower two-digit areas. Nevertheless, a protocol has been examined which was published by Mirdit Doda [1]. This protocol will be discussed later and a better understanding will be given, of why and how this protocol works. In the last and main step, this protocol will be improved by using special measurements.

# 2 Quantum communication

Before diving into high dimensionality and its complexity with quantum cryptography, a short introduction to the quantum physical world and especially in quantum communication will be given. Of course, both topics are huge fields on their own, but especially for readers who are not yet familiar with these topics, it may be beneficial to give a brief overview of the mentioned topics.

## 2.1 Two party system

The simplest form in communication in general is to consider two parties which want to share information. The convention in information theory is to name one party *Alice* and the other one *Bob*. In normal conditions, both parties possess modern technological standards and all resources which they will need. In this classical frame, Alice can send a message translated into a bit string consisting of 0 and 1 to Bob. He is able to decode the binary code into a message. In this little world, a third party (commonly named *Eve*) can interrupt this communication and try to get information about the message out of this channel without being noticed by the two other parties. In the classical world, Eve can put herself in the middle. She can receive a message from one party, copy it and send it to the other party. To prevent Eve from being able to read the message, thousands of cryptography protocols did show up such as the OTP from chapter 1.1.2. Nevertheless, Eve also has all the possibilities in her power to hack the code and there would be infinite ways for her to extract information out of this channel without being noticed. In the case of OTP, Eve can just get the key with which Alice encrypted her message. Nowadays, the problem of unwanted listeners is growing. Zoom calls can be hacked and emails can be stolen. For a third party, it is just a matter of time and patience to get access to information.
However, let's move back to the aforementioned two-party system. As one sees later, it is necessary to establish a way of using quantum physics for secure communication. In this huge topic of quantum information and quantum cryptography, *Quantum key distribution* (QKD) is one of the main topics. Most people (even physicists) use QKD as a synonym for Quantum cryptography, but clearly, this is not accurate. Quantum cryptography "comprises all possible tasks related to secrecy that are implemented with the help of quantum physics" [12]. Whereas QKD summarises all secure communication methods. For the realisation of a QKD, protocols are used which give strict guidelines on how to implement quantum communication between different parties. Each protocol should be consistent in itself and feasible. Secure in this context means, even if Eve has all possible resources (including a working quantum computer), it is impossible for her to interrupt a

quantum channel without being noticed.
QKD protocols and their impossibility to be hacked were mentioned before, so one might ask why these protocols are not used already.
Well, QKD always underlies the law of quantum physics. Therefore, in the paper of Gising et al. [18] five statements were formulated in regard to give a theoretical frame of quantum physics and quantum information. Only three of them will be important for this thesis.

*"1. Every measurement perturbs the system."*

Information has a strong dependence on measurement. Further, without measurement, there would be no information in the classical World. Similarly, to get information out of a quantum state (it does not matter if this state was prepared with information or not), someone has to measure it [8]. But each time information is extracted from the state by measuring it, it will change the state itself or in the worst case, the state get lost. In chapter 4.2 it will be discussed how a measurement acts on a state. Therefore only limited information can be extracted from the state. What sounds disappointing at first glance, is a strong law for quantum communication. If Alice prepares a quantum state, Eve only has the possibility to get information by measuring the state and sending the changed state to Bob. If he is measuring the state and compares his results with Alice in the end, they would get many errors in their key. Both can conclude that someone was listening and they can discard the channel.

*"2. One cannot determine simultaneously the position and the momentum of a particle with arbitrary high accuracy."*

This short statement is just another expression of the fundamental uncertainty principle which was introduced by Werner Heisenberg in 1927 [8] and was once a milestone in physics. If one has a state and wants to know its position and momentum, someone can only measure one variable with high accuracy. By measuring one observable variable, the other one has an uncertainty.

$$\Delta p \Delta x \geq \frac{\hbar}{2} \tag{2.1}$$

Even if $\Delta x$ is measured for example, $\Delta p$ has the uncertainty of $\Delta p \geq \frac{\hbar}{2\Delta x}$. Therefore, a quantum state follows just the principle of a statistical function where the truth lies somewhere in between a deviation. In fact, this is the nature of quantum physics and makes it so interesting.
An example can be given by an explicit QKD experiment in which the polarisation of a photon is used to produce a quantum state. Out of the statement above it follows, that it is not possible to "measure the polarisation of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis" [18]. If Alice prepares the information with the polarisation, Bob has only the chance to measure the state once. If the state was prepared from Alice in a different basis as Bob measures, he is only able to predict how

the quantum state was prepared or in other words, which polarisation the photon did have.

*"3. One cannot duplicate an unknown quantum state."*

One can now say, Eve can duplicate the state, measure one state and send the other one to Bob. Here is a second strong law which makes quantum communication so secure and interesting. The theory teaches us that there is not a function which can clone an arbitrary state [19]. It is only possible to clone a state which is orthogonal to the original state. The No-Cloning is just an extended thought of Heisenberg's uncertainty principle. The cloning of a quantum state would mean that it would be possible to measure two observables of a quantum state which is a contradiction. Experiments show that by trying to copy a state, one will always get false 'cloned' states. Proof of this issue will not be given here, however, if in need of further information, one can have a look at [18] or any other basic quantum physics book.
It would be impossible for Eve to clone a state and therefore, she has to use the original state to extract some information.

These 3 statements do not cover the whole quantum physics in general, however, they are nevertheless important in regards to understanding why quantum communication and such quantum communication protocols as it will be discussed in this thesis, works. So far, one can say that the main issue lies not only in the technological part. Each of these statements is relevant to QKD protocols. In the following chapters, each one of these statements will be discussed further and in more detail. A well-experienced reader might get a clue why quantum communication is so hard to realise. The following chapters are focused on the question, of why quantum communication is not available yet.

# 3 Issues in Quantum communication

Why is quantum communication so hard to realise? Which problems are someone faced with? The solutions to these questions cover whole books and constitute a topic in itself. In the following, only a short overview of this topic will be given.
Similar to classical communication, Alice prepares information and sends it through a channel to Bob. Here, neither the hardware of the system nor the technological part will be discussed in too much detail, since - as already discussed - the hard part already lies in the nature of quantum physics itself.

## 3.1 Resources

The smallest units in classical computer language are bits [20], basically $0, 1$. Depending on the order of these two numbers in a predefined string, it is possible for a computer to translate this string into letters, numbers and symbols. In contrast, in quantum information quantum physicist works with qubits. For a two-dimensional system, for example, a qubit is a superposition of $|0\rangle$ and $|1\rangle$. In other words, superposition means a linear combination of $|0\rangle$ and $|1\rangle$. This state can grow for higher dimensions.

### 3.1.1 Error Correction

In classical channels, errors will be made due to the nature of physics. These errors lead mostly to a bit flip. In fact, there is always a probability $p$ that the bit (or qubit) flips and $1 - p$ that there is no bit-flip error. Besides the fact that classical computers are fairly reliable and the failure rate is less than one error in $10^{17}$ operations, there are a couple of error corrections which can be done. The easiest way is to just clone the bit string which will be sent to the other party. Through two independent channels, both strings can be sent and compared. Another method is to redefine the bits. A small bit string is therefore referred to as a logical bit which is also known as *majority voting* [8].

$$0 \to 000$$
$$1 \to 111$$

If one bit is flipped, it is possible to conclude which bit was meant anyways. Clearly, this method fails if two or more bits flip, however, due to the small error rate, this can be neglected. The probability of a possible error minimises to $p_e = 3p^2 - 2p^3$.
As already mentioned, error correction plays also an important role in quantum communication. There is a whole theory behind the concept of quantum error correction. For further reading, the book of Nielsen and Chuang is highly recommended [8].

# 4 Basic Quantum Physics

It is hard to compromise a whole new mathematics in just a few pages, therefore, some fundamental quantum physical concepts which are necessary for the understanding of the research will be introduced.

## 4.1 Quantum State

Giving a precise definition of a state would lead to a huge discussion. In regards to quantum physics, this cannot be easily done.
If a system of particles in a liquid is considered in the classical world, these particles underlie the law of motion [21, 22]. If there was a force which moves the system, someone could calculate their momentum by determinism with the equation of motion. On the contrary, the dynamic of a quantum state can be completely described by the Schrödinger equation [21, 23]. It would mean that quantum theory is deterministic. But in the second statement of chapter 2.1 it was already concluded that quantum mechanics has a probabilistic nature. A spin-0 particle which decays in two spin 1/2 particles is completely described as probabilistic in a Stern-Gerlach experiment. Either particle 1 is found up and particle 2 down or vice versa, whereby the probability for each case would be 1/2 [21]. As a matter of fact, the concept of entanglement was introduced at this point. How can such a state can be described now, as probabilistic or deterministic? The disappointing answer is that one has to define it the way someone wants to use a quantum state.
A good definition is given by Nielsen and Chuang in their book *"Quantum Computation and Quantum Information"* [8] as their first postulate of quantum mechanics.

> *"Associated to any isolated physical system is a complex vector space with the inner product (that is, a Hilbert space) known as the state space of the system. The system is completely described by its states vector, which is a unit vector in the system's state space."*

The definition of this state space or the state vector depends on the system in which someone wants to study.
In QKD, and also in this master thesis, a pretty straightforward mathematical concept of the state space is used which is effective for calculations. Of course, this implies some simple assumptions, however, these will not be further elaborated in this thesis.
As already discussed in 3.1, the smallest unit of information in quantum information are qubits. In two-dimensional space they would be $|0\rangle$, $|1\rangle$ which is similar to classical information theory, but in comparison to it, qubits are not bounded by the dimension. In

this master thesis, quantum states are used with dimension $d$. Therefore, it is possible to create $|0\rangle, |1\rangle, ..., |d-1\rangle$ qubits. In this case, a state vector can be built for $d = 2$ by these two qubits $|0\rangle$ and $|1\rangle$ which form an orthonormal basis.

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{4.1}$$

Here, one is working in the Hilbert space, consequently $\alpha, \beta \in \mathbb{C}$. Because $|\Psi\rangle$ is a unit vector, it has to be normalised in such a way that $\langle\Psi|\Psi\rangle = 1$. Therefore, variables have to satisfy $|\alpha|^2 + |\beta|^2 = 1$. Next to entanglement, a second strong tool in quantum mechanics was introduced unintentionally, namely the *superposition*. With the probability $p$ the state is in 0 or 1 with $1 - p$. One can only determine in which one the state really is through measurements. In other words, if the state above 4.1 is used with $\alpha = -\beta = 1/\sqrt{2}$ than $|0\rangle$ has an amplitude of $1/\sqrt{2}$ and $|1\rangle$ an amplitude of $-1/\sqrt{2}$. This means that in the end there is a probability of $1/2$ of getting one of the outcomes 0 or 1.
As mentioned above, the state $|\Psi_i\rangle = \sum_{i=0}^{d-1} c_i\,|i\rangle$ with $\sum_{i=0}^{d-1} |c_i|^2 = 1$ is not a fixed eigenstate. It also underlies the physical concept of time and other factors which evolves with time. This propagation only depends on the space which the state is traveling through or the time in which the state exists. For closed systems, this evolution is described by a unitary transformation $U$ so that someone can find the state after the evolution.

$$|\Psi'\rangle = U\,|\Psi\rangle \tag{4.2}$$

Explicitly, time evolution, for example, can be classified by the Schrödinger equation.

$$i\hbar\frac{\partial}{\partial t}\,|\Psi(t)\rangle = \hat{H}\,|\Psi(t)\rangle \tag{4.3}$$

where $\hat{H}$ is the Hamiltonian operator. This operator corresponds to the total energy of a system. In this case, the Hamiltonian operator in quantum mechanics is described as $\hat{H} = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} + V(x,t)$ for a potential $V(x,t)$.

### 4.1.1 Density Matrix

For mathematical simplification, one works with the *density operator* $\rho$. A density operator fully describes an isolated physical system that operates in the Hilbert space $\mathcal{H}$. For a probability $p_i$, a density operator can be constructed out of a state vector [8].

$$\rho = \sum_i p_i\,|\Psi_i\rangle\,\langle\Psi_i| \tag{4.4}$$

But a quantum state does not only describe an ensemble of quantum states. The set of quantum states follows a strict characterisation of conditions which such an operator has to satisfy.

1. *Trace condition*

$$\mathrm{Tr}(\rho) = 1 \tag{4.5}$$

2. *Positivity condition*

$$\rho \geq 0 \tag{4.6}$$

A sphere can be seen as an example of a geometrical representation of the above introduced density operator. Such a sphere is known as a *Bloch sphere*. On the North- and Southpole $|0\rangle$ and $|1\rangle$ of the qubit can be found for a two-dimensional Hilbert space. On the equator lies the state which is already known as $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ for example. Each state vector in the two-dimensional world can be represented by such a Bloch sphere.
In this simple setting, one can ask: Do all density operators in and on this Bloch sphere satisfy the same condition? Clearly, if this question is asked, the answer is most likely 'no'. If the picture of the Bloch sphere is used, one can also find

- if $\mathrm{Tr}(\rho^2) = 1$ (or $\rho^2 = \rho$) the state is called pure state
- otherwise, if $\mathrm{Tr}(\rho^2) < 1$ (or $\rho^2 \neq \rho$) the state is called mixed state

In the second case, so the mixed state, the state vector does not lie on the surface of the Bloch sphere anymore. It lies somewhere in the Bloch sphere.
Of course, a density matrix underlies the evolution. From 4.2 one can conclude that such an evolution looks like

$$\rho' = U\rho U^\dagger \tag{4.7}$$

For now, it is unclear how such a quantum state looks mathematically or even how it can be realised such a state in experiments. The question of how to implement such a physical state is the topic of many current studies. Nowadays, scientists could achieve the manipulation of qubits by ions with lasers in an ion trap [24], photons or a superconducting circuit (SQUID with a Josephson Junction) [25]. It is even possible to send a quantum state through fiber or air to another party [12]. As will be discussed later, this quantum channel is used to communicate between two parties using quantum states. For now, there will be just a focus on the basic concepts which is needed in order to understand quantum communication.

### 4.1.2 Observable

In quantum physics, a property of a quantum system is described by an *observable* $\mathbf{A}$ [8]. An observable acts on a state

$$\mathbf{A} : |\Psi\rangle \rightarrow \mathbf{A}\,|\Psi\rangle \tag{4.8}$$

In this context, an observable works like an operator which basically maps vectors to vectors [26]. It describes the property of a system with the eigenstate $|\Psi\rangle$ so that the corresponding property is always the eigenvalue $a$.

$$\mathbf{A}\,|\Psi\rangle = a\,|\Psi\rangle \tag{4.9}$$

Later, one will see that there are some useful properties such as its linearity.

$$\mathbf{A}(a\,|\Psi\rangle + b\,|\Psi\rangle) = a\mathbf{A}\,|\Psi\rangle + b\mathbf{A}\,|\Psi\rangle \tag{4.10}$$

An interesting property of quantum mechanical observables is that they can be adjoint

$$\langle\varphi|\mathbf{A}\Psi\rangle = \langle\mathbf{A}^\dagger\varphi|\Psi\rangle \quad \forall\,|\varphi\rangle\,,|\Psi\rangle \in \mathcal{H} \tag{4.11}$$

Therefore **A** is called a *self-adjoint operator*.
Of course, there are more properties of an observable, however, their thematisation would go beyond the scope of this master thesis.

## 4.2 Measurement

Measurements and their impact on a quantum state were mentioned now several times. But what happens to our state after the measurement?
The basic concept of a measurement in quantum physics can be described mathematically. If an observable **A** is measured, then the eigenvalues describe the outcome of a measurement of an observable **A** (see equation 4.9). The state itself is in this case the eigenstate of **A** [26].
Here, the book "Quantum Computation and Quantum Information" by Nielsen and Chuang will be cited again, because this issue could not have been expressed in a better way.

> *"Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment."*

If one assume such a collection of measurement operators $\{M_m\}$ with the outcome $m$ which will act on a state $|\Psi\rangle$, someone can find the probability of outcome $m$

$$p(m) = \langle\Psi|M_m^\dagger M_m|\Psi\rangle \tag{4.12}$$

Of course, when summing up all of the probabilities of the outcome, they have to add up to 1, so $\sum_m p(m) = 1$. This implies that if all measurements of operators are summed up with their complex conjugate, one gets the identity operator

$$\sum_m M_m^\dagger M_m = I \tag{4.13}$$

After the measurement, the wave collapses from a physical perspective. This means that the quantum state changes by interacting with the measurement device.

$$|\Psi\rangle \to \frac{M_m\,|\Psi\rangle}{\sqrt{\langle\Psi|M_m^\dagger M_m\Psi\rangle}} \tag{4.14}$$

It can neither be said why this measurement with these operators behaves in this specific way nor can it be derived. This should be kept as a postulate.
There are several types of measurements whereby one has to find the best measurement

for their own specific problem via trying and consequently failing or succeeding. One main measurement concept is the *projective measurement*. This concept can be seen as frequently used as it also serves as the basis of many other measurement concepts. It also serves as a good overview of measurements on quantum systems. In chapter 10.3, a model of measurements will be discussed which is used to improve the QKD protocol.

### 4.2.1 Projective Measurement

Generally and simply spoken, if a quantum state is measured, one projects it to a basis state [8]. If geometrical explanation of the Bloch sphere in two dimensions is used again, the state lies somewhere on the Bloch sphere. If this state is measured now, the state projects onto the value $|0\rangle$ or $|1\rangle$ which would be our output.
Assuming one has a basis $\{|n\rangle\}$, then a collection of measurement operators can be found as

$$P_n = |n\rangle \langle n| \tag{4.15}$$

Let us now use the description of our quantum system in terms of the density matrix. The probability to get outcome $m$ is then

$$p(m) = \langle m|\rho|m\rangle = \mathrm{Tr}(P_m \rho P_m) = \mathrm{Tr}(P_m^2 \rho) \tag{4.16}$$

The state after the measurement $\rho'$ would be

$$\rho' = \frac{P_m \rho P_m}{p_m} \tag{4.17}$$

This kind of measurement covers the easiest measurement in quantum physics. Nevertheless, they can be seen as useful, for example, if one wants to measure a specific qubit and leave the other qubit untouched [27].

### 4.2.2 Positive operator valued measures

The general description of above measurement methods are *Positive operator valued measures* (POVM). It includes all the aspects and mathematical tools which have been discussed above. But the measurement operators are not projective. It is basically a generalisation of projective measurements.
If one goes back to the example above and consider the measurement operator $\{M_m\}$ acting on a quantum state $|\Psi\rangle$, then a positive operator $E_m$ can be defined so that

$$E_m = M_m^\dagger M_m \tag{4.18}$$

This operator $E_m$ satisfies the completeness condition of course: $\sum_m E_m = \mathbb{1}$ and $p(m) = \langle \Psi | E_m | \Psi \rangle$. The whole set of $\{E_m\}$ is what it calls POVM. An advantage lies in the fact that one does not have to know the post-measurement state to get to know some general statistics about a state in this special case of the measurement mechanism.

# 5 Basic Information theory

*"The fact that information is physical means that the laws of quantum mechanics can be used to process and transmit it in ways that are not possible with existing systems."*
Anton Zeilinger

Information grows to a highly demanded and valuable trade product. Some scientists even say that the 20th century is characterised by information. The word 'information' can be seen as broad as it contains everything in the human world, everything we as humans see, hear, taste, feel and do. To put it more philosophically, the whole life is based on receiving and sending information to the environment.
In this 'receiving-sending' information world, even small pieces of information or ones that are unimportant to us can be interesting to other people. However, this will be discussed later. First of all, information theory will be introduced. Information theory lies in this case mostly on how someone can send a message to another party (receiver) and how humans can optimise and simplify information.
In this broad context of information theory, quantum theory represents one upcoming field which grows more and more. It seems that this field is just theoretical, but there are several experimental research and experiments which show its practical realisation [28–30]. Quantum information theory means not only basic theoretical topics such as algorithms and cryptography, but it also includes the computation part such as quantum teleportation [8], no-cloning theorem [8], and many others. In contrast to classical information theory, quantum information theory, or more specifically, in quantum communication *quantum memories* plays an important role and in the past few years, this topic has grown more and more [31]. As already discussed in chapter 3.1.1 and as will also be discussed later, someone is not able to send a message through a cable or through the air with an arbitrary length. Noise would ruin the dreams and destroy the state. In contrast to other quantum cryptography protocols, in this master thesis there is an attempt to overcome noise with subspace selection using high dimensional entanglement without using quantum memories.

## 5.1 Classical Information theory

A basic communication channel is based on the *sending-receiving concept*. As depicted in figure 5.1, an information source sends the message to a transmitter which prepares the message in such a way that it can be sent via a channel to the destination party. This party uses a receiver to be able to read the message. In all these components, it is possible to get noise which will form errors in the message.
Consider a system which consists of $k$ symbols and $a$ letters, meaning $\mathcal{S} = \{a_1, a_2, ..., a_k\}$.

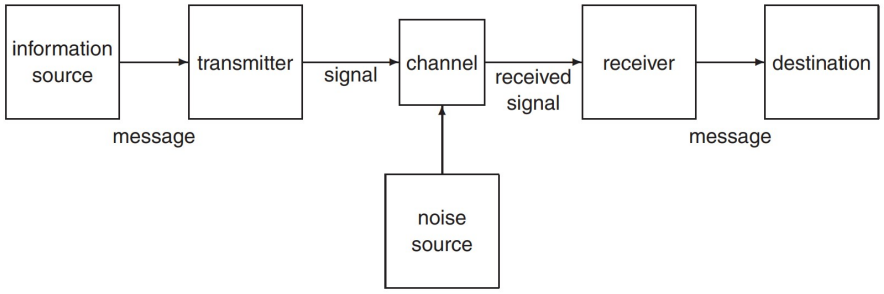


Figure 5.1: Schematic concept of classical information exchange. [32]

A message in this sense is transferred to a bit string $\mathcal{B}$ containing bits $j = \{0, 1, ..., d-1\}$ such that each $b \in \mathcal{B}$ can be dedicated to a symbol or letter $b_k = a_k$ for a partial bit string $b$. For example, in dimension two it is possible to define $A = 0$ and $B = 1$ so that a message '$AB$' would be transferred to 01. For a more complex system like the German or English language, there are two questions:
How many bits are needed for a system to at least express each letter or symbol? and
"At what rate can we communicate reliably over a noisy channel?" [26]
First such thoughts on transmitting information were already done in the 20th century, but nowadays, only one name is well known, namely *Claude Shannon*. Shannon's theorem will not be discussed in detail here, solely an explanation of the basics will be given.

### 5.1.1 Shannon Entropy

Let's suppose that someone wants to send $N$ messages to another party. In classical information theory, information is transformed into bits. Obviously, you can send $N = 2^n$ messages, however, there is not sufficient knowledge about the amount of information which the messages include. This amount of information can be calculated by $\log_2 N$. Note that the logarithm is used as a kind of convention in information theory. By considering two or more systems, the logarithm gives the best mathematical concept to describe these systems and their relationship to each other. Basis two of the logarithm is based on the units of bits which are used. Surely, one could also use different bases [33]. Mathematically it means that you just multiply a constant factor to $\log_2 N$ which only changes the convention but not the mathematics or physics behind the system.
If someone is talking about information theory, this person is also talking about entropy. Suppose a $x$, in which each $x$ corresponds to a point in a so-called *sample space*. Shannon entropy $H$ then describes the average level of information which can be extracted out of a set of random variables $x \in X$ [8].

$$H(X) = H(p_x) = -\sum_x p(x) \log_2 p(x) \tag{5.1}$$

Here, $p(x)$ denotes the probability for $x$. Because as $p \leq 1$, the minus sign ensures that the entropy is always $H(X) \geq 0$.

Similarly the joint entropy for a set $X, Y$

$$H(X,Y) = -\sum_{x,y} p(x,y) \log_2 p(x,y) \tag{5.2}$$

The probability for the outcome $y$ can easily be calculated by summing over all outcomes of $x$ $p(y) = \sum_x p(x,y)$. A mathematically experienced reader would ask what happens if $p_x = 0$ because the logarithm of zero is not defined. Here one just has to follow the convention and claim that $0 \log(0) = 0$ and $\lim_{x \to 0} \log x = 0$ [8].
An interpretation of the above equation lies in the stochastic ability of a third party (Eve). The higher the entropy of the communication between two parties, the higher the probability to make a guess $X$, which in the context of this example means that the eavesdropper has a higher chance to guess the outcome of the measurement of both parties. Let us suppose if $x$ is a message then $H(x)$ is the information which an eavesdropper could possibly get from the communication between two parties. Here also lies a weakness of quantum communication. Due to noise effects, an eavesdropper could make use of a winning strategy by just guessing the outcome of one party. Therefore, both parties have to minimise the guessing probability by defining some boundaries for their communication so that they can claim their communication is secure. In this thesis, the boundaries are set to the protocol in section 6.2
As already was seen in 3.1, resources play an important role in information theory. What is the lower bound of resources needed to share or store information without losing information? In other words, how many resources does one need to reconstruct the information later? In short, the entropy can be used in such a way that $H(X)$ bits are required per symbol. Clearly, this is a rough explanation, however, further information can be found in Nielsen and Chuang's book [8] for more details.
Above, the Shannon entropy was considered as a mathematical construct in which one can only extract information after the measurement. From a different point of view, one can also consider the Shannon entropy as the entropy before the measurement was done as the uncertainty about $X$. Therefore, both views consider how much information was gained from a message after the measurement and the uncertainty of the measurement before the measurement itself.
Even though an introduction to the concept of Shannon entropy was given, it might nevertheless be hard to understand it with the provided explanation. Let's put it in other words now. If you only consider the phrase *'Hello World'*, there are 10 letters (the space between the words is not considered). The probability of the letters within this phrase are

$$\begin{gathered} H = 1/10 \qquad e = 1/10 \qquad l = 3/10 \qquad d = 1/10 \\ o = 2/10 \qquad W = 1/10 \qquad r = 1/10 \end{gathered} \tag{5.3}$$

The minimal average number of bits which are needed per letter is:

$$H(x) = -\left[\frac{5}{10}\log_2\left(\frac{1}{10}\right) + \frac{3}{10}\log_2\left(\frac{3}{10}\right) + \frac{2}{10}\log_2\left(\frac{2}{10}\right)\right] \tag{5.4}$$

$$H(x) = -\left[-1.661 - 0.5211 - 0.4644\right] = 2.6465 \tag{5.5}$$

In summary, therefore one needs at least three bits per symbol to send the phrase *Hello World* to be biunique and only 30 bits for the whole message. More practically, out of the bit set $\{0, 1\}$ only three bits are needed in a given order to send the message to another party.
Coming back to the theory of entropy, it is even possible to calculate the uncertainty of $X$, if $Y$ is known, which is also known as the conditional entropy [8].

$$H(X|Y) = H(X, Y) - H(Y) \tag{5.6}$$

Note, $H(X|Y)$ reads as $X$ given $Y$.
If $X$ and $Y$ are denoted to the above example of the two parties, the average information which both can generate is just the sum of their own information which they received independently. However, it is also possible that both got the same information. In order to the second scenario, one can find the information which both get in the following way:

$$I(X : Y) = H(X) + H(Y) - H(X, Y) \tag{5.7}$$

## 5.2 Quantum Information theory

Certainly, one can think of which kind of information they can get from a quantum system.
Suppose a quantum state $\rho_A$ for a system $A$, the average information can be found via

$$S(A) = S(\rho_A) = -\operatorname{Tr}(\rho_A \log_2 \rho_A) \tag{5.8}$$

This is also known as the *von Neumann entropy*. Similar to the classical consideration, such a relation also exists for a shared system with the joint quantum state $\rho_{AB}$.
In the protocols like *BB84* and others, Alice uses classical variables in the classical system $A$ and prepares them in a quantum state $\rho_k^A$ "where $k = 0, 1, ...$ denotes the different possible states she may send and whereby each has the probability $p_k$" [8]. The corresponding coherent quantum information is just a lower bound and is also known as *Holevo's bound*

$$H(X, B) \leq S(\rho^A) - \sum_k p_k S(\rho_k^A) \tag{5.9}$$

The mutual information can be found as

$$I(X : B) \leq S(\rho_B) - \sum_x p(x) S(\rho_B^k) \tag{5.10}$$

The above expression is also the upper bound for the mutual information which an eavesdropper can get out of the system.

## 5.3 Noise

So far, a theoretical background of quantum information as well as a brief overview of how things work have been given. It would be a dream to simply apply the theory to the experiments. Even in the classical information world one has to deal with noise effects. Due to the setup, copying the information or sending it through fiber or air would result in a loss of information. But contrary to the quantum world, overcoming such noise in the classical world is very easy. The three bits error correction in section 3.1.1 was already shown, but the act of just copying the information and comparing both versions of the information with each other would get us the right information.
As one can imagine, quantum noise is more difficult to handle than one might think initially. In principle, noise is one main player in quantum experiments and one reason why quantum information is not used already in daily or at least academic life. Even though it would be a dream of all scientists, unfortunately, noise cannot be erased from an experiment. There is no ideal device that could create an optimal quantum state, that measures the state with a 100% accuracy or that can store a state without evolving it in time. Of course, the efficiency did increase tremendously (and miraculously) in the past years. Quantum devices could achieve a rate of 99% [34], but quantum noise leads to a cascade effect which makes the state unusable [35].
Nevertheless, in this chapter an overview of what quantum noise really is will be given. At the end of this master thesis, quantum noise as a general theoretical issue is considered. In fact, it was tried to overcome quantum noise by using the protocol which was proposed in [1].
Now, a brief introduction to some mathematical basics will be given in order to facilitate the comprehension of the following issues. One has already seen what a density operator $\rho$ is and how it behaves under different situations. Another transformation under the consideration of noise is done by the map $\mathcal{E}$ which is a quantum operator [8].

$$\rho' = \mathcal{E}(\rho) \tag{5.11}$$

Here, $\rho'$ is the density matrix after noise occurs. This is a general mapping. A similar notation is used in the discussion of the measurement of a quantum state.
All noise effects work to Eve's advantage.

### 5.3.1 Noisy Channel

In theory, for a noiseless channel an input information $x_i$ from an input alphabet $\mathcal{X}$ should be transmitted through the channel in such a way that the output information $y_i$ from an output alphabet $\mathcal{Y}$ [32] should be equal $x_i = y_i$.
In comparison, a discrete noisy channel maps an input $x_i$ to the output $y_i$. Such a transition happens with a probability $p(y_i, x_i)$ [32]. Of course, there are several effects which contribute to the transition probability and it depends on which channel is used. In this consideration, it was focused on a fiber channel which uses photons. Here two effects are named: [12]

1. *Chromatic dispersion*
   Wavelengths are travelling at different speeds through the fiber. In consequence, it is possible that wavelengths overlap.

2. *Polarisation mode dispersion*
   Leads to decoherence by depolarisation of the pulse. In fact, it is similar to a birefringe effect in which a beam is split into two components with a polarisation mode orthogonal to each other. Below, an example will be considered.

As already mentioned, such effects are not unique and this topic is too broad to be discussed in this thesis. A more detailed examination was undertaken by Charles Henry and Rudolf Kazarinov in [36] who focused on the photonic part of a quantum channel.

#### Example: Depolarizing channel

Imagine one uses qubit as an information input $x_i$. For example, depolarisation can happen with the probability $p$ if someone claims that the single qubit stays in its state with a probability of $1-p$. After noise happens to the state, the qubit is depolarised with the probability $p$ and gets replaced by a mixed state.

$$\mathcal{E}(\rho) = \frac{pI}{2} + (1-p)\rho \tag{5.12}$$

When illustrated in the example of a Bloch sphere, the sphere shrinks uniformly depending on the probability $p$ [8].

## 5.4 Noise in subspace selection protocol

Noise is too general to be defined in such a way that it could be analysed here. In this case, it can be said that the interaction of photons with their environment is the main source of noise [1]. Due to this effect, it can happen that photons are not in a quantum state anymore or at least to a very low degree. Or it appears that they got lost before they reached the measuring setting of the parties, but still, it can happen that the detector clicks without a photon being inside of the detector. In general, this is known as *dark counts*.
*How can all noise effects be considered?* Remember, one wants to calculate the guessing probability of Eve in the end. For this, the *isotropic state* is used.

$$\rho(v) = v\,|\Psi_d^+\rangle\,\langle\Psi_d^+| + (1-v)\frac{\mathbb{1}_d}{d^2} \tag{5.13}$$

The visibility $v$ is the quantity which includes all aspects of noise in this case. Of course, this is a simplification of the actual problem, however, as one will see later, the models work quite well. In contrast to the paper of Mirdit Doda [1], $v$ is a *free* variable. $|\Psi_d^+\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|ii\rangle$ is one of the $d^2$ bell states. This state is maximally entangled and $|\Phi^+\rangle$ is used because of the possibility to transform from this state to all the other

states [37].
In conclusion, if $v = 1$, the state which was described in 5.13, consists only of the bell state and is therefore entangled [8]. Otherwise, if $v = 0$, only the second part contributes to the state which is a complete noise effect and therefore it is just a classical state.
In the end, visibility decreases with every moment the state exists. Of course, the goal is to keep it as high as possible. The visibility was motivated here because in the end, the proof of robustness is based on it and with the help of the visibility it is possible to show that the protocol of [1] improves the communication between two parties.

# 6 Quantum key distribution

*Quantum key distribution* (QKD) is the answer to the question how a secure quantum communication can be built, or in other words, how it is possible to establish a secret key between two trustworthy parties. In principle, QKD is a secure communication method which summarises all protocols that describe quantum communication. For a better understanding of what is meant by sharing a secure key, one have to clarify what is meant with secure.
It is assumed here that Eve has full access to all resources and all the time to break the classical communication.
As already mentioned in chapter 2.1, there are 3 statements on which quantum physics is based on. For quantum communication two of them are crucial for QKD. They show the huge advantages of quantum communication compared to classical communication. The two fundamental concepts or statements are the following:

(i) The No-cloning theorem

(ii) It is impossible to extract information out of a quantum system without disturbing the state itself by a measurement because each measurement disturbs the state

Statement (ii) can also be seen as the impossibility for Eve to extract information out of a state without being noticed. If Alice prepares some information in a state, Bob can only measure the state with the consequence that the state gets disturbed or even destroyed by the measurement. Also, if Bob tries to get information by applying some unitary transformation, he would change the state without knowing which information was hidden before. Eve has to measure or interrupt the state which both sides will notice in the end. The possibilities for Eve to attack the communication will be discussed in more detail in chapter 6.2

## 6.1 QKD protocol

Each QKD protocol is based on the basic concept of *preparing-sending-measuring*. In the paper "Security proof methods for quantum key distribution protocols" [38], Ferenczi mentioned this concept and described them as followed:

1. *Preparation*
   For a set $S = \{|\Phi_x\rangle, x = 1, 2, ..., n\}$ of $n$ quantum states $|\Phi_x\rangle$ in a $d$-dimensional

Hilbert space $\mathcal{H}_S$, Alice chooses $m$ states from the set $S$ with the probability $p(x)$. These quantum states are used for encoding random variables of the key.

2. *Sending*
   Alice sends the quantum states to Bob, but before she does this, she keeps a record of the sequence she will send to Bob.

3. *Measurement*
   In Bob's laboratory, he measures the quantum state. Of course, he has different choices for the measurement which will be discussed later in chapter 4.2. In the end, he records the gained outcome of each measurement. According to the conditional probability distribution $p(y|x)$, these measurements results in a correlated data (raw data) which is shared between Alice and Bob.

Of course, Bob would not know what key Alice has sent only through the measurement. He has to extract the information out of his measurement. This can be done by sharing a classical open channel with Alice. Even a third party could have access to this channel. Without Bob's measurement, the third party is not able to conclude the information which was shared without knowing Bob's outcome. Therefore, Ferenczi described additional three statements in his paper: [38].

4. *Postprocessing*
   Alice and Bob have to extract a key from Bob's measured data. Via public channel, they communicate which outcome Bob measured and discard all of the unsuitable measurements for the key.

5. *Information reconciliation*
   This is nothing more than just error correction. Error correction is a huge topic in communication and has already been discussed to some extent in chapter 3.1.1. Note that information reconciliation here means a classical error correction, not a quantum error correction.

6. *Privacy amplification*
   In this last step, Alice and Bob eliminate Eve's knowledge about their key. In other words, they distill their key from Eve's information which she could probably get and is correlated to the information which Alice wants to send to Bob. In the end, they both obtain a shorter key $k = k_A = k_B$.
   In order to achieve successful quantum communication, Alice and Bob have to determine an upper bound of the amount of information which Eve could know about their correlated data.

## 6.2 Eavesdropper

QKD protocols claim to be secure from an eavesdropping attack. As already mentioned in chapter 2.1, Eve has all the power and best technological devices. Nevertheless, it would

be impossible for her to stay unnoticed if she would interrupt Alice and Bob's quantum channel. This consideration only works in an ideal framework, but in the real world, the security decreases with the quality of the system. With quality, it is meant the *fidelity* of a state which is sent from Alice to Bob via a cable or in the air. There are several attacks in which Eve can try to get some information. But first, one has to consider the framework in which Eve can interrupt the quantum communication between Alice and Bob.

(i) First of all, Eve should stay unnoticed by Alice and Bob for the whole process

(ii) It is not possible for Eve to interrupt the laboratories of Alice and Bob directly.

(iii) Eve can interrupt the quantum channel in the framework which is set by the law of physics.

(iv) Eve can extract all the messages and information which were sent over the classical channel, but she is not able to change the messages. Authentication does not allow her to interrupt this channel. [38]

In this consideration, the source is placed on Alice's side as per usual. It is also possible to put the source in the middle between Alice and Bob. The basic concept which will be presented in regard to Eve's attacks will be similar to the one presented here. But one has to consider that the source has to be trustworthy.
If the source is on Alice's side, the source produces a state $|\Phi\rangle_{AS}^{\otimes n}$ and sends it to Bob via quantum channel $S$. Eve interrupt in this channel and receive the state instead of Bob. She possesses an ancilla quantum system $E'$ and attaches it to the quantum state. A unitary transformation takes the joint systems $S^n E'$ to $B^n E$. For herself, she keeps the transformed ancilla $E$ and sends the other system $B^n$ to Bob [38]. The state which Alice and Bob share now is a completely unknown state $\rho_{AB}^n$. The attacks which Eve can now perform can be roughly summarised in three classes:

1. *Individual attacks*
   Eve gets all the signals which were sent by Alice and interacts with them individually which means that she attaches a quantum system $E'$ to each of the states $|\Phi\rangle_A$. She is using this unitary $U_E$ every time. As described above, she will keep $E$ and perform a measurement on each individual system $E$ to extract information. The mutual information which Eve can possess is basically the maximisation of the mutual information over Eve's strategies. This relation is also known as Csiszár-Körner bound.
   $$I_{AE} = \max_{\text{Eve}} I(A:E) \tag{6.1}$$
   Of course, the system is symmetric in such a way that it is possible to find a similar relation for $I_{BE}$ [12]. Here $I(A:E)$ describes how much someone can learn about $E$ by receiving $A$ (this is the mutual information between the classical symbols). Therefore, in the view of secure communication one wants that $I_{AE}$ is zero. An advanced reader knows that this is impossible. Consequently, someone wants that

$I_{AE}$ at least tends to be zero. One question which is still not completely clear in the common literature is, when does Eve has to perform her measurement. First, she is forced to do her measurements immediately after the interaction. Second, she can use quantum memory in such a way that she can keep the state until the sifting and error correction part.
In the basic literature of quantum cryptography, the common method is that Eve can catch a part of the quantum state which Alice sends to Bob. She will measure it, prepare a new arbitrary state and send it to Bob. This example is a subsection of individual attacks, but clearly, she will not remain undetected by the other parties, because she breaks the entanglement of the state. Alice and Bob will only get arbitrary results.

2. *Collective attacks*
   In collective attacks, the interaction of Eve with the sent quantum states is the same as in individual attacks. But further, at the end she applies a collective measurement on the signals jointly. She can use all of the information she got from the classical phase. More precisely, if collective attacks $\rho_{AB}^n$ are assumed, she can also suppose the product $\rho_{AB}^n = \rho_{AB}^{\otimes n}$
   The bound which describes the shared information is known as the Devetak-Winter bound.
   $$I_{AE} = \max_{\text{Eve}} \chi(A:E) \tag{6.2}$$
   Analog $I_{BE}$. Where $\chi$ describes the Holevo quantity which was already discussed 5.9. The optimisation of Eve's strategy is much easier than in the individual attacks. This lies in the nature of the Holevo quantity as $\chi$ only depends on $\rho_{E|x}$ which she couples to her unitary operation of her ancilla.

3. *Coherent attacks*
   In coherent attacks, all signals will be interacted coherently by using one huge ancilla on all $n$ systems by Eve.

In the following section, one scheme will be discussed to a certain extent.

### 6.2.1 Collective attacks

The process and especially the application of a unitary transformation $U_E$ is similar to the purification $|\Psi\rangle_{ABE}$ of $\rho_{ABE}$ in the shared Hilbert space $\mathcal{H}_{ABE}$. Eve has all possibilities which she is able to utilise for her attack. This includes that she has full control over $|\Psi\rangle_{ABE}$. The question is, what the state after Alice and Bob measured their system $AB$ is? [38]
Consider the POVMs $M_A = \{F_A^x\}$ and $M_B = \{F_B^y\}$, where $x$ and $y$ are some outcomes of Alice and Bob. Further, $|x\rangle$ and $|y\rangle$ are orthonormal bases. The shared state after the measurements is classical from Alice and Bob's view, but from Eve's perspective, the state is a quantum one in such a way that the resulting state is found as:

$$\rho_{XYE} = \sum_{x,y} p(x,y)|x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \otimes \rho_E^{xy} \tag{6.3}$$

with the probability distribution

$$p(x,y) = \mathrm{Tr}(F_A^x \otimes F_B^y \rho_{AB}) \tag{6.4}$$

Eve's quantum state can be found as

$$\rho_E^{xy} = \frac{1}{p(x,y)} \mathrm{Tr}_{AB}(F_A^x \otimes F_B^y \otimes \mathbb{1}_E |\Psi\rangle\langle\Psi|) \tag{6.5}$$

# 7 High Dimensional Entanglement

The use of high dimensionality is not a surprise. A larger number of studies have shown that high dimensional entanglement has higher noise resistance [39], but that it is also much more difficult to be realised. In this section, high dimensional entanglement will be discussed and the concept of *witnesses* will be introduced which will be important for the improved protocol later. In this section, also the experimental realisation will be themed.

## 7.1 Mathematical construct

As generally known, it can be roughly distinguished between separable and entangled states. In a $d \times d$-dimensional Hilbert space $\mathcal{H}$ where $\mathcal{H} = \mathcal{H}_A^d \otimes \mathcal{H}_B^d$ belongs to the subsystem Alice and Bob. A state $\rho_{\text{sep}}$ is called separable if the state can be written as [40]

$$\rho_{\text{sep}} = \sum_i p_i \rho_A^i \otimes \rho_B^i \tag{7.1}$$

Otherwise, the state is entangled. By considering the isotropic state $\rho_\alpha$ for example

$$\rho_\alpha = \alpha |\Phi_d^+\rangle\langle\Phi_d^+| + \frac{1-\alpha}{d^2}\mathbb{1} \tag{7.2}$$

one can easily see that this state is separable for

$$-\frac{1}{d^2-1} \leq \alpha \leq \frac{1}{d+1} \tag{7.3}$$

and entangled

$$\frac{1}{d+1} < \alpha \leq 1 \tag{7.4}$$

for $\alpha \in \mathbb{R}$ and $|\Phi_d^+\rangle = 1/\sqrt{d}\sum_{i=0}^{d-1} |ii\rangle$ is one of the bell states which is maximally entangled [41]. A mathematical tool which needs to be mentioned here, but will just be discussed shortly is the *Peres-Horodecki criterion.*
Suppose the state [41]

$$\rho = \sum_{i,j=0}^{d-1} \sum_{k,l}^{d-1} \rho_{ij,kl} \, |ik\rangle \, \langle jl| \tag{7.5}$$

A *partial transpose operation* of this state can be found for both sides, Alice and Bob.

$$\begin{aligned}\rho^{T_A} &:= \sum_{i,j=0}^{d-1}\sum_{k,l}^{d-1} \rho_{ji,kl} \left|ik\right\rangle \left\langle jl\right| \\ \rho^{T_B} &:= \sum_{i,j=0}^{d-1}\sum_{k,l}^{d-1} \rho_{ij,lk} \left|ik\right\rangle \left\langle jl\right|\end{aligned} \tag{7.6}$$

If the state is positive semidefinite, than the state is *positive under partial transpoe* (PPT). The theorem of Peres-Horodecki claims, that if a state is PPT than it is a separable state. In other words, if negative eigenvalues can be found of the partial transposition of a state, the state is entangled. An example, if the state 7.1 was used, then its partial transposition can be found as:

$$\rho_{\text{sep}}^{T_B} = \sum_i p_i \rho_A^i \otimes (\rho_B^i)^T \tag{7.7}$$

Note, this criterion is only sufficient for dimension $2 \times 2$ or $2 \times 3$ to show separability. For higher dimensions, it is not satisfactory enough to show if a state is seperable but if a violation of the PPT criterio was found, the state is entangled also for higher dimensions.

## 7.2 Witness

The main concept of entanglement witness is, to find a hermitian operator $W$ which shows if a state is entangled or not. Such an operator has to satisfies the following criteria [41].

1. $0 \leq \operatorname{Tr} W\rho_{\text{sep}}$ holds for all separable states $\rho_{\text{sep}} \in \text{SEP}$. Here SEP is a set of states $\rho_{\text{sep}}$ which are all separable.

2. $\operatorname{Tr} W\rho_{\text{ent}} < 0$ holds at least for some entangled states $\rho_{\text{ent}}$

An optimal interpretation of the separable and entanglement construct with a witness is shown in figure 7.1.
This figure shows that there are infinite ways to find a witness $W$, but not each witness proves that a state is not engangled. Therefore, the optimal witness $W_{\text{opt}}$ must be found. As one might imagine, $W_{\text{opt}}$ could be seen as the tangent plane to a set of separable sets. Furthermore, as described by R. A. Bertlmann, K. Durstberger, B. C. Hiesmayr and P. Krammer in study [40], a plane of optimal witness shows the maximum violation of the general bell inequality.

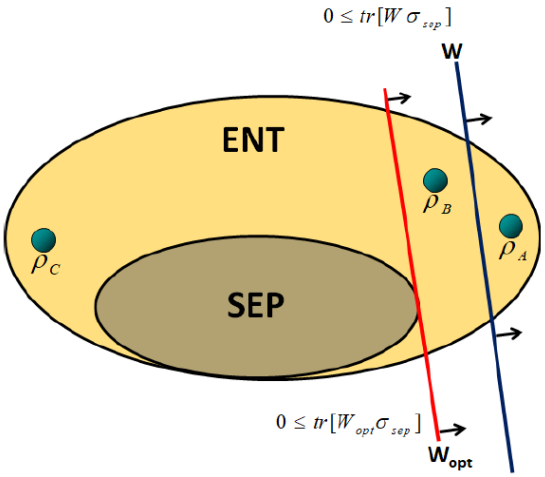


Figure 7.1: Optical illustration of the Witness operator $W$. Here $W_{\text{opt}}$ denote to the optimal Witness and $\rho_A$, $\rho_B$, $\rho_C$ are just random states.

## 7.3 Experimental realisation

Moreover, the experimental part of the mentioned study will be discussed as the questions of how high dimensionality can be achieved and why it is only possible to create low dimensions so far. This part is also important for the concept of the new protocol. There have already been some studies utilising the protocol used in this master thesis and confirming the results. For the purpose of a discussion, it would be therefore interesting to thematise how the experiment was achieved.

### 7.3.1 Spontaneous parametric down-conversion

A method to create high dimensional entanglement relies on the concept of spontaneous parametric down conversion (SPDC) [8]. One necessary condition which is used in SPDC is the nonlinear crystal. One of Maxwell's equations of electrodynamics describes how the polarisation of an electromagnetic radiation $E$ behaves in materials

$$P = \epsilon_0 \chi E \tag{7.8}$$

Here, $\chi$ is the constant characteristic electric susceptibility which differs from the material. In essence, the polarisation changes linearly for a constant $\chi$ which can be found in the daily classical world. If $\chi$ is now considered as a nonlinear optical component, it becomes apparent that these dielectric parameters depend on the energy of the field.

$$P = \epsilon_0 \chi E + \epsilon_0 \chi^{(2)} E^2 + \epsilon_0 \chi^{(3)} E^3 + \dots \tag{7.9}$$

Parametric down-conversion is found in the second order of the above equation. By doing some basic maths, a frequency $\omega_p$ of the pump beam can be divided into two different

frequencies $\omega_i$ and $\omega_s$, where the subscript 'i' stands for idler photon and 's' for signal.

$$\begin{aligned} \omega_p &= \omega_i + \omega_s \\ k_p &= k_s + k_i \end{aligned} \tag{7.10}$$

The last relation can be found by the energy conversation where $k$ is the wave vector.

### 7.3.2 Creating enganglement

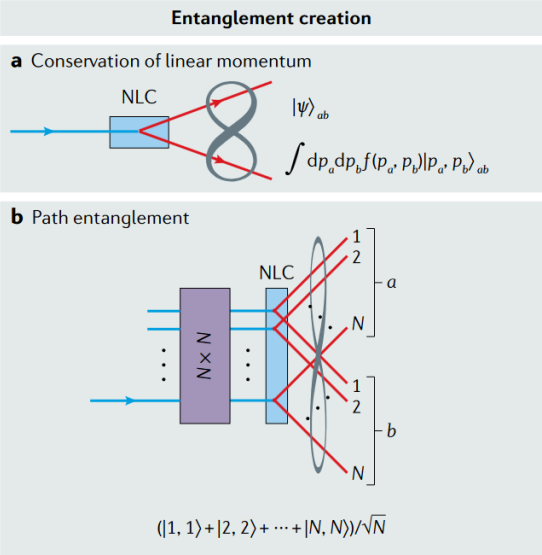


Figure 7.2: (a) The pump beam from the left hits the nonlinear crystal with $\chi$. An entangled pair with the state $|\Psi\rangle_{ab}$ is created under the phase matching condition 7.10 for $p_a$ and $p_b$ and a function $f(p_a, p_b)$ which describes the linear momentum of both photons. (b) The generation of a $N$ high dimensional state by the use of $N \times N$ input pump beams. [42]

There are several methods to create high-dimensional entangled pairs. Figure 7.2 shows two main methods. In (b) a pump beam is split by a $N \times N$ multiport to $N$ beams. Each of these pump beams creates an entangled pair in the NLC which takes path $a$ or path $b$. A $N$-dimensional state is produced which looks like $|\Psi\rangle = \frac{1}{\sqrt{N}}|NN\rangle$. The method which will be discussed more closely and which was used in the experiment later, uses the orbital angular momentum.

#### Angular orbital momentum

If propagating light beams with helical phase fronts along the z-axis is being considered, the wave can be described as

$$\Psi(r, \Phi, z) = \Psi_0(r, z) \exp(il\Phi) \tag{7.11}$$

The beam is described by the field amplitude $\Psi(r, \Phi, z)$ for an amplitude distribution $\Psi_0$ depending on the expansion of the light beam. The interesting part of this master thesis is the dependence of the beam with its azimuthal phase $\exp(il\Phi)$. The azimuthal phase index $l \in \mathbb{N}$ "represents the number of azimuthal phase rotations in one full cycle from 0 to $2\pi$" [43]. Interestingly, Laguerre and Gauss found a complete basis set of orthonormal modes. This equation will not be discussed in more detail, however, the visualisation of the intensity distribution of superposition modes looks like the atom picture for the azimuthal quantum number.
Of course, there have been more studies finding a complete basis set of orthonormal modes, such as Bessel-Gaus and Ince-Gauss study, which is also necessary because the LG basis does not describe the propagating light beam correctly.
An analogy of these concepts is the comparison of the azimuthal orbital momentum with a Poincaré sphere such as the well-known Bloch sphere as it is shown in figure 7.3.

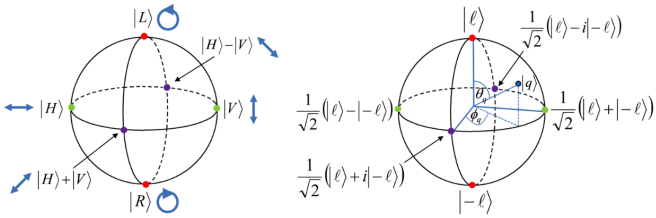

Figure 7.3: Analogy of representation of the OAM polarisation (right) with the Bloch sphere (left). [43]

The states which can be created with OAM lie on the surface of the sphere where $|l\rangle$ and $|-l\rangle$ describe the north and south pole and where all other states on the surface are superpositions.
A state in this picture depends on the spherical angles $\theta$ and $\phi$. Therefore, any state $|q\rangle$ in this representation can be found as

$$|q\rangle = \cos\left(\frac{\theta}{2}\right)|l\rangle + \exp(i\phi)\sin\left(\frac{\theta}{2}\right)|-l\rangle \tag{7.12}$$

The *Laguerre-Gaussian modes* (LG) carry the angular momentum to satisfy such a conservation of OAM [44]. A quantum state can be noted as

$$|\Psi\rangle = \sum_l a_{l,-l}\,|l\rangle\,|-l\rangle \tag{7.13}$$

Here, $|a_l|$ is the probability of finding the state in $l$ and the other in $-l$. If $|a_l|^2 = 1/d\ \forall l$ the state is maximally entangled. For the conversation of the orbital angular momentum, the pump beam has to have zero OAM. An advanced reader would know that this can be confirmed by simply considering Heisenberg's uncertainty relation with $\Phi$ as the angular width. The angular width of OAM describes the angular position which is just the conjugate variable of OAM. The uncertainty relation reads as

$$[\Delta(l\hbar)][\Delta(\Phi)] \geq \frac{\hbar}{2} \tag{7.14}$$

The violation of this relation satisfies the EPR criteria.

# 8 QKD using Subspaces with high d-Entaglement

As mentioned, this master thesis is based on a different QKD scenario [1]. In the common literature, Alice and Bob use the whole Hilbert space to measure the states. But in [1], the scholar proposed a protocol in which they use subspaces to get the key. For this scenario, some assumptions need to be made [45].

**Assumption 1:** First it is assumed that Eve can only perform collective attacks. A different view to this, because of the fact that the results are situated in the asymptotic setting, the de Finetti theorem can be used without the key rate being lowered. This can only be achieved by proving the level of security against general coherent attacks by using the de Finetti argument.
**Assumption 2:** Eve can be given more power by assuming that she prepares the entangled state which Alice and Bob share and measure in the end. Eve has therefore much more power and a huge advantage as well as implies the security of the protocol in a more "real world". In this context, it is worth mentioning that all noise effects are dedicated to Eve and are advantageous for Eve.
**Assumption 3:** Alice and Bob choose their setting randomly. There are no predefined or other variables which could determine their measurements. At each iteration, their measurements are independent and random.
**Assumption 4:** The string which both parties share is a short random string. They can use it for the authentication of their classical communication channel. It is assumed that they always have access to a classical channel in the QKD protocol.
**Assumption 5:** All parties can trust their devices and have full control over the measurements. Therefore, it is expected that the protocol is secure for all coherent attacks and that they have knowledge about their measurement. On the contrary, this means that one will not get the most efficient detectors, however, the detected events will nevertheless be sufficient enough for reliable correlations. Of course, Eve is not able to interact with the measurement setting of Alice and Bob.

In the following, these assumptions as well as the concept of a protocol discussed in section 6.1 will be implemented. Of course, the protocol which will be used here was already discussed in the paper of Mirdit Doda et al. [1], but in order to ensure a better understanding of the following procedure a short recap will be given.
One has to consider a full Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ where $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = d$. Here, the dimension is divided into multiple subspaces of size $k$. Therefore, there are $l$ subspaces of size $k$ so that $d = l \cdot k$. Suppose now that Alice and Bob are using $\{A_1^x\}_{x=0}^{d-1}$

and $\{B_1^y\}_{y=0}^{d-1}$ as computational bases in which they perform their measurement. This protocol is repeated $N$ times, so that they get a key which consists of $\mathcal{K}_A = \mathcal{K}_B \leq N$ symbols. (there are $N$ iteration $i \in \{1, 2, ..., N\}$). Note that Eve could find a winning strategy by measuring in the Z basis, therefore, one has to know about the measurements

1. Alice (or a trustworthy source in the middle of Alice and Bob) prepares a maximally entangled state $|\Psi\rangle_d$ for a dimension $d$. One part will be sent to Bob so that both share the entangled state. By sending this state to Bob, noise effects are decreasing the fidelity of the entangled state. As discussed before, if a minimum fidelity is reached, the state is useless in the sense of quantum physics. Here a method will be shown, that still uses the state for lower fidelity despite these noise effects.

2. Alice and Bob choose independently, uniformly and randomly a bit $\omega_A$ and $\omega_B$. If $\omega_A = 0$, Alice performs a measurement in the first basis $\{A_1^x\}_{x=0}^{d-1}$. Otherwise, she measures in the second basis $\{A_2^x\}_{x=0}^{d-1}$ with $\{A_2^x\} = UA_1^xU^\dagger$ for $U = \sum_{m=0}^{l-1}\sum_{i,j=0}^{k-1}\omega_k^{ij}|x\rangle\langle y|$ and $\omega_k = \exp(\frac{2\pi i}{k})$ and $x = mk + 1$, $y = mk + j$. Bob does the same, but his second basis is $\{B_2^y\} = U^* B_1^y U^T$

3. Subspace selection. Alice and Bob select a subspace and compare them to each other. This issue will be discussed in the next section.

4. Alice and Bob check the security of their channel by calculating the correlation. Here they use the results of the test round as well as some outcomes of the key rounds. The rest of the key forms the raw key.

5. After they have done some information reconciliation and privacy amplification, they are able to extract the final key.

## 8.1 Semi-definite programming

In the following, a short introduction will be given to explain what *semi-definite programming* (SDP) is and why it is used. Later, one will learn how to work with SDP by simply implementing it.
A SDP is a mathematical optimisation of a problem. Consider a function $f : \mathbb{R}^n \to \mathbb{R}$. This function is also known as a primal function. The aim is to optimise this function whereby optimisation in this context means the finding of an optimal $x*$ so that the function $f$ satisfies a given condition such *minimise* or *maximise* in specific boundaries. Therefore, the boundaries need to be defined, or in other words, one needs to define constraints via $g_i : \mathbb{R}^n \to \mathbb{R}$ for $i = 1, .., m$. A SDP reads in the form

$$\begin{aligned} \text{minimize} \quad & f(x) \\ \text{subject to} \quad & g_i(x) \leq b_i \qquad i = 1, ..., m \end{aligned} \tag{8.1}$$

Here the vector $x = (x_1, ..., x_n)$ was used as variables. The constants $b_1, ..., b_m$ are the bounds of the constraints. In the above equation, the minimal value of $x$ for the function

$f$ in the boundaries of $g_i$ was determined. Therefore, an optimal solution would be $f(z) \geq f(x^*)$ for $z \in x$.
In the following section, a mathematical tool of SDP on the protocol will be applied as it was used in [1]. Additionally, a new way to maximise the probability for Eve to guess the output for different noise effects will be tested theoretically.

## 8.2 Maximisation of the guessing probability as a SDP

Now, the generic quantum case where Alice, Bob and Eve share the tripartite state $\rho_{ABE}$ will be considered. Alice and Bob will make local measurements $\{A_{a|x}\}_{x=1,2}, \{B_{b|y}\}_{y=1,2}$ in two possible computational bases (two inputs): The first one will be used to generate the key (key basis), while the second one will allow them to certify the security of the protocol (security basis). Moreover, one has $d$ outputs for each party.

$$A_1^a = |a\rangle\langle a| \qquad B_1^b = |b\rangle\langle b|$$

The security bases are chosen in such a way that they are mutually unbiased and correspond to the key basis.

$$A_2^a = U_d A_1^a U_d^\dagger \qquad B_2^b = U_d B_1^b U_d^\dagger = (A_2^b)^T$$

for some unitary transformation $U = 1/\sqrt{d}\sum_{i,j}\omega^{ij}|i\rangle\langle j|$ and $\omega = \exp(2\pi i/d)$

Eve wants to get the key, that is, she wants to guess Alice's outcome when she measures in the first basis. Eve can act on her part of the state with some local measurement $\{E_e\}$. The guessing probability is defined as the probability that Eve's and Alice's outcomes coincide for that choice of basis for Alice and Bob. That is,

$$P_g = \sum_{e,b} p(e\, e\, b|11) = \sum_{e,b} \mathrm{Tr}(\rho_{ABE} A_{e|1} \otimes B_{b|1} \otimes E_e) \tag{8.2}$$

The figure of merit for the security of the protocol will be then the maximisation of that quantity over all possible states $\rho_{ABE}$, and Eve's strategy $\{E_e\}$:

$$P_g = \max_{\rho_{ABE},\{E_e\}} \sum_{e,b} \mathrm{Tr}(\rho_{ABE} A_{e|1} \otimes B_{b|1} \otimes E_e) \tag{8.3}$$

In order to win and get information from the communication between Alice and Bob, Eve has to get a high guessing probability. On the contrary, for secure communication, Alice and Bob need to minimise the guessing probability. A way for both of them to upper-bound the guessing probability will be, by checking the obtained results when measuring in the second basis. The idea is that observing some strong correlations between them limits the compatible tripartite states. One can, for instance, prove that observing the correlations of a singlet prevents any other entanglement with Eve [46, 47].

In general, some linear relation of the observed probabilities is used between Alice and Bob to upper-bound the guessing probability. In this case, constraints applying the Witness operator, which was already introduced in section 7.2 $\widehat{W}$, to the density matrix $\rho_{AB}$ so that $\mathrm{Tr}(\widehat{W}\rho_{AB}) = W$ holds can be created. Here, $\widehat{W}$ is a linear function of the local measurements which will be calculated later.

### 8.2.1 An example with a rank-2 separable state

For example, choosing the Witness operator $W = \sum_k p(kk|22)$, that is $\widehat{W} = \sum_k A_{k|2} \otimes B_{k|2}$, one obtains the following optimisation problem:

$$\begin{aligned} P_g = \quad & \max_{\rho_{ABE},\{E_e\}} \sum_{e,b} \mathrm{Tr}(\rho_{ABE}\, A_{e|1} \otimes B_{b|1} \otimes E_e) \\ \text{s.t.} \quad & \mathrm{Tr}(\widehat{W} \otimes \mathbb{1}\ \rho_{ABE}) = W, \\ & \rho_{ABE} \geq 0, \\ & \mathrm{Tr}(\rho_{ABE}) = 1, \\ & E_e \geq 0\ \forall e, \\ & \sum_e E_e = \mathbb{1}, \end{aligned} \tag{8.4}$$

where the conditions of the density matrix were used and Eves measurement. The SDP can be reformulated by merging the variables $\rho_{ABE}$ and $\{E_e\}$ as well as by defining $\rho_e \equiv \mathrm{Tr}_E(\rho_{ABE}\ \mathbb{1} \otimes \mathbb{1} \otimes E^e)$:

$$\begin{aligned} P_g = \quad & \max_{\{\rho_e\}} \sum_e \mathrm{Tr}(\rho_e A_{e|1} \otimes \mathbb{1}) \\ \text{s.t.} \quad & \mathrm{Tr}(\widehat{W} \sum_e \rho_e) = W, \\ & \rho_e \geq 0\ \ , \forall e, \\ & \mathrm{Tr}(\sum_e \rho_e) = 1, \end{aligned} \tag{8.5}$$

For example, if one sets $d = 2$ and $W = 1$, they would obtain $P_g^* = 1/2$, i.e. the lowest possible guessing probability. Then, the corresponding state of Alice and Bob $\rho_{AB} = \sum_e \rho_e$ can be taken to be equal to $\widehat{W}$.
There are different ways to find such a solution. In section 8.3 a general solution will be tried to find by solving the SDP analytically through the use of the dual function of the SDP.
By rewriting 8.6, it can be found as :

$$\begin{aligned} P_g(W,d) = \quad & \max_{\{\rho_e\}_e} \sum_e^{d-1} \mathrm{Tr}(\rho_e \, A_*^e \otimes \mathbb{1}_d) \\ \text{s.t.} \quad & \mathrm{Tr}(\widehat{W} \sum_e^{d-1} \rho_e) = W, \\ & \rho_e \geq 0, \quad \forall e \in \{0,...,d-1\}, \\ & \mathrm{Tr}(\sum_e^{d-1} \rho_e) = 1 \end{aligned} \tag{8.6}$$

## 8.3 Solving SDP by hand

Solving the SDP in Matlab or other mathematical programs is the easiest way to get quick solutions to the problem. But because of the nature of the Hilbert space, the problem grows with the dimension $d^2$. To get enough data for a useful plot, calculation times take hours just for $d = 10$. To avoid this problem, the SDP will be solved by hand. This was already done in [1], but the proof is not clear enough to be able to follow their train of thought. The proof will be improved in this thesis by a step by step instructions and solving the SDP. In essence, the proof which is used consists of three parts. Later, it will be tried to improve the SDP to find a more resistant way of quantum communication against noise 10.3. There, these 3 steps will be followed again.

**Step 1: Finding the dual function**

From the problem in equation 10.4, one can find the dual function. The solutions of the primal and dual functions bound the optimal value of the problem.

$$\begin{aligned} P_g = \quad & \min_{\gamma,S} \gamma + SW \\ \text{s.t.} \quad & \gamma \mathbb{1}_{d^2} + S\widehat{W} \geq |e\rangle \langle e| \otimes \mathbb{1}_d \quad \forall e \end{aligned} \tag{8.7}$$

**Step 2: Finding the eigenvalues**

This is just an eigenvalue problem which can be solved with the eigenvalues $\lambda$ of $S\widehat{W} - |e\rangle \langle e| \otimes \mathbb{1}_{d^2}$.

$$\lambda_\pm = \frac{S-1}{2} \pm \frac{\sqrt{(S-1)^2 + 4S(d-1)/d}}{2} \qquad \lambda_0 = 0 \tag{8.8}$$

For any dimension $d$, one can only find two non-zero eigenvalues $\lambda_\pm$ whereas all other eigenvalues are $\lambda_0 = 0$.
If $\lambda_- \leq 0$, one can find $\frac{\partial \lambda_-}{\partial S} = W$

$$W = \frac{1}{2}\left(1 - \frac{2S + 2 - \frac{4}{d}}{2\sqrt{(S-1)^2 + 4S(d-1)/d}}\right) \quad S = \frac{2}{d} - 1 + \frac{1-2W}{d}\sqrt{\frac{d-1}{W(1-W)}}$$

$$\lambda_- = -\frac{d-1}{d} - \frac{W}{d}\sqrt{\frac{d-1}{W(1-W)}} \tag{8.9}$$

**Step 3: Summarize**

In the end, the SDP can be written as

$$\begin{aligned} P_g = \quad & \min_{\gamma,S} \gamma + SW \\ \text{s.t.} \quad & \gamma + \lambda_- \geq 0 \end{aligned} \tag{8.10}$$

with the guessing probability $P_g = -\lambda_- + SW$

### 8.3.1 Finding Eigenvalue

Above, the eigenvalue was introduced without further considering it. Therefore, the eigenvalues will be derived for any dimension in this section. This is also a proof for the above equations.
Because of the guessing probability $P_g \leq 0$, one can rearrange the constraint and the primal function to the variable $\gamma$. Hence, since the goal is to find the minimal solution of the guessing probability, both expressions must be equal. In the second step, one can make use of the fact that the eigenvalues do not change by applying a unitary transformation. Therefore, the problem can be simplified to

$$U(S\widehat{W} - |e\rangle\langle e| \otimes \mathbb{1})U^\dagger = S|0\rangle\langle 0| - A \tag{8.11}$$

for some matrix $A$ with the rank 1 and the unitary transformation $U$.

### 8.3.2 Proof

Now, solely the eigenvalues of the above expression 8.11 need to be found. This sounds like an easy task, however, on a closer look, it becomes apparent that it is harder than initially expected. This is the part where mathematics is becoming a form of art.
One needs to divide the proof into steps which use some relations. In the first step, it will be shown that the eigenvalues are the same for all $e$.

$$U(S\widehat{W} - |e\rangle\langle e| \otimes \mathbb{1})U^\dagger = S\widehat{W} - |0\rangle\langle 0| \otimes \mathbb{1} \tag{8.12}$$

**Relation 1**

$$\widehat{W} = \sum_{t=0}^{d-1} |\Psi_t\rangle \langle\Psi_t| \otimes (|\Psi_t\rangle \langle\Psi_t|)^T = \sum_{b=0}^{d-1} |B_{0,b}\rangle \langle B_{0,b}| \tag{8.13}$$

with the general Bell state $|B_{a,b}\rangle = \mathbb{1} \otimes (X^b Z^a) |\Phi^+\rangle$ for $a, b \in \mathbb{N}$, $Z, X$, the general Pauli matrices $X_d |j\rangle = |j+1\rangle$, $Z_d |j\rangle = \omega^j |j\rangle$ (for $j = d-1$ and $\omega = \exp[2\pi i/d]$) and $|\Phi^+\rangle$ the Bell state for any dimension.

**Proof:** To prove this relation, it is necessary to recap how the state looks like. From section 8.2 and 8.2.1, we can conclude that $|\Psi_t\rangle = U|t\rangle$ for $t \in \mathbb{N}$ and the unitary transformation $U = \frac{1}{\sqrt{d}} \sum_{ij} \omega^{ij} |i\rangle \langle j|$

$$\sum_{t=0}^{d-1} |\Psi_t\rangle \langle\Psi_t| \otimes (|\Psi_t\rangle \langle\Psi_t|)^T = \sum_{t=0}^{d-1} U |t\rangle \langle t| U^\dagger \otimes U^* |t\rangle \langle t| U^T \tag{8.14}$$

extracting the unitary transformation leads to

$$= U \otimes U^* \left( \sum_{t=0}^{d-1} |t\rangle \langle t| \otimes |t\rangle \langle t| \right) U^\dagger \otimes U^T = \sum_{b=0}^{d-1} \mathbb{1} \otimes X^b |\Phi^+\rangle \langle\Phi^+| \mathbb{1} \otimes X^{-b} \tag{8.15}$$

the right hand side is the right hand side of the relation which we want to show.

$$\sum_{t=0}^{d-1} |t\rangle \langle t| \otimes |t\rangle \langle t| = U^\dagger \otimes U^T \left( \sum_{b=0}^{d-1} \mathbb{1} \otimes X^b |\Phi^+\rangle \langle\Phi^+| \mathbb{1} \otimes X^{-b} \right) U \otimes U^* \tag{8.16}$$

using the mixed product property

$$= \sum_{b=0}^{d-1} U^\dagger \otimes U^T X^b |\Phi^+\rangle \langle\Phi^+| U \otimes X^{-b} U^* \tag{8.17}$$

in the next step, a simple relation $\mathbb{1} \otimes X^b |\Phi^+\rangle = (X^b)^T \otimes \mathbb{1} |\Phi^+\rangle = X^{-b} \otimes \mathbb{1} |\Phi^+\rangle$ is used to rearrange the equation

$$= \sum_{b=0}^{d-1} U^\dagger X^{-b} U \otimes \mathbb{1} |\Phi^+\rangle \langle\Phi^+| U^\dagger X^b U \otimes \mathbb{1} \tag{8.18}$$

In the next step, the part $U^\dagger X^{-b} U$ is for interest.

$$U^\dagger X^{-b} U = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \omega^{-ij} |i\rangle \langle j| \sum_{s=0}^{d-1} |s\rangle \langle s \oplus b| \frac{1}{\sqrt{d}} \sum_{k,l=0}^{d-1} |k\rangle \langle l| \tag{8.19}$$

$$= \frac{1}{d} \sum_{i,j,s,k,l=0}^{d-1} \omega^{-ij+kl} |i\rangle \underbrace{\langle j|s\rangle}_{=\delta_{js}} \underbrace{\langle s \oplus b|k\rangle}_{\delta_{k,s}} \langle l| = \frac{1}{d} \sum_{i,j,l=0}^{d-1} \omega^{j(l-i)+bl} |i\rangle \langle l| \tag{8.20}$$

from the orthogonality of the root of unity, it is possible to sum over all summation such that $\sum_s \omega^{sf} = d\delta_{\delta,0}$. Using this for the above equation:

$$U^\dagger X^{-b} U = \sum_{i=0}^{d-1} \omega^{bi} |i\rangle \langle i| \tag{8.21}$$

Similar to this consideration, the other side can be found as $U^\dagger X^b U = \sum_{b,j} \omega^{-bj} |j\rangle \langle j|$. Inserting these results into equation 8.18 gives the expression:

$$U^\dagger \otimes U^T \left( \sum_{b=0}^{d-1} \mathbb{1} \otimes X^b |\Phi^+\rangle \langle \Phi^+| \mathbb{1} \otimes X^{-b} \right) U \otimes U^* = \sum_{b,i,j=0}^{d-1} (\omega^{bi} |i\rangle \langle i| \otimes \mathbb{1}) |\Phi^+\rangle \langle \Phi^+| (\omega^{-bj} |j\rangle \langle j| \otimes \mathbb{1} \tag{8.22}$$

$$= \sum_{b,i,j=0}^{d-1} \omega^{b(i-j)} (|i\rangle \langle i| \otimes \mathbb{1}) |\Phi^+\rangle \langle \Phi^+| (|j\rangle \langle j| \otimes \mathbb{1}) \tag{8.23}$$

Now, the orthogonality of the root of unity can be used again.

$$= d \sum_{i=0}^{d-1} (|i\rangle \langle i| \otimes \mathbb{1})(|\Phi^+\rangle \langle \Phi^+|)(|i\rangle \langle i| \otimes \mathbb{1}) \tag{8.24}$$

Now, bringing the definition of the bell state into the equation $|\Phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |kk\rangle$

$$= d \sum_{i,k,l=0}^{d-1} \frac{1}{d} (|i\rangle \langle i| \otimes \mathbb{1})(|k\rangle \langle l| \otimes |k\rangle \langle l|)(|i\rangle \langle i| \otimes \mathbb{1}) \tag{8.25}$$

$$= \sum_{i,k,l=0}^{d-1} (|i\rangle \underbrace{\langle i|k\rangle}_{\delta_{i,k}} \langle l| \otimes |k\rangle \langle l|)(|i\rangle \langle i| \otimes \mathbb{1}) = \sum_{i,l=0} |i\rangle \underbrace{\langle l|i\rangle}_{\delta_{i,l}} \langle i| \otimes |i\rangle \langle l| \tag{8.26}$$

$$= \sum_{i=0}^{d-1} |i\rangle \langle i| \otimes |i\rangle \langle i| \tag{8.27}$$

which is the desired form of equation 8.16.

### Relation 2

Here, it will be shown that a unitary transformation has no impact on $\widehat{W}$.

$$\mathbb{1} \otimes X^e \widehat{W} (\mathbb{1} \otimes X^e)^\dagger = \widehat{W} \tag{8.28}$$

*Proof:* One can use the definition which was derived from Relation 1 8.13 and the definition of $|B_{a,b}\rangle$

$$\mathbb{1} \otimes X^e \left|B_{0,b}\right\rangle \left\langle B_{0,b}\right| (\mathbb{1} \otimes X^e)^\dagger \tag{8.29}$$

$$= \sum_{b=0}^{d-1} \underbrace{(\mathbb{1} \otimes X^e)(\mathbb{1} \otimes X^b}_{\mathbb{1} \otimes X^{eb}} \left|\Phi^+\right\rangle)(\left\langle\Phi^+\right| \underbrace{\mathbb{1} \otimes (X^b)^\dagger)(\mathbb{1} \otimes X^e)^\dagger)}_{\mathbb{1} \otimes (X^{be})^\dagger} \tag{8.30}$$

$$= \sum_{b'=0}^{d-1} (\mathbb{1} \otimes X^{b'} \left|\Phi^+\right\rangle)(\left\langle\Phi^+\right| \mathbb{1} \otimes (X^{b'})^\dagger) = \widehat{W} \tag{8.31}$$

Because $S$ is just a variable, the first part $S\widehat{W}$ of equation 8.12 does not contribute to the calculation of the eigenvalues.

**Relation 3**

On the first view, one might think that all eigenvalues for all $e \in d+1$ need to be calculated independently. However, only the eigenvalues for $\left|0\right\rangle \left\langle 0\right|$ need to be calculated, because the eigenvalues are equal for all $e \in d+1$:

$$X^e \left|0\right\rangle \left\langle 0\right| (X^e)^\dagger = \left|e\right\rangle \left\langle e\right| \tag{8.32}$$

*Proof:* Relation 3 follows by calculating $X^e \left|0\right\rangle \left\langle 0\right| (X^e)^\dagger$ for $d = e+1$
For $e = 1$

$$\sum_{j=0}^{d-1} (\left|j+1\right\rangle \left\langle j|0\right\rangle = \left|1\right\rangle \tag{8.33}$$

and for $e = 2$

$$\sum_{j,j',=0}^{d-1} \left|j+1\right\rangle \left\langle j|j'+1\right\rangle \underbrace{\left\langle j'|0\right\rangle}_{0 \text{for} j'=0} = \left|2\right\rangle \tag{8.34}$$

It follows that the $X$ operator acting on the state $\left|0\right\rangle$ increases the state by 1. Therefore, $X^e \left|0\right\rangle = \left|e\right\rangle$ can be found and similarly $\left\langle 0\right| (X^e)^\dagger$.

$$X^e \left|0\right\rangle \left\langle 0\right| (X^e)^\dagger = \left|e\right\rangle \left\langle e\right| \tag{8.35}$$

### 8.3.3 Simplifying

Through these three relations, it was shown that it is only necessary to calculate the eigenvalues in one specific case for a given dimension. All the other eigenvalues are equal. Therefore, one only has to compute the eigenvalues of $S\widehat{W} - \left|0\right\rangle \left\langle 0\right| \otimes \mathbb{1}$.

The second step is to show

$$U(S\widehat{W} - \left|0\right\rangle \left\langle 0\right| \otimes \mathbb{1})U^\dagger = S \left|0\right\rangle \left\langle 0\right| - A \tag{8.36}$$

Here the unitary transformation is used

$$U = \sum_{a,b}^{d-1} |a,b\rangle \langle B_{a,b}| \tag{8.37}$$

Applied to the problem, the first term can be found

**Relation 4**

$$S\widehat{UW}U^\dagger = S\,|a,b\rangle \langle B_{a,b}|B_{0,b}\rangle \langle B_{0,b}|B_{a,b}\rangle |a,b\rangle$$

$$= \sum_{b=0}^{d-1} |0,b\rangle \langle 0,b| = |0\rangle \langle 0| \otimes \mathbb{1} \tag{8.38}$$

**Relation 5**

The second part of the above equation 8.36 is more challenging than one might initially expect. A matrix $A$ will be introduced which definition follows by the proof.

$$U(|0\rangle \langle 0| \otimes \mathbb{1})U^\dagger = A \otimes \mathbb{1} \tag{8.39}$$

*Proof:* Because this proof is much more complex, it is better to divide it into steps. First, one needs to consider

$$K = U(|0\rangle \otimes \mathbb{1}) \tag{8.40}$$

so that

$$KK' = U(|0\rangle \langle 0| \otimes \mathbb{1})U' \tag{8.41}$$

The second part of the equation 8.12 has been defined as a vector $K$ applied by some unitary transformation which, as it is already known, has no impact on the eigenvalues in the end. The expression $K$ can be simplified as

$$K = \sum_{a,b=0}^{d-1} |a,b\rangle \langle B_{a,b}| \,(|0\rangle \otimes \mathbb{1}) \tag{8.42}$$

$$= \sum_{a,b=0}^{d-1} |a,b\rangle \langle \Phi^+| \,(\mathbb{1} \otimes X^b Z^a)^\dagger (|0\rangle \otimes \mathbb{1}) \tag{8.43}$$

$$= \sum_{a,b=0}^{d-1} |a,b\rangle \langle \Phi^+| \,(|0\rangle \otimes X^b Z^a)^\dagger \tag{8.44}$$

$$= \sum_{a,b=0}^{d-1} \sum_{i}^{d-1} |a,b\rangle \frac{1}{\sqrt{d}} \langle ii| \,(|0\rangle \otimes X^b Z^a)^\dagger \tag{8.45}$$

$$= \sum_{a,b=0}^{d-1} \sum_{i}^{d-1} |a,b\rangle \frac{1}{\sqrt{d}} \underbrace{\langle i|0\rangle}_{=1 \text{ for } i=0} \otimes \langle i| X^b Z^a)^\dagger \tag{8.46}$$

$$= \sum_{a,b=0}^{d-1} |a,b\rangle \frac{1}{\sqrt{d}} \langle 0| X^b Z^a)^\dagger \tag{8.47}$$

Considering now that $a = 0$

$$= \sum_{b=0}^{d-1} |0,b\rangle \frac{1}{\sqrt{d}} \langle 0| X^b \mathbb{1})^\dagger \tag{8.48}$$

$$= \frac{1}{\sqrt{d}} \sum_{b=0}^{d-1} \sum_{k}^{d-1} |0,b\rangle \langle 0| (|j\rangle \langle j+1|)^b \tag{8.49}$$

$$= \frac{1}{\sqrt{d}} \sum_{k}^{d-1} (|0,0\rangle \langle 0| + \sum_{j} |0,1\rangle \underbrace{\langle 0|j\rangle}_{=1 \text{for } j=0} \langle j+1| +$$

$$\sum_{j',j''} \underbrace{\langle 0|j'\rangle}_{1 \text{if} j'=0} \underbrace{\langle j'+1|j''\rangle}_{1 \text{if} j''=j'+1} \langle j''+1| + ...) \tag{8.50}$$

Therefore, one can find

$$= \frac{1}{\sqrt{d}} \sum_{a,b=0}^{d-1} |0,b\rangle \langle b| \tag{8.51}$$

Now, one need to consider the case that $b = 0$ and $a \in \mathbb{N}$

$$= \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a,0\rangle \langle 0| (Z^a)^\dagger \tag{8.52}$$

$$= \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} \sum_{j=0}^{d-1} |a,0\rangle \langle 0| (\omega'^j |j\rangle \langle j|)^a \tag{8.53}$$

$$= \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} \sum_{j,j',j''=0}^{d-1} |0,0\rangle \langle 0| + \omega'^{j} |1,0\rangle \underbrace{\langle 0|j\rangle}_{1 \text{if} j=0} \langle j| + \omega'^{2j'j''} |2,0\rangle \underbrace{\langle 0|j'\rangle \langle j'|j''\rangle}_{1 \text{if} j'=j''=0} \langle j''| + ... \tag{8.54}$$

$$= \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a,0\rangle \langle 0| \tag{8.55}$$

Because of the fact that the Pauli matrices and their multiple acts are independent, the equation can be summarised as 8.42

$$K = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} |a,b\rangle \langle b| \tag{8.56}$$

Therefore,

$$KK' = \frac{1}{\sqrt{d}} \sum_{a,b=0}^{d-1} \sum_{c,d}^{d-1} |a,b\rangle \underbrace{\langle b|d\rangle}_{1 \text{if} d=b} \langle c,d| \tag{8.57}$$

$$= \frac{1}{\sqrt{d}} \sum_{a,c}^{d-1} |a\rangle \langle c| \otimes \mathbb{1} = A \otimes \mathbb{1} \tag{8.58}$$

It was shown that the expression $|0\rangle \langle 0| \otimes \mathbb{1}$ can be expressed by a matrix $A = \frac{1}{\sqrt{d}} \sum_{a,c}^{d-1} |a\rangle \langle c|$ $\forall a, c \in \mathbb{N}$. Lastly, the eigenvalues of the expression solely need to be computed.

$$S |0\rangle \langle 0| - \frac{1}{\sqrt{d}} \sum_{a,c}^{d-1} |a\rangle \langle c| = S |0\rangle \langle 0| - A \tag{8.59}$$

For $d = 2$, one can find the eigenvalue

$$\lambda_{\pm} = \frac{S-1}{2} \pm \sqrt{\frac{(S-1)^2}{4} + \frac{S}{2}} \qquad \lambda_0 = 0 \tag{8.60}$$

This resembles the eigenvalue in equation 8.8 to a high degree. Truly, the general eigenvalues for $d \in \mathbb{N}$ of the equation 8.59 are described by the above eigenvalues 8.8. For finding the guessing probability and consequently solving the SDP, one just has to follow the derivative of the steps which was discussed in chapter 8.3.

### 8.3.4 Key rate

Alice and Bob want to build a secure and resistant quantum channel to share a key which can only be seen by both of them. This can be quantified by the key rate $K$. In the case of subspace selection one has to deal with $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. The protocol of Mirdit Doda et al. [1] divides the quantum system into $l$ subspaces of the sizes $k$ $\mathcal{H}_A = \mathcal{H}_{A0} \oplus \mathcal{H}_{A1} \oplus \cdots \oplus \mathcal{H}_{Al}$ and $\mathcal{H}_B = \mathcal{H}_{B0} \oplus \mathcal{H}_{B1} \oplus \cdots \oplus \mathcal{H}_{Bl}$.
The key rate can be found as

$$K \geq H(X|E_T) - H(X|Y) \tag{8.61}$$

with $H(X|E_T)$ as the von Neumann entropy of Alice's key outcome $X$ in respect of the total information available to Eve as it was discussed in 5.2. $H(X|Y)$ is the conditional Shannon entropy with Alice's key outcome $X$ and Bob's key outcome $Y$. Here a minimal bound of the key rate $K_m$ can be found for an effective state $\tilde{\rho}^m$ between Alice and Bob.

$$K_m = H_{\min}(X'|E_T)_{\tilde{\rho}^m} - H(X'|Y')_{\tilde{\rho}^m} \tag{8.62}$$

It is possible to extract a key rate $K(\rho)$ from a given protocol which uses subspace post-selection. The key rate can be found as

$$K_j(\rho) = P(I_j, I_j) K \left( \frac{(\mathbb{1}_I \otimes \mathbb{1}_I)\rho(\mathbb{1}_I \otimes \mathbb{1}_I)}{P(I_j, I_j)} \right) \tag{8.63}$$

The total key rate is just the summation over all subspaces $n$ $K_{\text{Tot}} = \sum_{j=1}^{n} K_j(\rho)$. Finally, the concluding and total key rate which is needed can be found as the upper bound of the key rate whereby Alice and Bob probably observe an outcome in subspace $m$.

$$K_{\text{Tot}} \geq \sum_{m=0}^{l-1} P(M = m) K_m \tag{8.64}$$

Considering the definition of the von Neumann entropy and the guessing probability $P_g^e$ of Eve described in the previous chapters, one can find a lower bound of $H_{\min}(X'|E_T)_{\tilde{\rho}^m} = -\log P_g^e$. For the second term (the key between Alice and Bob), one can consider the fact that the key probability of the outcome on both sides depends on the different measurements $\{A_1^x\}_{x=0}^{d-1}$ and $\{B_1^y\}_{y=0}^{d-1}$ of the shared quantum state $|\Psi_{AB}\rangle$ with $\langle\Psi_{AB}| A_1^x \otimes B_1^y |\Psi_{AB}\rangle = \text{tr}(|x\rangle\langle x| \otimes |y\rangle\langle y| \rho_{AB})$. Therefore, one can find the probability for equal outcomes between Alice and Bob in the first basis

$$P^{AB}(x, y) = \sum_{k=0}^{d-1} P_{AB}(xy|11) \tag{8.65}$$

with $\rho_{AB} = v|\psi^+\rangle\langle\psi^+| + \frac{1-v}{d^2}\mathbb{1}_{d\otimes d}$ and $|\psi^+\rangle = \sum_{i=0}^{d-1} \frac{1}{\sqrt{d}} |ii\rangle$. For the conditional Shannon entropy, one has to sum over all outputs of Alice and Bob

$$P_{AB} = \text{tr}(|x\rangle\langle x| \otimes |y\rangle\langle y| \rho_{AB}) = \sum_{j=0}^{d-1} \langle j| (|x\rangle\langle x| \otimes |y\rangle\langle y|) \rho_{AB} |j\rangle \tag{8.66}$$

$$= \sum_{j=0}^{d-1} \langle j| (|x\rangle\langle x| \otimes |y\rangle\langle y|)(v|\psi^+\rangle\langle\psi^+| + \frac{1-v}{d^2}\mathbb{1}_{d\otimes d}) |j\rangle$$

$$= \sum_{j=0}^{d-1}\sum_{i=0}^{d-1} \frac{v}{d} \underbrace{\langle j| (|x\rangle\langle x| \otimes |y\rangle\langle y|)(|ii\rangle\langle ii|) |j\rangle}_{1\delta_{xy}} + \frac{1-v}{d^2} \sum_{j=0}^{d-1}\sum_{i=0}^{d-1} \underbrace{\langle j| (|x\rangle\langle x| \otimes |y\rangle\langle y|)\mathbb{1}_{d\otimes d} |j\rangle}_{1}$$

$$= \frac{v}{d}\delta_{xy} + \frac{1-v}{d^2}$$

To get to know the outcome probability of Alice, it is necessary to do the summation of all possible outcomes of Bob. This leads to

$$P_{AB}(y) = \sum_{y=0}^{d-1} P_{AB}(x, y) = \frac{v}{d} + \frac{1-v}{d^2} d = \frac{1}{d} \tag{8.67}$$

$$H(X|Y) = -\sum_{x,y=0}^{d-1} P_{AB}(x,y)\log_2\left(\frac{P_{AB}(x,y)}{P_{AB}(y)}\right) \tag{8.68}$$

$$H(X|Y) = -\sum_{x,y=0}^{d-1}\left(\frac{v}{d}\delta_{xy}+\frac{1-v}{d^2}\right)\log_2\left(v\delta_{xy}+\frac{1-v}{d}\right) \tag{8.69}$$

$$= -\left(v+\frac{1-v}{d}\right)\log_2(v+\frac{1-v}{d}) - \left(\frac{1-v}{d}(d-1)\right)\log_2\left(\frac{1-v}{d}\right) \tag{8.70}$$

In the end, the lower bound of the key rate can be found as

$$K_{tot} = \sum_{m=0}^{l-1} P(M=m)K_m \geq \sum_{m=0}^{l-1} P(M=m)(-\log(P_g^e) - H(X|Y)) \tag{8.71}$$

### 8.3.5 for $k$ subspaces

Now, the conditional Shannon entropy $H(X|Y)$ can be computed

$$H(X|Y) = -\sum_{x,y=0}^{k-1} P_k^{AB}(x,y)\log_2\left(\frac{P_k^{AB}(x,y)}{P_k^{AB}(y)}\right) \tag{8.72}$$

$$\Pi_k = \sum_{i,j}^{k-1} |i\rangle\langle i| \otimes |j\rangle\langle j| \tag{8.73}$$

Is the projector onto the $m=0$ subspace of size $k$. The state projected onto this subspace is then

$$\rho_k^{\text{iso}} = \frac{\Pi_k \rho_{AB} \Pi_k}{\text{tr}(\Pi_k \rho_{AB})} \tag{8.74}$$

Note that the state will be the same for all other $m$, so $m=0$ can be used without hesitation.
Therefore, for $k$ subspaces one gets a state which looks like the isotropic state $\rho_k^{\text{iso}} = \frac{v}{k}\sum_{i=0}^{k-1}|ii\rangle\langle ii| + \frac{1-\tilde{v}}{k^2}\mathbb{1}_{d^2}$ with $\tilde{v} = \frac{vd}{vd+k-vk}$

$$P_k^{AB}(x,y) = \text{tr}(|x\rangle\langle x| \otimes |y\rangle\langle y|\, \rho_k^{\text{iso}}) \tag{8.75}$$
$$= \frac{\tilde{v}}{k}\delta_{xy} + \frac{1-\tilde{v}}{k^2}$$

$$P_k^{AB}(y) = \sum_{y=0}^{k-1} P_k^{AB}(x,y) = \frac{\tilde{v}}{k} + \frac{1-\tilde{v}}{k^2}k = \frac{1}{k} \tag{8.76}$$

$$H(X|Y)_k = -\sum_{x,y=0}^{k-1} \left(\frac{\tilde{v}}{k}\delta_{xy} + \frac{1-\tilde{v}}{k^2}\right) \log_2 \left(\tilde{v}\delta_{xy} + \frac{1-\tilde{v}}{k}\right) \tag{8.77}$$

$$= -\left(\tilde{v} + \frac{1-\tilde{v}}{k}\right) \log_2(\tilde{v} + \frac{1-\tilde{v}}{k}) - \left(\frac{1-\tilde{v}}{k}(k-1)\right) \log_2 \left(\frac{1-\tilde{v}}{k}\right) \tag{8.78}$$

Similar to the case for $d = k$, the key rate can be found as

$$K_{tot} \geq \sum_{m=0}^{l-1} P(M=m) K_m^k \geq \sum_{m=0}^{l-1} P(M=m)(-\log_2(P_m) - H(X|Y)_k) \tag{8.79}$$

In the end, there is:

$$K_{tot} \geq \frac{vd + k - vk}{d} \left(-\log_2(P_{\tilde{v},k}) - H(X|Y)_{\tilde{v},k}\right) \tag{8.80}$$

## 8.4 Results

In section 8.3, the mathematical concept of such a problem was derived and solved and a solution of the SDP for the guessing probability was found.

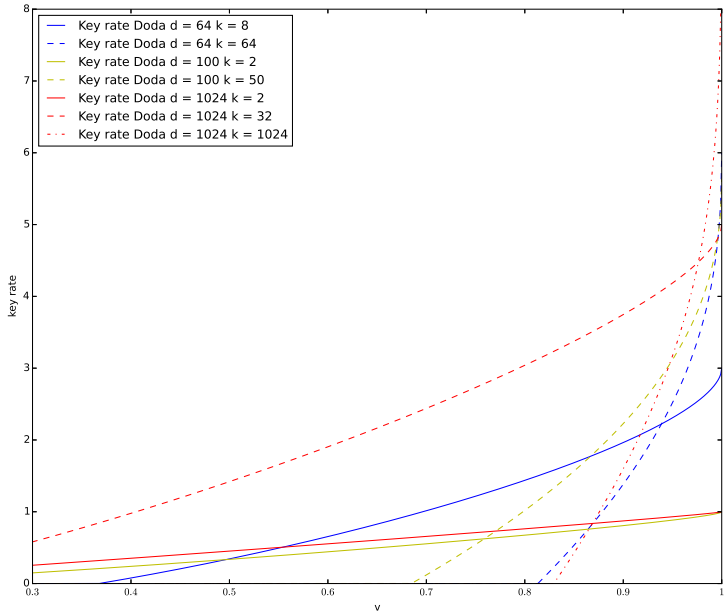


Figure 8.1: Key rate against visibility $v$. Here, $v$ is used as a general value which are all kinds of noise included for different dimension and subspaces.

The visibility includes all noise effects which could happen in the quantum system. It was already discussed in section 5.4 which effect $v$ has on a quantum state like 5.13. The results of above figure 8.1 are based on Mirdit Doda's calculations from his paper [1]. The number of subspaces $l$ which are used depends on the dimension and their size $k$. In other words, $d = l \cdot k$. Further, one can see that the key rate shows a more increasing behaviour if more subspaces are used. Moreover, as it can be concluded from this figure above, there is a strong correlation between the improvement of the key rate depending on the subspace which is used. As it was discussed by Mirdit Doda et al. [1], there is an optimal number of subspaces for each dimension which have to be figured out.

## 8.5 Why does this protocol work?

One may ask why the protocol works, or in other words, why dividing a $d$-dimensional Hilbert space into subspaces in QKD improves a quantum channel in the resistance to noise. Here, it was tried to describe a more intuitive procedure on how to approach such

an understanding. For this consideration, it is possible to go back to the main foundation of quantum entanglement, namely the Bell inequality.

### 8.5.1 EPR Paradoxon and Bell inequality

The essence of Bell's consideration which leads to his famous Bell inequality was the Gedankenexperiment of Einstein, Podolsky, Rosen (EPR Paradoxon) [48]. They claimed that quantum mechanics is not complete and that there are some existing hidden variables. In the paper in which Einstein, Podolsky and Rosen proposed their EPR paradoxon, they claimed that there have to be some hidden variables $\lambda$ which pre-determine the outcome in such a way that the state is locally defined. In Bell's words, "$\lambda$ denote any number of hypothetical additional variables needed to complete quantum mechanics in the way envisioned by EPR" [49]. Or as he mentioned in [50], "[...] the result of a measurement on one system to be unaffected by operations on a distant system with which it has interacted in the past, that creates the essential difficulty."
He disproved Einstein, Podolsky and Rosen with a simple mathematical disprove. Consider a two measurements on Alice and Bob's side $A_{a|x}$, $B_{b|y}$, where $a, b$ denote the outcome of the measuring setting $x, y$. By measuring a state $\rho$, the probability of outcome $a, b$ in the setting $x, y$ can be detected [51]

$$p(ab|xy) = \mathrm{Tr}(A_{a|x} \otimes B_{b|y}\rho) \tag{8.81}$$

In the sense of the local realism in the EPR paradoxon, the following relation should hold.

$$\mathrm{Tr}(A_{a|x} \otimes B_{b|y}\rho) = \int_\lambda d\lambda P(\lambda) p_A(a|x,\lambda) p_B(b|y,\lambda) \tag{8.82}$$

Here $P(\lambda)$ describes the density function of a hidden variable.
There are many ways to disprove the above relation and it is true that

$$\mathrm{Tr}(A_{a|x} \otimes B_{b|y}\rho) \neq \int_\lambda d\lambda P(\lambda) p_A(a|x,\lambda) p_B(b|y,\lambda) \tag{8.83}$$

The nature of quantum physics lies in the interpretation of this relation. The physics of such systems is not pre-defined by a hidden variable. The physics in this system is non-local. A measurement on one side influences the measurement on the other side and vice versa. Albert Einstein called this a "spooky action at a distance"[1].

### 8.5.2 Example

The Bell inequality can be interpreted in different ways and therefore, there is more than one clear definition of his inequality. In the following, an example of this theory will be given by considering Nielsen and Chuang's book [8].
For further clarification, the example of Alice and Bob will be utilised again. Alice and

[1] This expression from Einstein was given quite a few times in papers and articles but there cannot be found any origin text. It is assumed that it was an oral transmission from Einstein.

Bob share a quantum channel whereby Alice wants to send a key to Bob. Both are able to apply two different measurements on the system which are labeled $P_Q$ and $P_R$ on Alice's side and $P_S$ and $P_T$ on Bob's side. The outcomes of these measurements are $\pm 1$. Both choose their measurements randomly and do not know in which bases they measure. Moreover, after receiving the quantum state they measure simultaneously and independently. In summary, there is a quantum channel with two parties named Alice and Bob. Both choose a measurement out of a measurement set consisting of two possibilities. The outcome of their independent and random measurements are some objective properties ($Q$,$R$,$S$,$T$, respectively to the measurements) of which the value can be either $+1$ or $-1$.
By doing some simple algebra, the system can be quantified by considering each possible outcome

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T \tag{8.84}$$

It follows that $QS + RS + RT - QT = 2$ because either $(Q + R)S$ or $(R - Q)T$ is equal to zero.
The *Bell inequality* or the also known CHSH inequality is found as

$$\mathbf{E}(QS) + \mathbf{E}(RS) + \mathbf{E}(RT) - \mathbf{E}(QT) \leq 2 \tag{8.85}$$

$\mathbf{E}(\ldots)$ denotes the mean value of a quantity. Here, it was considered that there is a probability $p(Q, R, S, T)$ in which the state could be before the measurements. The mean value therefore reads as follows: $\mathbf{E}(QS) = \sum_{QRST} p(Q, R, S, T)QS$. This means with the probability $p(Q, R, S, T)$ Alice and Bob were measured with the measurement setting $P_Q$ and $P_S$ in such a way that the outcome $Q$ and $S$ were objected.
This consideration was a more classical description of this problem. In quantum physics, both parties share a bell state, for example $|\Psi\rangle = 1/\sqrt(2)(|01\rangle - |10\rangle)$. As one already knows, an observable classifies a measurement. Similar to the above measurements of Alice and Bob, the observables can be found

$$\begin{aligned} Q = Z_1 \quad S = \frac{-Z_2 - X_2}{\sqrt{2}} \\ R = X_1 \quad T = \frac{Z_2 - X_2}{\sqrt{2}} \end{aligned} \tag{8.86}$$

Here,$Z, X$ are the Pauli matrices and the subscription denotes the qubit on which they act. Nevertheless, the mean values can be found as

$$\langle QS\rangle = \frac{1}{\sqrt{2}} \quad \langle RS\rangle = \frac{1}{\sqrt{2}} \quad \langle RT\rangle = \frac{1}{\sqrt{2}} \quad \langle QT\rangle = \frac{1}{\sqrt{2}} \tag{8.87}$$

This can be now inserted into the Bell equation:

$$\langle QS\rangle + \langle RS\rangle + \langle RT\rangle - \langle QT\rangle = 2\sqrt{2} \tag{8.88}$$

This is completely contradictory to what was just derived in the equation 8.85. However, this is the nature of quantum physics and at the same time, the essence which quantum

communication is based on. From a philosophical view on physics, this means that the assumptions - or at least one of them - on which the derivatives are based, is or are false. These aforementioned assumption are

1. "The assumption that the physical properties $P_Q$,$P_R$,$P_S$,$P_T$ have definite values $Q, R, S, T$ which exist independent of observation. This is sometimes known as the assumption of *realism* " [8]

2. "The assumption that Alice performing her measurement does not influence the result of Bob's measurement. This is sometimes known as the assumption of *locality*." [8]

### 8.5.3 Filtering

As it was discussed above, the basic conclusion of Bell's mathematical disprove is that nonlocal quantum entanglement exists. It was claimed that Bell's inequality can be seen as something untouchable, as something that satisfies all entangled quantum states. However, one may ask if all entangled quantum states violate Bell's inequality. Truly, Popescu showed that some states do not hold Bell's inequality [52]. More precisely, he gave an example in which he used a specific Werner state which is locally separated in two systems:

$$W = \frac{1}{d^2}\left(\frac{\mathbb{1}^{d\times d}}{d} + 2\sum_{i<j;i,j=1}^{d} |S_{ij}\rangle\langle S_{ij}|\right) \tag{8.89}$$

for a spin $1/2$ singlet state

$$|S_{ij}\rangle = \frac{1}{\sqrt{2}}(|i\rangle_1 |j\rangle_2 - |j\rangle_1 |i\rangle_2 \tag{8.90}$$

This state shows classical behaviour after a single perfect measurement. In other words, it does not correspond to Bell's inequality for entangled quantum states. On the other hand, this Werner state is clearly entangled and can even be used for quantum teleportation [53, 54] for example.
Nevertheless, Popescu examined what happens if there were two perfect measurements following after one another on each particle.
Here, the ideas of his publication will be recapped. Consider a Werner state of dimension $d \geq 5$ and a two-dimensional projection operator measurement on each particle

$$P = |1\rangle_{11}\langle 1| + |2\rangle_{11}\langle 2| \quad Q = |1\rangle_{22}\langle 1| + |2\rangle_{22}\langle 2| \tag{8.91}$$

These measurement operators are called *filters*. If these filter measurements are complete, Alice chooses the measurement operators of the second measurement. Note that a complete measurement describes the circumstance that if Alices possesses particle 1, she has to perform the measurement operator $P$. After this first measurement, Alice can choose between $A$ and $A'$ in such a way that their outcome is one of the three eigenvalues $1, -1, 0$. Their outcome can be $1, -1, 0$. In this case, the eigenvalues 1 and $-1$ are nondegenerate.

Their eigenstates belongs to the subspaces $\{|1\rangle_1, |2\rangle_1\}$ and $\{|1\rangle_2, |2\rangle_2\}$. On the contrary, the eigenvalues of 0 are highly degenerate. Their eigenstates belong to all the other subspaces in the Hilbert space $\{|3\rangle_2, ..., |d\rangle_2$. This is also applied to Bob in regards to the second measurement operators $B, B'$. As one can see, this leads to the algebraic version of Bell's inequality so that

$$\langle S_{12}| AB + AB' + A'B - A'B' |S_{12}\rangle = 2\sqrt{2} \tag{8.92}$$

At first, it might be confusing and probably several questions will arise.
*Which role do the first measurements of $P$ and $Q$ play?*
In fact, these measurements select the subensemble of the initial state. This subensemble selection is independent of the second measurement. Of course, one could also apply $A, A', B, B'$ directly to the state and then select the subensemble, but consider for example that the hidden variable is true and particle 1 yields by measuring in $A$ the value 1 and $A'$ would get 0. The outcome of $A$ would therefore be in the subensemble after the selection, depending on the outcome of particle 2. On the other hand, the outcome of $A'$ will not be in the selection.
A measurement of $P$ and $Q$ beforehand would force the state into one of the outcomes $\pm 1, 0$ without knowing which result would give the second measurement in the end. $P = 1$ would get $\pm 1$ of the second measurement, irrespective of whether someone measures in $A$ or $A'$.
*Which role does the second measurement $A, A', B, B'$ play?*
Quantum mechanics claims that the outcomes of all measurements have the same probability $P_1(A, \lambda)$ in the measurements. The result $\pm 1$ has the same probability as the result 0 in the measurement $A$ or $A'$. In the expression of local hidden variable theory as it was discussed in 8.5.1, this means

$$\int d\lambda \rho(\lambda) P_1(A = 0, \lambda) = \int d\lambda \rho(\lambda) P_1(A' = 0, \lambda) \tag{8.93}$$

for $\lambda$ as hidden variable and $\rho(\lambda)$ the probability distribution of $\lambda$. But it does not follow that $P_1(A = 0, \lambda) = P_1(A' = 0, \lambda)$. Which is also true for the general case. The consequence, this would support the hidden variable theory because it would conclude that there is a pre-defined variable which supports one outcome and hinder the outcome of the other one.

In short, Popescu showed that a mixed quantum state which would show classical behaviour in a Bell experiment can be tested as a quantum state via Bell's inequality by using filters.

### 8.5.4 Filters in subspace QKD

What does this mathematical concept of filtering have to do with the protocol and subspace selection?
In an unpublished sketched paper, Mirdit Doda derived the exact same consideration

as above by selecting a subspace of a state and showing that this state improves the visibility [45].
Now, it will be considered in an example of one subspace $S_I$ for dimension $k < d$. Here, $I$ is the set which spans the subspace and $k = [I]$ is the number of elements in $I$ (elements of the computational basis of $\mathcal{H}_A$ for Alice and of $\mathcal{H}_B$ for Bob). The projector of the subspace can be described as $\mathbb{1}_I = \sum_{i\in I} |i\rangle\langle i|$. The probability of both parties getting an outcome in $I$ for an entangled state $\rho$ is

$$P(I,I) = \mathrm{Tr}[(\mathbb{1}_I \otimes \mathbb{1}_I)\rho(\mathbb{1}_I \otimes \mathbb{1}_I)] \tag{8.94}$$

Thinking further, it can now be tried out what would happen if these projectors $\mathbb{1}_I$ would be applied on an isotropic state of the full Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$.

$$\rho_d(v) = v|\Psi_d^+\rangle\langle\Psi_d^+| + (1-v)\frac{\mathbb{1}_{d^2}}{d^2} \tag{8.95}$$

Similarly, the isotropic state $\rho_I$ in the subspace for visibility $v$ can be introduced here.

$$\rho_I(v) = v|\Psi_I^+\rangle\langle\Psi_I^+| + (1-v)\frac{\mathbb{1}_I \otimes \mathbb{1}_I}{k^2} \tag{8.96}$$

If a projector of the subspace is now applied to the full Hilbert space state, one gets

$$(\mathbb{1}_I \otimes \mathbb{1}_I)\rho_d(v)(\mathbb{1}_I \otimes \mathbb{1}_I) = \frac{vk}{d}|\Psi_I^+\rangle\langle\Psi_I^+| + \frac{(1-v)k^2}{d^2}\frac{\mathbb{1}_I \otimes \mathbb{1}_I}{k^2} \tag{8.97}$$

with the probability of getting an outcome

$$P(I,I) = \mathrm{Tr}[(\mathbb{1}_I \otimes \mathbb{1}_I)\rho_d(v)(\mathbb{1}_I \otimes \mathbb{1}_I)] = \frac{vk}{d} + \frac{(1-v)k^2}{d^2} \tag{8.98}$$

Here, a subensemble was selected as it was the case with the projective measurement $P, Q$ in the previous chapter. One can also see that no subspace has a higher probability to get selected. They are all equal.
The observed visibility of this state is

$$\tilde{v}(d,v,k) = \frac{vk}{dP(I,I)} = \frac{vd}{vd + k - vk} \tag{8.99}$$

The first measurement was applied to the system to select the subspaces, therefore, the state within the subspaces can be found as

$$\rho_I(\tilde{v}) = \tilde{v}|\Psi_I^+\rangle\langle\Psi_I^+| + (1-\tilde{v})\frac{(\mathbb{1}_I \otimes \mathbb{1}_I)}{k^2} = \frac{(\mathbb{1}_I \otimes \mathbb{1}_I)\rho_d(v)(\mathbb{1}_I \otimes \mathbb{1}_I)}{P(I,I)}$$

$$= \frac{vd}{vd + k - vk}|\Psi_I^+\rangle\langle\Psi_I^+| + \frac{(1-v)k}{vd + k - vk}\frac{(\mathbb{1}_I \otimes \mathbb{1}_I)}{k^2} \tag{8.100}$$

This is the state that both parties observe by performing the post-selection, or under the consideration of the example in the chapter above, on this state, the second measurement

of $A, A', B, B'$ would be performed in order to get an outcome.
Further, one can recognise the advantages of this subspace selection by considering the visibility of the state and comparing them. In fact, the visibility increases and consequently this has a positive impact on the noise resistance of a QKD protocol.

$$\tilde{v} = \frac{vd}{vd + (1-v)k} = \tilde{v} > v = \frac{vd}{vd + (1-v)d} \tag{8.101}$$

In regard to these short calculations, one can see three things. First, there is no preferred subspace in this protocol. All subspaces are equally good or bad. Second, even for the one subspace considered above, the noise resistance increased in such a way that the key rate could potentially increase as well. Third and most importantly, "the entanglement may be distributed only in some of the degrees of freedom of the Hilbert space; in these situations, extracting a key from the total space will bring a positive contribution from the 'correlated part' and a negative one from the error correction of the uncorrelated part. Via post-selection can be removed beforehand the parts of the key that are uncorrelated and as such only give advantage to Eve." [45]
Showing that subspace selection (post-selection) removes the uncorrelated parts relies on the basic concept of filtering, such that subspace selection is a kind of filter.

# 9 Subspace QKD with Self-testing

Self-testing has been a strong tool over the last centuries. If a source emits a quantum state, a quantum experimentalist would use a Beam splitter, half-wave plates, detectors etc. to measure the state which they receive [55]. In the end, they can conclude through the use of statistics if the state is entangled or not. But neither Alice nor Bob can conclude which state was used (in case the source emits the Bell states, it is only possible to detect if a singlet state was used). Nevertheless, with self-testing the whole measurement process can be treated as a black box. One is not interested in, how devices act on a state. Only the output is important. This is also called *device independent*. Even the mechanism behind the source is not a topic of interest. More precisely, both parties have different settings. Alice has $x = 0, 1, ...$ possible settings and Bob $y = 0, 1, ...$ with the outcome $a = 0, 1, ...$ for Alice and $b = 0, 1, ...$ for Bob. Note that both of their settings are independent and do not affect one another. After collecting some data, it is possible to find a correlation (probability) of the results $a$ and $b$ given that setting $x$ and $y$ were used.

$$p(a, b|x, y) \tag{9.1}$$

With the Bell inequality, which consists of a function $\mathcal{I}$, it is easy to prove that the state which the source produces is either entangled or not.

$$\mathcal{I}(p(a, b|x, y)) \leq \beta \tag{9.2}$$

$\beta$ can be seen as a bound which sets the condition for a source producing non entangled states. If $\mathcal{I}(p(a, b|x, y)) > \beta$, a contradiction to the Bell inequality was found. In the case of the experiment explained above, this means that one has detected an entangled quantum state if this equation 9.2 is contradicted. However, this is already well known. The main goal of device independent self-testing is to get to know which entangled state the source is producing. A huge advantage and the justification for self-testing is that Alice and Bob can assure that their devices are working correctly without knowing how exactly.

## 9.1 Self-Test scenario

From quantum physics it is already known that Alice and Bob each have their own Hilbert space $\mathcal{H}_A$ and $\mathcal{H}_B$. Now, consider Alice and Bob having a set of POVM $M_{a|x}$ and $N_{b|y}$ as discussed in chapter 4.2.2 [56]. So

$$\sum_a M_{a|x} = \mathbb{1} \quad M_{a|x} M_{a'|x} = \delta_{a,a'} M_{a|x} \quad \forall x, a, a' \tag{9.3}$$

similar to Bob's setting $N_{b|y}$. It is now possible to express the correlation $p(a,b|x,y) = \langle\Psi'|M_{a|x} \otimes N_{b|y}|\Psi'\rangle$, but in order to define the self-test scenario, one is facing two issues. First, one cannot assure that the state $|\Psi'\rangle$ and the measurements $\{M'_{a|x}\}$, $\{N'_{b|y}\}$ are reproduced. Instead, it is possible that one gets the rotated state $U \otimes V\,|\Psi'\rangle$ and $\{UM'_{a|x}U^\dagger\}$,$\{VN'_{b|y}V^\dagger\}$ for some unitary transformation $U, V$. Second, POVMs are performing on extra degrees of freedom that are not used. Therefore, one needs the mathematical concept known as *local isometry*.

### 9.1.1 Isometry

An isometry is a linear map $\Phi : \mathcal{H}_{A_1} \to \mathcal{H}_{A_2}$. In essence, it is a linear transformation which preserves the inner product. This does not imply that the linear isometries are unitary operators. For such a statement, one has to make the assumption that the spaces in which the isometry acts are all equal. In this case, the isometry of a state $|\Psi_{A_1}\rangle$ is just $\Phi[|\Psi_{A_1}\rangle] = U\,|\Psi_{A_2}\rangle$.

**Local Isometry**
Local isometries describe the tensor product of two isometries which are acting locally.

$$\Phi_{A_1} \otimes \Phi_{B_1} : \mathcal{H}_{A_1} \otimes \mathcal{H}_{B_1} \to \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2} \tag{9.4}$$

Note that probabilities and also correlations are invariant under the isometry mapping. Therefore, one can consider the two Hilbert spaces of Alice and Bob as identical. In practice, to achieve a local isometry one needs to use an ancilla state and perform a local unitary transformation. But for the purpose of this thesis, local isometries are just a mathematical tool which helps to show how self-testing works.

### 9.1.2 Self-testing of states

In regards to the self-test scenario, one has to assume that there is an existing local isometry between Alice and Bob $\Phi = \Phi_A \otimes \Phi_B : \mathcal{H}_A \otimes \mathcal{H}_B \to \mathcal{H}_{A'\bar{A}} \otimes \mathcal{H}_{B'\bar{B}}$. Therefore, one can find a state $\rho_{AB} \in \mathcal{H}_{AB}$

$$\Phi[\rho_{AB}] = |\Psi'\rangle\langle\Psi'|_{A'B'} \otimes \sigma_{\bar{A},\bar{B}} \tag{9.5}$$

Here $\sigma_{\bar{A},\bar{B}} = \mathrm{Tr}_p\,|junk\rangle\langle junk|$. These $|junk\rangle$ states are actually physical states. But they will vanish in further consideration and therefore are not for interest. Note that in the whole explanation of this protocol, the purification aspect is not considered. In equation 9.5 the trace over a third Hilbert space $\mathcal{H}_p$ was taken, in which the purification process takes place. This Hilbert space stays untouched by the isometry. For further details and information the papers "Device-independent entanglement certification of all entangled states" by J. Bowles [57] and "Self-testing of quantum systems: a review" by I. Šupić and J. Bowles [55] needs to be mentioned here.
Further, one can find another relationship if the projection operators $\Pi_{a|x}$, $\Pi_{b|y}$ satisfies the commutation relation $[\Pi_{a|x}, \Pi_{b|y}] = 0$.

$$\Phi([M_{a|x} \otimes N_{b|y}]\,|\Psi'\rangle) = |junk\rangle \otimes \Pi_{a|x} \otimes \Pi_{b|y}\,|\Psi\rangle \tag{9.6}$$

## 9.2 An example with a partially entangled state

This example is also the first try to improve the optimisation problem and therefore the SDP. As can be seen in the equation 8.6, getting $W = 1$ can only be achieved with a maximally entangled state. But what if Alice and Bob only share a partially entangled state? That is, $\rho_{AB} = |\psi_\theta\rangle\langle\psi_\theta|$, where

$$|\psi_\theta\rangle = \sin(\theta)\,|00\rangle + \cos(\theta)\,|11\rangle \tag{9.7}$$

and $\theta \in [0, \pi/4]$
For the purpose of self-testing such a state, the equations 9.5 and 9.6 can be used. One can find that the following conditions are fulfilled [58]:

$$Z_A\,|\psi\rangle = Z_B\,|\psi\rangle$$

$$\sin(\theta)X_A(\mathbb{1} + Z_B)\,|\psi\rangle = \cos(\theta)X_B(\mathbb{1} - Z_A)\,|\psi\rangle \tag{9.8}$$

with the hermitian Pauli matrices $X$, and $Z$ which are acting on Alice's or Bob's side. One can prove that $|\psi\rangle$ is a pure partially entangled state. However, it is not yet clear how to transform such conditions into a linear combination of probabilities for Alice and Bob. As shown in [56], it even follows for $|\Psi'\rangle$ that $|\Psi'\rangle \overset{\sim}{=} |\Psi\rangle$ which Alice and Bob can conclude by their shared state.

### 9.2.1 Using a Bell inequality to certify the state

For the protocol and in order to improve the SDP, equation 9.8 is hard or even impossible to implement. Alternatively, one can regard the following Bell operator defined with the observables $A_n = A_{1|n} - A_{2|n}$, $B_n = B_{1|n} - B_{2|n}$ :

$$\mathcal{B} = \alpha A_0 + A_0(B_0 + B_1) + A_1(B_0 - B_1) \tag{9.9}$$

Of which the maximal violation $\max_\rho \mathrm{Tr}(\mathcal{B}\rho) = \sqrt{8 + 2\alpha^2}$ for $\rho = |\psi_\theta\rangle\,\langle\psi_\theta|$ and which ensures that the state is equivalent to (9.7), for $\tan(2\theta) = \sqrt{\frac{4-\alpha^2}{2\alpha^2}}$.
In the classical approach of the Bell inequality, one can find:

$$\mathcal{B} = \langle A_0B_0\rangle + \langle A_1B_0\rangle + \langle A_0B_1\rangle - \langle A_1B_1\rangle \leq 2 \tag{9.10}$$

for $\langle A_nB'_n\rangle = \sum_{a,b} a \cdot bp(a, b|n, n')$ for the outcome $a, b = \pm 1$ in the settings $n, n' = 0, 1$. In the case of a maximally entangled state, one can find a maximal violation of

Bell's inequality $\mathcal{B} = 2\sqrt{2}$ as it was defined in chapter 8.5.1. One can now replace the measurement part of the SDP:

$$\begin{aligned} P_g = \quad & \max_{\{\rho_e\}_e} \sum_e \mathrm{Tr}(\rho_e A_{e|1} \otimes \mathbb{1}_d) \\ \text{s.t.} \quad & \mathrm{Tr}(\mathcal{B} \sum_e \rho_e) = \sqrt{8 + 2\alpha^2}, \\ & \rho_e \geq 0 \ \ , \forall e, \\ & \mathrm{Tr}(\sum_e \rho_e) = 1, \end{aligned} \tag{9.11}$$

for local measurements $\{A_{a|x}\}, \{B_{b|y}\}$ corresponding to the maximal violation of the Bell operator (9.9). This corresponds to Alice and Bob sharing a pure partially entangled state (with the parameter $\theta = \frac{1}{2}\arctan(\sqrt{\frac{4-\alpha^2}{2\alpha^2}})$ ). An explicit expression of $\mathrm{Tr}(\mathcal{B}\sum_e \rho_e)$ can be easily calculated by inserting different expressions.

$$\mathrm{Tr}(\mathcal{B} \sum_e \rho_e) = \mathrm{Tr}([\alpha Z_A + 2 Z_A Z_B \cos(\nu) + 2 X_A X_B \sin(\nu)]\rho) \tag{9.12}$$

for $\nu = \arctan(\sin(2\theta))$

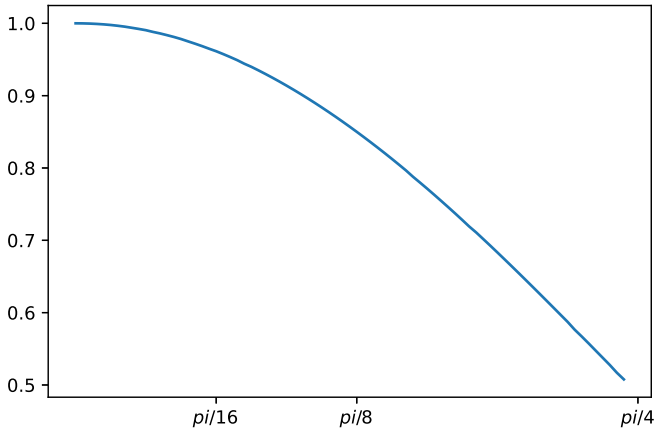


Figure 9.1: Guessing probability $P_g^*$ (y-axis) in dependence of the angle $\vartheta$ (x-axis)

Figure 9.1 shows how the guessing probability behaves under different $\theta \in [0, \pi/4]$.

### 9.2.2 Noisy state

As it was already mentioned above, in any actual implementation of the above protocol there will be some noise that could typically or conservatively be modeled as some white noise on the state. Therefore, the family of states will be considered in the following:

$$\rho(v,\theta) = v|\psi_\theta\rangle\langle\psi_\theta| + (1-v)\mathbb{1}/4 \tag{9.13}$$

where $|\psi_\theta\rangle = \sin(\theta)\,|00\rangle + \cos(\theta)\,|11\rangle)$, $\theta \in [0, \pi/4]$ and $0 \leq v \leq 1$. This is also called an *isotropic state*. The new SDP reads

$$\begin{aligned} P_g = \quad & \max_{\{\rho_e\}_e} \sum_e \mathrm{Tr}(\rho_e A_{e|1} \otimes \mathbb{1}_d) \\ \text{s.t.} \quad & \mathrm{Tr}(\mathcal{B}\sum_e \rho_e) = V(v,\theta), \\ & \rho_e \geq 0 \ \ ,\forall e, \\ & \mathrm{Tr}(\sum_e \rho_e) = 1, \end{aligned} \tag{9.14}$$

where $V(v,\theta)$ is the maximal violation observed for state $\rho(v,\theta)$ which is just $V(v,\theta) = v\sqrt{8+2\alpha^2}$

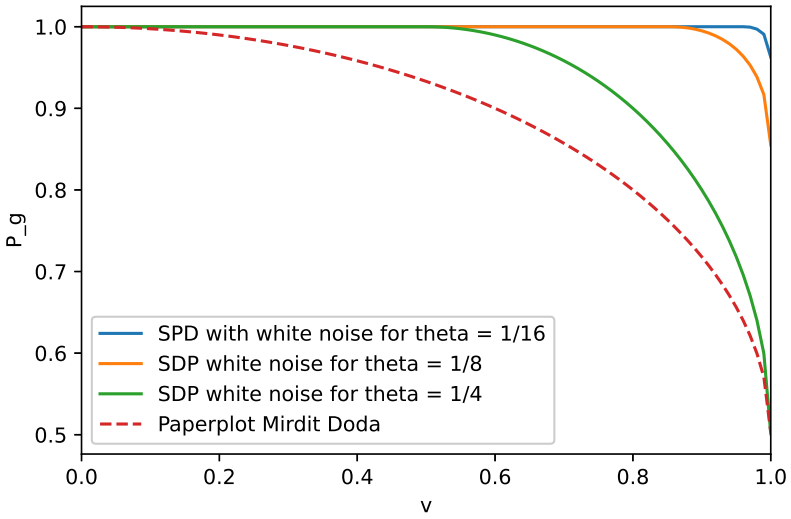


Figure 9.2: Guessing probability $P_g^*$ with white noise resistance for different $\vartheta$. Paperplot describes the case without noise compared to the white noise cases for different $\vartheta$ from the equation 9.14.

As one can see, for different $\theta$ the guessing probability is increasing. The conclusion of figure 9.2 is that the self-test scenario increases the guessing probability of Eve for different noise values $v$. As already was pointed out, if $P_g$ is higher, Eve has more chances to guess the outcome of Alice's and Bob's measurements. Therefore, this scenario does not lead to an improvement of the protocol which is why further considerations to improve the SDP needs to be made.

# 10 Subspace QKD with MUB

## 10.1 Mutually unbiased Bases

*Mutual unbiased Bases* (MUB) were first described by Julian Schwinger in the 1960s [59]. In the cited paper, he considers two sets of vectors which form a unitary matrix. In regards to these two sets of vectors he "realised that no information can be retrieved when a quantum system which is prepared in a basis state from B' is measured with respect to the basis B" [60]. A new method and approach to MUBs was published by Somshubhro Bandyopadhyay in his publication "A new proof for the existence of mutually unbiased bases" [61] which will be presented here shortly.
An intuitive way to introduce MUBs is by considering the basic concept of quantum mechanics, namely the Heisenberg uncertainty relation.

$$|\langle x|p\rangle|^2 = \text{const.} \tag{10.1}$$

This relation is well-known and its interpretation is discussed in many papers [62, 63] and more. But further, one can think about how it would relate for some bases in the Hilbert space.
Consider the two orthonormal bases $\mathcal{B}_1 = \{|\phi_1\rangle, ..., |\phi_d\rangle\}$ and $\mathcal{B}_2 = \{|\psi\rangle, ..., |\psi_d\rangle\}$ in $\mathbb{C}^d$ for the dimension $d$. MUBs are defined as

$$|\langle \psi_k|\phi_k\rangle|^2 = \text{const.} = \frac{1}{d} \tag{10.2}$$

for $1 \leq j, k \leq d$
Such an orthonormal basis consists of no more than $d + 1$ bases in any prime power dimension [64]. Moreover, it was shown that the measurement of $d + 1$ MUBs can reconstruct a density matrix of a quantum state [65]. There are many ways to construct such bases. An intuitive and well known example in quantum physics is described by a spin 1/2 system. The normalised eigenvectors of the Pauli matrices $\sigma_x$, $\sigma_z$ and $\sigma_y$ construct such a complete set of MUBs.

$$\mathcal{B}_1 = \{|0\rangle, |1\rangle\}$$

$$\begin{aligned} \mathcal{B}_2 &= \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\} \\ \mathcal{B}_3 &= \{\frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle)\} \end{aligned} \tag{10.3}$$

For higher prime power dimension, the general form of the Pauli matrices $X_d$, $Z_d \in \mathbb{C}^d$ is used

$$X_d |j\rangle = |j+1\rangle$$

$$Z_d |j\rangle = \omega^j |j\rangle \tag{10.4}$$

for $j = d-1$ and $\omega = \exp 2\pi i/d$ (consider, with $|j+1\rangle$ means the modulo with respect to $d$ ($|\mathrm{mod}(j+1)_d\rangle$)). Out of the general form of $X_d$ and $Z_d$ it is now possible to compose $d+1$ unitary operators to get MUBs $Z_d, X_d(Z_d)^k$ for $0 \leq k$ (note that $X_d(Z_d)^k |j\rangle = (\omega^k)^j |j+1\rangle$). As it was written above, there are many ways to construct such MUBs for different cases.

## 10.2 Another way to look at MUBs

The above description and construction of MUBs can be seen as fairly straightforward. However, the MUBs of prime power dimensions cannot be found, since "the special status of prime numbers has to do with the fact that Weyl's representation theorem requires a phase factor which is a primitive root of unity so that $q^k \neq 1$ for $k < N$. This is only true for all the roots of unity if $N$ is prime." [66] But one might wonder how to construct MUBs for prime power dimension?
In the following description, a way is presented to find such MUBs. These kind of MUBs are also used for solving the SDP in the following chapter (10.3.1). Above, the focus was laid upon some unitary operator $X$,$Z$. Weyl showed that these operators satisfy the following relation [67].

$$XZ = qZX \tag{10.5}$$

for a phase factor $q = \exp(\frac{2\pi i}{d})$. As already known, the eigenvectors of the unitary operator $X$,$Y$ represent the MUBs.
However, if the eigenvector of $Z$ is considered as a standard eigenvector, then a Fourier matrix $F$ whose columns are the eigenbasis of $X$ can be found. Its elements are just the phase factor powered by its position in the matrix [66]

$$F_{ab} = q^{ab} \qquad 0 \leq a, b \leq d-1 \tag{10.6}$$

where $a \in \{0, ..., d-1\}$ describes the columns and $b \in \{0, ..., d-1\}$ the rows.
Now, the question on how such a Fourier matrix looks, might arise. The Hadamard matrix, which has been well studied the past decades, can be used as an example. Note, that not all complex Hadamard matrices are known so far. To complete the set of MUBs which can be found for a dimension $d$ (as discussed, there are $d+1$ MUBs), one just needs to multiply the Fourier matrix from the left to a unitary diagonal matrix. Surely, one might ask if MUBs can also be constructed in the real Hilbert space, but this is only true for the dimension $d = 2$ or any other dimension which can be divided by 4. Bengsston gave a geometrical proof why there are no MUBs in the real Hilbert space for

other dimensions [66]. Shortly, one can construct such vectors for any other dimension but they do not form a basis.
Further, the case $d = 6$ and why it is so difficult to find MUBs will be discussed. However, here, the quality of MUBs in order to understand the case $d = 6$ better will be in the focus of attention.

### 10.2.1 Special case d=6

For this special case, there are more Hadamard matrices known [68]. Nowadays, it is not clear if there are more MUBs despite the 3. For $d = 6$, there are more possibilities to find such Hadamard matrices from which MUBs can be formed. Currently, there are 5 Hadamard matrices known. Here an example is sketched which Bengtsson showed in his publication. From this example one can conclude why it is so difficult to find more than 3 MUBs for $d = 6$.
Consider the Fourier Matrix

$$F_6(\Phi_1, \Phi_2) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & q^{i\Phi_1} & q^2 e^{i\Phi_2} & q^3 & 1^4 e^{i\Phi_1} & q^5 e^{i\Phi_2} \\ 1 & q^2 & q^4 & 1 & q^2 & q^4 \\ 1 & q^3 e^{i\Phi_1} & e^{i\Phi_2} & q^3 & e^{i\Phi_1} & q^3 e^{i\Phi_2} \\ 1 & q^4 & q^2 & 1 & q^4 & q^2 \\ 1 & q^5 e^{i\Phi_1} & q^4 e^{i\Phi_2} & q^3 & q^2 e^{i\Phi_1} & q e^{i\Phi_2} \end{pmatrix} \tag{10.7}$$

For the phase factor $q = \exp(\frac{2\pi i}{6})$. A Fourier transformation can be found

$$\tilde{x}_a = \frac{1}{\sqrt{d}} \sum_{a=0}^{d-1} x_b q^{ba} \tag{10.8}$$

In regards to the biunimodular array (an array of unimodular complex numbers $x_a$), one can find

$$\gamma_b = \frac{1}{d} \sum_{a=0}^{d-1} \tilde{x}_a x_{a+b} = \frac{1}{d} \sum_{a=0}^{d-1} |\tilde{x}_a|^2 q^{-ab} = \delta_{b,0} \tag{10.9}$$

which shows that $x_a$ and $x_{a+b}$ form orthogonal vectors for a fixed $b$. Furthermore, it was shown that 16 possible choices of MUB exist.
On the first glance, this might seem satisfactory since 16 possible choices of MUBs are more than one needs for a complete set of 7 MUBs for $d = 6$. However, when looking into their possibility to be used as proper MUBs. It will appear that 13 of them are not useable. As Bengtsson discussed, MUBs have to satisfy the distance condition. The distance $D_c^2$ should satisfy:

$$0 \leq D_c^2 \leq d - 1 \tag{10.10}$$

"the distance attains its maximum value if and only if the bases are MUB." [66]
Four of these MUBs for $d = 6$ form a square with $D_c^2 = 2$. In regards to the other MUBs, their maximum distance only gets close to $D_c^2 \approx 4.64$ which is not enough to reach a

value of 5. Only three MUBs satisfy the Grassmannian distance.

In the first view, one might think that there only has to solve the optimisation problem of the maximisation

$$\max_{D_c^2} F = \sum_{i,j} D_c^2(P_i, P_j) \tag{10.11}$$

to find a set of MUBs.
Indeed this might work for some dimensions, such as $d = 4$, but in regards to $d = 6$ it might be an unsolvable problem.
An easy set of MUB for example can be found by a spin 1/2 particle. Each unbiased basis is just the normalised eigenvectors of the Pauli matrices [61].

## 10.3 Using MUBs for higher Dimension

In the following, a way will be presented which shows how to optimise the QKD protocol of Mirdit Doda et al. [1]. This system will be more resistant against noise. Therefore MUBs are used which were introduced before in chapter 10.1 [61,66]. In order to optimise Doda's et al. protocol against noise, MUBs are used to create a new constraint which projects the state on the high-dimensional Bloch sphere. To use the definition of the above explanations, it is possible to define $P_{j|k} = |j\rangle_k \langle j|_k$ corresponding to the $j$th eigenvector of the unitary transformation $X_d(Z_d)^k$ for $k \in \{0, \ldots, d-1\}$ and $j \in \{0, \ldots, d-1\}$. By defining $P_{j|d}$ as the eigenvectors of the unitary $Z_d$. With the following expression, it is useful to write $\Gamma_k = \sum_{j=0}^{d-1} P_{j|k} \otimes P_{j|k}^T$. Similar for $\Gamma_d = \sum_{j=0}^{d-1} P_{j|d} \otimes P_{j|d}^T$ with $P_{j|d}$.
As it was done in the self-test scenario 9 we can construct new constraints for the measurement constraints to the SDP 8.6.

$$\begin{aligned}
P_g = \quad & \max_{\{\rho_e\}} \sum_e \mathrm{Tr}(\rho_e A_{e|1} \otimes \mathbb{1}) \\
\text{s.t.} \quad & \mathrm{Tr}(\Gamma_d \sum_e \rho_e) = W \\
& \mathrm{Tr}(\Gamma_k \sum_e \rho_e) = W \qquad \forall k \in \{0, \ldots, d-1\} \\
& \rho_e \geq 0 \\
& \mathrm{Tr}(\sum_e \rho_e) = 1
\end{aligned} \tag{10.12}$$

The data of figure 10.1 was calculated in Matlab. As it can be seen, for each dimension the behaviour of $P_g$ improves. Nowadays, there are only 3 MUBs known for $d = 6$. Nevertheless, it is possible to run the code for only 3 measurements (and for 4 measurements).

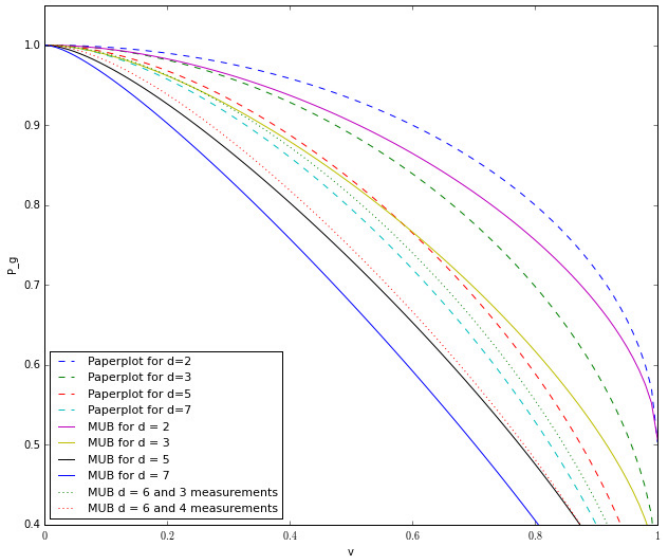


Figure 10.1: Guessing probability $P_g^*$ for different dimensions. For $d = 6$ a given dataset is used of three MUBs which were already found.

### 10.3.1 Solving SDP with MUBs

The Matlab code for small dimensions shows that using MUBs for measurement improves the behaviour of Eve's guessing probability as can be seen in chapter 10.3. Here, the SDP 10.12 was used with the MUBs which were composed from the general Pauli matrices as in equation 10.4. Therefore, the dual function can be found in a similar way as shown in the paper [1] and in section 8.3.

$$\begin{aligned} &\min_{\{\gamma,\vartheta,\lambda\}} \gamma + W(\vartheta + \sum_k \lambda_k) \\ &\text{s.t.} \quad \gamma + \vartheta\Gamma_d + \sum_{k=1}^{d} \lambda_k \Gamma_k \geq A_{e|1} \otimes \mathbb{1}_d \end{aligned} \tag{10.13}$$

Note that the label $k$ means that the eigenvalues belong to $X_d(Z_d)^k$.
Similar to the previous problem, one can solve the SDP by finding eigenvalues of $\vartheta\Gamma_d + \sum_{k=0}^{d} \lambda_k\Gamma_k - A_{e|1} \otimes \mathbb{1}_d$
In regards to the proof, firstly it will be shown that the eigenvalues are the same for all $e$ (similar to the problem above 8.3). After doing that, the problem is divided into 3 terms and simplified in a similar way as it was shown in the above chapter, namely with the help of unitary transformation.

### 10.3.2 Calculate eigenvalues

In this case, just the MUBs expression has to be simplified. One still wants to calculate the eigenvalue of

$$\vartheta\Gamma_d + \sum_{k=0}^{d} \lambda_k \Gamma_k - |0\rangle\langle 0| \otimes \mathbb{1}_d \tag{10.14}$$

where already the fact was used that all eigenvalues are the same for all $e$ (see chapter 8.3).
Here, the following relation is useful to simplify the problem. In this thesis it is called, *Marcus magical identity.*

$$\sum_{k=0}^{d} \Gamma_k + \Gamma_d = \mathbb{1}_{d^2} + d\,|\Phi^+\rangle\langle\Phi^+| \tag{10.15}$$

***Proof:***
If MUBs are considered as projective 2-designs, which was proven in [69], then one can write:

$$\frac{1}{d(d+1)} \sum_i |\psi_i\rangle\langle\psi_i|^{\otimes 2} = \int d\,|\phi\rangle\,|\phi\rangle\langle\phi|^{\otimes 2} \tag{10.16}$$

in which $|\psi_i\rangle$ are all $d(d+1)$ vectors in all the $d+1$ MUBs for dimension $d$. This integral is well known and can be done over the Haar measurement. In essence, a solution can be found

$$\int d\,|\phi\rangle\,|\phi\rangle\langle\phi|^{\otimes 2} = \frac{P_{\text{sym}}}{\operatorname{Tr} P_{\text{sym}}} \tag{10.17}$$

The action of the symmetric operator $P_{\text{sym}}$ is just $P_{\text{sym}}|\Psi\rangle\langle\Psi| = |\Psi\rangle\langle\Psi|$ and $\operatorname{Tr} P_{\text{sym}} = \frac{d(d+1)}{2}$. Therefore, it is possible to rearrange some aspects and get:

$$\sum_i |\psi_i\rangle\langle\psi_i|^{\otimes 2} = 2P_{\text{sym}} \tag{10.18}$$

The partial trace on both sides leads us to

$$\sum_i |\psi_i\rangle\langle\psi_i| \otimes |\psi_i\rangle\langle\psi_i||^T = 2P_{\text{sym}}^{T_B} \tag{10.19}$$

If now is assumed that $2P_{\text{sym}} = \mathbf{1} + S$, in which $S$ defines the SWAP operator $S = \sum_{ij} |i\rangle\langle j| \otimes |j\rangle\langle i|$, the partial trace of this SWAP is just $S^{T_B} = \sum_{ij} |i\rangle\langle j| \otimes |i\rangle\langle j|$. In summary, one and up with

$$\sum_i |\psi_i\rangle\langle\psi_i| \otimes |\psi_i\rangle\langle\psi_i||^T = I + \underbrace{\sum_{ij} |i\rangle\langle j| \otimes |i\rangle\langle j|}_{=|\Phi^+\rangle\langle\Phi^+|} \tag{10.20}$$

which is what one wanted to show for the Bell state $|\Phi^+\rangle$.

In a more summarised manner, the problem can be defined as

$$(\vartheta - \lambda)\Gamma_d + \lambda(\mathbb{1}_{d^2} + d\,|\Phi^+\rangle\langle\Phi^+|) - |0\rangle\langle 0| \otimes \mathbb{1}_d \tag{10.21}$$

For the non-trivial eigenvalues apply a non-Unitary and non-Isometric matrix

$$R = \sum_{i=0}^{d-1} |i\rangle\langle ii| \tag{10.22}$$

which will just take subspaces spanned by $|00\rangle, |11\rangle, |22\rangle, ...$ and extract all other parts $|01\rangle, |02\rangle, |10\rangle, |21\rangle, ....$ Here, this tool can be used, because all of these parts $|01\rangle, |02\rangle, |10\rangle, |21\rangle, ...$ are diagonal.

$$R\left((\vartheta - \lambda)\Gamma_d + \lambda(\mathbb{1}_{d^2} + d\,|\Phi^+\rangle\langle\Phi^+|) - |0\rangle\langle 0| \otimes \mathbb{1}_d\right) R^\dagger \tag{10.23}$$

The first term is simply

$$R(\vartheta - \lambda)\Gamma_d R^\dagger = (\vartheta - \lambda) \sum_{i,i'=0}^{d-1} \sum_{j=0}^{d-1} |i\rangle\langle ii| \left(|jj\rangle\langle jj|\right) |i'i'\rangle\langle i'| = (\vartheta - \lambda)\mathbb{1} \tag{10.24}$$

The second term is

$$\lambda R(\mathbb{1} + d\,|\Phi^+\rangle\langle\Phi^+|)R^\dagger = \lambda\mathbb{1} + \sum_{i,i'=0}^{d-1} \sum_{j,j'=0}^{d-1} |j\rangle\langle jj| \left(|ii\rangle\langle i'i'|\right) |j'j'\rangle\langle j'| = \lambda\mathbb{1} + \sum_{j,j'=0}^{d-1} |j\rangle\langle j'| \tag{10.25}$$

One can find a $|u\rangle = \sum_{j=0}^{d-1} \frac{1}{\sqrt{d}} |j\rangle$ in such a way so that a matrix A can be found $A = d\,|u\rangle\langle u|$
The third term

$$R\,|0\rangle\langle 0| \otimes \mathbb{1}R^\dagger = \sum_{j,i=0}^{d-1} |j\rangle \left(\langle j|0\rangle\langle 0|i\rangle \otimes \langle j|i\rangle\right)\langle i| = |0\rangle\langle 0| \tag{10.26}$$

After applying $R$, the problem can be found as:

$$(\vartheta - \lambda)\mathbb{1} + \lambda(\mathbb{1} + |u\rangle\langle u|) - |0\rangle\langle 0| \tag{10.27}$$

This is just a $d \times d$ Matrix and its eigenvalues $\zeta$ are depending on the dimension $d = 2, 3, 4, ..., N$

$$\zeta_\pm = \frac{d\lambda - 1}{2} + \vartheta \pm \frac{1}{2}\sqrt{(1 + d\lambda)^2 - 4\lambda} \qquad \zeta_{d-2} = \vartheta \tag{10.28}$$

All other eigenvalues are $\zeta_{(d-1)^2} = \lambda$ and $\zeta_{d-1} = \lambda - 1$. Here, the subscript shows the number of eigenvalues which correspond to the expression.

### 10.3.3 New dual Function

The SDP can be solved with the dual function in a similar manner as it was done by Mirdit Doda et al. in [1]. Only the minimal eigenvalue has to be found. It can be easily seen that $\vartheta > \zeta_-$ and $\zeta_+ > \zeta_-$ because all variables are positive and therefore the expression under the root is positive. Hence, it is possible to conclude $\lambda > \lambda - 1$. Consequently, there are two eigenvalues which could be minimal $\zeta_{\min} = \lambda - 1$ and $\zeta_-$. From equation 10.13 a new SDP can be found which is already simplified.

$$\begin{aligned} P_g = \min_{\{\gamma,\vartheta,\lambda\}} \; & \gamma + W(\vartheta + d\lambda) \\ \text{s.t.} \quad & \gamma + \zeta_- \geq 0 \\ & \gamma + \zeta_{\min} \geq 0 \end{aligned} \tag{10.29}$$

Rewriting the SDP into a simple form

$$P_g = \min[\underbrace{-\zeta_- + W(\vartheta + d\lambda)}_{g(\vartheta,\lambda)}, \underbrace{-\lambda + 1 + W(\vartheta + d\lambda)}_{f(\vartheta,\lambda)}] \tag{10.30}$$

The solution of the SDP lies somewhere between $g(\vartheta, \lambda) \geq f(\vartheta, \lambda)$ or $g(\vartheta, \lambda) \leq f(\vartheta, \lambda)$. But only if the minimum point of

$$g(\vartheta, \lambda) = f(\vartheta, \lambda) \tag{10.31}$$

is found, it is possible to find a solution of the SDP which holds for the given conditions. From 10.3.3, one can calculate $\vartheta$ by just comparing both minimal eigenvalues $\zeta_-$ and $\lambda - 1$

$$\zeta_- = \lambda - 1 \tag{10.32}$$

which leads to

$$\vartheta = \frac{\lambda(2-d) - 1}{2} + \frac{1}{2}\sqrt{(1 + d\lambda)^2 - 4\lambda} \tag{10.33}$$

To find $\lambda$, just $\frac{dg(\vartheta,\lambda)}{d\lambda} = 0$ or $\frac{df(\vartheta,\lambda)}{d\lambda} = 0$ has to be solved.

$$\lambda_\pm = -\frac{d-2}{d^2} \pm \sqrt{\frac{(-2+d)^2}{d^4} - \frac{(2W-1)(dW-1)}{d^2(W-1)(W+dW-1)}} \tag{10.34}$$

Now, one just have to find $\min[\lambda_-, \lambda_+]$. For $W \geq \frac{2}{d+2}$ ($v \geq \frac{3d+2}{d^2+3d+2}$) it follows that $\lambda_+ \geq \lambda_-$ and vice versa. The final guessing probability $P_g$ can now be found as

$$P_g = \begin{cases} -\lambda_- + 1 + W(\vartheta(\lambda_-) + d\lambda_-) & W \geq \frac{2}{d+2} \\ -\lambda_+ + 1 + W(\vartheta(\lambda_+) + d\lambda_+) & W \leq \frac{2}{d+2} \end{cases} \tag{10.35}$$

### 10.3.4 Summary

In order to write down the analytical solution in accordance with the equation 8.79, it is necessary to merge the above equation into one. By looking at its structure, consider $\lambda_\pm$

$$P_g = -\lambda_\pm + 1 + W\frac{\lambda_\pm(2-d)-1}{2} + \frac{W}{2}(\sqrt{(1+d\lambda_\pm)^2 - 4\lambda_\pm} + d\lambda_\pm) \tag{10.36}$$

$$= 1 - \frac{W}{2} + \lambda_\pm\frac{-2+W(2+d)}{2} + \frac{W}{2}\sqrt{(1+d\lambda_\pm)^2 - 4\lambda_\pm} \tag{10.37}$$

The expression under the root does not depend on the sign of $\lambda_\pm$. Therefore, the only expression which is of interest is $\lambda_\pm\frac{-2+W(2+d)}{2}$. This expression can be found as $\frac{-2+(2+d)W}{d^2} - \frac{-2+(2+d)W}{2d} \pm \frac{-2+(2+d)W}{2}\sqrt{\frac{(d-2)^2}{d^4} - \frac{(2W-1)(dW-1)}{d^2(W-1)(W+dW-1)}}$. In summary, the sign of the above equation changes with $-2+(2+d)W$. By taking its absolute value, one can find a unit expression of equation 10.37.

$$P_g = 1 - \frac{W}{2} + \frac{-2+(2+d)W}{d^2} - \frac{-2+(2+d)W}{2d}$$

$$-\left|\frac{-2+(2+d)W}{2}\right|\sqrt{\frac{(d-2)^2}{d^4} - \frac{(2W-1)(dW-1)}{d^2(W-1)(W+dW-1)}} \tag{10.38}$$

$$+\frac{W}{2}\sqrt{-\frac{(d-1)W^2}{(W-1)(W+dW-1)}} \tag{10.39}$$

$$P_g = 1 - W + \frac{1}{d} + \frac{2(W-1)}{d^2} + \frac{2\sqrt{(d-1)(1-W)(dW+W-1)}}{d^2} \tag{10.40}$$

$$P_g = \frac{d+v(1-d)}{d} + \frac{2(d-1)}{d^3}((v-1) + \sqrt{(1-v)(1+(d^2-1)v)}) \tag{10.41}$$

Note that $W = v + \frac{1-v}{d}$.
In regards to the key rate, one has to write down $K_{tot}$ for the solved SDP with MUBs according to equation 8.80.

$$K_{tot} \geq \frac{vd+k-vk}{d}\left(-\log_2(P_g) - H(X|Y)_{v,k}\right) \tag{10.42}$$

with

$$H(X|Y)_{v,k} = \frac{1+(d-1)v}{k(v-1)-dv}\log_2\left(\frac{1+(d-1)v}{k+dv-kv}\right) + \frac{k+v-kv-1}{(k(v-1)-dv)}\log_2\left(\frac{1-v}{k+dv-kv}\right) \tag{10.43}$$

## 10.4 Proof optimal solution

Now that an analytical solution to the SDP was found, it is also necessary to show that the result of the derived solution is optimal for this given problem. Here, the Ansatz is used that the problem of the primal function is equal to the dual function. In other words, that equation 8.5 is equal to 10.13

$$\sum_e \mathrm{tr}(\rho_e A_{e|1} \otimes \mathbb{1}) = \gamma + W(\vartheta + \lambda) \tag{10.44}$$

To prove that one has found the optimal solution, we will only prove it for one case. For example for $d = 3$.
The density matrix $\rho_e$ should be in the shape of

$$\rho_e = |\Psi\rangle\langle\Psi| + \frac{1-v}{d^2} A_{e|1} \otimes \mathbb{1} - \frac{1-v}{d^2} |ee\rangle\langle ee| \tag{10.45}$$

In this case, $|\Psi\rangle = a|00\rangle + b|11\rangle + c|22\rangle$. By looking at its shape, it is possible to conclude from the symmetry that $b = c$. Two constraints can be used to find $a_{d,v}$ and $b_{d,v}$. The subscript $v, d$ shows the dependence of variables on visibility and dimension.

$$a_{d,v}^2 + b_{d,v}^2 + c_{d,v}^2 = a_{d,v}^2 + 2b_{d,v}^2 = \frac{v}{d} + \frac{1-v}{d^2} \tag{10.46}$$

$$2a_{d,v}b_{d,v} + b_{d,v}^2 = \frac{v}{d} \tag{10.47}$$

The last constraints come from the fact that $\sum_e \rho_e = \rho_{\mathrm{iso}} = v|\Phi^+\rangle\langle\Phi^+| + \frac{1-v}{d^2}\mathbb{1}$.
Therefore, one can find

$$a_{d,v} = \sqrt{\frac{v}{d} + \frac{1-v}{d^2} - 2b_{d,v}^2} \tag{10.48}$$

and finding $b$

$$b_{d,v} = \pm\frac{1}{6d}\sqrt{12dv - 2\sqrt{-(16v-16)(3dv-v+1)} - 8v + 8} \tag{10.49}$$

Here, only the plus term is interesting.

$$a_{d,v} = \frac{1}{3d}\sqrt{3dv + \sqrt{-(16v-16)(3dv-v+1)} - 5v + 5} \tag{10.50}$$

Taking the main equation 10.44 into consideration, it is practicable to apply $|\Psi\rangle = \sum_{i=0}^{2} a_{d,v}|ii\rangle\langle ii|$ to the left hand side

$$\sum_e \mathrm{Tr}[(|\Psi\rangle\langle\Psi| + \frac{1-v}{d^2}|e\rangle\langle e| \otimes \mathbb{1} - \frac{1-v}{d^2}|ee\rangle\langle ee|)(|e\rangle\langle e| \otimes \mathbb{1})]$$

$$= \sum_e a_{(d,v)}^2 \underbrace{\mathrm{tr}[|ee\rangle\langle ee|]}_{=d} + \frac{1-v}{d^2}\underbrace{\mathrm{tr}[|e\rangle\langle e| \otimes \mathbb{1}]}_{d^2} - \frac{1-v}{d^2}\underbrace{\mathrm{tr}[|ee\rangle\langle ee|]}_{=d} \tag{10.51}$$

$$= da_{(d,v)}^2 + 1 - v - \frac{1-v}{d} \tag{10.52}$$

$$P_g = d\left(\frac{1}{3d}\sqrt{3dv + \sqrt{-(16v-16)(3dv-v+1)} - 5v + 5}\right)^2 + 1 - v - \frac{1-v}{d}$$

$$P_g = \frac{4}{9d}\sqrt{-(v-1)(3dv-v+1)} - \frac{4(1-v)}{9d} + 1 - \frac{2}{3}v \tag{10.53}$$

Note that still only dimension $d = 3$ is considered.

$$= \frac{4}{27}\sqrt{-(v-1)(9v-v+1)} - \frac{4(1-v)}{27} + 1 - \frac{2}{3}v \tag{10.54}$$

Therefore, it is possible to use 10.41 for the right hand side which is already an optimal solution

$$P_g = \underbrace{\frac{d + v(1-d)}{d}}_{1-\frac{2}{3}v} + \underbrace{\frac{2(d-1)}{d^3}(v-1)}_{-\frac{4(1-v)}{27}} + \underbrace{\frac{2(d-1)}{d^3}\sqrt{(1-v)(1+(d^2-1)v)}}_{\frac{4}{27}\sqrt{-(v-1)(9v-v+1)}} \tag{10.55}$$

In this chapter, it was shown that for a fixed dimension ($d = 3$) the primal function is equal to the dual function.

## 10.5 Results subspace QKD with MUBs

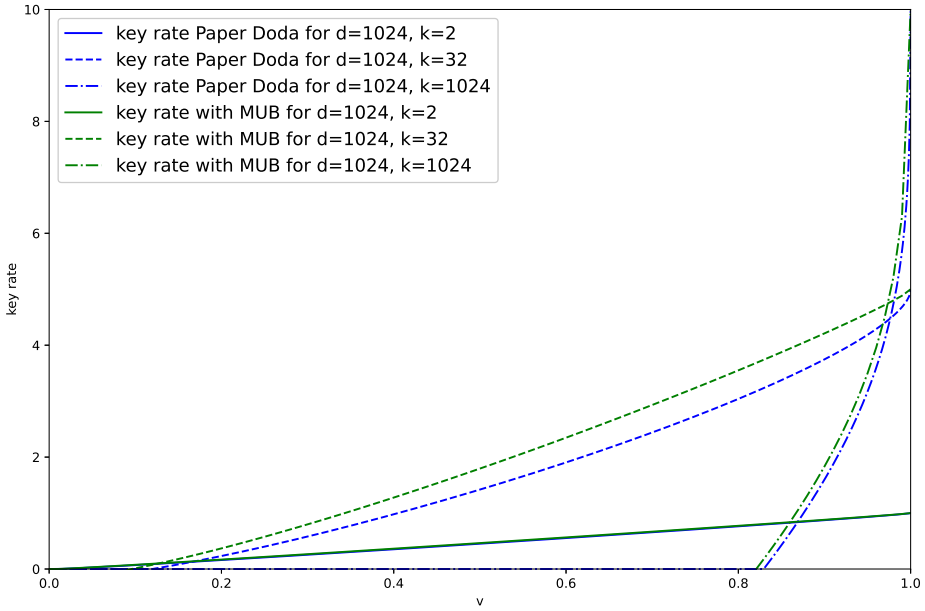


Figure 10.2: Comparison of the key rate with the solution of the protocol which was found by Mirdit Doda et al. [1] (blue) and the improved protocol with MUB (green).

In the figure above 10.2, it is possible to see the improvement of the SDP without and with MUBs. It was already discussed in chapter 8.4, the protocol works more effectively if the right amount of subspaces was found. If both concepts are considered (with and without MUB) one see perfectly that for $d = 1024$ and $k = 32$ the key rate is much more resistant against noise if MUBs are used.

# 11 Conclusion

In the first part of this master thesis, an overview of research in quantum information and especially quantum communication conducted over many decades was given. Hereby, the concept of information in the classical as well as the quantum regime was introduced. Moreover, it was shown how quantum communication works and how one could create such communication between two parties. Their advantages and the main issue of quantum communication, namely quantum noise were discussed as well.
In the second part, all these basic concepts were used in order to understand why a QKD protocol and especially the QKD protocol with subspaces which was introduced in Mirdit Doda's et al. paper [1] works. By reading through the mentioned paper, it was not exactly clear why the subspace QKD works so well, therefore, an explanation was given with the help of *Filtering* 8.5, which could probably constitute the theory behind the whole protocol. Finally, a more elegant solution to the optimisation problem of the SDP was found 8.3. Moreover, an improvement of the protocol by undertaking a specific measurement, called *MUB*, was done and solved 10.3.1. Such MUBs improve the protocol as it can be seen in figure 10.2. In this chapter, the results of the above solution of the SDP will be discussed. Moreover, this theoretical concept is not just a theory. In the end, there is a short explanation of how Carlos Sevilla et al. from Fraunhofer institute in Jena could build an experiment and realise the theory which was presented in this thesis.

## 11.1 Experiment

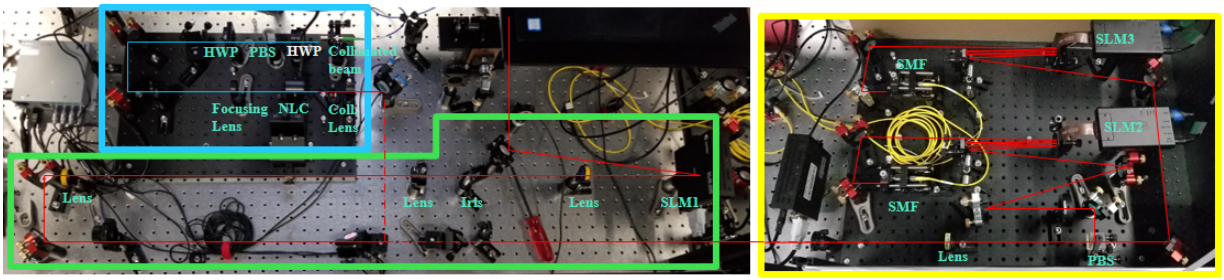


Figure 11.1: Blue: SDPC characterisation. Green: classical beam shaping (alignment). Yellow: Detection system

With permission of Carlos Sevilla, one can see in figure 11.1 the setup which he used for the experiment. Here, a collimated beam acts as a photon source. After the beam interacts with some optical devices, it comes to the NLC which stands for *Non-linear*

*crystal*. As already discussed in chapter 7.3, a NLC creates entanglement by using the characteristic electric susceptibility of the NLC under the phase matching condition and energy conservation. The red lines indicate the way which the entangled photons use. One beam will be measured in the detection system. In essence, a *spatial light modulator (SML)* was used. This device "sculpts" the photon. In this setup, they are using it for measuring on different bases. The general idea, as used in most measurements in the world, is that a measurement can only be done in a fixed basis $|i\rangle$. Then, in order to measure in a different basis $|\gamma_i\rangle$, one finds a unitary transformation $U$ so that $|\gamma_i\rangle = U|i\rangle$. By applying $U^\dagger$ to the quantum state $|\psi\rangle$, one gets the desired probabilities $|\langle\gamma_i|\psi\rangle|^2 = |\langle i|U^\dagger|\psi\rangle|^2$. The SLM creates such a unitary transformation $U$ [70].
For the measurement they chose tomography. Here, they measured the mutually entangled bases. Let $\Pi_k$ be the $i$th projector of the $k$th MUB. Then, if one measures $\mathrm{Tr}(\rho\Pi_k \otimes \Pi_l^j)$ $\forall i, j, k, l$, there is a single state $\rho$ that can reproduce these statistics. The actual measurement is then done by the *single mode fiber (SMF)*.

### 11.1.1 Results

In theory, it is easy to say "we measure a state". Every time an experiment is conducted, experimentalists struggle with the question of how to find a measuring system for a specific experiment. For example, it is impossible for a quantum measurement to distinguish with certainty between non-orthogonal states such as $|0\rangle$ and $(|0\rangle + |1\rangle)/\sqrt{2}$ [8]. In general, it is impossible to obtain an outcome with 100% certainty. Instead, statistics such as the estimation of a state $\rho$ is used. An experiment will be repeated many times which creates many copies of $\rho$. Through measuring, one gets a statistics on, how the states could look like. Now, an example from [8] will be discussed shortly for further understanding. Suppose that one wants to get the statistical outcome of $\rho$ whereby the set of an orthonormal set of matrices in the Hilbert space are $I/\sqrt{2}$, $X/\sqrt{2}$, $Y/\sqrt{2}$, $Z/\sqrt{2}$. The density matrix can be found as

$$\rho = \frac{\mathrm{Tr}(\rho)I + \mathrm{Tr}(X\rho)X + \mathrm{Tr}(Y\rho)Y + \mathrm{Tr}(Z\rho)Z}{2} \tag{11.1}$$

For example, $\mathrm{Tr}(X\rho)$ has the obtained outcome $x_1, x_2, ..., x_m$ equal to $+1$ or $-1$ for a large number $m$ of run through. The average of this quantity is simply $\sum_i x_i/m$ which is an estimation of $\mathrm{Tr}(X\rho)$.
Finally, a map of each possible case of a quantum state in a dimension $d$ indicating their number of clicks of an $n$ times repeated experiment is obtained.

## 11.2 Final remarks

As already written, a more resistant QKD protocol than described in [1] was found. Clearly, this will not be “The One” QKD protocol which will solve all problems of physicists. Still, there is a long way to go to finally use quantum communication. Of course, there are some startups which already build quantum devices for quantum communication [71],

however, they are not working well enough yet. Nevertheless, quantum information is one the most promising ways to start a new decade of information theory and therefore of communication. Perhaps it will never completely supersede classical information as quantum theory right now teaches us. It is just too powerful for private use. But clearly, there will be a time when both methods coexist and will be used frequently. Quantum computation could solve our limitation of the power of our computer. It would be possible to simulate and calculate scientific models much more easily and quicker than a classical computer could ever do. Nobody can estimate when the time for useful quantum computers and quantum technology will come. Still, there is a long way to go and quantum physicists are still in the beginning of this fascinating world. Therefore, this research will hopefully positively contribute to the next huge steps in quantum computation and quantum information.

# Bibliography


[1] Mirdit Doda, Marcus Huber, Gláucia Murta, Matej Pivoluska, Martin Plesch, and Chrysoula Vlachou. Quantum key distribution overcoming extreme noise: simultaneous subspace coding using high-dimensional entanglement. 2020. URL: `https://arxiv.org/abs/2004.12824`, `arXiv:2004.12824`.

[2] Henrik Nordström. *Emotional communication in the human voice*. PhD thesis, Department of Psychology, Stockholm University, 2019.

[3] Colin Cherry. On human communication. 1966.

[4] Andrew Adamatzky. Language of fungi derived from their electrical spiking activity. *Royal Society Open Science*, 9(4):211926, 2022.

[5] JH Sudd. Interaction between ants on a scent trail. *Nature*, 183(4675):1588–1588, 1959.

[6] Michael W Fox. A comparative study of the development of facial expressions in canids; wolf, coyote and foxes. *Behaviour*, 36(1-2):49–73, 1970.

[7] Steven Roger Fischer. *History of writing*. Reaktion books, 2003.

[8] Michael A Nielsen and Isaac Chuang. Quantum computation and quantum information, 2010.

[9] Dennis Luciano and Gordon Prichett. Cryptology: From caesar ciphers to public-key cryptosystems. *The College Mathematics Journal*, 18(1):2–17, 1987.

[10] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nature Photonics*, 8(8):595–604, 2014.

[11] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

[12] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301, 2009.

[13] Gilles Brassard. Brief history of quantum cryptography: A personal perspective. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.*, pages 19–23. IEEE, 2005.

[14] G Brassard and Charles H Bennett. Quantum cryptography: Public key distribution and coin tossing. In *International conference on computers, systems and signal processing*, 1984.

[15] Artur K Ekert. Quantum cryptography and bell's theorem. In *Quantum Measurements in Optics*, pages 413–418. Springer, 1992.

[16] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, 94(23):230504, 2005.

[17] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018, 1998.

[18] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.

[19] William K Wootters and Wojciech H Zurek. The no-cloning theorem. *Physics Today*, 62(2):76–77, 2009.

[20] Michel Le Bellac et al. *A short introduction to quantum information and quantum computation*. Cambridge University Press, 2006.

[21] Roger G Newton. What is a state in quantum mechanics? *American Journal of Physics*, 72(3):348–350, 2004.

[22] Matthew F Pusey, Jonathan Barrett, and Terry Rudolph. On the reality of the quantum state. *Nature Physics*, 8(6):475–478, 2012.

[23] Luigi Del Debbio. Lecture notes 1. quantum states. *Edinburgh University*, 2006.

[24] Juan I Cirac and Peter Zoller. Quantum computations with cold trapped ions. *Physical review letters*, 74(20):4091, 1995.

[25] Brian David Josephson. Possible new effects in superconductive tunnelling. *Physics letters*, 1(7):251–253, 1962.

[26] John Preskill. Lecture notes for physics 229: Quantum information and computation. *California Institute of Technology*, 16(1):1–8, 1998.

[27] Peter Shor. Lecture notes quantum computing. 18.435 / 2.111. fall 2008. *MIT*.

[28] P Campagne-Ibarcq, A Eickbusch, S Touzard, E Zalys-Geller, NE Frattini, VV Sivak, P Reinhold, S Puri, S Shankar, RJ Schoelkopf, et al. A stabilized logical quantum bit encoded in grid states of a superconducting cavity. *arXiv preprint arXiv:1907.12487*, 2019.

[29] LJ Stephenson, DP Nadlinger, BC Nichol, S An, P Drmota, TG Ballance, K Thirumalai, JF Goodwin, DM Lucas, and CJ Ballance. High-rate, high-fidelity entanglement of qubits across an elementary quantum network. *Physical review letters*, 124(11):110501, 2020.

[30] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[31] Wei Zhang, Dong-Sheng Ding, Yu-Bo Sheng, Lan Zhou, Bao-Sen Shi, and Guang-Can Guo. Quantum secure direct communication with quantum memory. *Physical review letters*, 118(22):220501, 2017.

[32] Markus Grassl. Classical information theory and classical error correction. *Quantum Information: From Foundations to Quantum Technology Applications*, pages 1–17, 2016.

[33]

[34] Lachlan Gilbert. Quantum computing in silicon hits 99 per cent accuracy, 18.October 2022. URL: `https://newsroom.unsw.edu.au/news/science-tech/quantum-computing-silicon-hits-99-cent-accuracy`.

[35] Alexandru Paler and Simon J Devitt. An introduction into fault-tolerant quantum computing. In *Proceedings of the 52nd Annual Design Automation Conference*, pages 1–6, 2015.

[36] Charles H Henry and Rudolf F Kazarinov. Quantum noise in photonics. *Reviews of Modern Physics*, 68(3):801, 1996.

[37] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of modern physics*, 81(2):865, 2009.

[38] Agnes Ferenczi. Security proof methods for quantum key distribution protocols. 2013.

[39] Sebastian Ecker, Frédéric Bouchard, Lukas Bulla, Florian Brandt, Oskar Kohout, Fabian Steinlechner, Robert Fickler, Mehul Malik, Yelena Guryanova, Rupert Ursin, et al. Overcoming noise in entanglement distribution. *Physical Review X*, 9(4):041042, 2019.

[40] Reinhold A Bertlmann, Katharina Durstberger, Beatrix C Hiesmayr, and Philipp Krammer. Optimal entanglement witnesses for qubits and qutrits. *Physical Review A*, 72(5):052331, 2005.

[41] Beatrix Hiesmayer. Lecture notes: Quantum information i. *Universität Wien.*

[42] Manuel Erhard, Mario Krenn, and Anton Zeilinger. Advances in high-dimensional quantum entanglement. *Nature Reviews Physics*, 2(7):365–381, 2020.

[43] Melanie G McLaren, Filippus S Roux, and Andrew Forbes. Realising high-dimensional quantum entanglement with orbital angular momentum. *South African Journal of Science*, 111(1-2):01–09, 2015.

[44] Alois Mair, Alipasha Vaziri, Gregor Weihs, and Anton Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412(6844):313–316, 2001.

[45] Mirdit Doda. Unpublished notes. *Universität Wien*.

[46] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:052306, Apr 2000. URL: https://link.aps.org/doi/10.1103/PhysRevA.61.052306, doi:10.1103/PhysRevA.61.052306.

[47] Dominic Mayers and Andrew Yao. Self testing quantum apparatus. *Quantum Info. Comput.*, 4(4):273–286, July 2004.

[48] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[49] John S Bell. Speakable and unspeakable in quantum mechanics, 1989.

[50] John S Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[51] Marek Żukowski and Časlav Brukner. Quantum non-locality—it ain't necessarily so... *Journal of Physics A: Mathematical and Theoretical*, 47(42):424009, oct 2014. doi:10.1088/1751-8113/47/42/424009.

[52] Sandu Popescu. Bell's inequalities and density matrices: revealing "hidden" nonlocality. *Physical Review Letters*, 74(14):2619, 1995.

[53] Jinhyoung Lee and MS Kim. Entanglement teleportation via werner states. *Physical review letters*, 84(18):4236, 2000.

[54] Sandu Popescu. Bell's inequalities versus teleportation: What is nonlocality? *Physical review letters*, 72(6):797, 1994.

[55] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, 2020.

[56] T. Yang and M. Navascués. Robust self testing of unknown quantum systems into any entangled two-qubit states. *Physical Review A*, 87, 2013. URL: https://arxiv.org/abs/1210.4409.

[57] Joseph Bowles, Ivan Šupić, Daniel Cavalcanti, and Antonio Acín. Device-independent entanglement certification of all entangled states. *Physical Review Letters*, 121(18), Oct 2018. URL: http://dx.doi.org/10.1103/PhysRevLett.121.180503, doi:10.1103/physrevlett.121.180503.

[58] Miguel Navascués and Tamás Vértesi. Activation of nonlocal quantum resources. *Phys. Rev. Lett.*, 106:060403, Feb 2011. URL: https://link.aps.org/doi/10.1103/PhysRevLett.106.060403, doi:10.1103/PhysRevLett.106.060403.

[59] Julian Schwinger. Unitary operator bases. *Proceedings of the national academy of sciences of the United States Of America*, 46(4):570, 1960.

[60] Andreas Klappenecker and Martin Rötteler. Constructions of mutually unbiased bases. In *International Conference on Finite Fields and Applications*, pages 137–144. Springer, 2003.

[61] Somshubhro Bandyopadhyay, P Oscar Boykin, Vwani Roychowdhury, and Farrokh Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, 2002.

[62] Martin Ringbauer, Devon N Biggerstaff, Matthew A Broome, Alessandro Fedrizzi, Cyril Branciard, and Andrew G White. Experimental joint quantum measurements with minimum uncertainty. *Physical review letters*, 112(2):020401, 2014.

[63] William H Louisell. Amplitude and phase uncertainty relations. *Phys. Letters*, 7, 1963.

[64] Christoph Spengler, Marcus Huber, Stephen Brierley, Theodor Adaktylos, and Beatrix C Hiesmayr. Entanglement detection via mutually unbiased bases. *Physical Review A*, 86(2):022311, 2012.

[65] ID Ivonovic. Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General*, 14(12):3241, 1981.

[66] Ingemar Bengtsson. Three ways to look at mutually unbiased bases. In *AIP Conference Proceedings*, volume 889, pages 40–51. American Institute of Physics, 2007.

[67] Hermann Weyl. Gruppentheorie und quantenmechanik, hirzel, leipzig. *Theory of Groups and Quantum Mechanics, 2nd ed.(1931), transl. HP Robertson, Dover, NY (1950)*, pages 100–101, 1928.

[68] Wojciech Tadej and Karol Życzkowski. A concise guide to complex hadamard matrices. *Open Systems & Information Dynamics*, 13(2):133–177, 2006.

[69] Andreas Klappenecker and M Rotteler. Mutually unbiased bases are complex projective 2-designs. In *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005.*, pages 1740–1744. IEEE, 2005.

[70] Mateus Araújo. Mail. *IQOQI Wien*.

[71] Jeff Vance. 10 hot quantum-computing startups to watch, 17.October 2022. URL: `https://www.networkworld.com/article/3489098/10-hot-quantum-computing-startups-to-watch.html`.