Towards Secure Quantum Cloud Computing

through NV-center enabled MDI-QKD

W. Hordijk

Technische Universiteit Delft

TU Delft Delft University of Technology

Challenge the future

Towards Secure Quantum Cloud Computing

through NV-center enabled MDI-QKD

by

W. Hordijk

in partial fulfillment of the requirements for the degree of

Master of Science
in Applied Physics

at the Delft University of Technology,
to be defended publicly on Thursday July 17, 2014 at 10:00 AM.

Supervisor:	Dr. M. Blaauboer	
Thesis committee:	Prof. dr. Y. M. Blanter,	TU Delft
	Prof. dr. R. Hanson,	TU Delft

This thesis is confidential and cannot be made public until July 17, 2014.

TU Delft Delft University of Technology

PREFACE

To understand how nature works. That was the goal I had in mind when I started studying "Technische Natuurkunde" at TU Delft in 2008, after first having spent a number of years on figuring out what it was that I wanted to do. Soon I realized my underestimation of the set goal and that I needed to find a field of interest somewhere in between astrophysics and quantum physics for me to sink my teeth in. I chose to dive into the world of the smallest. In 1959, Richard Feynman said in a talk at the annual meeting of the American Physical Society that "there is plenty of room at the bottom", meaning that the there is much physics to still be discovered and understood at the smallest scale. The research being done "at the bottom" at TU Delft is groundbreaking and on the cutting edge of today's science and technology, and I am proud to say that I have been given the opportunity to be a part of that.

With this work I present the research that I have been conducting at the theoretical physics research group as part of the department of quantum nanoscience for the past nine months. This work will be my last achievement as a student and so it symbolizes an important part of my life. We live in an exciting time and doing theory in Delft is in particular exhilarating as it often forms the foundation for concepts in the thrilling science of quantum information. It's a humbling experience to walk and sit among the people who are on the verge of changing the world, or actually already in the process of doing so, by exploring the newest, most promising directions of modern science and technology.

As for everything else, I would like to thank my girlfriend Deborah for being the best girlfriend one could imagine. Without her understanding, love, and support I would have never been where I am today. The same goes for my parents, whose support I can always count on. Thanks for everything.

W. Hordijk
Delft, July 2014

Contents

1

Introduction

There is no question that at the time of writing this thesis, quantum information science and technology is a hot topic. The world's largest and most influential universities, research institutes and companies are massively investing in getting on board with the development of quantum computing. A quantum computer is a machine that relies on characteristically quantum phenomena, such as quantum interference and quantum entanglement, in order to perform computation. The advantages of exploiting these phenomena become apparent mostly in theoretical research as there are still big and many engineering challenges to be overcome before an actual quantum computer may be built.

1.1. Quantum Information Science

Quantum information science explores the processing and communication of information based on control and measurement of registers of quantum bits (qubits). The difference between qubits and classical bits is that qubits can be in a superposition and that they can be entangled: two concepts that have a no classical equivalent. Algorithms that are devised to exploit these properties may offer tremendous speedups in comparison with their classical counterparts. Famous examples are the generally theorized simulation of quantum systems by Richard Feynman [1], Grover's algorithm for searching [2], and Shor's algorithm for factoring [3]. Another exploit of the concepts of superposition and entanglement yields methods that guarantee the security of communication by means of encryption techniques and key distribution based on the exchange of qubits.

In the last few decades, the interest in quantum information technology has been rapidly increasing and in industry there already exist companies that supply quantum key distribution systems [4] or even a full-blown quantum computer [5], though both arguably not fully matured. In research, there is the Dutch Quantum Technology Institute (QuTech) that was announced near the end of 2013: a collaboration between Delft University of Technology and research institute TNO to ultimately develop a quantum computer.

However, useful implementations of quantum computing and quantum communication are still a thing of the future and currently the focus lies mainly with proof-of-principle experiments. As a very recent example, the concept of unconditional quantum state teleportation has been demonstrated by the Quantum Transport group at Delft University of Technology [6], providing an important step towards several theoretical schemes that rely on the principle of quantum teleportation.

1.1.1. Quantum bits

Quantum data storage, being one of the building blocks in quantum computation, calls for a solid-state implementation. This because we require qubits to be localized and have ideally long coherence times. Several implementations of solid-state qubits exist.

In a vacuum, charged atomic particles may be trapped by electromagnetic fields. The actual qubit is defined by the electronic states within each ion and qubit states may be coupled by lasers to allow for

single qubit operations. The discretized motion states of the trapped ions are coupled to each other via the Coulomb force, i.e. phonon coupling, and allow for information processing. One of the main advantages of this type of qubits is that they can be very well controlled and have coherence times that can exceed a second. Furthermore, they provide an interface to photons that can in turn be used for long distance communication, however the coupling rate to photons, which is in the order of a second, is considered to be quite low. Another downside to this type of qubits is the lack of scalability as phonon coupling hardly scales up for ensembles of more than several tens of atoms.

Another way to realize a qubit is that it is possible to localize electrons within a solid-state environment, so that a qubit may be defined by their spin. The main advantage of this type of qubits is the scalability since it is technically possible to create a large density of quantum dots which can be electronically addressed. However, decoherence times are such that proper control proves to be the main challenge. Furthermore, the nature of creating quantum wells is a process that is very hard to exactly reproduce.

To the family of superconducting qubits, qubits that are defined by some device that is linked to a superconducting circuit, belong the so-called flux qubits, charge qubits and phase qubits. Flux qubits, conceived, proposed and implemented in Delft first [7], can be formed by near-microscopically sized loops of a superconducting metal with one ore more Josephson junctions. By applying an external flux, a persistent current may rung through the loops. The qubit is defined by the direction of this current. Charge qubits can be formed by a superconducting island coupled by a Josephson junction to a superconducting reservoir. The qubit is defined by the number of Cooper pairs that have tunneled through the junction, onto the island. Finally, phase qubits are closely related to both flux qubits and charge qubits, but are based on a superconductor-insulator-superconductor Josephson junction. The main advantage of superconducting qubits is that they can be designed with great variety and on a relatively large scale. This can also be a drawback for scaling many qubits onto a limited surface. Another downside is that the coherence times for superconducting qubits are still limited.

Arguably the most promising type of qubit may be defined within a solid state by means of dopant atoms, for instance a nitrogen-vacancy center (NV-center) in diamond, where a qubit can be defined in multiple ways, as we will see later on. One of the main advantages of this type of qubits is that they can be very well controlled and with long coherence times. In specific configurations it may be possible to electronically control the qubits and in principle it is possible to scale the qubits down to the size that they can be used on a chip. Furthermore, just like trapped atoms, the provide an interface to photons that can in turn be used for long distance communication. A disadvantage is that coupling NV-centers requires great control over their localization, which is a technologically challenging task.

Within quantum communication, we have the need for speed-of-light data transfer and a low decoherence rate. The use of the fundamental quantum of light, the photon, readily comes to mind and it turns out that it might be very useful for this purpose. A qubit in a photon may be defined by for instance its polarization or the number of photons in a signal. Note that due to its velocity photons are usually very difficult to control electronically.

1.1.2. QUANTUM NETWORKS

In quantum networks [8], data is communicated as quantum states through the technique of entanglement via an optical fiber link. Given the favorable properties of the different kinds of qubits as described earlier, it seems logical to implement NV-centers as the solid-state solution to store data and photons as the medium to communicate data. A quantum network may contain quantum repeaters that are based on teleportation schemes, solid state solutions to store states and mobile states to send data: again the types of qubit come into play and we can opt for the NV-center combined with photons.

1.2. THESIS LAYOUT

In chapter 2 of this thesis, an analysis of the electronic structure of the negatively charged NV-center (simply referred to as NV-center) will be performed to gain an insight on how this structure allows for the use of it as a qubit. The choice to analyze the NV-center has been made because of its promising characteristics regarding a coherent coupling to photons, scalability and long coherence time. Chapter 3 focuses on several quantum key distribution protocols, starting from the prototype of quantum key

distribution and finally reviewing a state of the art concept that is known as a measurement-device-independent protocol, closing some of the existing loopholes in the established schemes. In chapter 4, a solid state implementation of a quantum random access memory will be discussed. We will in particular look into the dynamics of the photon switching mechanism that is required to realize such a device. A generalized model will be proposed and some initial results will be discussed. Chapter 5 will cover some insights on the use of the NV-center as a solid-state qubit in both the measurement-device-independent quantum key distribution protocol and the earlier proposed photon switching device, which might be a useful analysis in the conceptual development of secure cloud based quantum computing and be one of the fundamental building blocks.

2

THE NV-CENTER

2.1. INTRODUCTION

An NV-center in diamond is known to consist of a nitrogen atom and a first-neighbor vacancy in the carbon lattice, as depicted in figure 2.1. Due to the vacancy, there are three dangling carbon bonds and at the nitrogen site, there are two. This adds up to a total of five electrons. Several experiments have however revealed that the ground state is a spin triplet, implying that the number of active electrons at the center is even. It is taken that the neutral NV-center has acquired an additional electron from elsewhere in the lattice, most likely from another substitutionary nitrogen atom. A total of six electrons then occupy the dangling electron bonds of the vacancy complex. This model is known as the Loubser and Van Wyk model [9] and effectively describes a negatively charged NV-center, or NV^--center. From now on, when the NV-center is mentioned, we in fact refer to this NV^--center.

In this chapter we will perform an analysis of the electronic structure of the NV-center, utilizing group theory to exploit the configurational symmetries to categorize states in terms of energy [10–13]. First, we will categorize the orbital functions and find the ground state, first excited state and second excited state of an NV-center containing two free electrons, which we will than translate into the states for a NV-center containing two holes, effectively describing the Loubser and Van Wyck model [9]. We will conclude with a diagram presenting an overview of the electronic structure of the NV-center and all the associated states.

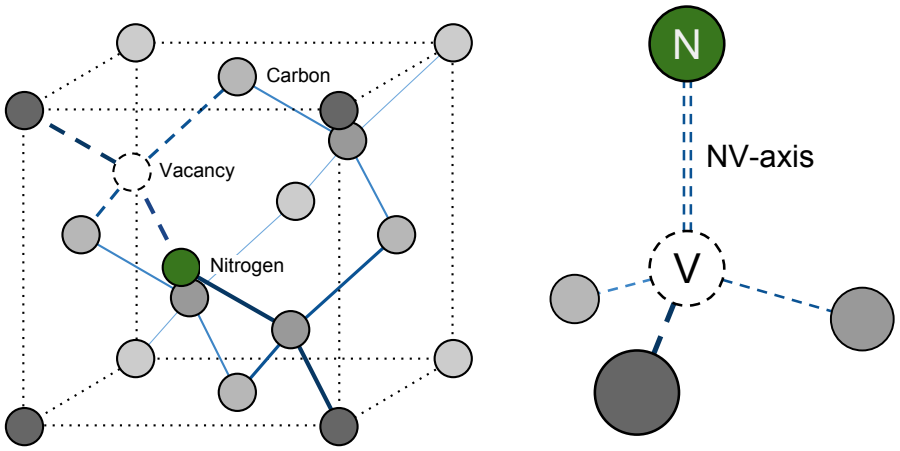

Figure 2.1: The NV-center in a unit cell of the diamond lattice structure (left) and the axial C_{3v} symmetry structure for the dangling bonds (right).

2.2. ELECTRONIC MODEL AND ASSOCIATED DYNAMICS

The dangling bonds are formed from sp^3 orbitals of the carbon and nitrogen atoms [14]. The orbitals from the carbon atoms we will refer to as a, b and c and the orbital from the nitrogen atom we will refer to as d. Figure 2.1 shows the structure to have a C_{3v} symmetry, so that the orbitals can be constructed as orthonormal linear combinations of the atomic orbitals a, b, c, and d through projection operator techniques as follows [10, 13]:

$$u = d - \lambda v, \quad v = \frac{a+b+c}{\sqrt{3+6S}} \tag{2.1}$$

$$e_x = \frac{2c-a-b}{\sqrt{6-6S}}, \quad e_y = \frac{a-b}{\sqrt{2-2S}} \tag{2.2}$$

with:

$$\lambda = \int (ab)\ \mathrm{d}^3 r \tag{2.3}$$

$$S = \int (dv)\ \mathrm{d}^3 r \tag{2.4}$$

The non-degenerate orbital functions u and v transform as the one dimensional irreducible A_1 symmetry, whereas the degenerate $\{e_x, e_y\}$ transform as the three dimensional irreducible $E_{\{x,y\}}$ symmetry [10]. The lowest energy is associated with the u state as this state is localized on the highly polarized nitrogen. The state v is the next lowest orbital state since it is totally symmetric. The doubly degenerate e states have the highest energy among the basis states [13, 15].

We start the analysis by regarding the case in which we have $n = 2$ active electrons. This case corresponds to the physical situation in which the two electrons from the nitrogen dominate the electromagnetic response. We will later show that when regarding the electrons as holes this case is perfectly analogous to the case in which $n = 6$, corresponding to a negatively charged NV-center (Ground state e^2, first excited state ve, and second excite state v^2).

2.2.1. MULTI-ELECTRON STATES

At this point it is convenient to introduce the multi-electron states, which can be done through the use of Slater determinants, guaranteeing the required anti-symmetric wave functions. We define:

$$|a\bar{b}\cdots r\rangle \equiv \frac{1}{\sqrt{N!}} \begin{vmatrix} a(1)\,\alpha(1) & a(2)\,\alpha(2) & \cdots & a(N)\,\alpha(N) \\ b(1)\,\beta(1) & b(2)\,\beta(2) & \cdots & b(N)\,\beta(N) \\ \vdots & \vdots & \ddots & \vdots \\ r(1)\,\alpha(1) & r(2)\,\alpha(2) & \cdots & r(N)\,\alpha(N) \end{vmatrix} \tag{2.5}$$

$$= \frac{1}{\sqrt{N!}} \sum_P (-1)^{\Theta(P)} \left[a(1)\,\alpha(1)\,b(2)\,\beta(2)\cdots r(N)\,\alpha(N)\right]_P \tag{2.6}$$

where overlined wave functions have a spin opposite to non-overlined wave functions, P is the permutation operator and:

$$\Theta(P) = \begin{cases} 1, & P \text{ is an odd permutation} \\ 0, & P \text{ is an even permutation} \end{cases} \tag{2.7}$$

2.2.2. TWO ACTIVE ELECTRONS, OR THE NITROGEN DOMINANT NV-CENTER

GROUND STATE MANIFOLD

For $n = 2$, the lowest energy configurations are u^2, v^2, and uv. These are all orbital singlets which transform in real space as $A_1 \otimes A_1 = A_1$ [10]. Only a spin singlet, two-electron state can satisfy the Pauli principle in the u^2 configuration, which in the Slater determinant notation is given by:

$$|u\bar{u}\rangle \equiv \tfrac{1}{\sqrt{2}} \left[u(1)\,\bar{u}(2) - u(2)\,\bar{u}(1)\right] \tag{2.8}$$

where u (i) denotes the $i$the electron occupying the u orbital. Similarly, the v^2 configuration is given by $|v\overline{v}\rangle$.

The uv configuration is spanned by the states $|uv\rangle$, $|u\overline{v}\rangle$, $|\overline{u}v\rangle$, and $|\overline{u}\overline{v}\rangle$, which we can combine into the singlet/triplet state configurations:

$$\frac{1}{\sqrt{2}}\left(|u\overline{v}\rangle - |\overline{u}v\rangle\right) \qquad \text{(singlet)} \tag{2.9}$$

$$|uv\rangle\,, \quad \frac{1}{\sqrt{2}}\left(|u\overline{v}\rangle + |\overline{u}v\rangle\right), \quad |\overline{u}\overline{v}\rangle \quad \text{(triplet)} \tag{2.10}$$

based on the singlet/triplet spin configurations [16].

FIRST EXCITED STATE MANIFOLD

Looking at the manifold of the first excited states, we have that the candidate configurations are ue and ve, which transform in real space as $A_1 \otimes E = E$ [10]. The Slater states spanning the ue configuration space are $|ue_x\rangle$, $|ue_y\rangle$, $|\overline{u}e_x\rangle$, $|\overline{u}e_y\rangle$, $|u\overline{e}_x\rangle$, $|u\overline{e}_y\rangle$, $|\overline{u}\overline{e}_x\rangle$, and $|\overline{u}\overline{e}_y\rangle$, which can be combined into singlet and triplet states as done for the configurations in the ground state manifold. A similar result applies to the ve configuration, yielding a first excited state manifold containing a total of 16 basis states, as can be seen in table 2.1

SECOND EXCITED STATE MANIFOLD

Moving into the next set of excited states, we have the e^2 configuration which transforms as $E \otimes E = A_1 \oplus A_2 \oplus E$ in real space [10]. According to Pauli's exclusion principle and the indistinguishableness of states we end up with merely six states spanning the e^2 configuration, namely: $|e_x\overline{e}_x\rangle$, $|e_y\overline{e}_y\rangle$, $|e_xe_y\rangle$, $|e_x\overline{e}_y\rangle$, $|\overline{e}_xe_y\rangle$, and $|\overline{e}_x\overline{e}_y\rangle$.

Note that states in which electrons occupy the orbital with the same angular momentum are necessarily singlet states, whereas states in which the electrons occupy different orbitals may be either singlet or triplet. However, these states are fully analogous to u^2 when the electrons occupy the same orbital and they are fully analogous to uv when they occupy different orbitals. We may thus generalize the states and introduce the following notation: $u\overline{u} \to e_i\overline{e}_i$ and $uv \to e_xe_y$. The singlet states are then:

$$\frac{1}{\sqrt{2}}\left(|e_x\overline{e}_x\rangle + |e_y\overline{e}_y\rangle\right), \quad \frac{1}{\sqrt{2}}\left(|\overline{e}_xe_y\rangle - |e_x\overline{e}_y\rangle\right), \quad \frac{1}{\sqrt{2}}\left(|e_x\overline{e}_x\rangle - |e_y\overline{e}_y\rangle\right) \tag{2.11}$$

and the triplets are found to be:

$$|e_xe_y\rangle\,, \quad \frac{1}{\sqrt{2}}\left(|\overline{e}_xe_y\rangle + |e_x\overline{e}_y\rangle\right), \quad |\overline{e}_x\overline{e}_y\rangle \tag{2.12}$$

For an overview of the configurations, the associated states, of which the degeneracy and symmetry for each is given, see table 2.1.

2.2.3. TOTAL WAVE FUNCTIONS

With the multi-electron spin eigenstates as given in table 2.1, total wave functions spanning the entire product space can be readily constructed. It is our goal to form linear combinations of spin eigenstates such that they transform according to the C_{3v} point group of the NV-center and are thus irreducible with respect to both spin S and orbital angular momentum Ω.

For $n = 2$, we had the lowest energy states to be in the u^2, v^2, uv, ue, ve, and e^2 configurations. Preparing states based on these configurations, which are irreducible in C_{3v} symmetry, can be done for a small number of electrons using the basis-function generating machine [10]. The mentioned configurations transform as $A_2 \otimes A_2, A_1 \otimes A_1, A_2 \otimes A_1, A_2 \otimes E, A_1 \otimes E$, and $E \otimes E$ under C_{3v} point-group symmetry, respectively. Product states of the form $\Gamma_i \otimes A_1$ transform as irreducible representations of Γ_i, $A_2 \otimes A_2$ transforms as A_1 and $A_{1,2} \otimes E$ transform as E (see C_{3v} point group product table), which are all obviously irreducible. Thus, the states as previously constructed that are in the u^2, v^2, uv, ue, and ve configurations are already in the proper form to represent the full multi-electron wave-functions. The e^2 configuration however transforms as $E \otimes E = A_1 \oplus A_2 \oplus E$ and is thus not in the irreducible form. In order to identify four wave functions which are irreducible in terms of S and Ω we need to take additional steps.

Configuration	Γ	g	Wave function
u^2	$^1A_1$	1	$\|u\bar{u}\rangle$
v^2	$^1A_1$	1	$\|v\bar{v}\rangle$
uv	$^1A_1$	1	$\frac{1}{\sqrt{2}}\left(\|u\bar{v}\rangle - \|\bar{u}v\rangle\right)$
	$^3A_1$	3	$\|uv\rangle, \frac{1}{\sqrt{2}}\left[\|u\bar{v}\rangle + \|\bar{u}v\rangle\right], \|\bar{u}\bar{v}\rangle$
ue	^1E	2	$\frac{1}{\sqrt{2}}\left(\|u\bar{e}_x\rangle - \|\bar{u}e_x\rangle\right), \frac{1}{\sqrt{2}}\left(\|u\bar{e}_y\rangle - \|\bar{u}e_y\rangle\right)$
	^3E	6	$\|ue_x\rangle, \frac{1}{\sqrt{2}}\left(\|u\bar{e}_x\rangle + \|\bar{u}e_x\rangle\right), \|\bar{u}\bar{e}_x\rangle, \|ue_y\rangle, \frac{1}{\sqrt{2}}\left(\|u\bar{e}_y\rangle + \|\bar{u}e_y\rangle\right), \|\bar{u}\bar{e}_y\rangle$
ve	^1E	2	$\frac{1}{\sqrt{2}}\left(\|v\bar{e}_x\rangle - \|\bar{v}e_x\rangle\right), \frac{1}{\sqrt{2}}\left(\|v\bar{e}_y\rangle - \|\bar{v}e_y\rangle\right)$
	^3E	6	$\|ve_x\rangle, \frac{1}{\sqrt{2}}\left(\|v\bar{e}_x\rangle + \|\bar{v}e_x\rangle\right), \|\bar{v}\bar{e}_x\rangle, \|ve_y\rangle, \frac{1}{\sqrt{2}}\left(\|v\bar{e}_y\rangle + \|\bar{v}e_y\rangle\right), \|\bar{v}\bar{e}_y\rangle$
e^2	$^1A_1$	1	$\frac{1}{\sqrt{2}}\left(\|e_x\bar{e}_x\rangle + \|e_y\bar{e}_y\rangle\right)$
	^3E	3	$\|e_xe_y\rangle, \frac{1}{\sqrt{2}}\left(\|e_x\bar{e}_y\rangle + \|\bar{e}_xe_y\rangle\right), \|\bar{e}_x\bar{e}_y\rangle$
	^1E	2	$\frac{1}{\sqrt{2}}\left(\|e_x\bar{e}_x\rangle - \|e_y\bar{e}_y\rangle\right), \frac{1}{\sqrt{2}}\left(\|\bar{e}_xe_y\rangle - \|e_x\bar{e}_y\rangle\right)$

Table 2.1: Wave functions for the NV-center for $n = 2$ active electrons in Slater determinant notation. The symmetry of each state is given as Γ and its degeneracy is tabulated under g.

A way to find irreducible total wave functions Ψ is to apply the projection operator [10] to the reducible product of two functions Ψ^{Γ_p} and Ψ^{Γ_q}, describing spin and orbital angular momentum portions of the wave function, respectively. The projection operator for the jth representation, denoted by $P^{(j)}$, is defined as:

$$P^{(j)} = \frac{l_j}{h}\sum_R \chi_j(R)\, P_R \tag{2.13}$$

where l_j is the degree of the representation, h is the number of elements in the group, $\chi(R)$ is the character for operation R, and P_R is the symmetry operation R. For example, a wave function with an A_1 symmetry may be determined as follows [10]:

$$P^{A_1}\left(\psi^{E_x}\psi^{E_y}\right) = 0, \quad P^{A_1}\left(\psi^{E_x}\psi^{E_x}\right) = \frac{1}{2}\left(\psi^{E_x}\psi^{E_x} + \psi^{E_y}\psi^{E_y}\right) = P^{A_1}\left(\psi^{E_y}\psi^{E_y}\right) \tag{2.14}$$

Applying this projection principle to the singlet state $|e_x\bar{e}_x\rangle$ and its degenerate counterpart $|e_y\bar{e}_y\rangle$ we find the irreducible representation with an A_1 symmetry:

$$|\Psi^{A_1}\rangle = \frac{1}{\sqrt{2}}\left(|e_x\bar{e}_x\rangle + |e_y\bar{e}_y\rangle\right) \tag{2.15}$$

The remaining wave functions are [10]:

$$|\Psi^{A_2}\rangle = \frac{1}{\sqrt{2}}\left(|\bar{e}_xe_y\rangle + |e_x\bar{e}_y\rangle\right), \quad |\Psi^E_x\rangle = \frac{1}{\sqrt{2}}\left(|e_x\bar{e}_x\rangle - |e_y\bar{e}_y\rangle\right), \quad |\Psi^E_y\rangle = \frac{1}{\sqrt{2}}\left(|\bar{e}_xe_y\rangle - |e_x\bar{e}_y\rangle\right) \tag{2.16}$$

The notation of the wave functions is $|\Psi^{\Gamma_r}_\alpha\rangle$, where Γ is the representation within manifold r (ground or excited state) and α distinguishes x and y components of the degenerate E representation where applicable.

We may directly go into a representation of a two-hole wave function, including space and spin degrees of freedom, by means of a direct product of the representation of each hole Γ_{hn} and its spin $\Gamma_\psi = \prod_n \Gamma_{hn} \otimes D_{1/2}$, where $D_{1/2}$ is the spin representation for a spin-1/2 particle in the corresponding point group to obtain the states as listed in table 2.2 [11–13]. Note that the states containing any u configuration are removed because they belong to a higher excited state manifold.

2.2.4. ENERGETIC ORDERING OF STATES

For ordering the states in terms of energy, we consider the order of the hole-hole Coulomb interaction energies. The hole-hole Coulomb interaction energy is minimized when the holes are in an antisymmetric spatial configuration. This means that the spin configuration must be symmetric in order to have an

Configuration	Γ	Total wave function	Symmetry
v^2 (singlet)	${}^1A_1$	$\lvert vv\rangle \otimes (\lvert\alpha\beta\rangle - \lvert\beta\alpha\rangle)$	A_1
ve (singlet)	${}^1E_x$	$(\lvert ve_x\rangle + \lvert e_x v\rangle) \otimes (\lvert\alpha\beta\rangle - \lvert\beta\alpha\rangle)$	E_1
	${}^1E_y$	$(\lvert ve_y\rangle + \lvert e_y v\rangle) \otimes (\lvert\alpha\beta\rangle - \lvert\beta\alpha\rangle)$	E_2
ve (triplet)	A_1	$\lvert E_-\rangle \otimes \lvert\alpha\alpha\rangle - \lvert E_+\rangle \otimes \lvert\beta\beta\rangle$	A_1
	A_2	$\lvert E_-\rangle \otimes \lvert\alpha\alpha\rangle + \lvert E_+\rangle \otimes \lvert\beta\beta\rangle$	A_2
	E_1	$\lvert E_-\rangle \otimes \lvert\beta\beta\rangle - \lvert E_+\rangle \otimes \lvert\alpha\alpha\rangle$	E_1
	E_2	$\lvert E_-\rangle \otimes \lvert\beta\beta\rangle + \lvert E_+\rangle \otimes \lvert\alpha\alpha\rangle$	E_2
	E_y	$\lvert Y\rangle \otimes (\lvert\alpha\beta\rangle + \lvert\beta\alpha\rangle)$	E_1
	E_x	$\lvert X\rangle \otimes (\lvert\alpha\beta\rangle + \lvert\beta\alpha\rangle)$	E_2
e^2 (singlet)	${}^1E_1$	$(\lvert e_x e_x\rangle - \lvert e_y e_y\rangle) \otimes (\lvert\alpha\beta\rangle - \lvert\beta\alpha\rangle)$	E_1
	${}^1E_2$	$(\lvert e_x e_y\rangle + \lvert e_y e_x\rangle) \otimes (\lvert\alpha\beta\rangle - \lvert\beta\alpha\rangle)$	E_2
	${}^1A_1$	$(\lvert e_x e_x\rangle + \lvert e_y e_y\rangle) \otimes (\lvert\alpha\beta\rangle - \lvert\beta\alpha\rangle)$	A_1
e^2 (triplet)	${}^3A_{2-}$	$\lvert E_0\rangle \otimes \lvert\beta\beta\rangle$	$E_1 \oplus E_2$
	${}^3A_{20}$	$\lvert E_0\rangle \otimes (\lvert\alpha\beta\rangle + \lvert\beta\alpha\rangle)$	A_1
	${}^3A_{2+}$	$\lvert E_0\rangle \otimes \lvert\alpha\alpha\rangle$	$E_1 \ominus E_2$

Table 2.2: Unnormalized total wave functions for the ground state and the first excited states of the NV-center with two holes, split into a spatial and a spin part. α and β denote opposing spins and $\lvert E_\pm\rangle \equiv \lvert ve_\pm\rangle - \lvert e_\pm v\rangle$, where $e_\pm \equiv \mp\left(e_x \pm \mathrm{i}e_y\right)$. Additionally, $\lvert E_0\rangle \equiv \lvert e_x e_y\rangle - \lvert e_y e_x\rangle$ and $\lvert X\,(Y)\rangle \equiv \lvert ve_{x(y)}\rangle - \lvert e_{x(y)} v\rangle$.

antisymmetric overall wave function. The state with the largest multiplicity thus has a lower energy. The ground state of the NV-center should by this reasoning be the ${}^3A_2$ triplet state, which has also been confirmed experimentally and backed up by different theoretical approaches [11–13]. The expectation value of the Coulomb interaction energy, given some two hole state wave function $\psi\left(\boldsymbol{r}_1, \boldsymbol{r}_2\right)$ where $\boldsymbol{r}_i$ is the position of the ith hole, is given by:

$$\langle V_{\mathrm{C}}\left(\psi\right)\rangle = \langle\psi|\,\hat{V}_{\mathrm{C}}\,|\psi\rangle = \iint \psi^*\left(\boldsymbol{r}_1, \boldsymbol{r}_2\right) V\left(r_{12}\right) \psi\left(\boldsymbol{r}_1, \boldsymbol{r}_2\right) \mathrm{d}^3 r_1\, \mathrm{d}^3 r_2 \equiv V_{\mathrm{C}}^{abcd} \tag{2.17}$$

with a, b, c, and d the characterization of the wave function associated with each hole in order of appearance in the integral and:

$$V\left(r_{12}\right) = \frac{e^2}{4\pi\epsilon_0\left|\boldsymbol{r}_1 - \boldsymbol{r}_2\right|} \tag{2.18}$$

For the ground state we thus have the following relevant Coulomb interactions:

$$\left\langle V_{\mathrm{C}}\left({}^3A_2\right)\right\rangle = \frac{1}{2}\left(V_{\mathrm{C}}^{xyxy} - V_{\mathrm{C}}^{xyyx} - V_{\mathrm{C}}^{yxxy} + V_{\mathrm{C}}^{yxyx}\right) \tag{2.19}$$

$$\left\langle V_{\mathrm{C}}\left({}^1E_1\right)\right\rangle = \frac{1}{2}\left(V_{\mathrm{C}}^{xyxy} + V_{\mathrm{C}}^{xyyx} + V_{\mathrm{C}}^{yxxy} + V_{\mathrm{C}}^{yxyx}\right) \tag{2.20}$$

$$\left\langle V_{\mathrm{C}}\left({}^1E_2\right)\right\rangle = \frac{1}{2}\left(V_{\mathrm{C}}^{xxxx} - V_{\mathrm{C}}^{xxyy} - V_{\mathrm{C}}^{yyxx} + V_{\mathrm{C}}^{yyyy}\right) \tag{2.21}$$

$$\left\langle V_{\mathrm{C}}\left({}^1A_1\right)\right\rangle = \frac{1}{2}\left(V_{\mathrm{C}}^{xxxx} + V_{\mathrm{C}}^{xxyy} + V_{\mathrm{C}}^{yyxx} + V_{\mathrm{C}}^{yyyy}\right) \tag{2.22}$$

As states from ${}^1E_1$ and ${}^1E_2$ both belong to the same irreducible representation, they should have the same expectation value for their Coulomb interaction energy. Note that the expectation value should be invariant under any operation in the C_{3v} of the NV-center as it should not depend on the coordinate system that is being used. As the Coulomb interaction is symmetric it is not affected by any rotation so the wave functions $\left\{e_x, e_y\right\}$ transform as the irreducible representation E [10]. By now projecting these states onto the totally symmetric irreducible representation A_1:

$$\langle ab|\,\hat{V}_{\mathrm{C}}\,|cd\rangle = \frac{1}{h}\sum_{R=1}^{h} \chi_e\,\langle P_R\left(a\right) P_R\left(b\right)|\,\hat{V}_{\mathrm{C}}\,|P_R\left(c\right) P_R\left(d\right)\rangle \tag{2.23}$$

we find that:

$$\langle {}^1E_1|\,\hat{V}_C\,|{}^1E_1\rangle = \frac{1}{2}\langle {}^1E_1|\,\hat{V}_C\,|{}^1E_1\rangle + \frac{1}{2}\langle {}^1E_2|\,\hat{V}_C\,|{}^1E_2\rangle = \langle {}^1E_2|\,\hat{V}_C\,|{}^1E_2\rangle \tag{2.24}$$

With this information, we acquire that:

$$\left\langle V_C\left({}^1A_1\right)\right\rangle - \left\langle V_C\left({}^1E_2\right)\right\rangle = \left\langle V_C\left({}^1E_1\right)\right\rangle - \left\langle V_C\left({}^3A_2\right)\right\rangle \equiv J \tag{2.25}$$

So, the ordering of the states is $\{{}^3A_2, {}^1E_{1,2}, {}^1A_1\}$ with relative energies $\{0, J, 2J\}$. Note that we did not take into account any other holes besides the active holes in the Coulomb interaction and this result should be interpreted in a qualitative manner. A more thorough investigation may be found in for instance [12].

2.2.5. INCLUDING INTERACTION TERMS

In order to further specify the electronic structure of the negatively charged NV-center, we will include the most important interactions that result in the fine splittings of energy levels for the states as listed in table 2.2. These interactions are spin-orbit interaction and spin-spin interaction, where spin-orbit interaction is calculated to find the energy associated with the self-interaction for each hole in the NV-center and the spin-spin interaction is calculated to find the energy associated with the coupling between both hole spins. After determining the energy splittings due to these types of interaction we may identity the so-called selection rules that dictate the allowed transitions within the NV-center.

We are aware of the presence of other spins surround the hole-configuration, namely the nitrogen nucleus and the carbon nuclei, but these interactions are not considered in this model due to their relatively weak influence on the energy levels.

SPIN-ORBIT INTERACTION

The spin orbit interaction splits the energies of the multiplet states that have a non-zero angular momentum and differ in the projection of the angular momentum onto the z-axis. Given the nuclear potential ϕ, a magnetic field of $\nabla\phi \times \boldsymbol{v}/c^2$ is produced, where $\boldsymbol{v}$ is the velocity vector of the hole. The spin orbit interaction Hamiltonian is given by:

$$\hat{H}_{SO} = \sum_i \hat{\boldsymbol{\Omega}}_i \cdot \hat{\boldsymbol{S}}_i \tag{2.26}$$

with $\hat{\boldsymbol{\Omega}}_i = \frac{m^2c^2}{2}\left(\nabla V \times \hat{\boldsymbol{p}}_i\right)$ in which $V = e\phi$, the orbital momentum operator for the ith hole. Furthermore, $\hat{\boldsymbol{S}}_i = \frac{\hbar}{2}\left(\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z\right)_i^{\mathrm{T}}$, with σ_j the Pauli operators. As ϕ is produced by the nuclear potential, which is totally symmetric, it transforms as A_1. Therefore, $\nabla V \equiv \left(V_x, V_y, V_z\right)^{\mathrm{T}}$, with $V_i = \frac{\partial V}{\partial x_i}$, transforms as a vector in real space. Since $\hat{\boldsymbol{p}}$ transforms as a vector in real space as well, we may identify the irreducible forms of the orbital operator components of $\hat{\boldsymbol{\Omega}}$. In the C_{3v} point group, vectors transform as $(E_1, E_2, A_1)^{\mathrm{T}}$, so $\hat{\boldsymbol{\Omega}}$ transforms as $(E_2, E_1, A_2)^{\mathrm{T}}$ [10, 13]. The non-zero matrix elements of $\hat{\boldsymbol{\Omega}}$ in the basis $\{v, e_x, e_y\}$ can be found by checking if $\langle\phi_n|\,\Omega_i\,|\phi_m\rangle \supset A_1$. We find:

$$\hat{\boldsymbol{\Omega}} \doteq \left(\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & \mathrm{i}A \\ 0 & -\mathrm{i}A & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & -\mathrm{i}A \\ 0 & 0 & 0 \\ \mathrm{i}A & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -\mathrm{i}B & 0 \\ -\mathrm{i}B & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}\right)^{\mathrm{T}} \tag{2.27}$$

where $A = \langle e_y|\,\Omega_x\,|v\rangle$ and $B = \langle e_x|\,\Omega_z\,|e_y\rangle$. The spin-orbit interaction can now be written in terms of the angular momentum operator $\hat{\boldsymbol{L}}$ and reads as follows:

$$\hat{H}_{SO} = \sum_i \left[\lambda_\perp\left(\hat{L}_i^x\hat{S}_i^x + \hat{L}_i^y\hat{S}_i^y\right) + \lambda_z\hat{L}_i^z\hat{S}_i^z\right] \tag{2.28}$$

In this case, we have that due to the symmetry of the NV-center that $A = B$ and therefore $\lambda_\perp = \lambda_z$. We may write in the excited state triplet manifold $\{A_1, A_2, E_x, E_y, E_1, E_2\}$:

$$\hat{H}_{SO} = \lambda_z\left(|A_1\rangle\langle A_1| + |A_2\rangle\langle A_2| - |E_1\rangle\langle E_1| - |E_2\rangle\langle E_2|\right) \tag{2.29}$$

Manifold (configuration)	State (T/S)	Energy	Degeneracy
0 (e^2)	${}^3A_2$ (T)	0	3
	${}^1E_{1,2}$ (S)	J	2
	${}^1A_1$ (S)	$2J$	1
1 (ve)	$A_{1,2}$ (T)	$+\lambda_z$	2
	$E_{1,2}$ (T)	$-\lambda_z$	2
	$E_{x,y}$ (T)	0	2
	${}^1E_{x,y}$ (S)	?	2
2 (v^2)	${}^1A_1$ (S)	0	1

Table 2.3: Overview of energy splitting of states after including spin-orbit interaction energy.

Regarding non-radiative transitions we note that the axial part of the spin-orbit interaction (λ_z) links states with $m_s = 0$ spin projections with states of the same electronic configuration while the non-axial part $(\lambda_{x,y})$ links states with non-zero spin projections with singlets among different electronic configurations [13]. A non-radiative transition that is well-known experimentally is the transition of $A_1\,(ve) \rightarrow {}^1A_1\,(e^2)$. Other non-radiative allowed transitions are $E_{1,2}\,(ve) \rightarrow {}^1E_{1,2}\,(e^2)$ and in particular $E_{x,y}\,(ve) \rightarrow {}^1E_{x,y}\,(ve)$. Calculations as performed by Ma *et al.*[12] have shown that the energy of the singlet state ${}^1E_{x,y}\,(ve)$ lies close to the energy of the triplet states in the ve configuration, making this transition very probable. As for the non-axial part of the spin-orbit interaction, $\lambda_\perp\left(\hat{L}_+\hat{S}_- + \hat{L}_-\hat{S}_+\right)$, does not mix states of the triplet in the ve configuration as the raising and lowering operators, $\hat{L}_+$ and $\hat{L}_-$, link states of different electronic configurations. In a higher order approach one might argue that these interactions do eventually mix these states but because of the relatively large energy gap between electronic configurations this effect will be severely suppressed. By the same reasoning, it is not likely that the spin-orbit interaction mixes the singlet state ${}^1E_1\,(e^2)$ with any of the triplet states in ${}^3A_1\,(v^2)$. In this sense, the suggestion [11] that the singlet state ${}^1E\,(e^2)$ has a lower energy than the singlet state ${}^1A_1\,(e^2)$ is a reasonable one, as the inter-system crossing, which is technically allowed via spin-orbit interaction, will be weak and the triplet states $E_{1,2}\,(e^2)$, with spin states ± 1, will not be populated through this transition.

SPIN-SPIN INTERACTION

The spin-spin interaction Hamiltonian is given by:

$$\hat{H}_{\mathrm{SS}} = -\frac{g^2\mu_B^2}{2\hbar^2}\sum_{i\neq j}\left[\frac{3\left(\hat{\boldsymbol{S}}_i\cdot\boldsymbol{r}_i\right)\left(\hat{\boldsymbol{S}}_j\cdot\boldsymbol{r}_j\right)}{r_{ij}^5} - \frac{\hat{\boldsymbol{S}}_i\cdot\hat{\boldsymbol{S}}_j}{r_{ij}^3}\right] \tag{2.30}$$

with g the spin g factor, $\mu_B = \frac{e\hbar}{2mc}$ the Bohr magneton, $\boldsymbol{r}_i$ the position vector of the ith electron, and r_{ij} the distance between electron i and electron j. Again, $\hat{\boldsymbol{S}}_i = \frac{\hbar}{2}\left(\hat{\sigma}_x,\hat{\sigma}_y,\hat{\sigma}_z\right)_i^{\mathrm{T}}$, with σ_j the Pauli operators. For two particles, this reduces to:

$$\hat{H}_{\mathrm{SS}} = -\frac{g^2\mu_B^2}{\hbar^2 r^3}\left[3\left(\hat{\boldsymbol{S}}_1\cdot\hat{\boldsymbol{r}}\right)\left(\hat{\boldsymbol{S}}_2\cdot\hat{\boldsymbol{r}}\right) - \hat{\boldsymbol{S}}_1\cdot\hat{\boldsymbol{S}}_2\right] \tag{2.31}$$

We may express this Hamiltonian in terms of spatial and spin operators that transform as irreducible objects as follows [13]:

$$\begin{aligned}\hat{H}_{\mathrm{SS}} = -\frac{g^2\mu_B^2}{\hbar^2 r^3}\Bigg[&\frac{1-3\hat{z}^2}{4}\left(\hat{S}_{1+}\hat{S}_{2-} + \hat{S}_{1-}\hat{S}_{2+} - 4\hat{S}_{1z}\hat{S}_{2z}\right) + \frac{3\left(\hat{x}^2-\hat{y}^2\right)}{4}\left(\hat{S}_{1-}\hat{S}_{2-} + \hat{S}_{1+}\hat{S}_{2+}\right)\\ &+ \frac{\mathrm{i}3\hat{x}\hat{y}}{2}\left(\hat{S}_{1-}\hat{S}_{2-} - \hat{S}_{1+}\hat{S}_{2+}\right) + \frac{3\hat{x}\hat{z}}{2}\left(\hat{S}_{1-}\hat{S}_{2z} + \hat{S}_{1z}\hat{S}_{2-} + \hat{S}_{1+}\hat{S}_{2z} + \hat{S}_{1z}\hat{S}_{2+}\right)\\ &\frac{\mathrm{i}3\hat{y}\hat{z}}{2}\left(\hat{S}_{1-}\hat{s}_{2z} + \hat{S}_{1z}\hat{S}_{2-} - \hat{s}_{1+}\hat{S}_{2z} - \hat{S}_{1z}\hat{S}_{2+}\right)\Bigg]\end{aligned} \tag{2.32}$$

where $\hat{S}_\pm \equiv \hat{S}_x \pm \mathrm{i}\hat{S}_y$ and $\hat{x}, \hat{y}$, and $\hat{z}$ directional cosines. Note that in the given expression, the spatial part in the top line transforms as the totally symmetric representation A_1. The other terms transform as the irreducible representation E [10]. We can then write the expectation values for each term as follows:

$$\frac{g^2\mu_B^2}{\hbar^2}\left\langle\frac{1-3\hat{z}^2}{4r^3}\right\rangle = \Delta\left(|X\rangle\langle X| + |Y\rangle\langle Y|\right) \tag{2.33}$$

$$\frac{g^2\mu_B^2}{\hbar^2}\left\langle\frac{3\hat{x}^2-3\hat{y}^2}{4r^3}\right\rangle = \Delta'\left(|X\rangle\langle X| - |Y\rangle\langle Y|\right) \tag{2.34}$$

$$\frac{g^2\mu_B^2}{\hbar^2}\left\langle\frac{3\hat{x}\hat{y}+3\hat{y}\hat{x}}{4r^3}\right\rangle = \Delta'\left(|X\rangle\langle Y| + |Y\rangle\langle X|\right) \tag{2.35}$$

$$\frac{g^2\mu_B^2}{\hbar^2}\left\langle\frac{3\hat{x}\hat{z}+3\hat{z}\hat{x}}{4r^3}\right\rangle = \Delta''\left(|Y\rangle\langle Y| - |X\rangle\langle X|\right) \tag{2.36}$$

$$\frac{g^2\mu_B^2}{\hbar^2}\left\langle\frac{3\hat{z}\hat{y}+3\hat{y}\hat{z}}{4r^3}\right\rangle = \Delta''\left(|X\rangle\langle Y| + |Y\rangle\langle X|\right) \tag{2.37}$$

with the states $|X,Y\rangle$ as defined before. We may also write the spin operators in terms of the spin basis for two holes, i.e. $\{|\alpha\alpha\rangle, |\alpha\beta\rangle, |\beta\alpha\rangle, |\beta\beta\rangle\}$:

$$\hat{S}_{1z}\hat{S}_{2z} = \frac{1}{4}\left(|\alpha\alpha\rangle\langle\alpha\alpha| - |\alpha\beta\rangle\langle\alpha\beta| - |\beta\alpha\rangle\langle\beta\alpha| + |\beta\beta\rangle\langle\beta\beta|\right) \tag{2.38}$$

$$\hat{S}_{1-}\hat{S}_{2-} = |\alpha\alpha\rangle\langle\beta\beta|, \quad \hat{S}_{1-}\hat{S}_{2+} = |\alpha\beta\rangle\langle\beta\alpha| \tag{2.39}$$

$$\hat{S}_{1+}\hat{S}_{2-} = |\beta\alpha\rangle\langle\alpha\beta|, \quad \hat{S}_{1+}\hat{S}_{2+} = |\beta\beta\rangle\langle\alpha\alpha| \tag{2.40}$$

$$\hat{S}_{1-}\hat{S}_{2z} = \frac{1}{2}\left(|\alpha\beta\rangle\langle\beta\beta| - |\alpha\alpha\rangle\langle\beta\alpha|\right), \quad \hat{S}_{1+}\hat{S}_{2z} = \frac{1}{2}\left(|\beta\beta\rangle\langle\alpha\beta| - |\beta\alpha\rangle\langle\alpha\alpha|\right) \tag{2.41}$$

$$\hat{S}_{1z}\hat{S}_{2+} = \frac{1}{2}\left(|\beta\beta\rangle\langle\beta\alpha| - |\alpha\beta\rangle\langle\alpha\alpha|\right), \quad \hat{S}_{1z}\hat{S}_{2-} = \frac{1}{2}\left(|\beta\alpha\rangle\langle\beta\beta| - |\alpha\alpha\rangle\langle\alpha\beta|\right) \tag{2.42}$$

so that we may write the spin-spin interaction Hamiltonian as follows:

$$\begin{aligned}\hat{H}_{\mathrm{SS}} = &-\Delta\left(|X\rangle\langle X| + |Y\rangle\langle Y|\right)\otimes\left[|\alpha\alpha\rangle\langle\alpha\alpha| + |\beta\beta\rangle\langle\beta\beta| - 2\left(|\alpha\beta\rangle + |\beta\alpha\rangle\right)\left(\langle\alpha\beta| + \langle\beta\alpha|\right)\right]\\ &-\Delta'\left(|X\rangle\langle X| - |Y\rangle\langle Y|\right)\otimes\left(|\alpha\alpha\rangle\langle\beta\beta| + |\beta\beta\rangle\langle\alpha\alpha|\right)\\ &-\mathrm{i}\Delta''\left(|X\rangle\langle Y| + |Y\rangle\langle X|\right)\otimes\left(|\beta\beta\rangle\langle\alpha\alpha| - |\alpha\alpha\rangle\langle\beta\beta|\right)\\ &+\Delta'\left(|Y\rangle\langle Y| - |X\rangle\langle X|\right)\otimes\left[\left(|\alpha\beta\rangle + |\beta\alpha\rangle\right)\left(\langle\alpha\alpha| - \langle\beta\beta|\right) + \left(|\alpha\alpha\rangle - |\beta\beta\rangle\right)\left(\langle\alpha\beta| + \langle\beta\alpha|\right)\right]\\ &+\mathrm{i}\Delta'\left(|Y\rangle\langle Y| - |X\rangle\langle X|\right)\otimes\left[\left(|\alpha\beta\rangle + |\beta\alpha\rangle\right)\left(\langle\alpha\alpha| + \langle\beta\beta|\right) - \left(|\alpha\alpha\rangle + |\beta\beta\rangle\right)\left(\langle\alpha\beta| + \langle\beta\alpha|\right)\right]\end{aligned} \tag{2.43}$$

Using the decomposition of the basis states into spatial and spin parts in terms of irreducible representations, as shown in table 2.2, we may express the spin-spin interaction Hamiltonian in terms of basis states:

$$\begin{aligned}\hat{H}_{\mathrm{SS}} = &\Delta\left(|A_1\rangle\langle A_1| + |A_2\rangle\langle A_2| + |E_1\rangle\langle E_1| + |A_2\rangle\langle A_2|\right)\\ &-2\Delta\left(|E_x\rangle\langle E_x| + |E_y\rangle\langle E_y|\right) + 2\Delta'\left(|A_2\rangle\langle A_2| - |A_1\rangle\langle A_1|\right)\\ &+\Delta''\left(|E_1\rangle\langle E_y| + |E_y\rangle\langle E_1| - \mathrm{i}\,|E_2\rangle\langle E_x| + \mathrm{i}\,|E_x\rangle\langle E_2|\right)\end{aligned} \tag{2.44}$$

from which we can see that a gap arises between the $m_s = \pm 1$ states and the $m_s = 0$ states:

$$3\Delta = \frac{3g^2\mu_B^2}{\hbar^2}\langle X|\frac{1-3\hat{z}^2}{4r^3}|X\rangle \equiv -\frac{3}{4}D_{zz} \tag{2.45}$$

and a gap between the A_1 and the A_2 states:

$$4\Delta' = \frac{4g^2\mu_B^2}{\hbar^2}\langle X|\frac{3\hat{x}^2-3\hat{y}^2}{4r^3}|X\rangle \equiv D_{x^2-y^2} \tag{2.46}$$

Also, there is the mixing term:

$$\Delta'' = \frac{g^2\mu_B^2}{\hbar^2}\langle X|\frac{3\hat{x}\hat{z}}{\sqrt{2}r^3}|X\rangle \tag{2.47}$$

State	H_{SO}	H_{SS}
${}^3A_{2-}$	0	3Δ
${}^3A_{20}$	0	0
${}^3A_{2+}$	0	3Δ

State	H_{SO}	H_{SS}
A_1	$+\lambda_z$	$\Delta + 2\Delta'$
A_2	$+\lambda_z$	$\Delta - 2\Delta'$
E_1	$-\lambda_z$	Δ
E_2	$-\lambda_z$	Δ
E_x	0	-2Δ
E_y	0	-2Δ

Table 2.4: Overview of energy splitting of states after including both spin-orbit ($\hat{H}_{SO}$) and spin-spin ($\hat{H}_{SS}$) interaction energy for the triplet state configurations in the ground state manifold (left) and the excited state manifold (right).

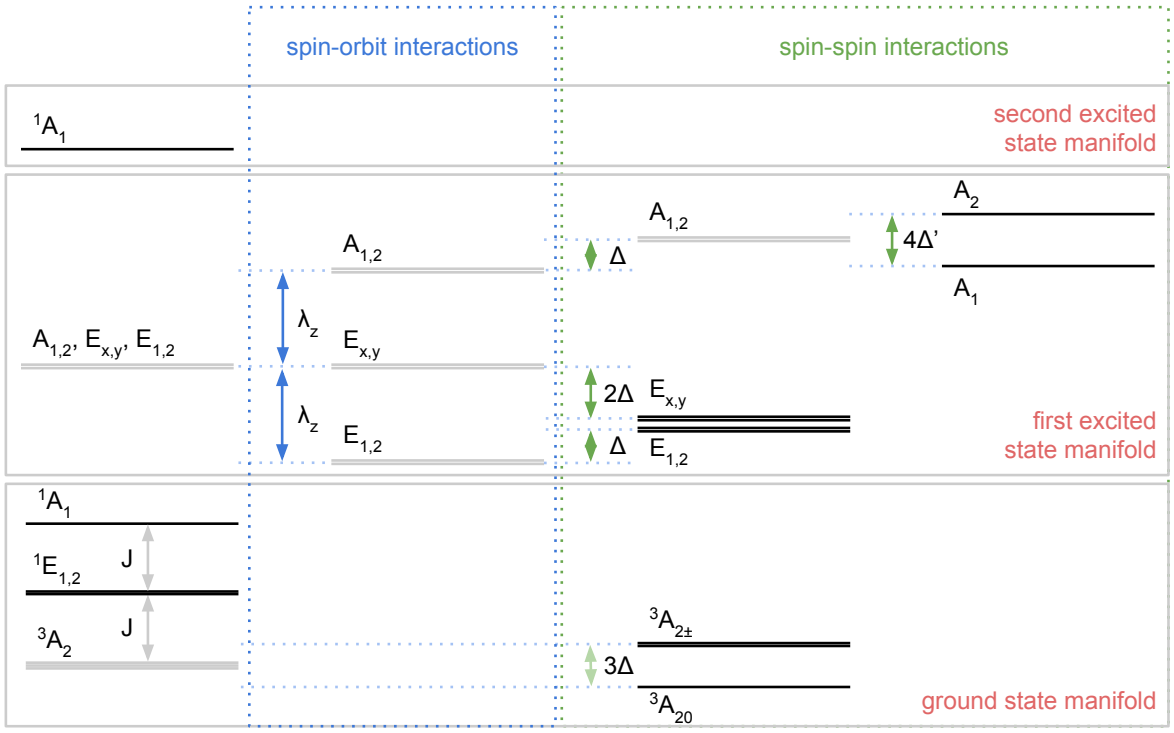

Figure 2.2: Electronic structure of the NV-center, explicitly showing the splitting due to spin-orbit and spin-spin interaction.

which is not considered in the theory paper by Lenef and Rand [17]. The table including spin-spin interactions for the excited state manifold triplet states, but not yet including the mixing terms, is given in table 2.4. Also, a schematic of the electronic structure of the NV-center is shown in figure 2.2.

SELECTION RULES

Transitions might be dipole allowed if the matrix element in the length representation contains the totally symmetric irreducible form, i.e. $\langle \phi_f | \hat{\epsilon} \cdot \boldsymbol{r} | \phi_i \rangle \subset A_1$, where $\hat{\epsilon}$ is the polarization of the electric field. The matrix elements $\langle v | x | e_x \rangle$ and $\langle v | y | e_y \rangle$ are non-zero allowing us to deduce the selection rules among the 15 states given in table 2.2. The relevant optical transitions between the triplet states of the first excited state manifold ve and the ground state manifold e^2 are shown in table 2.5. For the sake of completeness, we should also include the possible optical transitions between the singlet states in the first excited state manifold ve and the ground state manifold e^2, and between the singlet states in the second excited state manifold v^2 and the first excited state manifold ve. These transitions are shown in table 2.6.

	$\lvert A_1\rangle$	$\lvert A_2\rangle$	$\lvert E_x\rangle$	$\lvert E_y\rangle$	$\lvert E_1\rangle$	$\lvert E_2\rangle$
$\langle {}^3A_{2+}\rvert$	$\hat{\sigma}_-$	$\hat{\sigma}_-$			$\hat{\sigma}_+$	$\hat{\sigma}_+$
$\langle {}^3A_{20}\rvert$			$\hat{x}$	$\hat{y}$		
$\langle {}^3A_{2-}\rvert$	$\hat{\sigma}_+$	$\hat{\sigma}_+$			$\hat{\sigma}_-$	$\hat{\sigma}_-$

Table 2.5: Selection rules for optical transitions between the triplet excited state in the ve configuration and the triplet ground state in the e^2 configuration. The operators are the ones for which $\langle \phi_f \rvert \hat{\epsilon} \cdot \boldsymbol{r} \lvert \phi_i \rangle \neq 0$. Note that the circularly polarized photons have a polarization vector of $\hat{\sigma}_\pm \equiv \hat{x} \pm i\hat{y}$.

	$\lvert {}^1E_x\rangle$	$\lvert {}^1E_y\rangle$
$\langle {}^1A_1\rvert$	$\hat{x}$	$\hat{y}$
$\langle {}^1E_1\rvert$	$\hat{x}$	$\hat{y}$
$\langle {}^1E_2\rvert$	$\hat{y}$	$\hat{x}$

	$\lvert {}^1A_1\rangle$
$\langle {}^1E_1\rvert$	$\hat{x}$
$\langle {}^1E_2\rvert$	$\hat{y}$

Table 2.6: Selection rules for optical transitions between the singlet states in the ve (v^2) configuration and the singlet states in the e^2 (ve) configuration.

2.3. STRAIN EFFECTS

Strain refers to the displacement Δu of the atomic positions when the crystal is stretched by Δx. It is expressed in a dimensionless tensor $\boldsymbol{e}$ with elements expressing the fractional change under stretching, i.e. $e_{ij} = \frac{\partial \delta R_i}{\partial r_j}$. Strain can be produced by mechanical stress, electric field or temperature. As the displacement of atomic atomic positions may alter the symmetries on which the energy levels of states are based, strain may shift these energy levels. Looking at the elements of $\boldsymbol{e}$ it becomes apparent that not all components actually shift the energy levels. The anti-symmetric part of $\boldsymbol{e}$ transforms as a generator of the rotational group and rotates the entire structure as a result. As rotation does not alter the symmetry analysis of the structure the unperturbed states are not affected and the associated energy levels do not change. Merely the symmetric part of the strain matrix $\boldsymbol{\epsilon} \equiv \boldsymbol{e} + \boldsymbol{e}^{\mathrm{T}}$ affects the structure of a defect. We may express the strain in terms of matrices that transform according to the irreducible form of the point group under consideration. These matrices can be found by projecting a general strain matrix $\boldsymbol{\epsilon}$ on each irreducible form:

$$\boldsymbol{\epsilon}_r = \frac{l_r}{h} \sum_e \chi_e^* \boldsymbol{R}_e^\dagger \boldsymbol{\epsilon} \boldsymbol{R}_e \tag{2.48}$$

For simplicity, in the case of the NV-center, we only write the effect of strain in the manifold $\{e_x, e_y, v\}$:

$$\boldsymbol{H}_{\text{strain}} = \delta^a_{A_1} \boldsymbol{A}^a_1 + \delta^b_{A_1} \boldsymbol{A}^b_1 + \delta^a_{E_1} \boldsymbol{E}^a_1 + \delta^a_{E_2} \boldsymbol{E}^a_2 + \delta^b_{E_1} \boldsymbol{E}^b_1 + \delta^b_{E_2} \boldsymbol{E}^b_2 \tag{2.49}$$

where:

$$\delta^a_{A_1} = \frac{1}{2}(e_{xx} + e_{yy}), \quad \delta^b_{A_1} = e_{zz} \tag{2.50}$$

$$\delta^a_{E_1} = \frac{1}{2}(e_{xx} - e_{yy}), \quad \delta^b_{E_1} = \frac{1}{2}(e_{xz} + e_{zx}) \tag{2.51}$$

$$\delta^a_{E_2} = \frac{1}{2}(e_{xy} + e_{yx}), \quad \delta^a_{A_1} = \frac{1}{2}(e_{yz} + e_{zy}) \tag{2.52}$$

and:

$$\boldsymbol{A}_1^a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \boldsymbol{A}_1^b = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{2.53}$$

$$\boldsymbol{E}_1^a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \boldsymbol{E}_1^b = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \tag{2.54}$$

$$\boldsymbol{E}_2^a = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \boldsymbol{E}_2^b = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \tag{2.55}$$

In the NV-center we may safely neglect the effect of the $\boldsymbol{E}_{1,2}^b$ matrices as there is a large energy gap between the orbitals v and $e_{x,y}$. The relevant strain matrices that will actually lower the C_{3v} symmetry and shift the energy levels considerably are the $\boldsymbol{E}_{1,2}^a$ matrices, so that the relevant Hamiltonian is given by:

$$\hat{H}'_{\text{strain}} = \delta^a_{E_1} \left(|e_x\rangle \langle e_x| - |e_y\rangle \langle e_y| \right) + \delta^a_{E_2} \left(|e_y\rangle \langle e_x| + |e_y\rangle \langle e_x| \right) \tag{2.56}$$

For the manifolds $\{A_1, A_2, E_x, E_y, E_1, E_2\}$, $\{{}^1E_1, {}^1E_2, {}^1A_1\}$, and $\{{}^1E_x, {}^1E_y\}$ this yields the following matrix representations:

$$\boldsymbol{H}'_{\text{strain}} = \begin{pmatrix} & & & & \delta^a_{E_1} & \mathrm{i}\delta^a_{E_2} \\ & & & & -\mathrm{i}\delta^a_{E_2} & \delta^a_{E_1} \\ & & \delta^a_{E_1} & \delta^a_{E_2} & & \\ & & \delta^a_{E_2} & \delta^a_{E_1} & & \\ \delta^a_{E_1} & \mathrm{i}\delta^a_{E_2} & & & & \\ -\mathrm{i}\delta^a_{E_2} & \delta^a_{E_1} & & & & \end{pmatrix}, \quad \begin{pmatrix} & & 2\delta^a_{E_1} \\ & & 2\delta^a_{E_2} \\ 2\delta^a_{E_1} & 2\delta^a_{E_2} & \end{pmatrix}, \quad \begin{pmatrix} \delta^a_{E_1} & \delta^a_{E_2} \\ \delta^a_{E_2} & -\delta^a_{E_1} \end{pmatrix} \tag{2.57}$$

The effect of strain is thus that the states E_2 or E_1 state can mix in with the A_2 state when strain factors $\delta^a_{E_1}$ and $\delta^a_{E_2}$ are taken into consideration, breaking down the entanglement as the dominant polarization becomes linear. In chapter 5 we will briefly discuss the consequences of this behavior.

3

Secure Communication

The key element in secure communication is the successful encryption of secret messages. This may be done by utilizing a shared secret key. So-called one-time pad encryption allows a party, named Alice, to encrypt a plaintext message with the secret key into a cyphertext, which is then sent to some other party, named Bob. Bob may use the secret key to decrypt the ciphertext into plaintext, thus recovering the original message. After the process has been completed, the secret key is discarded. Note that some eavesdropping party, called Eve, can in principle only obtain the ciphertext, which to her appears as nonsense as long as she has no knowledge of the shared secret key.

In this chapter we will first introduce the concept of quantum key distribution after which we discuss the limitations that arise from any practical implementation. These limitations may open up loopholes that can be exploited by some malevolent eavesdropper. We discuss a more involved device independent protocol that attempts to close these loopholes and expand on it, effectively removing the strict requirement of near perfect detection. This protocol is known as a measurement-device independent quantum key distribution scheme and will be discussed in detail.

3.1. Quantum Key Distribution

An essential yet classically difficult tasks is for Alice and Bob to produce a shared random secret key known only to them, which can be used to encrypt and decrypt their message. This is where quantum mechanics comes in, guaranteeing that Eve can not listen in on the shared key without Alice and Bob noticing. The act of producing the secret shared key by means of quantum bits (qubits) is known as Quantum Key Distribution (QKD) and relies on the fact that it is forbidden by quantum mechanics to create identical copies of an arbitrary unknown quantum state, known as the no-cloning theorem [18]. The no-cloning theorem can be proven by assuming there exists a unitary operator $\hat{U}$ such that we can copy an arbitrary state $|\psi\rangle$ onto some standard pure state $|s\rangle$:

$$\hat{U}\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle \tag{3.1}$$

i.e. $\hat{U}$ is a cloning operator. Suppose the copying procedure works for two particular states $|\psi\rangle$ and $|\phi\rangle$, yielding:

$$\hat{U}\left(|\psi\rangle \otimes |s\rangle\right) = |\psi\rangle \otimes |\psi\rangle \tag{3.2}$$
$$\hat{U}\left(|\phi\rangle \otimes |s\rangle\right) = |\phi\rangle \otimes |\phi\rangle \tag{3.3}$$

Taking the inner product of these two states:

$$\langle\phi|\psi\rangle = \left(\langle\phi|\psi\rangle\right)^2 \tag{3.4}$$

which is only true if either $|\psi\rangle = |\phi\rangle$ or if $|\psi\rangle$ and $|\phi\rangle$ are orthogonal states.

3.2. THE BB84 AND E91 PROTOCOLS

The father of QKD might be considered to be the protocol introduced by Bennet and Brassard in 1984 [19], from hereon referred to as the BB84 protocol. The protocol is as follows. Alice creates two strings of bits, a and b, each n bits long. She encodes these strings into one string of n qubits as follows:

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle \tag{3.5}$$

where a_i and b_i are the ith bits of the strings a and b, respectively. Together, $a_i b_i$ gives us an index into the following four qubit states:

$$|\psi_{00}\rangle \equiv |0\rangle, \quad |\psi_{10}\rangle \equiv |1\rangle \tag{3.6}$$

$$|\psi_{01}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\psi_{11}\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{3.7}$$

Note that b_i denotes the basis in which a_i is encoded.

Alice now sends $|\psi\rangle$ over to Bob, who receives the state $\mathcal{E}(|\psi\rangle\langle\psi|)$, in which $\mathcal{E}$ is a noise super operator. Noise may be due to the channel but it can also be attributed to the interference of Eve. Bob generates a string b' of length n and performs measurements a' on the state received from Alice. After the transmission has finished, Alice publicly shares her string b. Over a public channel, Bob communicates with Alice which b_i and b'_i are not equal. Both Alice and Bob discard the qubits in a and a' where b and b' do not match.

From the remaining k bits, called the sifted key, Alice randomly chooses $k/2$ bits and communicates with Bob publicly which bits she has selected. Alice and Bob then both announce these bits publicly and they check if less than p bits differ. The number p is a theoretical limit in which methods of error correction may be used to recover the key through individual or block parity checks after which privacy amplification may be used to hide any information from Eve. This process is known as key distillation.

The BB84 protocol was extended by Artur Ekert in 1991 [20] by using entangled pairs of photons. These pairs may be generated by any source, including sources that are under the full control of Alice, Bob, or Eve. The photons are distributed such that Alice and Bob both receive one photon from each pair. The protocol is then executed in the same manner as BB84, but Alice's strings a and b follow from measurement and not from preparation.

3.2.1. PRACTICAL IMPLEMENTATION

An implementation of the BB84 (or E91) protocol may be realized by using photons as quantum bits. The polarization of a photon may be prepared in either the rectilinear basis (i.e. with horizontal or vertical polarization) or in the diagonal basis (i.e. with diagonal or anti-diagonal polarization). Encoding the qubits in these bases and following the BB84 protocol, Alice and Bob obtain a sifted key. An illustration of this polarization scheme and obtaining the sifted key is depicted in figure 3.1.

After the sifted key has been obtained, the key may be further distilled by first correcting the errors, introduced by noise or perhaps an eavesdropper, in the sifted key by means of an error correction protocol as described in more detail in appendix B. After error correction, a precise estimation of the Quantum Bit Error Rate (QBER) may be obtained. The QBER is the ratio of an error rate to the key rate and contains information on the existence of an eavesdropper and how much she knows.

$$\text{QBER} = p_f + \frac{p_d n q \Sigma f_r t_l}{2} \mu \tag{3.8}$$

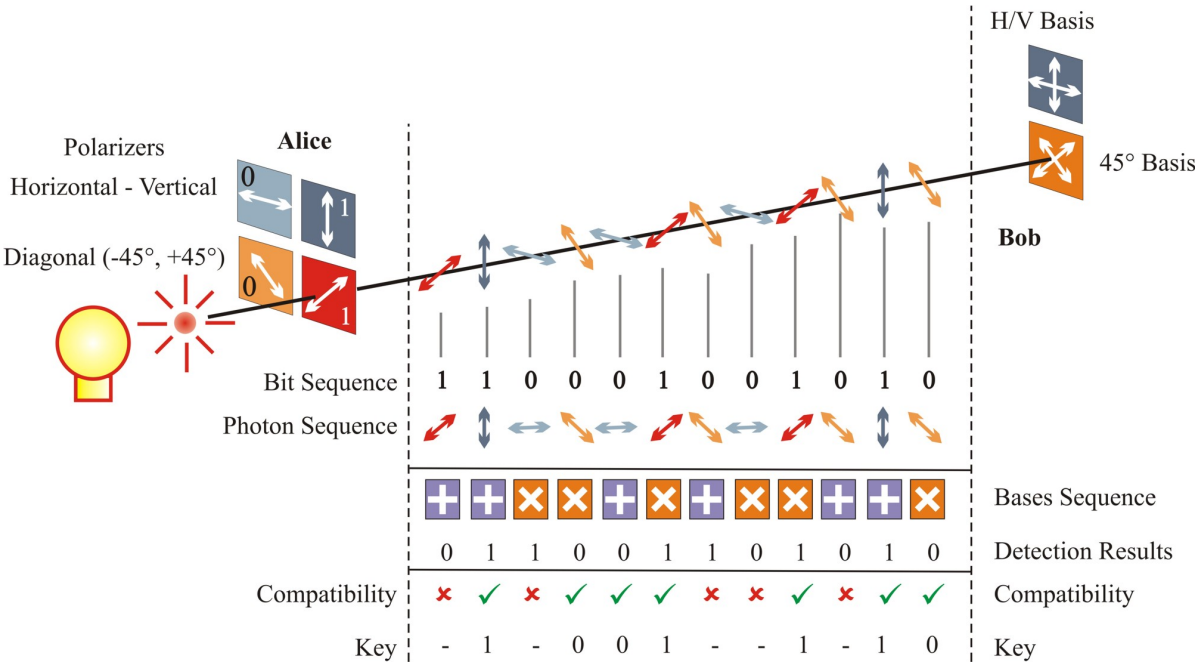

Figure 3.1: Obtaining a sifted key with the BB84 protocol, courtesy of Swiss Quantum [21]

with:

p_f : probability for a wrong 'click' (1-2%)
p_d : probability for a wrong photon signal (Si: 10 - 7; GaAs 10 - 5)
n : number of detections
q : phase = 1/2 (better for optical fibres); polarization = 1 (better in the air)
Σ : detector efficiency
f_r : pulse repeat frequency
t_l : transmission rate (for large distances this is small)
μ : attenuation for light pulses (single photons = 1)

If the measured QBER exceeds the predicted QBER, the protocol is aborted as this might be a sign of eavesdropping. This relates to the factor p as mentioned in the theoretical protocol. Now, privacy amplification is used to compress the key such that finally the secret key is obtained. The process of privacy amplification is described in appendix B. From hereon error correction and privacy amplification will be regarded as a means to extract a secret key from the sifted key, but we will not further describe this process in detail.

3.2.2. LOOPHOLES

The generation of secure keys from the BB84 (or E91) protocol calls for the following conditions to be met:

- Quantum mechanics is correct
- Alice and Bob's laboratories are perfectly isolated, i.e. the information entering and leaving the laboratories is foreseen by the QKD protocol
- Alice and Bob have sufficiently good control over their devices
- Alice and Bob share an authenticated classical channel

- Alice and Bob's devices are causally independent, i.e. they have no memory of past events

These conditions are rather strict, and when not fully met they allow for loopholes that may be exploited to have the key being eavesdropped on without it being noticed, i.e. error correction and privacy amplification do not yield a necessarily secret key. One of these loopholes is the detection loophole. We assume fair sampling, meaning that photons that are detected give the same results as measurements would give on the photons that are not detected. We can imagine that only photons that look entangled are detected and that a measurement on all photons would not violate Bell's inequality. In order to close this loophole a very high detection efficiency would be needed. Furthermore, there is the communication loophole in which we assume that settings at Alice (Bob) can influence the measurements being performed at Bob (Alice), even if the distance is large.

3.3. TOWARDS DEVICE-INDEPENDENT QKD

With the concept of Bell's theorem and the inequality derived by John Clauser, Michael Horne, Abner Shimony, and Richard Holt [22] (the CHSH inequality) we may relax on the beforementioned conditions, effectively removing the loopholes. This results in a new class of device-independent QKD (DI-QKD) protocols, for which we will discuss the main ingredient in this section.

3.3.1. BELL'S THEOREM

Bell's theorem, in its simplest form, states:

> No physical theory of local hidden variables can ever reproduce all of the predictions of quantum mechanics.

The empirical proof for this theorem follows from Bell's inequality, stating that if there would be local variables, there is a mathematical limit to a certain correlation ratio which we call S. By exceeding this limit in an experiment, one can show that it is impossible for a theory including local variables to be correct.

The Hilbert space in which the polarization state of a single photon resides is spanned by a basis of two orthogonal base states. We choose these states to be $|H\rangle$ and $|V\rangle$, where $|H\rangle$ denotes the fully horizontally polarized state and $|V\rangle$ denotes the fully vertically polarized state. We may thus describe the state of a photon, in terms of polarization, using the following notation:

$$|\psi\rangle = \alpha\,|H\rangle + \beta\,|V\rangle \tag{3.9}$$

Furthermore, the state $|\psi\rangle$ needs to be normalized, i.e. $\langle\psi \mid \psi\rangle = 1$, so that we require that $|\alpha|^2 + |\beta|^2 = 1$.

We now regard a system of two photons. The Hilbert space in which the full system polarization state resides is then spanned by four base states, namely $|H_1\rangle \otimes |H_2\rangle$, $|H_1\rangle \otimes |V_2\rangle$, $|V_1\rangle \otimes |H_2\rangle$ and $|V_1\rangle \otimes |V_2\rangle$. Introducing a shorthand notation, we may also write $|HH\rangle$, $|HV\rangle$, $|VH\rangle$ and $|VV\rangle$. The system state can thus be represented as follows:

$$|\psi\rangle = \alpha\,|HH\rangle + \beta\,|HV\rangle + \gamma\,|VH\rangle + \delta\,|VV\rangle \tag{3.10}$$

with $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. We may now define the so-called Bell states as follows:

$$|\Phi^+\rangle \equiv \frac{1}{\sqrt{2}}\left[|HH\rangle + |VV\rangle\right], \quad |\Phi^-\rangle \equiv \frac{1}{\sqrt{2}}\left[|HH\rangle - |VV\rangle\right] \tag{3.11}$$

$$|\Psi^+\rangle \equiv \frac{1}{\sqrt{2}}\left[|HV\rangle + |VH\rangle\right], \quad |\Psi^-\rangle \equiv \frac{1}{\sqrt{2}}\left[|HV\rangle - |VH\rangle\right] \tag{3.12}$$

Note that these states form a basis of the Hilbert space for the two-photon system. Furthermore, each Bell state is a special case of the previously described general state of a system of two photons and can not be written as a product state of two separate photons, i.e. $|\psi_1\rangle \otimes |\psi_2\rangle$. The Bell states all describe a so called maximally entangled state, a state in which a measurement of the polarization of one photon carries full information on the polarization of the other photon, even though it has not been measured.

Bell's inequality more formally states that if there are any hidden variables within a quantum state, a certain inequality with respect to correlations must hold. To derive this inequality, we assume that measurement results are a function of the polarizer angle and of some hidden variable λ. The outcome of the measurement of the photon in direction A will be given by $A(a,\lambda) = \pm 1$ and the outcome of the measurement of the photon in direction B will be given by $B(b,\lambda) = \pm 1$. Note that we implicitly assume that the principle of locality holds, i.e. the setting of the polarizers a and b does not influence the measurement at B and A, respectively.

We define $\rho(\lambda)$ to be the probability density function of λ, so that we may write for the measurement correlation:

$$\begin{aligned} \left|C(a,b) - C(a,b')\right| &\leq \int \left|A(a,\lambda)\, B(b,\lambda) - A(a,\lambda)\, B(b',\lambda)\right| \rho(\lambda)\, \mathrm{d}\lambda && (3.13) \\ &\leq \int \left|B(b,\lambda) - B(b',\lambda)\right| \rho(\lambda)\, \mathrm{d}\lambda && (3.14) \end{aligned}$$

and likewise:

$$\begin{aligned} \left|C(a',b) + C(a',b')\right| &\leq \int \left|A(a',\lambda)\, B(b,\lambda) + A(a',\lambda)\, B(b',\lambda)\right| \rho(\lambda)\, \mathrm{d}\lambda && (3.15) \\ &\leq \int \left|B(b,\lambda) + B(b',\lambda)\right| \rho(\lambda)\, \mathrm{d}\lambda && (3.16) \end{aligned}$$

so that:

$$\left|C(a,b) - C(a,b')\right| + \left|C(a',b) + C(a',b')\right| \leq \int \left[\left|B(b,\lambda) - B(b',\lambda)\right| + \left|B(b,\lambda) + B(b',\lambda)\right|\right] \rho(\lambda)\, \mathrm{d}\lambda \tag{3.17}$$

As we have that B can only take on values ± 1, we have that $|B(b,\lambda) - B(b',\lambda)| + |B(b,\lambda) + B(b',\lambda)| = 2$. Introducing $S \equiv |C(a,b) - C(a,b')| + |C(a',b) + C(a',b')|$ we then finally obtain the CHSH form of Bell's inequality:

$$S \leq 2 \tag{3.18}$$

Note that violating Bell's inequality immediately proves Bells' theorem, stating that no physical theory of local hidden variables can ever reproduce all of the predictions of quantum mechanics. Defining $\mathcal{A}(a) = \hat{S}_z, \mathcal{A}(a') = \hat{S}_x, \mathcal{B}(b) = \frac{1}{\sqrt{2}}\left(\hat{S}_z + \hat{S}_x\right)$, and $\mathcal{B}(b') = \frac{1}{\sqrt{2}}\left(\hat{S}_z - \hat{S}_x\right)$, we may write the correlation factor C as an expectation value as follows:

$$C\left(a^{(\prime)}, b^{(\prime)}\right) \equiv \left\langle \mathcal{A}\left(a^{(\prime)}\right) \otimes \mathcal{B}\left(b^{(\prime)}\right) \right\rangle \tag{3.19}$$

For a Bell state $|\Phi^-\rangle \equiv \frac{1}{\sqrt{2}}\left[|00\rangle - |11\rangle\right]$ it then readily follows that $S = 2\sqrt{2}$, which is the theoretical maximum of S.

3.3.2. THE CHSH INEQUALITY

Based on Bell's inequality, we may also define the CHSH operator $\hat{\mathcal{B}}_{AB} = \hat{A}_1 \otimes \left(\hat{B}_1 + \hat{B}_2\right) + \hat{A}_2 \otimes \left(\hat{B}_1 - \hat{B}_2\right)$ where $\hat{A}_1$ and $\hat{A}_2$ ($\hat{B}_1$ and $\hat{B}_2$) have real eigenvalues and are thus Hermitian operators with a spectrum in $[-1,+1]$. As shown before, all correlations that are described by a local hidden variable (LHV) model satisfy the CHSH inequality:

$$\left|\langle \hat{\mathcal{B}}_{AB} \rangle_{\mathrm{LHV}}\right| \leq 2 \tag{3.20}$$

Given some quantum state $\hat{\rho}$ shared by A and B, it was proven by Tsirelson that this inequality may be violated and is reduced to:

$$\left|\mathrm{Tr}\left(\hat{\mathcal{B}}_{AB}\hat{\rho}\right)\right| \leq 2\sqrt{2} \tag{3.21}$$

for all observables A_1, A_2, B_1, and B_2 for any state $\hat{\rho}$. Finally, considering the even more general case of hypothetical non-signaling theories we find the maximum violation $\langle \hat{\mathcal{B}}_{AB} \rangle_{\mathrm{NL}} = 4$ violates the Tsirelson bound.

3.3.3. REFORMULATION

In order to provide a security proof based on the monogamy of the violation of Bell's inequality we first introduce an equivalent form of the CHSH inequality, to wit:

$$\beta(\mathcal{X},\mathcal{Y}) \equiv \frac{1}{4}\sum_{x,y} P(X \oplus Y = xy \mid x,y) \leq \frac{3}{4} \tag{3.22}$$

where $\mathcal{X}$ and $\mathcal{Y}$ are the parties involved, for instance Alice and Bob, $x,y \in \{0,1\}$ are measurement settings, for instance the z-basis and the x-basis, and $X,Y \in \{0,1\}$ are measurement outcomes. For quantum states, the theoretical maximum to this value is given by the Tserelson bound: $\frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)$.

In non-signaling theories, i.e. theories in which information can not be sent faster than the speed of light, it has been shown [23–25] that in a composed quantum system of three separated parties $\mathcal{A},\mathcal{B}$ and $\mathcal{E}$ the following monogamy relation must hold:

$$\beta(\mathcal{A},\mathcal{B}) + \beta(\mathcal{A},\mathcal{E}) \leq \frac{3}{2} \tag{3.23}$$

3.3.4. LOOPHOLE-FREE QKD CONDITIONS

With Bell's theorem and the CHSH quality now at our disposal, it is possible to construct a new protocol that takes on these conditions and effectively lowers the conditions to be met to the following:

- Alice and Bob's laboratories are perfectly isolated, i.e. the information entering and leaving the laboratories is foreseen by the QKD protocol.
- Alice and Bob can both locally carry out classical computations using trusted devices having access to trusted sources of randomness.
- Alice and Bob share an authenticated classical channel.
- Alice and Bob's devices are causally independent, i.e. they have no memory of past events.

3.4. DI-QKD ANALYSIS

A DI-QKD protocol has been proposed by Lim *et al.* in 2013 [26] and will be discussed in detail here. We will describe the protocol and sketch an outline of the security analysis. Furthermore, we will highlight the fact that the DI-QKD requires the hard to fulfil condition of near perfect photon detection efficiency.

3.4.1. PROTOCOL TOPOLOGY

The protocol relies on the time-reversed BB84 protocol, i.e.:

1) Alice and Bob both generate a pair of qubits in the maximally entangled Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$, consisting of a solid state spin state and a polarized photon state.
2) Alice and Bob send their photons to a measuring unit Charlie.
3) Charlie performs a Bell state measurement and broadcasts the outcome to Alice and Bob, effectively projecting the NV-center spin states into a Bell state.
4) Alice performs the appropriate bit and phase flips in order to convert the joint state to $|\Phi^+\rangle$.
5) Alice and Bob measure their NV-centers in one of the BB84 bases.

Note that the security of time-reversed BB84 depends on the quality of the state preparation of Alice and Bob and their measurement qualities. The novelty is the addition of a CHSH measurement on the side of Alice, providing a bound on the overlap between the two basis vectors of the two measurements that Alice may perform. Using this overlap bound, the entropic uncertainty relation may be applied so that without any other assumption on the devices of Alice and Bob may security be inferred.

At Alice's site are thus three devices: two measurement devices $\mathbb{M}_{\text{key}}$ and $\mathbb{M}_{\text{test}}$, and one source device $\mathbb{S}$. The source device $\mathbb{S}$ generates entangled NV-center-photon pairs. The measurement device $\mathbb{M}_{\text{key}}$ has two settings $\{X, Z\}$ and measures the NV-center spin state in one of these settings, outputting a binary result. The measurement device $\mathbb{M}_{\text{test}}$ has three settings $\{R, L, P\}$ and measures the photon polarization one of the first two settings, outputting a binary result, or, in case of the P setting, sends the photon to Charlie.

At Bob's site are two devices: one measurement device $\mathbb{M}'_{\text{key}}$ and one source device $\mathbb{S}'$. The source device $\mathbb{S}'$ generates entangled NV-center-photon pairs. The measurement device $\mathbb{M}'_{\text{key}}$ has two settings $\{X, Z\}$ and measures the NV-center spin state in one of these settings, outputting a binary result. The photon is always sent to Charlie.

3.4.2. PROTOCOL DESCRIPTION

The protocol is parametrized by the key length l, the classical post-processing block size m_x, the sample size of the error estimation m_z, the local CHSH test sample size m_j, the tolerated CHSH value S_{tol}, the tolerated channel error rate Q_{tol}, the tolerated efficiency in Charlie's operation η_{tol}, the error correction leakage leak_{EC}, and the required correctness ϵ_{cor}.

(1) STATE PREPARATION AND DISTRIBUTION

Alice selects an operating mode $h_i \in \{\Gamma_{\text{CHSH}}, \Gamma_{\text{QKD}}\}$, selecting mode Γ_{QKD} with a probability $p_S = \frac{\eta_{\text{tol}} m_j}{\eta_{\text{tol}} m_j + (\sqrt{m_x} + \sqrt{m_z})^2}$ and Γ_{CHSH} with a probability $1 - p_S$. These probabilities are chosen such that the number of iterations in the protocol is minimized. If the Γ_{CHSH} operation mode is selected, Alice measures both the NV-center spin and the photon polarization. The bases in which these measurements are performed are based on the uniformly and randomly chosen bit values u_i and v_i. The value of u_i determines the $\mathbb{M}_{\text{key}}$ setting $\{X, Z\}$ and the value of v_i determines the $\mathbb{M}_{\text{test}}$ setting $\{R, L\}$. The bit value outcomes are stored in s_i and t_i, respectively. If the Γ_{QKD} operation mode is selected, Alice chooses a measurement setting $a_i \in \{X, Z\}$ with probabilities $p_x = \frac{1}{1+\sqrt{m_z/m_x}}$ and $1 - p_x$, respectively. She measures the NV-center spin state in the selected basis and sends the photon to Charlie. The measurement outcome is stored in y_i. Bob always selects a measurement setting $b_i \in \{X, Z\}$ with probabilities p_x and $1 - p_x$, respectively, and stores the binary result of measuring the NV-center spin in this basis in y'_i. The photon he sends to Charlie.

(2) CHARLIE'S OPERATION

Charlie performs a projective Bell state measurement on the photons he receives from Alice and Bob. If the measurement is successful he broadcasts $f_i = \text{pass}$, otherwise he broadcasts $f_i = \text{fail}$. If $f_i = \text{pass}$, Charlie additionally broadcasts $g_i = \{0, 1\}^2$, providing the information for the bit flip and phase flip that Alice has to perform.

(3) SIFTING

The bit values $\{h_i\}_i$, $\{a_i\}_i$, and $\{b_i\}_i$ are publicly announced by Alice and Bob. They identify the following sets:

- Key generation $\mathcal{X} = \{i \mid (h_i = \Gamma_{\text{QKD}}) \wedge (a_i = b_i = X) \wedge (f_i = \text{pass})\}$
- Channel error rate estimation $\mathcal{Z} = \{i \mid (h_i = \Gamma_{\text{QKD}}) \wedge (a_i = b_i = Z) \wedge (f_i = \text{pass})\}$
- Alice's local Bell-test set $\mathcal{J} = \{i \mid h_i = \Gamma_{\text{CHSH}}\}$

The protocol steps (1) to (3) are repeated until the sifting condition, which is set by $(|\mathcal{X}| \geq m_x) \wedge (|\mathcal{Z}| \geq m_z) \wedge (|\mathcal{J}| \geq m_j)$, $\{m_x, m_z, m_j\} \in \mathbb{N}$, is met.

(4) PARAMETER ESTIMATION

From the set $\mathcal{J}$ the CHSH value can be computed by:

$$S_{\text{test}} \equiv 8 \sum_{i \in \mathcal{J}} f(u_i, v_i, s_i, t_i) - 4 \tag{3.24}$$

where $f(u_i, v_i, s_i, t_i) = 1$ if $s_i \oplus t_i = u_i \wedge v_i$ and 0 otherwise. The error rate is computed by:

$$Q_{\text{test}} \equiv \frac{1}{|Z|} \sum_{i \in \mathcal{Z}} y_i \oplus y_i' \tag{3.25}$$

Finally, the efficiency of Charlie's operation is calculated:

$$\eta \equiv \frac{|\mathcal{X}|}{|\tilde{\mathcal{X}}|} \tag{3.26}$$

where $\tilde{\mathcal{X}} \equiv \{i \mid (h_i = \Gamma_{\text{QKD}}) \wedge (a_i = b_i = X)\}$. The protocol is aborted if $(S_{\text{test}} < S_{\text{tol}}) \vee (Q_{\text{test}} < Q_{\text{tol}}) \vee (\eta < \eta_{\text{tol}})$.

(5) ONE-WAY CLASSICAL POST-PROCESSING

Alice and Bob select a random subset of size m_x of $\mathcal{X}$ for post-processing. An error-protection protocol that leaks at most leak_{EC} bits is applied after which an error-verification protocol that leaks $\log_2 \frac{1}{\epsilon_{\text{cor}}}$ bits of information is applied. If error verification fails, the protocol is aborted. Finally, Alice and Bob apply privacy amplification with two-universal hashing to their bit strings to extract a secret key of length l.

3.4.3. SECURITY DEFINITION

In general, if a QKD protocol does not abort, it provides Alice with a key string S_A and Bob with a key string S_B. Now, let E denote the information that an eavesdropper gathers during the protocol execution, so that the joint state of S_A and E can be described by a classical-quantum state $\hat{\rho}_{S_A,E} = \sum_s |s\rangle\langle s| \otimes \hat{\rho}_E^s$, where $\{\hat{\rho}_E^s\}_s$ are the quantum states held by Eve, being conditioned on S_A, taking the values s. The protocol is now called ϵ_{cor}-correct if $P(S_A \neq S_B) \leq \epsilon_{\text{cor}}$ and it's called ϵ_{sec}-secret if $(1 - p_{\text{abort}}) \frac{1}{2} \left\| \hat{\rho}_{S_A,E} - \hat{U}_{S_A} \otimes \hat{\rho}_E \right\|_1 \leq \epsilon_{\text{sec}}$, where p_{abort} is the probability that the protocol aborts and $\hat{U}_{S_A}$ is the uniform mixture of all possible values of S_A. Accordingly, the QKD protocol is said to be $(\epsilon_{\text{cor}} + \epsilon_{\text{sec}})$-secure if it is both ϵ_{cor}-correct and ϵ_{sec}-secret. This security definition guarantees that the QKD protocol is universally composable, meaning that the pair of key strings may be safely used in any application that requires a perfectly secure key [27].

3.4.4. SECURITY ANALYSIS

Details of the security analysis can be found in [26] and [27], here follows just a sketch of the proof. First, we note that the correctness of the protocol, parameterized by the required correctness ϵ_{cor}, is guaranteed by the error-verification protocol.

Claim: the protocol, parameterized by $l, m_x, m_z, m_j, S_{\text{tol}}, Q_{\text{tol}}, \eta_{\text{tol}}, \text{leak}_{\text{EC}}$, and ϵ_{cor}, is ϵ_{sec}-secret if:

$$l \leq m_x \left[1 - \log_2 \left(1 + \frac{\hat{S}_{\text{tol}}}{4\eta_{\text{tol}}} \sqrt{8 - \hat{S}_{\text{tol}}^2} + \frac{\zeta}{\eta_{\text{tol}}} \right) - h\left(\hat{Q}_{\text{tol}}\right) \right] - \text{leak}_{\text{EC}} - \log_2 \frac{1}{\epsilon_{\text{cor}} \epsilon^4} \tag{3.27}$$

for $\epsilon = \frac{\epsilon_{\text{sec}}}{9}$ and $2 \leq \hat{S}_{\text{tol}} \leq 2\sqrt{2}$, where h denotes the binary entropy function, $\hat{S}_{\text{tol}} \equiv S_{\text{tol}} - \xi$, and $\hat{Q}_{\text{tol}} \equiv Q_{\text{tol}} + \mu$, with the statistical deviations given by:

$$\xi \equiv \sqrt{\frac{32}{m_j} \log \frac{1}{\epsilon}} \tag{3.28}$$

$$\zeta \equiv \sqrt{\frac{2(m_x + m_j\eta)(m_j + 1)}{m_x m_j^2} \log \frac{1}{\epsilon}} \tag{3.29}$$

$$\mu \equiv \sqrt{\frac{(m_x + m_z)(m_z + 1)}{m_x m_z^2} \log \frac{1}{\epsilon}} \tag{3.30}$$

Sketch of the proof: in the case that all tests in the parameter estimation are passed, let X_A be the random variable of length m_x that Alice obtains from $\mathcal{X}$ and let E' denote Eve's information on X_A

after error-correction and error-verification. From Renner's thesis [27] we find that by using privacy amplification with two-universal hashing, a Δ-secret key of length l can be generated from X_A, where:

$$\Delta \leq 6\epsilon + 2^{-\frac{1}{2}\left[H_{\min}^{3\epsilon}(X_A|E')-l\right]-1} \tag{3.31}$$

for any $\epsilon > 0$, where $H_{\min}^{3\epsilon}(X_A \mid E')$ is the smooth min-entropy function as described in Renner's thesis [27]. By using the chain rule for smooth min-entropies, we may deduce that $H_{\min}^{3\epsilon}(X_A \mid E') \geq H_{\min}^{3\epsilon}(X_A \mid E) - \text{leak}_{\text{EC}} - \log_2 \frac{2}{\epsilon_{\text{cor}}}$., where E denotes Eve's information after the step of parameter estimation has been performed. Using the generalized entropic uncertainty relation [28] we find:

$$H_{\min}^{3\epsilon}(X_A \mid E) \geq \log_2 \frac{1}{c^*} - H_{\max}^{\epsilon}(Z_A \mid Z_B) - \log_2 \frac{2}{\epsilon^2} \tag{3.32}$$

where c^* is the effective overlap of Alice's measurements, which is a function of the measurements corresponding to the settings Z and X and the marginal state. Here, Z_A can be seen as the bit string Alice would have obtained if she had chosen the Z setting for selecting the key instead. Likewise, Z_B represents the bit string obtained by Bob with setting Z. The smooth max-entropy function $H_{\max}^{\epsilon}(Z_A \mid Z_B)$ is bounded by the error rate sample on the set $\mathcal{Z}$ of size m_z, as we have that $H_{\max}^{\epsilon}(Z_A \mid Z_B) \leq m_x h\left(\hat{Q}_{\text{tol}}\right)$. In words, we have that the error rate between Z_A and Z_B is smaller than $Q_{\text{tol}} + \mu$, with high probability.

Finally, we need to bound the effective overlap c^* with S_{tol} and η_{tol}. Note that the set $\tilde{\mathcal{X}}$ is independent of Charlie's output and $\mathcal{X} \subseteq \tilde{\mathcal{X}}$ with an equality only if Charlie always outputs a "pass". Assuming the worst-case scenario, it can be shown that $c^* \leq \frac{1}{2} + \frac{\tilde{c}^* - 1/2}{\eta}$, where $\eta = \frac{|\mathcal{X}|}{|\tilde{\mathcal{X}}|}$ is the efficiency of Charlie's operation and $\tilde{c}^*$ is the effective overlap of $\tilde{\mathcal{X}}$. It can be shown that:

$$\tilde{c}^* \leq \frac{1}{2}\left(1 + \frac{\hat{S}_{\text{tol}}}{4}\sqrt{8 - \hat{S}_{\text{tol}}^2} + \zeta\right) \tag{3.33}$$

Note that ξ in $\hat{S}_{\text{tol}}$ quantifies the statistical deviation between the expected CHSH value and the observed CHSH value and ζ quantifies the statistical deviation between the effective overlaps of $\tilde{\mathcal{X}}$ and $\mathcal{J}$, respectively. Putting everything together, the secret key length as given earlier is obtained.

It is interesting and insightful to look at the limit of the secret fraction, defined as $f_{\text{sec}} \equiv \frac{l}{m_x}$, in the asymptotic limit as $N \to \infty$ and using that $\frac{\text{leak}_{\text{EC}}}{m_x} \to h\left(Q_{\text{tol}}\right)$ (corresponding to the Shannon limit). In this limit the statistical deviations $\{\mu, \xi, \zeta\} \to 0$ so that all remaining is:

$$\lim_{N\to\infty} f_{\text{sec}} = 1 - \log_2\left(\frac{S_{\text{tol}}}{4\eta_{\text{tol}}}\sqrt{8 - S_{\text{tol}}^2}\right) - 2h\left(Q_{\text{tol}}\right) \tag{3.34}$$

in which we can clearly see the roles of the operation modes Γ_{CHSH} and Γ_{QKD}. The first provides a bound on the quality of the devices, taken into account by the $\log_2$ term and the latter expression is a measure for the quality of the quantum channel, aside from actually generating the key.

3.4.5. DISCUSSION

This DI-QKD protocol provides security even if the loss between Alice and Bob does not allow for a detection-loophole-free Bell test. The security does of course depend on the losses, which is taken into account by supplying a minimum tolerated value for Charlie's efficiency, η_{tol}, in terms of the local CHSH test performed by Alice, with which she estimates how often her devices behave badly. In a practical sense, it is useful to relax the conditions for η_{tol} so that larger distances can be covered. As a direct result, this requires a more perfect device on Alice's side.

3.5. MEASUREMENT-DEVICE-INDEPENDENT QKD

The previously proposed protocols for QKD all required a near perfect photon detection efficiency. Either for heralding measurements or key generation the protocol is rendered seriously flawed as detection efficiency drops: an eavesdropper might even be present by performing side channel attacks and acquire information on the signals that are considered to be lost due to detector imperfections.

Imagine Alice and Bob to have perfectly secure laboratories in which they can independently prepare a photon in a desired state. We define two bases: the rectilinear basis which is spanned by the orthonormal states $|H\rangle$ and $|V\rangle$, and the diagonal basis which is spanned by the orthonormal states $|D\rangle \equiv \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|A\rangle \equiv \frac{1}{\sqrt{2}}(-|H\rangle + |V\rangle)$. Alice and Bob each create any of these four states and share it with an untrusted relay Charlie. At Charlie, the photons are incident on two ports of a beam splitter after which a Bell state measurement on the output states is performed, i.e. each of the output ports leads to a polarized beam splitter with detectors.

In the most general case, we have that the state by Alice and Bob is given by:

$$|\psi\rangle_{1,2} = (\alpha|H\rangle + \beta|V\rangle)_1 \otimes (\gamma|H\rangle + \delta|V\rangle)_2 \tag{3.35}$$

upon being incident on the beam splitter, the state on which the Bell state measurement is performed is given by:

$$\hat{B}|\psi\rangle_{1,2} = \frac{1}{2}\begin{cases} \mathrm{i}\alpha\gamma\,[|H_3H_3\rangle + |H_4H_4\rangle] \\ + \\ \mathrm{i}\beta\delta\,[|V_3V_3\rangle + |V_4V_4\rangle] \\ + \\ (\alpha\delta + \beta\gamma)\,[|H_3V_3\rangle + |H_4V_4\rangle] \\ + \\ (\alpha\delta - \beta\gamma)\,[|H_3V_4\rangle - |V_3H_4\rangle] \end{cases} \tag{3.36}$$

Here we have used that upon beam splitter interaction $\hat{B}|X_{1,2}\rangle = \frac{1}{\sqrt{2}}(|X_{1,2}\rangle + \mathrm{i}|X_{2,1}\rangle)$. Note that the first two cases can never be distinguished by a Bell state measurement as we cannot distinguish between measuring two photons at once and having lost a photon. Note that the choices of values for α, β, γ, and δ are limited in choice. Let's review the possibilities.

3.5.1. RECTILINEAR BASIS

If Alice and Bob both choose to send their states in the rectilinear basis we have that either α or β are equal to ± 1, the other being zero, and that either γ or δ are equal to ± 1. In the case that $|\psi\rangle = \pm|H,H\rangle$ or $|\psi\rangle = \pm|V,V\rangle$ we witness the famous Hong-Ou-Mandel effect: both photons are scattered into the same output port and yield only one click at one of the four detectors. This case is discarded. In the case that $|\psi\rangle = \pm|H,V\rangle$ or $|\psi\rangle = \pm|V,H\rangle$, either two detectors click on one side or on both sides. In the case that the detectors click on one side, the Bell state measurement projects the shared state after the beam splitter onto the $|\Psi^+\rangle \equiv \frac{1}{\sqrt{2}}(|HV\rangle + |HV\rangle)$ state. In the other case that the detectors on both sides click, the Bell state measurement projects the shared state after the beam splitter onto the $|\Psi^-\rangle \equiv \frac{1}{\sqrt{2}}(|HV\rangle - |HV\rangle)$ state. As Charlie broadcasts either of these results, either Alice or Bob needs to apply a bit flip on their input state so that the signals are perfectly correlated.

3.5.2. DIAGONAL BASIS

If Alice and Bob both choose to send their states in the diagonal basis we have that $\alpha = \pm\beta = \pm\frac{1}{\sqrt{2}}$, and that $\gamma = \pm\delta = \pm\frac{1}{\sqrt{2}}$. In the case that $|\psi\rangle = \pm|D,D\rangle$ or $|\psi\rangle = \pm|A,A\rangle$ we find that after the beam splitter interaction:

$$\hat{B}|\psi\rangle_{1,2} = \frac{1}{4}\begin{cases} \mathrm{i}\,[|H_1H_1\rangle + |H_2H_2\rangle] \\ + \\ \mathrm{i}\,[|V_1V_1\rangle + |V_2V_2\rangle] \\ + \\ 2\,[|H_1V_1\rangle + |H_2V_2\rangle] \end{cases} \tag{3.37}$$

The Bell state measurement $|\Psi^+\rangle$ thus corresponds to a perfect correlation and a bit flip is not needed. In the case that $|\psi\rangle = \pm|D,A\rangle$ or $|\psi\rangle = \pm|A,D\rangle$ we find that after the beam splitter interaction:

$$\hat{B}|\psi\rangle_{1,2} = \frac{1}{4}\begin{cases} -\mathrm{i}\left[|H_1H_1\rangle + |H_2H_2\rangle\right] \\ + \\ \mathrm{i}\left[|V_1V_1\rangle + |V_2V_2\rangle\right] \\ + \\ 2\left[|H_1V_1\rangle - |H_2V_2\rangle\right] \end{cases} \tag{3.38}$$

The Bell state measurement $|\Psi^-\rangle$ thus corresponds to a perfect anti-correlation and a bit flip is required. The detection of the Bell states thus requires the following post-processing: We denote by $Q^{n,m}_{\mathrm{rect}}$, $Q^{n,m}_{\mathrm{diag}}$,

Alice & Bob	Relay output $\|\Psi^-\rangle$	Relay output $\|\Psi^+\rangle$
Rectilinear basis	Bit flip	Bit flip
Diagonal basis	Bit flip	No bit flip

$e^{n,m}_{\mathrm{rect}}$, and $e^{n,m}_{\mathrm{diag}}$ the gain and Quantum Bit Error rate (QBER), respectively, of the signal states sent by Alice and Bob, where n and m denote the number of photons sent by the legitimate users, and rect or diag represent their basis choice. We use the rectilinear basis as the key generation basis and the diagonal basis is used for testing only. From the error analysis on the rectilinear basis we thus deduce the required error correction and from the error analysis on the diagonal basis we deduce the required privacy amplification.

RECTILINEAR BASIS

An error would be the case where the relay output is successful when Alice and Bob prepare the same polarization state. Assuming ideal optical elements and detectors, and no misalignment, we have that when Alice and Bob send, respectively, n and m photons, the relay will never output a successful result. So, $e^{n,m}_{\mathrm{rect}} = 0 \;\forall\; n,m$. This means that no error correction is needed for the sifted key. Note that even though we are utilizing weak coherent pulse (WCP) sources (rather than single photon sources) in this protocol, the key rate is not substantially lowered in the error correction part.

DIAGONAL BASIS

An error would be the case where the relay reports a singlet state detection $|\Psi^-\rangle$ when Alice and Bob prepare the same polarization state or the case in which the relay reports a triplet state detection $|\Psi^+\rangle$ when Alice and Bob prepare orthogonal polarizations. Again assuming the ideal scenario as described earlier, we have that in the single photon case $e^{1,1}_{\mathrm{diag}} = 0$. This is shown in the previous section. Again, this means that the usage of WCP sources does not substantially lower the key generation rate in the privacy amplification part.

KEY GENERATION RATE

In the ideal case as described earlier, the key generation rate will be given by $R = Q^{1,1}_{\mathrm{rect}}$ in the asymptotic limit of an infinitely long key. If we however take into account imperfections like basis misalignment and dark counts, the key generation rate will be given by [29, 30]:

$$R = Q^{1,1}_{\mathrm{rect}}\left[1 - H\left(e^{1,1}_{\mathrm{diag}}\right)\right] - Q_{\mathrm{rect}} f\left(E_{\mathrm{rect}}\right) H\left(E_{\mathrm{rect}}\right) \tag{3.39}$$

where $Q_{\mathrm{rect}} = \sum_{n,m} Q^{n,m}_{\mathrm{rect}}$ and $E_{\mathrm{rect}} = \sum_{n,m} Q^{n,m}_{\mathrm{rect}} e^{n,m}_{\mathrm{rect}} / Q_{\mathrm{rect}}$. Furthermore, $f\left(E_{\mathrm{rect}}\right) > 1$ is an inefficiency function for the error correction process, and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. We implicitly assume that we can use the decoy state method to acquire the key generation rate by estimating the gain $Q^{1,1}_{\mathrm{rect}}$ and the QBER $e^{1,1}_{\mathrm{rect}}$. We can show that this is indeed a correct assumption. In the standard decoy state technique applied to conventional QKD we assume

that Alice and Bob can estimate the yield Y_n and error rate e_n of an n-photon signal for all n. That is, the set of linear equations:

$$Q^i = \sum_{k=0}^{\infty} Y_k \mathrm{e}^{-\mu_i} \frac{\mu_i^k}{k!} \tag{3.40}$$

$$Q^i E^i = \sum_{k=0}^{\infty} Y_k \mathrm{e}^{-\mu_i} \frac{\mu_i^k e_k}{k!} \tag{3.41}$$

where i denotes a specific decoy setting, can be solved and Alice and Bob and the parameters Y_n and e_n may be obtained for all n. In MDI-QKD we have that both Alice and Bob apply the decoy state technique for sending their bits to Charlie, hence we have following sets of equations:

$$Q^{i,j}_{\mathrm{rect}} = \sum_{n,m=0}^{\infty} Y^{n,m}_{\mathrm{rect}} \mathrm{e}^{-\mu_i} \frac{\mu_i^n}{n!} \mathrm{e}^{-\mu_j} \frac{\mu_j^m}{m!} \tag{3.42}$$

$$Q^{i,j}_{\mathrm{diag}} = \sum_{n,m=0}^{\infty} Y^{n,m}_{\mathrm{diag}} \mathrm{e}^{-\mu_i} \frac{\mu_i^n}{n!} \mathrm{e}^{-\mu_j} \frac{\mu_j^m}{m!} \tag{3.43}$$

and:

$$Q^{i,j}_{\mathrm{rect}} E^{i,j}_{\mathrm{rect}} = \sum_{n,m=0}^{\infty} Y^{n,m}_{\mathrm{rect}} \mathrm{e}^{-\mu_i} \frac{\mu_i^n}{n!} \mathrm{e}^{-\mu_j} \frac{\mu_j^m}{m!} e^{n,m}_{\mathrm{rect}} \tag{3.44}$$

$$Q^{i,j}_{\mathrm{diag}} E^{i,j}_{\mathrm{diag}} = \sum_{n,m=0}^{\infty} Y^{n,m}_{\mathrm{diag}} \mathrm{e}^{-\mu_i} \frac{\mu_i^n}{n!} \mathrm{e}^{-\mu_j} \frac{\mu_j^m}{m!} e^{n,m}_{\mathrm{rect}} \tag{3.45}$$

where the indices i and j denote the decoy settings for Alice and Bob, respectively.

The gain can be rewritten as:

$$Q^{i,j}_{\mathrm{rect}} = \sum_{n=0}^{\infty} \mathrm{e}^{-\mu_i} \frac{\mu_i^n}{n!} Y^j_{n,\mathrm{rect}} \tag{3.46}$$

with:

$$Y^j_{n,\mathrm{rect}} \equiv \sum_{m=0}^{\infty} \mathrm{e}^{-\mu_j} \frac{\mu_j^m}{m!} Y^{n,m}_{\mathrm{rect}} \tag{3.47}$$

For a fixed j, we have that the parameter $Y^j_{n,\mathrm{rect}}$ can be estimated because it is equivalent to the equations as seen in decoy state QKD. Doing this for all j, we have that the parameters $Y^{n,m}_{\mathrm{rect}}$ can be estimated. The same argument goes for the parameters $Y^{n,m}_{\mathrm{diag}}$.

The QBER $E^{i,j}_{\mathrm{rect}}$ can be rewritten as:

$$Q^{i,j}_{\mathrm{rect}} E^{i,j}_{\mathrm{rect}} = \sum_{n=0}^{\infty} \mathrm{e}^{-\mu_i} \frac{\mu_i^n}{n!} W^j_{n,\mathrm{rect}} \tag{3.48}$$

with:

$$W^j_{n,\mathrm{rect}} = \sum_{m=0}^{\infty} \mathrm{e}^{-\mu_j} \frac{\mu_j^m}{m!} Y^{n,m}_{\mathrm{rect}} e^{n,m}_{\mathrm{rect}} \tag{3.49}$$

Again, for fixed j we have that the parameter $W^j_{n,\mathrm{rect}}$ can be estimated because it is equivalent to the equations as seen in decoy state QKD. Doing this for all j, we have that the parameters $e^{n,m}_{\mathrm{rect}}$ can be estimated as the parameters $Y^{n,m}_{\mathrm{rect}}$ are known at this point. The same argument goes for the parameters $e^{n,m}_{\mathrm{diag}}$. Note that in particular:

$$Q^{1,1}_{\mathrm{rect}} = \mu_A \mu_B \mathrm{e}^{-(\mu_A+\mu_B)} Y^{1,1}_{\mathrm{rect}} \tag{3.50}$$

where μ_A and μ_B are the mean photon number sent by Alice and Bob, respectively.

4

Quantum Random Access Memory

An essential component of a quantum computer will be quantum random access memory (QRAM), just like the random access memory (RAM) is an essential component in a classical computer. RAM is a flexible architecture to store information in an array of memory cells. Each cell of this memory array is associated with a unique numerical address and by using an address register the content of the specified memory cell can be returned at an output register. In this chapter we will be looking into a design for QRAM which relies on a switching mechanism for photons of which we will study the dynamics.

4.1. Introduction to QRAM

A QRAM as proposed by Giovannetti *et al.* [31] consists of three components:

- A memory array d, consisting of N bits, which may be classic bits or qubits, depending on the usage of the QRAM
- An input or address register a containing $n = \log_2 N$ qubits
- An output register o, also containing n qubits

The address register must contain a superposition of addresses $\sum_j \psi_j |j\rangle_a$, so that the QRAM may return a superposition of data in the data register by the following correlation:

$$\sum_j \psi_j |j\rangle_a \xrightarrow{\text{QRAM}} \sum_j \psi_j |j\rangle_a |D_j\rangle_d \tag{4.1}$$

D_j being the content of the jth memory cell. If the memory is disposed in a d-dimensional lattice, it can be shown that conventional architectures require $\mathcal{O}\left(N^{1/d}\right)$ switches, or quantum gates, to be thrown in order to access one of the $N = 2^n$ memory slots. This is a computationally expensive task.

Looking at the graph as shown in figure 4.1, it can be seen that all memory cells may be reached by interpreting the address register as a route through the graph. For instance, the address register 010 can be interpreted as going left from the root node to the first level, going right from the first to the second and again going left from the second to the third, reaching the proper memory slot. This scheme is highly demanding in practice for any reasonably sized memory. In fact, to query a superposition of memory cells, the address qubits are generally entangled with $\mathcal{O}(N)$ switches or quantum gates, i.e. a state of the form:

$$\sum_j \psi_j |j_0 j_1 \cdots j_{n-1}\rangle_a \otimes |j_0\rangle_{s_0} |j_1\rangle_{s_1}^{\otimes 2} \cdots |j_{n-1}\rangle_{s_{n-1}}^{\otimes 2^{n-1}} \tag{4.2}$$

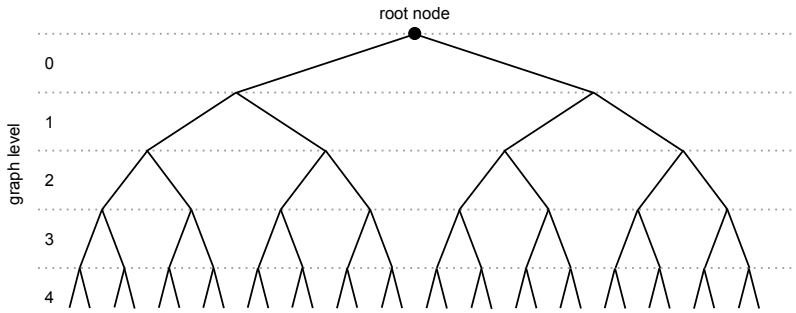

Figure 4.1: A schematic overview of the RAM accessing.

where j_k is the kth bit of the address register and s_k is the state of the 2^k switches controlled by it. Note that such a large superposition is highly impractical due to decoherence effects and will require a lot of error correction.

4.2. BUCKET BRIGADE ARCHITECTURE

The idea of the Bucket Brigade approach [31] is that each node in the graph is a trit, i.e. a three-level memory element, which is labeled *left*, *right*, or *wait*. A trit in the *wait* state can be set by an incoming bit, changing its value to *left* if the incoming bit is 0 and to *right* if the incoming bit is 1. Once the trit is in any of the directional states it will deviate incoming bits according to its value. The protocol for querying the memory is then as follows. First, all trits in the graph are initialized in the *wait* state after which the first bit of the address register is sent. This bit sets the root node to either *left* or *right*. The next bit is sent, which is deviated by the root node and consecutively sets the node on the next graph level according to its value. After all $\log_2 N$ bits of the address register have been sent, there is a single route of $n = \log_2 N$ trit states that have been set to a specific state. All other trits remain in the *wait* state. Now, a "bus" signal is sent, which follows the route to the memory cell, extracts data from it and backtracks its route while resetting all trits it meets to the *wait* state, finishing the protocol. Note that only n trist have been involved in the memory call.

Now to translate the protocol into a quantum one, we replace the concept of trits with quantum trits, or qutrits. These are three-level quantum systems, described by the vectors $|\text{left}\rangle$, $|\text{right}\rangle$ and $|\text{wait}\rangle$. We define a unitary operator $\hat{U}$ which switches the qutrit $|\text{wait}\rangle$ state according to the input qubit state from the address register, i.e.:

$$\hat{U}\,|0\rangle\,|\text{wait}\rangle = |f\rangle\,|\text{left}\rangle\,, \quad \hat{U}\,|1\rangle\,|\text{wait}\rangle = |f\rangle\,|\text{right}\rangle \tag{4.3}$$

the state $|f\rangle$ being a fiduciary qubit state. One all register qubits have passed the graph, a superposition of routes has been carved. Now a bus qubit is injected which reaches the end of the graph along the requested superposition of routes and interacts with the addressed memory cells. According to the memory content, the state of the bus state is changed after which the bus returns to the root node, resetting all qutrits to the $|\text{wait}\rangle$ state on its way back by means of the inverse transformation $\hat{U}^\dagger\,|f\rangle\,|\text{left}\rangle = |0\rangle\,|\text{wait}\rangle$ or $\hat{U}^\dagger\,|f\rangle\,|\text{right}\rangle = |1\rangle\,|\text{wait}\rangle$.

For a query with a superposition of r memory cells, only $\mathcal{O}\left(r \log_2 N\right)$ qutrits need to be entangled, the state of the device being of the type:

$$\sum_j \psi_j\,|j_0\rangle_{t_0}\,|j_1\rangle_{t_1(j_0)} \cdots |j_{n-1}\rangle_{t_{n-1}(j_{n-2})} \bigotimes_{l_j} |\text{wait}\rangle_{t_{l_j}} \tag{4.4}$$

where t_k represents the state of the one qutrit at the kth level which is aimed to by the non-$|\text{wait}\rangle$ qutrit at the $(k-1)$th level, and where l_j spans the other qutrits. Even if all of the qutrits are involved in the superposition, the state is still highly resilient to noise.

4.2.1. IMPLEMENTATION OF BUCKET-BRIGADE QRAM

The only assumption in the Bucket Brigade architecture is the possibility of operating coherently on a small number $\mathcal{O}(\log_2 N)$ out of a large number $\mathcal{O}(N)$ of first-neighbor connected quantum memory elements. Furthermore, it does not depend on macroscopic superposition states composed of an exponentially large number of quantum gates. A proof-of-principle implementation could be the following:

The qutrits at the nodes as shown in the graph are composed of NV-centers in diamond, which have a energy level structure such that we may define a ground state $|\text{wait}\rangle$ which may selectively be excited to the $|\text{left}\rangle$ or $|\text{right}\rangle$ state. The register and the bus qubits are composed of photons, whose encoding is in the polarization. It is now possible to use a photon in the polarization state $|0\rangle$ to muster a $|\text{wait}\rangle \rightarrow |\text{left}\rangle$ atomic transition, and a photon in the polarization state $|1\rangle$ to muster a $|\text{wait}\rangle \rightarrow |\text{right}\rangle$ transition.

4.2.2. REPLACING QUTRITS WITH QUBITS

In a QRAM we desire to supply some input, or address, state $\sum_i \alpha_i |x_i\rangle$ that is accepted by the QRAM which returns an output state $\sum_i \alpha_i |q_i\rangle$ in the data register, where $|q_i\rangle$ is the state containing the quantum information that is stored in the ith memory cell, associated with the address state $|x_i\rangle$.

Again, consider the level graph as displayed in figure 4.1 but now we just require node qubits instead of qutrits. The jth state of an address register, which typically looks like $|01011001\rangle$, is associated with a route in the node system. If the address qubit is $|0\rangle$, the left path is chosen; if the address qubit is $|1\rangle$, the right path is chosen. All node qubits are initialized in the $|\text{left}\rangle$ state. Then, the first qubit of the address register is dispatched through the circuit. At the first node encountered, the address qubit incurs a unitary operation $\hat{U}$ on the node qubit with the help of a control pulse $\Omega(t)$: $\hat{U}|0\rangle|\text{left}\rangle = |0\rangle|\text{left}\rangle$ and $\hat{U}|1\rangle|\text{left}\rangle = |1\rangle|\text{right}\rangle$. The second qubit is dispatched in the circuit, follows the left or right route set by the previous qubit and arrives at one of the two nodes at the second level of the graph. Illuminated by the control pulse, the node qubit will then make a corresponding state change according to the state of the second address register qubit, and so on. Note that the ith control pulse $\Omega(t)$ must address all 2^{k-1} node qubits in the kth level of the graph simultaneously. After all n qubits of the address register have passed through the circuit, a single photon will be sent along the carved route to single out a memory cell. After that, an arbitrary unknown state in the data register can be transferred to the selected memory cell along the same route or the state of the selected memory cell can be read out to the data register. Finally, all node qubits are reset to the $|\text{left}\rangle$ state.

On average, as in the case that the address register qubit is in the state $|0\rangle$ and does not interact with the node qubit, only $n/2$ control operations are performed in a memory call. The mean comprehensive error rate per memory address is then $n\epsilon/2 = \frac{\epsilon}{2}\log_2 N$ with ϵ the assumed error rate per node qubit flip event.

4.3. CONCEPT OF A SINGLE PHOTON TRANSISTOR

A single photon transistor should be capable of absorbing a single gate photon into the atom near the resonator with a control field $\Omega(t)$ while a state flip of the atom is induced that will influence the propagation of the signal photon. To fully understand the mechanisms at work in the device that will be proposed later, we first need to understand how an electron and a two-level system interacts with light, i.e. an electromagnetic field.

4.3.1. INTERACTION OF AN ELECTRON WITH AN ELECTROMAGNETIC FIELD

In this section we will discuss the dynamics of an electron that interacts with an electromagnetic field. We do this by first setting up the classical Hamiltonian for the system in the Coulomb gauge after which we will quantize the auxiliary field. After having done so, we may work out the separate interaction terms that are in the Hamiltonian.

COULOMB GAUGE

The Hamiltonian for a system containing an electron of mass m_0, charge e and spin $\boldsymbol{S}$ and an electromagnetic field $\boldsymbol{B} = \nabla \times \boldsymbol{A}$, where $\boldsymbol{A}$ is called the auxiliary field, in some stationary potential field V,

where the electron interacts will all fields mentioned, is given by:

$$\mathcal{H} = \mathcal{H}_0 + \mathcal{H}_\mathrm{f} + \mathcal{H}_\mathrm{int} \tag{4.5}$$

where:

$$\begin{aligned}\mathcal{H}_0 + \mathcal{H}_\mathrm{int} &= \frac{1}{2m_0}\left[\boldsymbol{p} - \frac{e}{c}\boldsymbol{A}\left(\boldsymbol{r},t\right)\right]^2 + V\left(\boldsymbol{r}\right) - \frac{e}{2m_0 c}\boldsymbol{S}\cdot\boldsymbol{B}\left(\boldsymbol{r},t\right) \\ &= \underbrace{\frac{\boldsymbol{p}^2}{2m_0} + V\left(\boldsymbol{r}\right)}_{\mathcal{H}_0} \underbrace{- \frac{e}{m_0 c}\boldsymbol{A}\left(\boldsymbol{r},t\right)\cdot\boldsymbol{p} + \frac{e^2}{2m_0 c^2}\boldsymbol{A}^2\left(\boldsymbol{r},t\right) - \frac{e}{m_0 c}\boldsymbol{S}\cdot\boldsymbol{B}\left(\boldsymbol{r},t\right)}_{\mathcal{H}_\mathrm{int}}\end{aligned} \tag{4.6}$$

Note that this last expression is merely valid if we choose to be in the Coulomb gauge, i.e. $\nabla\cdot\boldsymbol{A} = 0$, resulting in the fact that $\boldsymbol{p}$ and $\boldsymbol{A}$ will commute:

$$\begin{aligned}\boldsymbol{p}\cdot\boldsymbol{A}f &= -\mathrm{i}\hbar\nabla\cdot\boldsymbol{A}f \\ &= -\mathrm{i}\hbar\left(\nabla\cdot\boldsymbol{A}f + \boldsymbol{A}\cdot\nabla f\right) \\ &= -\mathrm{i}\hbar\boldsymbol{A}\cdot\nabla f \\ &= \boldsymbol{A}\cdot\boldsymbol{p}f\end{aligned} \tag{4.7}$$

From Maxwell's equations we have that in the Coulomb gauge we also have that $\boldsymbol{E} = -\frac{\partial\boldsymbol{A}}{\partial t}$, so that $\boldsymbol{A}$ satisfies the following homogeneous wave equation:

$$\nabla^2\boldsymbol{A}\left(\boldsymbol{r},t\right) = -\frac{1}{c^2}\frac{\partial^2\boldsymbol{A}\left(\boldsymbol{r},t\right)}{\partial t^2} \tag{4.8}$$

QUANTIZING THE $\boldsymbol{A}$ FIELD

We may express the vector field $\boldsymbol{A}$ as a linear combination of plane waves, i.e. we take a discrete Fourier transform:

$$\boldsymbol{A}\left(\boldsymbol{r},t\right) = \frac{1}{\sqrt{\epsilon_0 L^3}}\sum_{\boldsymbol{k}}\boldsymbol{A}_{\boldsymbol{k}}\mathrm{e}^{\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}} \tag{4.9}$$

Substituting this expansion in equation (4.8) we obtain:

$$\nabla^2\left(\frac{1}{\sqrt{\epsilon_0 L^3}}\sum_{\boldsymbol{k}}\boldsymbol{A}_{\boldsymbol{k}}\mathrm{e}^{\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}}\right) = -\frac{1}{c^2}\frac{\partial^2}{\partial t^2}\left(\frac{1}{\sqrt{\epsilon_0 L^3}}\sum_{\boldsymbol{k}}\boldsymbol{A}_{\boldsymbol{k}}\mathrm{e}^{\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}}\right) \iff -k^2\boldsymbol{A}_{\boldsymbol{k}} = \frac{1}{c^2}\frac{\partial^2\boldsymbol{A}_{\boldsymbol{k}}}{\partial t^2} \tag{4.10}$$

Defining $\omega_k \equiv ck$ we have the following solutions:

$$\boldsymbol{A}_{\boldsymbol{k}} = \boldsymbol{c}_{\boldsymbol{k}}\mathrm{e}^{-\mathrm{i}\omega_k t} + \boldsymbol{c}'_{\boldsymbol{k}}\mathrm{e}^{\mathrm{i}\omega_k t} \tag{4.11}$$

From the Coulomb gauge we furthermore have that:

$$\nabla\cdot\left(\frac{1}{\sqrt{\epsilon_0 L^3}}\sum_{\boldsymbol{k}}\boldsymbol{A}_{\boldsymbol{k}}\mathrm{e}^{\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}}\right) = 0 \iff \boldsymbol{k}\cdot\boldsymbol{A}_{\boldsymbol{k}} = 0 \tag{4.12}$$

Substituting accordingly using equation (4.11) we find:

$$\boldsymbol{k}\cdot\left(\boldsymbol{c}_{\boldsymbol{k}}\mathrm{e}^{-\mathrm{i}\omega_k t} + \boldsymbol{c}'_{\boldsymbol{k}}\mathrm{e}^{\mathrm{i}\omega_k t}\right) = 0\ \forall\ t \iff \boldsymbol{k}\cdot\boldsymbol{c}_{\boldsymbol{k}} = \boldsymbol{k}\cdot\boldsymbol{c}'_{\boldsymbol{k}} = 0 \tag{4.13}$$

from which we may conclude that the vectors $\boldsymbol{c}_{\boldsymbol{k}}$ and $\boldsymbol{c}'_{\boldsymbol{k}}$ are normal to $\boldsymbol{k}$. We may define an orthonormal basis $\boldsymbol{e}_{\boldsymbol{k}\sigma}$, with $\sigma \in \{1,2\}$ which is normal to $\boldsymbol{k}$ per definition. The vectors $\boldsymbol{e}_{\boldsymbol{k}\sigma}$ are so-called polarization vectors. We may thus write $\boldsymbol{c}^{(\prime)}_{\boldsymbol{k}} = \sum_\sigma c^{(\prime)}_{\boldsymbol{k}\sigma}\boldsymbol{e}_{\boldsymbol{k}\sigma}$ and for now we have that:

$$\boldsymbol{A}\left(\boldsymbol{r},t\right) = \frac{1}{\sqrt{\epsilon_0 L^3}}\sum_{\boldsymbol{k}}\left(\boldsymbol{c}_{\boldsymbol{k}}\mathrm{e}^{-\mathrm{i}\omega_k t} + \boldsymbol{c}'_{\boldsymbol{k}}\mathrm{e}^{\mathrm{i}\omega_k t}\right)\mathrm{e}^{\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}} \tag{4.14}$$

Note that the vector field $\boldsymbol{A}$ should be real and we require that $\boldsymbol{A}^* = \boldsymbol{A}$. From this requirement we then have that:

$$\sum_{\boldsymbol{k}} \left(c_{\boldsymbol{k}} \mathrm{e}^{-i\omega_k t} + c'_{\boldsymbol{k}} \mathrm{e}^{i\omega_k t} \right) \mathrm{e}^{i\boldsymbol{k}\cdot\boldsymbol{r}} = \sum_{\boldsymbol{k}} \left(c^*_{\boldsymbol{k}} \mathrm{e}^{i\omega_k t} + c'^*_{\boldsymbol{k}} \mathrm{e}^{-i\omega_k t} \right) \mathrm{e}^{-i\boldsymbol{k}\cdot\boldsymbol{r}} \tag{4.15}$$

$$\iff \sum_{\boldsymbol{k}} \left(c_{\boldsymbol{k}} \mathrm{e}^{-i\omega_k t} + c'_{\boldsymbol{k}} \mathrm{e}^{i\omega_k t} \right) \mathrm{e}^{i\boldsymbol{k}\cdot\boldsymbol{r}} = \sum_{\boldsymbol{k}} \left(c^*_{-\boldsymbol{k}} \mathrm{e}^{i\omega_k t} + c'^*_{-\boldsymbol{k}} \mathrm{e}^{-i\omega_k t} \right) \mathrm{e}^{i\boldsymbol{k}\cdot\boldsymbol{r}} \tag{4.16}$$

$$\iff \left(c_{\boldsymbol{k}} - c'^*_{-\boldsymbol{k}} \right) \mathrm{e}^{-i\omega_k t} = \left(c^*_{-\boldsymbol{k}} - c'_{\boldsymbol{k}} \right) \mathrm{e}^{i\omega_k t} \tag{4.17}$$

If this requirement must be met for all t we have that $c_{\boldsymbol{k}} = c'^*_{-\boldsymbol{k}}$ and we thus obtain:

$$\boldsymbol{A}(\boldsymbol{r}, t) = \frac{1}{\sqrt{\epsilon_0 L^3}} \sum_{\boldsymbol{k},\sigma} \left(c_{\boldsymbol{k}\sigma} \boldsymbol{e}_{\boldsymbol{k}\sigma} \mathrm{e}^{-\mathrm{i}\omega_k t} \mathrm{e}^{\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}} + \mathrm{c.c.} \right) \tag{4.18}$$

Defining the time dependent, complex coefficients $u_{\boldsymbol{k}\sigma}(t) \equiv c_{\boldsymbol{k}\sigma} \mathrm{e}^{-\mathrm{i}\omega_k t}$ we have:

$$\boldsymbol{A}(\boldsymbol{r}, t) = \frac{1}{\sqrt{\epsilon_0 L^3}} \sum_{\boldsymbol{k},\sigma} \left[u_{\boldsymbol{k}\sigma}(t) \boldsymbol{e}_{\boldsymbol{k}\sigma} \mathrm{e}^{\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}} + \mathrm{c.c.} \right] \tag{4.19}$$

Introducing the canonical variables $q_{ks\sigma}(t) \equiv u_{\boldsymbol{k}\sigma} + u^*_{\boldsymbol{k}\sigma}$ and $p_{\boldsymbol{k}\sigma}(t) \equiv -\mathrm{i}\omega_k \left(u_{\boldsymbol{k}\sigma} - u^*_{\boldsymbol{k}\sigma} \right)$, we may rewrite the Hamiltonian for the electromagnetic field as:

$$\mathcal{H}_{\mathrm{f}} = \frac{1}{2} \sum_{\boldsymbol{k},\sigma} \left[p^2_{\boldsymbol{k}\sigma}(t) + \omega^2_k q^2_{\boldsymbol{k}\sigma}(t) \right] \tag{4.20}$$

meaning that every photon in a mode $\boldsymbol{k}$ with polarization σ independently contributes to the system energy. We have that $u_{\boldsymbol{k}\sigma}(t) = \frac{q_{\boldsymbol{k}\sigma}(t)}{2} + \frac{\mathrm{i} p_{\boldsymbol{k}\sigma}(t)}{2\omega_k}$ and we may thus write:

$$\boldsymbol{A}(\boldsymbol{r}, t) = \frac{1}{2\sqrt{\epsilon_0 L^3}} \sum_{\boldsymbol{k},\sigma} \left[\left(q_{\boldsymbol{k}\sigma}(t) + \frac{\mathrm{i}}{\omega_k} p_{\boldsymbol{k}\sigma}(t) \right) \boldsymbol{e}_{\boldsymbol{k}\sigma} \mathrm{e}^{\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}} + \mathrm{c.c.} \right] \tag{4.21}$$

Based on the postulates of quantum mechanics, the canonical variables obey the following commutation relations:

$$\left[\hat{q}_{\boldsymbol{k}\sigma}(t), \hat{p}_{\boldsymbol{k}'\sigma'}(t') \right] = \mathrm{i}\hbar \delta_{\boldsymbol{k}\boldsymbol{k}'} \delta_{\sigma\sigma'} \delta(t - t') \tag{4.22}$$

$$\left[\hat{q}_{\boldsymbol{k}\sigma}(t), \hat{q}_{\boldsymbol{k}'\sigma'}(t') \right] = \left[\hat{p}_{\boldsymbol{k}\sigma}(t), \hat{p}_{\boldsymbol{k}'\sigma'}(t') \right] = 0 \; \forall \; \boldsymbol{k}, \boldsymbol{k}', \sigma, \sigma', t, t' \tag{4.23}$$

Defining the creation and annihilation operators:

$$\hat{a}^{(\dagger)}_{\boldsymbol{k}\sigma}(t) = \frac{1}{\sqrt{2\hbar\omega_k}} \left(\omega_k q_{\boldsymbol{k}\sigma}(t) \mp i p_{\boldsymbol{k}\sigma}(t) \right) = \hat{a}^{(\dagger)}_{\boldsymbol{k}\sigma} \mathrm{e}^{\mp i\omega_k t} \tag{4.24}$$

obeying the following commutation relations:

$$\left[\hat{a}_{\boldsymbol{k}\sigma}(t), \hat{a}^{\dagger}_{\boldsymbol{k}'\sigma'}('t) \right] = \delta_{\boldsymbol{k}\boldsymbol{k}'} \delta_{\sigma\sigma'} \delta(t - t') \tag{4.25}$$

$$\left[\hat{a}^{(\dagger)}_{\boldsymbol{k}\sigma}(t), \hat{a}^{(\dagger)}_{\boldsymbol{k}'\sigma'}('t) \right] = 0 \; \forall \; \boldsymbol{k}, \boldsymbol{k}', \sigma, \sigma', t, t' \tag{4.26}$$

We may deduce:

$$\hat{q}_{\boldsymbol{k}\sigma}(t) = \sqrt{\frac{\hbar}{2\omega_k}} \left[\hat{a}_{\boldsymbol{k}\sigma}(t) + \hat{a}^{\dagger}_{\boldsymbol{k}\sigma}(t) \right], \quad \hat{p}_{\boldsymbol{k}\sigma}(t) = \mathrm{i} \sqrt{\frac{\hbar\omega_k}{2}} \left[\hat{a}^{\dagger}_{\boldsymbol{k}\sigma}(t) - \hat{a}_{\boldsymbol{k}\sigma}(t) \right] \tag{4.27}$$

Using the commutation relations we find:

$$\hat{p}^2_{\boldsymbol{k}\sigma}(t) = \hbar\omega_k \left(\hat{a}^{\dagger}_{\boldsymbol{k}\sigma} \hat{a}_{\boldsymbol{k}\sigma} + \frac{1}{2} \right) = \omega_k \hat{q}^2_{\boldsymbol{k}\sigma}(t) \tag{4.28}$$

allowing us to write the quantized Hamiltonian as:

$$\hat{H}_{\mathrm{f}} = \sum_{\boldsymbol{k},\sigma} \hbar\omega_k \left(\hat{a}^{\dagger}_{\boldsymbol{k}\sigma} \hat{a}_{\boldsymbol{k}\sigma} + \frac{1}{2} \right) \tag{4.29}$$

Furthermore we may write, with $A_k \equiv \sqrt{\frac{\hbar}{2\epsilon_0 L^3 \omega_k}}$:

$$\boldsymbol{A}(\boldsymbol{r},t) = \sum_{\boldsymbol{k},\sigma} A_k \left[\hat{a}_{\boldsymbol{k}\sigma} \boldsymbol{e}_{\boldsymbol{k}\sigma} \mathrm{e}^{\mathrm{i}(\boldsymbol{k}\cdot\boldsymbol{r} - \omega_k t)} + \mathrm{H.c.} \right] \tag{4.30}$$

SEPARATE INTERACTION TERMS

In $\mathcal{H}_{\mathrm{int}}$ the part that is proportional to $\boldsymbol{A}^2(\boldsymbol{r},t)$ may safely be ignored because this term describes the photon-photon interaction which may be considered weak compared to the photon-electron interaction. The term proportional to $\boldsymbol{S}\cdot\boldsymbol{B}$ may also be ignored [32].

In the Schrödinger picture, where any time dependence is absorbed into the eigenvectors rather than the Hamiltonian, we are left with the following interaction part:

$$\hat{H}_{\mathrm{int}} = -\frac{e}{m_0 c} \sum_{\boldsymbol{k},\sigma} A_k \left(\hat{a}_{\boldsymbol{k}\sigma} \boldsymbol{e}_{\boldsymbol{k}\sigma} \cdot \boldsymbol{p}\, \mathrm{e}^{\mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}} + \mathrm{H.c.} \right) \tag{4.31}$$

Note the following Taylor expansion:

$$\mathrm{e}^{\pm \mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r}} = 1 \pm \mathrm{i}\boldsymbol{k}\cdot\boldsymbol{r} - \frac{(\boldsymbol{k}\cdot\boldsymbol{r})^2}{2!} \mp \frac{(\boldsymbol{k}\cdot\boldsymbol{r})^3}{3!} + \cdots \tag{4.32}$$

where the first term describes the interaction with the electric dipole, the second with the magnetic dipole, the third with the magnetic quadrupole, and so on. Limiting ourselves to just the interaction with the electric dipole we may approximate $\mathrm{e}^{\pm i\boldsymbol{k}\cdot\boldsymbol{r}} \approx 1$ and equation (4.31) becomes:

$$\hat{H}_{\mathrm{int}} = -\frac{e}{m_0 c} \sum_{\boldsymbol{k},\sigma} A_k \left(\hat{a}_{\boldsymbol{k}\sigma} \boldsymbol{e}_{\boldsymbol{k}\sigma} \cdot \boldsymbol{p} + \mathrm{H.c.} \right) \tag{4.33}$$

4.3.2. INTERACTION OF A TWO-LEVEL SYSTEM AND LIGHT

In this subsection we derive the famous Jaynes-Cummings Hamiltonian [33]: a regular starting point for deriving the dynamics in interacting systems [32, 34].

We limit ourselves to an electric dipole in a two-dimensional Hilbert space with the basis states $|0\rangle$ and $|1\rangle$. These basis states are eigenstates of the Hamiltonian $\mathcal{H}_0$ and have an energy difference of $\hbar\omega_0$ around some offset energy E_0. The external potential will be set to zero. The Hamiltonian including the coupling of the electric dipole to some external field then is the following:

$$\hat{H} = E_0 + \frac{\hbar\omega_0}{2}\hat{\sigma}_z + \sum_{\boldsymbol{k}\sigma} \left\{ \hbar\omega_k \hat{a}^{\dagger}_{\boldsymbol{k}\sigma} \hat{a}_{\boldsymbol{k}\sigma} - \frac{e A_k}{m_0 c} \left[\hat{a}_{\boldsymbol{k}\sigma} \boldsymbol{e}_{\boldsymbol{k}\sigma} \cdot \boldsymbol{p} + \mathrm{H.c.} \right] \right\} \tag{4.34}$$

where $\hat{\sigma}_z = \hat{b}^{\dagger}\hat{b} - \hat{b}\hat{b}^{\dagger}$ and:

$$\begin{aligned} b|0\rangle &= 0, \quad b|1\rangle = |0\rangle \\ b^{\dagger}|0\rangle &= |1\rangle, \quad b^{\dagger}|1\rangle = 0 \end{aligned} \tag{4.35}$$

We now regard just the interaction part of the Hamiltonian and assume that at some time $t = 0$ the state of the system can be written as a tensor product of two completely decoupled Hilbert spaces, i.e.:

$$\hat{\rho}_0 = |\{n\}\rangle\langle\{n\}| \otimes |\psi\rangle\langle\psi| \tag{4.36}$$

where $|\psi\rangle$ is the state of the two-level system and $|\{n\}\rangle$ is the state of the photonic field containing $n_{\boldsymbol{k}\sigma}$ photons in mode $\boldsymbol{k},\sigma$. In the previously mentioned basis the matrix elements of $|\psi\rangle\langle\psi|$ may be represented as follows:

$$\begin{aligned} |1\rangle\langle 1| &= \hat{b}^{\dagger}\hat{b}, \quad |0\rangle\langle 0| = \hat{b}\hat{b}^{\dagger} \\ |0\rangle\langle 1| &= \hat{\sigma}_-, \quad |1\rangle\langle 0| = \hat{\sigma}_+ \end{aligned} \tag{4.37}$$

with $\hat{\sigma}_{\pm}$ the so-called ladder operators. The matrix elements for the coupling between the states $|0\rangle$ en $|1\rangle$ by a single field mode, with wave vector $\boldsymbol{k}$ and spin σ, and the effective dipole moment is as follows:

$$\begin{aligned}\hat{a}_{k\sigma}\boldsymbol{e}_{k\sigma}\cdot\boldsymbol{p}+\text{H.c.} = a_{k\sigma}\left(\hat{\sigma}_{-}\langle 0|\,\boldsymbol{e}_{k\sigma}\cdot\boldsymbol{p}\,|1\rangle+\hat{\sigma}_{+}\langle 1|\,\boldsymbol{e}_{k\sigma}\cdot\boldsymbol{p}\,|0\rangle\right)\\ +\hat{a}^{\dagger}_{k\sigma}\left(\hat{\sigma}_{+}\langle 1|\,\boldsymbol{e}^{*}_{k\sigma}\cdot\boldsymbol{p}\,|0\rangle+\hat{\sigma}_{-}\langle 0|\,\boldsymbol{e}^{*}_{k\sigma}\cdot\boldsymbol{p}\,|1\rangle\right)\end{aligned} \tag{4.38}$$

In the rotating wave approximation we neglect the terms containing $\hat{a}_{k\sigma}\hat{\sigma}_{-}$ and $\hat{a}^{\dagger}_{k\sigma}\hat{\sigma}_{+}$ because the time evolution of these transitions is $e^{\mp i(\omega_0+\omega_k)}$, respectively. Note that the time evolution of $\hat{a}_{k\sigma}\hat{\sigma}_{+}$ and $\hat{a}^{\dagger}_{k\sigma}\hat{\sigma}_{-}$ goes as $e^{\mp i(\omega_0-\omega_k)}$, respectively. As ω_0 and ω_k are generally large, the fast oscillating terms can be safely ignored. Assuming the polarization vector to be real, we define:

$$\hbar g_{k\sigma}\equiv-\frac{e}{m_0 c}A_k\langle 1|\,\boldsymbol{e}_{k\sigma}\cdot\boldsymbol{p}\,|0\rangle=-\frac{e}{m_0 c}A_k\langle 0|\,\boldsymbol{e}^{*}_{k\sigma}\cdot\boldsymbol{p}\,|1\rangle \tag{4.39}$$

Setting $E_0\equiv 0$ we thus end up with:

$$\mathcal{H}=\frac{\hbar\omega_0}{2}\hat{\sigma}_z+\hbar\sum_{k\sigma}\omega_k\hat{a}^{\dagger}_{k\sigma}\hat{a}_{k\sigma}+\hbar\sum_{k\sigma}g_{k\sigma}\left(\hat{a}_{k\sigma}\hat{\sigma}_{+}+\hat{a}^{\dagger}_{k\sigma}\hat{\sigma}_{-}\right) \tag{4.40}$$

This is the famous Jaynes-Cummings model [33]. This Hamiltonian describes the interaction of a single two-level atom with a multi-mode field by adding the separate free energies of both and systems and accounting for a coupling energy associated with any transitions between the atom state and the field modes.

4.3.3. SETTING UP THE MODEL

A microtoroidal resonator has two internal counterpropagating modes a and b, which have a common frequency ω_c in the absence of scattering. In the presence of scattering with strength h, those two modes will be coupled. The intracavity field decays at a rate $\kappa=\kappa_i+\kappa_e$, where κ_i and κ_e respectively describe intrinsic losses and extrinsic loss due to adjustable interaction with the modes of a tapered fiber. The evanescent fields of modes a and b have coherent interactions with a ground state $|g\rangle$, metastable intermediate state $|s\rangle$ with energy ω_s, and excited state $|e\rangle$ with energy ω_e of a three-level atom described by the operators $\hat{\sigma}_{ij}=|i\rangle\langle j|$, $i,j=\{g,s,e\}$, near the external surface of the resonator. It is convenient to describe the interaction in normal modes $A=\frac{a+b}{\sqrt{2}}$ and $B=\frac{a-b}{\sqrt{2}}$ with coupling rates g_A and g_B, respectively. We have that $g_{A,B}\sim g_0 e^{\delta\rho}\{\cos kx,\sin kx\}$, $\delta\sim 1/\lambda$, where ρ is the radial distance from the surface of the toroid to the atom, x is the position around the circumference of the resonator, and k is the vacuum wave vector. We assume the position of the atom to be such that $kx=\pi$, so that $g_B=0$, yielding mode B to be decoupled from the interaction with the atom. All atom states are coupled by a classic control field $\Omega(t)$ with frequency ω_F.

The cavity mode a (b) is coupled with a coupling constant $\sqrt{\kappa_e/\pi}$ to the input field $\beta_{1\text{in}}(t)$ ($\beta_{2\text{in}}(t)$), described by annihilation operator $\hat{a}_{1\omega}$ ($\hat{a}_{2\omega}$) in the tapered fiber. Figure 4.2 shows a schematic drawing of the system, including all couplings and decay rates.

We first discuss the coherent absorption of a single photon by the atom through the toroid. We assume that $\beta_{1,\text{in}}(t)=\beta_{2,\text{in}}(t)$, and thus $\langle B\rangle=0$. The Hamiltonian modeling our system can then be written as:

$$\hat{H}=\hat{H}_0+\underbrace{\hat{H}_{\text{intr.}}+\hat{H}_{\text{extr.}}+\hat{H}_{\text{Rabi}}}_{\hat{H}_1} \tag{4.41}$$

Setting $\hbar\equiv 1$, we find for the unperturbed Hamiltonian, giving the self-energies for respectively the each state of the atom, the fiber modes and the cavity mode:

$$\hat{H}_0=\omega_g\hat{\sigma}_{gg}+\omega_s\hat{\sigma}_{ss}+\omega_e\hat{\sigma}_{ee}+\int\omega\,\mathrm{d}\omega\sum_{j=1}^{2}\hat{a}^{\dagger}_{j\omega}\hat{a}_{j\omega}+(\omega_c+h)\,\hat{A}^{\dagger}\hat{A} \tag{4.42}$$

The Hamiltonian for the intrinsic losses, given that $\gamma_{\{s,e\}}$ are the atomic spontaneous emission rates, describing the decay of both excited states of the atom and the cavity mode, reads:

$$\hat{H}_{\text{intr.}}=-i\frac{\gamma_s}{2}\hat{\sigma}_{ss}-i\frac{\gamma_e}{2}\hat{\sigma}_{ee}-i\frac{\kappa_i}{2}\hat{A}^{\dagger}\hat{A} \tag{4.43}$$

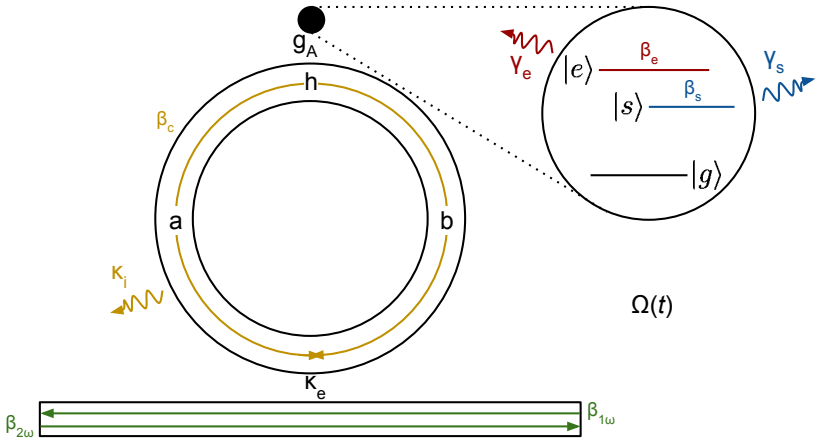

Figure 4.2: A schematic overview of the system that defines the single photon transistor, including the relevant couplings and decay rates.

The Hamiltonian for the extrinsic losses, describing the losses in the interaction between the cavity mode and the different atom states and the interaction between the fiber modes and the cavity mode, is given by:

$$\hat{H}_{\text{extr.}} = \int \mathrm{d}\omega \sqrt{\frac{\kappa_e}{2\pi}} \left(\mathrm{i} \sum_{j=1}^{2} \hat{a}_{j\omega}^{\dagger} \hat{A} + \text{H.c.} \right) + \left[\mathrm{i} \left(g_A^{eg} \hat{\sigma}_{eg} + g_A^{sg} \hat{\sigma}_{sg} + g_A^{es} \hat{\sigma}_{es} \right) \hat{A} + \text{H.c.} \right] \tag{4.44}$$

Finally, the Hamiltonian for the driven oscillations, describing the energy associated with the transitions between the atom modes that are driven by the external field, is then finally:

$$\hat{H}_{\text{Rabi}} = \mathrm{i}\Omega(t)\, \mathrm{e}^{-\mathrm{i}\omega_L t} \left[\hat{\sigma}_{eg} + \hat{\sigma}_{es} + \hat{\sigma}_{sg} \right] + \text{H.c.} \tag{4.45}$$

The ansatz time-dependent wave function for a system containing exactly one photon can be given by the following:

$$|\psi(t)\rangle = \int \mathrm{d}\omega \sum_{j=1}^{2} \beta_{j\omega}(t)\, \hat{a}_{j\omega}^{\dagger} |g,0,\text{vac}\rangle + \beta_e(t) |e,0,\text{vac}\rangle + \beta_s(t) |s,0,\text{vac}\rangle + \beta_c(t) |g,1,\text{vac}\rangle \tag{4.46}$$

with $|m,n,\text{vac}\rangle$ the state denoting the atom to be in state $|m\rangle$, n the number of photons in the mode A, and $|\text{vac}\rangle$ the vacuum state of the fiber mode. Note that since we are including interactions with the environment, phenomenologically introduced with the parameters γ_e, γ_s, and κ_i, the normalization conditions is weakened to be $\sum_{j=1}^{2} |\beta_{j\omega}(t)|^2 + |\beta_e(t)|^2 + |\beta_s(t)|^2 + |\beta_c(t)|^2 \leq 1$. For clarity, all parameters are listed and summarized in table 4.1.

The Schrödinger equation in the interaction picture reads:

$$\mathrm{i} |\dot{\psi}(t)\rangle = \hat{H}_{1,I} |\psi(t)\rangle = \mathrm{e}^{\mathrm{i}\hat{H}_0 t} \hat{H}_1 \mathrm{e}^{-\mathrm{i}\hat{H}_0 t} |\psi(t)\rangle \tag{4.47}$$

We find that, restricting ourselves to the solution space in which the general one photon state lives by letting the Hamiltonian act on the ansatz wave function as given in equation (4.46):

$$\begin{aligned} \mathrm{e}^{-\mathrm{i}\hat{H}_0 t} |\psi(t)\rangle = \mathrm{e}^{-\mathrm{i}\omega_g t} \int \mathrm{d}\omega\, \mathrm{e}^{-\mathrm{i}\omega t} \sum_j \beta_{j\omega}(t)\, a_{j\omega}^{\dagger} |g,0,\text{vac}\rangle + \mathrm{e}^{-\mathrm{i}\omega_e t} \beta_e(t) |e,0,\text{vac}\rangle \\ + \mathrm{e}^{-\mathrm{i}\omega_s t} \beta_s(t) |s,0,\text{vac}\rangle + \mathrm{e}^{-\mathrm{i}(\omega_g + \omega_c + h)t} \beta_c(t) |g,1,\text{vac}\rangle \end{aligned} \tag{4.48}$$

so that we find for the constituent parts of $\hat{H}_{1,I} |\psi(t)\rangle$:

$$\hat{H}_{\text{intr.},I} |\psi(t)\rangle = -\mathrm{i}\beta_c(t) \frac{\kappa_i}{2} |g,1,\text{vac}\rangle - \mathrm{i}\frac{\gamma_e}{2} \beta_e(t) |e,0,\text{vac}\rangle - \mathrm{i}\frac{\gamma_s}{2} \beta_s(t) |s,0,\text{vac}\rangle \tag{4.49}$$

Parameter	Physical interpretation
ω_g	Ground state energy of the three level atom
ω_s	Meta-stable state energy of the three level atom
ω_e	Excited state energy of the three level atom
ω	Energy associated with a fiber mode
ω_c	Energy of the cavity mode
h	Energy associated with cavity scattering
γ_s	Spontaneous emission rate of the metastable state of the three level atom
γ_e	Spontaneous emission rate of the excited state of the three level atom
κ_i	Intrinsic loss rate from the cavity
κ_e	Extrinsic loss rate from the cavity
$g_A^{\{eg,sg,es\}}$	Coupling rate between the specified atom state transitions and the resonator mode

Table 4.1: Model parameters and their physical meaning.

and:

$$\begin{aligned}\hat{H}_{\text{extr.},I}\left|\psi\left(t\right)\right\rangle = {} & \mathrm{i}\mathrm{e}^{-\mathrm{i}(\omega_c+h)t}\beta_c\left(t\right)\sqrt{\frac{\kappa_e}{2\pi}}\int \mathrm{d}\omega\,\mathrm{e}^{\mathrm{i}\omega t}\sum_j a_{j\omega}^{\dagger}\left|g,0,\text{vac}\right\rangle \\ & -\mathrm{i}\mathrm{e}^{\mathrm{i}(\omega_c+h)t}\sqrt{\frac{\kappa_e}{2\pi}}\int \mathrm{d}\omega\,\mathrm{e}^{-\mathrm{i}\omega t}\sum_j \beta_{j\omega}\left(t\right)\left|g,1,\text{vac}\right\rangle \\ & +\mathrm{i}\mathrm{e}^{-\mathrm{i}\left(\omega_g+\omega_c+h-\omega_e\right)t}g_A^{eg}\beta_c\left(t\right)\left|e,0,\text{vac}\right\rangle+\mathrm{i}\mathrm{e}^{-\mathrm{i}\left(\omega_g+\omega_c+h-\omega_s\right)t}g_A^{sg}\beta_c\left(t\right)\left|s,0,\text{vac}\right\rangle \\ & -\mathrm{i}\mathrm{e}^{\mathrm{i}\left(\omega_g+\omega_c+h\right)}\left[\mathrm{e}^{-\mathrm{i}\omega_s t}\left(g_A^{sg}\right)^*\beta_s\left(t\right)+\mathrm{e}^{-\mathrm{i}\omega_e t}\left(g_A^{eg}\right)^*\beta_e\left(t\right)\right]\left|g,1,\text{vac}\right\rangle\end{aligned} \tag{4.50}$$

and finally:

$$\hat{H}_{\text{Rabi},I}\left|\psi\left(t\right)\right\rangle = \mathrm{i}\Omega\left(t\right)\mathrm{e}^{-\mathrm{i}(\omega_L+\omega_s-\omega_e)t}\beta_s\left(t\right)\left|e,0,\text{vac}\right\rangle-\mathrm{i}\Omega^*\left(t\right)\mathrm{e}^{\mathrm{i}(\omega_F+\omega_s-\omega_e)t}\beta_e\left(t\right)\left|s,0,\text{vac}\right\rangle \tag{4.51}$$

We thus find the equations of motion for our system by means of the Schrödinger equation in the interaction picture as given in equation (4.47) to be:

$$\dot{\beta}_{j\omega}\left(t\right) = \mathrm{e}^{-\mathrm{i}(\omega_c+h-\omega)t}\beta_c\left(t\right)\sqrt{\frac{\kappa_e}{2\pi}} \tag{4.52a}$$

$$\dot{\beta}_e\left(t\right)+\frac{\gamma_e}{2}\beta_e\left(t\right) = \mathrm{e}^{-\mathrm{i}\left(\omega_g+\omega_c+h-\omega_e\right)t}g_A^{eg}\beta_c\left(t\right)+\Omega\left(t\right)\mathrm{e}^{-\mathrm{i}(\omega_L+\omega_s-\omega_e)t}\beta_s\left(t\right) \tag{4.52b}$$

$$\dot{\beta}_s\left(t\right)+\frac{\gamma_s}{2}\beta_s\left(t\right) = -\Omega^*\left(t\right)\mathrm{e}^{\mathrm{i}(\omega_L+\omega_s-\omega_e)t}\beta_e\left(t\right)+\mathrm{e}^{-\mathrm{i}\left(\omega_g+\omega_c+h-\omega_s\right)t}g_A^{sg}\beta_c\left(t\right) \tag{4.52c}$$

$$\begin{aligned}\dot{\beta}_c\left(t\right)+\frac{\kappa_i}{2}\beta_c\left(t\right) = -\Big[& \mathrm{e}^{-\mathrm{i}\omega_e t}\left(g_A^{eg}\right)^*\beta_e\left(t\right)+\mathrm{e}^{-\mathrm{i}\omega_s t}\left(g_A^{sg}\right)^*\beta_s\left(t\right) \\ & +\mathrm{e}^{-\mathrm{i}\omega_g t}\sqrt{\frac{\kappa_e}{2\pi}}\int \mathrm{d}\omega\,\mathrm{e}^{-\mathrm{i}\omega t}\sum_j \beta_{j\omega}\left(t\right)\Big]\mathrm{e}^{\mathrm{i}\left(\omega_g+\omega_c+h\right)t}\end{aligned} \tag{4.52d}$$

We may readily solve equation (4.52a) by directly integrating it:

$$\beta_{j\omega}\left(t\right) = \beta_{j\omega}\left(-\infty\right)+\sqrt{\frac{\kappa_e}{2\pi}}\int_{-\infty}^{t}\mathrm{d}t'\,\mathrm{e}^{-\mathrm{i}(\omega_c+h-\omega)t'}\beta_c\left(t'\right) \tag{4.53}$$

Substituting the equation (4.53) into equation (4.52d) and defining:

$$\beta_{j\text{in}}\left(t\right) \equiv \frac{1}{\sqrt{2\pi}}\int \mathrm{d}\omega\,\mathrm{e}^{-\mathrm{i}(\omega-\omega_c-h)t}\beta_{j\omega}\left(-\infty\right) \tag{4.54}$$

we find, using the Wigner-Weisskopf approximation:

$$\dot{\beta}_c(t) + \left(\frac{\kappa_i}{2} + \kappa_e\right)\beta_c(t) = -\mathrm{e}^{\mathrm{i}\left(\omega_g+\omega_c+h-\omega_e\right)t}\left(g_A^{eg}\right)^*\beta_e(t) - \mathrm{e}^{\mathrm{i}\left(\omega_g+\omega_c+h-\omega_s\right)t}\left(g_A^{sg}\right)^*\beta_s(t) - \sqrt{\kappa_e}\sum_j \beta_{j\mathrm{in}}(t) \tag{4.55}$$

At resonance conditions, i.e. $\omega_e - \omega_s = \omega_L$ and $\omega_e - \omega_g = \omega_c + h$, this expression reduces to:

$$\dot{\beta}_c(t) + \left(\frac{\kappa_i}{2} + \kappa_e\right)\beta_c(t) = -\left(g_A^{eg}\right)^*\beta_e(t) - \mathrm{e}^{\mathrm{i}\omega_L t}\left(g_A^{sg}\right)^*\beta_s(t) - \sqrt{\kappa_e}\sum_j \beta_{j\mathrm{in}}(t) \tag{4.56}$$

As an additional condition, we may assume that as t approaches infinity, there is no output field in the fiber, i.e. $\lim_{t\to\infty}\beta_{j\omega}(t) = 0$. We then find by taking the limit of equation (4.53) accordingly:

$$\lim_{t\to\infty}\beta_{j\omega}(t) = \beta_{j\omega}(-\infty) + \sqrt{\frac{\kappa_e}{2\pi}}\int \mathrm{d}t'\,\mathrm{e}^{-\mathrm{i}(\omega_c+h-\omega)t'}\beta_c(t') = 0 \tag{4.57}$$

$$\iff \frac{1}{\sqrt{2\pi}}\int \mathrm{d}\omega\,\mathrm{e}^{-\mathrm{i}(\omega-\omega_c-h)t}\beta_{j\omega}(-\infty) = -\frac{\sqrt{\kappa_e}}{2\pi}\int \mathrm{d}\omega\int \mathrm{d}t'\,\mathrm{e}^{-\mathrm{i}(\omega-\omega_c-h)(t-t')}\beta_c(t') \tag{4.58}$$

Using that:

$$\int \mathrm{d}\omega\int \mathrm{d}t'\,\mathrm{e}^{-\mathrm{i}\omega(t-t')}f(t') = 2\pi f(t) \tag{4.59}$$

we find that equation (4.58) yields:

$$\beta_{j\mathrm{in}}(t) = -\sqrt{\kappa_e}\beta_c(t) \tag{4.60}$$

Substituting equation (4.60) into equation (4.56) we thus obtain:

$$\dot{\beta}_{j\mathrm{in}}(t) + \left(\frac{\kappa_i}{2} - \kappa_e\right)\beta_{j\mathrm{in}}(t) = \sqrt{\kappa_e}\left(g_A^{eg}\right)^*\beta_e(t) + \mathrm{e}^{\mathrm{i}\omega_L t}\sqrt{\kappa_e}\left(g_A^{sg}\right)^*\beta_s(t) \tag{4.61}$$

Note that we have reduced the problem, under resonance conditions and substituting equation (4.60), to the following set of equations:

$$\dot{\beta}_e(t) + \frac{\gamma_e}{2}\beta_e(t) = -\frac{g_A^{eg}}{\sqrt{\kappa_e}}\beta_{j\mathrm{in}}(t) + \Omega(t)\beta_s(t) \tag{4.62a}$$

$$\dot{\beta}_s(t) + \frac{\gamma_s}{2}\beta_s(t) = -\Omega^*(t)\beta_e(t) - \mathrm{e}^{-\mathrm{i}\omega_L t}\frac{g_A^{sg}}{\sqrt{\kappa_e}}\beta_{j\mathrm{in}}(t) \tag{4.62b}$$

$$\dot{\beta}_{j\mathrm{in}}(t) + \left(\frac{\kappa_i}{2} - \kappa_e\right)\beta_{j\mathrm{in}}(t) = \sqrt{\kappa_e}\left(g_A^{eg}\right)^*\beta_e(t) + \mathrm{e}^{\mathrm{i}\omega_L t}\sqrt{\kappa_e}\left(g_A^{sg}\right)^*\beta_s(t) \tag{4.62c}$$

4.3.4. OBTAINING AN APPROXIMATION FOR $\Omega(t)$

Equations (4.62a), (4.62b), and (4.62c) form a set of three non-linear, coupled first order differential equations for four unknown functions, which is in general not solved. In a first simplification of the system, we set $\gamma_s = 0$, $g_A^{sg} = 0$ so that these equations reduce to:

$$\dot{\beta}_e(t) + \frac{\gamma_e}{2}\beta_e(t) = -\frac{g_A^{eg}}{\sqrt{\kappa_e}}\beta_{j\mathrm{in}}(t) + \Omega(t)\beta_s(t) \tag{4.63a}$$

$$\dot{\beta}_s(t) = -\Omega^*(t)\beta_e(t) \tag{4.63b}$$

$$\dot{\beta}_{j\mathrm{in}}(t) + \left(\frac{\kappa_i}{2} - \kappa_e\right)\beta_{j\mathrm{in}}(t) = \sqrt{\kappa_e}\left(g_A^{eg}\right)^*\beta_e(t) \tag{4.63c}$$

We may rewrite equation (4.63c) as:

$$\beta_e(t) = \frac{\sqrt{\kappa_e}}{\left(g_A^{eg}\right)^*}\left[\frac{\dot{\beta}_{1\mathrm{in}}(t)}{\kappa_e} + \left(\frac{\kappa_i}{2\kappa_e} - 1\right)\beta_{1\mathrm{in}}(t)\right] \tag{4.64}$$

Furthermore, we may write the complex function $\beta_s(t)$ in the following form:

$$\beta_s(t) = |\beta_s(t)| \, e^{i\theta(t)} \tag{4.65}$$

where both $|\beta_s(t)|$ and $\theta(t)$ are real-valued functions. Note that:

$$\frac{d}{dt}|\beta_s(t)|^2 = \dot{\beta}_s(t)\,\beta_s^*(t) + \dot{\beta}_s^*(t)\,\beta_s(t) \tag{4.66}$$

We may substitute accordingly to find:

$$\begin{aligned}
\frac{d}{dt}|\beta_s(t)|^2 &= -\beta_e(t)\left[\dot{\beta}_e(t) + \frac{\gamma_e}{2}\beta_e(t) + \frac{g_A^{eg}}{\sqrt{\kappa_e}}\beta_{jin}(t)\right]^* + \text{H.c.} \\
&= -2\Re\left\{\beta_e(t)\left[\dot{\beta}_e(t) + \frac{\gamma_e}{2}\beta_e(t) + \frac{g_A^{eg}}{\sqrt{\kappa_e}}\beta_{jin}(t)\right]^*\right\} \\
&= -\left(\frac{d}{dt}|\beta_e(t)|^2 + \gamma_e|\beta_e(t)|^2 + 2\Re\left\{\frac{g_A^{eg}}{\sqrt{\kappa_e}}\beta_e^*(t)\,\beta_{jin}(t)\right\}\right)
\end{aligned} \tag{4.67}$$

and the phase term:

$$\begin{aligned}
\dot{\theta}(t) &= \frac{i}{|\beta_s(t)|^2}\left\{\beta_e(t)\left[\dot{\beta}_e(t) + \frac{\gamma_e}{2}\beta_e(t) + \frac{g_A^{eg}}{\sqrt{\kappa_e}}\beta_{jin}(t)\right]^* + \frac{1}{2}\frac{d}{dt}|\beta_s(t)|^2\right\} \\
&= -\frac{1}{|\beta_s(t)|^2}\Im\left\{\beta_e(t)\left[\dot{\beta}_e(t) + \frac{\gamma_e}{2}\beta_e(t) + \frac{g_A^{eg}}{\sqrt{\kappa_e}}\beta_{jin}(t)\right]^*\right\}
\end{aligned} \tag{4.68}$$

After solving for $\beta_s(t)$, we may then solve for $\Omega(t)$ from equation (4.62a):

$$\Omega(t) = \frac{1}{\beta_s(t)}\left[\dot{\beta}_e(t) + \frac{\gamma_e}{2}\beta_e(t) + \frac{g_a^{eg}}{\sqrt{\kappa_e}}\beta_{jin}(t)\right] \tag{4.69}$$

We choose the input photon pulse to be:

$$\beta_{jin}(t) = \frac{e^{-(t/\zeta)^2}}{\sqrt{\zeta\sqrt{2\pi}}} \tag{4.70}$$

so that $\sum_j \int |\beta_{jin}|^2 \, dt = 1$ and by setting the critical coupling conditions [35]:

$$(g_A, \kappa_i, \kappa_e, \gamma_e) = (-70, 5, 250, 1)\, 2\pi \text{ MHz} \tag{4.71}$$

and setting $\zeta = 0.1$ μs, we find the results utilizing a numerical method as plotted in figure 4.3

4.3.5. ANALYSIS OF THE GENERALIZED MODEL

Now that we have solved $\Omega(t)$ for the simplified model, we may use variations of this solution to verify the behavior of our generalized model. We may rewrite equations (4.62a), (4.62b), and (4.62c) as the following system:

$$\frac{d}{dt}\begin{pmatrix}\beta_e(t)\\ \beta_s(t)\\ \beta_{jin}(t)\end{pmatrix} = \begin{pmatrix}-\frac{\gamma_e}{2} & \Omega(t) & -\frac{g_A^{eg}}{\sqrt{\kappa_e}} \\ -\Omega^*(t) & -\frac{\gamma_s}{2} & -e^{-i\omega_L t}\frac{g_A^{sg}}{\sqrt{\kappa_e}} \\ \sqrt{\kappa_e}\left(g_A^{eg}\right)^* & e^{i\omega_L t}\sqrt{\kappa_e}\left(g_A^{sg}\right)^* & \kappa_e - \frac{\kappa_i}{2}\end{pmatrix}\begin{pmatrix}\beta_e(t)\\ \beta_s(t)\\ \beta_{jin}(t)\end{pmatrix} \tag{4.72}$$

There are no known analytical methods to solve this type of equations, but as a first attempt to approximate some solution we may use the solutions as found in the simplified model, meaning that

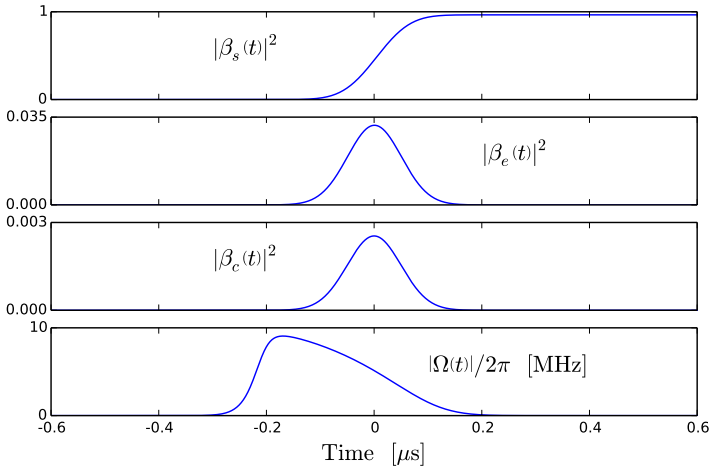

Figure 4.3: Plots of $|\beta_s(t)|^2$, $|\beta_e(t)|^2$, $|\beta_c(t)|^2$, and $|\Omega(t)|/2\pi$ for the case that $\gamma_s = 0$.

we take $\Omega(t)$ and $\beta_{\text{jin}}(t)$ to be known functions. We can then reduce our model to the following system of equations:

$$\frac{\mathrm{d}}{\mathrm{d}t}\begin{pmatrix}\beta_e(t)\\ \beta_s(t)\end{pmatrix} = \begin{pmatrix}-\frac{\gamma_e}{2} & \Omega(t)\\ -\Omega^*(t) & -\frac{\gamma_s}{2}\end{pmatrix}\begin{pmatrix}\beta_e(t)\\ \beta_s(t)\end{pmatrix} + \begin{pmatrix}g_A^{eg}\\ \mathrm{e}^{\mathrm{i}\omega_L t}g_A^{sg}\end{pmatrix}\beta_c(t) \tag{4.73}$$

We may define:

$$\boldsymbol{\beta}(t) \equiv \begin{pmatrix}\beta_e(t)\\ \beta_s(t)\end{pmatrix}, \quad \boldsymbol{A}(t) \equiv \begin{pmatrix}-\frac{\gamma_e}{2} & \Omega(t)\\ -\Omega^*(t) & -\frac{\gamma_s}{2}\end{pmatrix}, \quad \boldsymbol{\xi}(t) \equiv \begin{pmatrix}g_A^{eg}\\ \mathrm{e}^{\mathrm{i}\omega_L t}g_A^{sg}\end{pmatrix}\beta_c(t) \tag{4.74}$$

so that we are left to solve:

$$\dot{\boldsymbol{\beta}}(t) = \boldsymbol{A}(t)\boldsymbol{\beta}(t) + \boldsymbol{\xi}(t) \tag{4.75}$$

We may numerically solve this differential equation with the midpoint method. This method implies that we approximate $\dot{\boldsymbol{\beta}}(t)$ as follows:

$$\dot{\boldsymbol{\beta}}(t) \approx \frac{\boldsymbol{\beta}(t+h) - \boldsymbol{\beta}(t)}{h} \tag{4.76}$$

and the right hand side of equation (4.75) is approximated as follows:

$$\boldsymbol{A}(t)\boldsymbol{\beta}(t) + \boldsymbol{\xi}(t) \approx \tfrac{1}{2}\left(\boldsymbol{A}(t+h)\boldsymbol{\beta}(t+h) + \boldsymbol{\xi}(t+h) + \boldsymbol{A}(t)\boldsymbol{\beta}(t) + \boldsymbol{\xi}(t)\right) \tag{4.77}$$

By equating the approximations we then obtain:

$$\boldsymbol{\beta}(t+h) = \left[\mathbf{1} - \tfrac{h}{2}\boldsymbol{A}(t+h)\right]^{-1}\left\{\left[\mathbf{1} + \tfrac{h}{2}\boldsymbol{A}(t)\right]\boldsymbol{\beta}(t) + \tfrac{h}{2}\left[\boldsymbol{\xi}(t+h) + \boldsymbol{\xi}(t)\right]\right\} \tag{4.78}$$

so that we can iterate from some initial vector $\boldsymbol{\beta}(t=-\infty) = \mathbf{0}$. With this method we obtain the results as shown in figure 4.4. Furthermore, in table 4.2 we list some numerical values of $|\beta_s(t)|^2$ and $|\beta_s(t)|^2$ at $t = \{0.4, 0.5, 0.6\}$ μs for different values of γ_s and $g_A sg$. From these values it immediately becomes clear that there is an issue regarding normalization as $|\beta_s|^2 > 1$ in the case that we set $\gamma_s = 0$ and $g_A^{sg} = 0.1 g_A^{eg}$. This will be further discussed in chapter 5.

From the plots we do see the qualitative behavior that is expected to be seen: the cavity mode $|1\rangle$ now couples to the excitation of the ground state $|g\rangle$ of the atom to the metastable state $|s\rangle$, so that $|\beta_s|^2$ is larger than with this coupling switched off, i.e. $g_A^{sg} = 0$. Due to this effect the Rabi oscillations for the transition between the atom states $|s\rangle$ and $|e\rangle$, that are addressed by the external field $\Omega(t)$, cause a larger value of $|\beta_e(t)|^2$. Finally, when $\gamma_s \neq 0$, the state $|s\rangle$ is subject to decoherence, so we see a decline in $|\beta_s|^2$ over time.

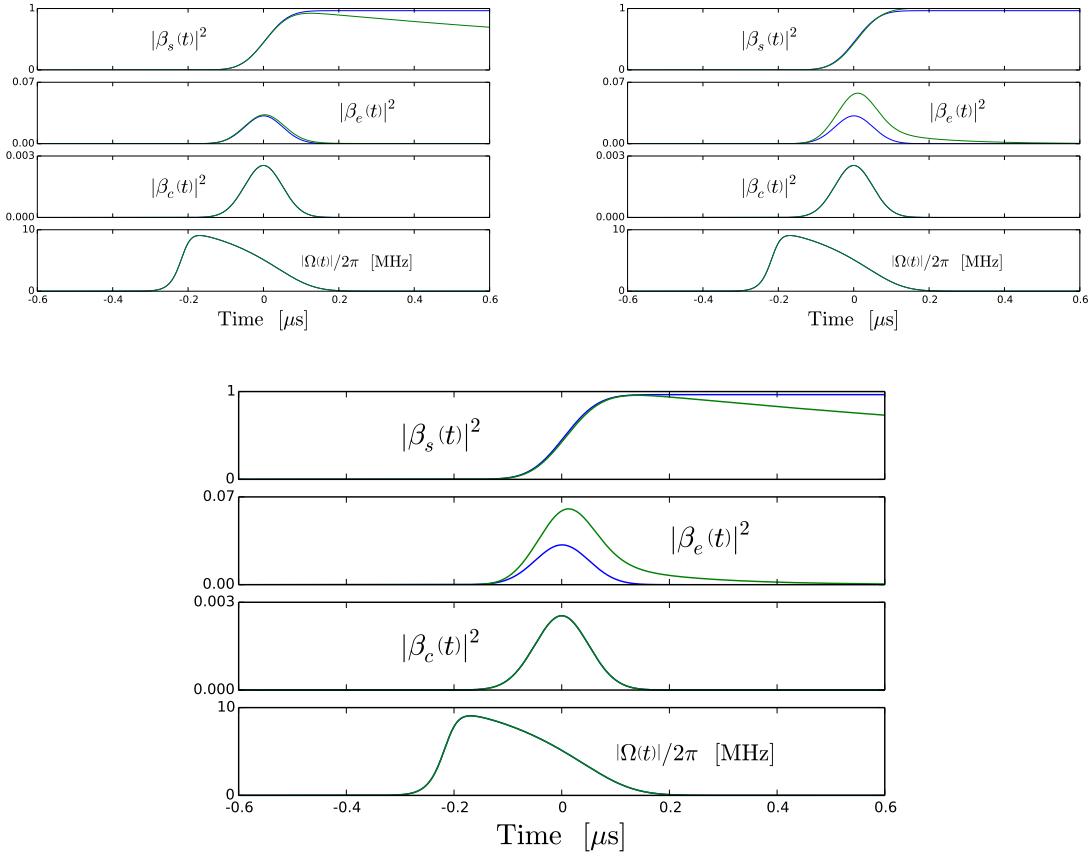

Figure 4.4: The green curves are plots of $|\beta_s(t)|^2$, $|\beta_e(t)|^2$, and $|\beta_c(t)|^2$, and $|\Omega(t)|/2\pi$ for the case that $\gamma_s = 0.1\gamma_e$ and $g_A^{sg} = 0$ (top left), the case that $\gamma_s = 0$ and $g_A^{sg} = 0.1g_A^{eg}$ (top right), and the case that $\gamma_s = 0.1g_e$ and $g_A^{sg} = 0.1g_A^{eg}$ (bottom middle). The blue curves are the earlier results.

$\gamma_s = 0$ $g_A^{sg} = 0$	0.4 μs	0.5 μs	0.6 μs	$\gamma_s = 0$ $g_A^{sg} = 0.1g_A^{eg}$	0.4 μs	0.5 μs	0.6 μs
$\lvert\beta_s\rvert^2$	0.96	0.97	0.97	$\lvert\beta_s\rvert^2$	1.01	1.01	1.01
$\lvert\beta_e\rvert^2$	0.0000	0.0000	0.0000	$\lvert\beta_e\rvert^2$	0.0060	0.0017	0.0005
$\gamma_s = 0.1\gamma_e$ $g_A^{sg} = 0$	0.4 μs	0.5 μs	0.6 μs	$\gamma_s = 0.1\gamma_e$ $g_A^{sg} = 0.1g_A^{eg}$	0.4 μs	0.5 μs	0.6 μs
$\lvert\beta_s\rvert^2$	0.89	0.79	0.70	$\lvert\beta_s\rvert^2$	0.94	0.83	0.73
$\lvert\beta_e\rvert^2$	0.0004	0.0001	0.0000	$\lvert\beta_e\rvert^2$	0.0074	0.0020	0.0006

Table 4.2: Numerical values of $|\beta_s(t)|^2$ and $|\beta_s(t)|^2$ at $t = \{0.4, 0.5, 0.6\}$ μs for different values of γ_s and $g_A sg$.

5

Towards Secure Quantum Cloud Computing

5.1. Research Conclusions and Discussion

In this section we will put the research that was performed on the electronic structure of the NV-center as in chapter 2, the measurement-device-independent quantum key distribution protocol as discussed in chapter 3 and the concept of the single photon transistor as analyzed in chapter 4 into context regarding the implementation of the NV-center in a secure quantum communication and information storing protocol. We will do so by identifying the NV-center as an entanglement source and as a three level system.

5.1.1. The NV-center as an entanglement source

As discussed in chapter 4, the NV-center is found to have a electron spin-triplet configuration ground state, which when taking hyperfine interaction into account splits into the magnetic sublevels $^3A_{2\pm}$, split with an energy Δ from the ground state $^3A_0$ in the absence of a magnetic field and any strain field. Experimentally, it has been found that $\Delta \approx 2.88$ GHz [11].

the NV-center may be used a a single photon source, the photon being entangled to the NV-center spin state. By exciting the NV-center to the $|A_2\rangle$ state, we have that after some time the state will have decayed to either the $|+1\rangle \equiv |^3A_{2+}\rangle$ state through emitting a left-handed polarized photon $|\sigma_-\rangle$ or to the $|-1\rangle \equiv |^3A_{2-}\rangle$ state through emitting a right-handed polarized photon $|\sigma_+\rangle$. In the ideal case of low strain, the probability is equally large for each event and we will end up in the state:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|-1\rangle \otimes |\sigma_+\rangle + |+1\rangle \otimes |\sigma_-\rangle\right) \tag{5.1}$$

Using NV-centers for QKD key storing

As the NV-center has been shown to provide a suitable single photon source with desirable entanglement properties. In a more general case, we have that after exciting an NV-center into the $|A_2\rangle$ state, which should be addressable due to its split off energy level based on a perturbation theory analysis of spin-orbit and spin-spin interactions, it relaxes into the following entangled state:

$$|\psi\rangle = \alpha\,|-1\rangle \otimes |\sigma_+\rangle + \beta\,|+1\rangle \otimes |\sigma_-\rangle\,, \quad \alpha, \beta \in \mathbb{C} \tag{5.2}$$

such that $|\alpha|^2 + |\beta|^2 = 1$. Ideally, we have that $\alpha = \beta = \frac{1}{\sqrt{2}}$, but due to for instance strain in the lattice the state might be a little 'skewed' with respect to the maximally entangled state.

In the MDI-QKD protocol we rely on the emission of two single photons in order to fully avoid the use of the decoy state protocol. However, having a simultaneous emission of a single photon at both Alice and Bob is practically demanding and therefore limiting in terms of a key generation rate.

We now assume that both Alice and Bob emit, at the same time, a photon associated with the decay of the $|A_2\rangle$ state of the NV-center, that is:

$$|\psi\rangle_A = \alpha\,|-1\rangle_A \otimes |\sigma_+\rangle_A + \beta\,|+1\rangle_A \otimes |\sigma_-\rangle_A\,, \quad |\psi\rangle_B = \gamma\,|-1\rangle_B \otimes |\sigma_+\rangle_B + \delta\,|+1\rangle_B \otimes |\sigma_-\rangle_B \tag{5.3}$$

Upon beam-splitter incidence of both photons, the following state is acquired:

$$\hat{B}\,|\psi\rangle_{AB} = \frac{\mathrm{i}}{4}\begin{cases} [|H_3H_3\rangle + |H_4H_4\rangle] \otimes [\alpha\gamma\,|-1,-1\rangle + \alpha\delta\,|-1,+1\rangle + \beta\gamma\,|+1,-1\rangle + \beta\delta\,|+1,+1\rangle] \\ + \\ [|V_3V_3\rangle + |V_4V_4\rangle] \otimes [-\alpha\gamma\,|-1,-1\rangle + \alpha\delta\,|-1,+1\rangle + \beta\gamma\,|+1,-1\rangle - \beta\delta\,|+1,+1\rangle] \\ + \\ 2\,[|H_3V_3\rangle + |H_4V_4\rangle] \otimes [\alpha\gamma\,|-1,-1\rangle - \beta\delta\,|+1,+1\rangle] \\ + \\ 2\,[|H_3V_4\rangle - |V_3H_4\rangle] \otimes [-\alpha\delta\,|-1,+1\rangle + \beta\gamma\,|+1,-1\rangle] \end{cases} \tag{5.4}$$

In the case that Alice and Bob send a perfectly entangled photon, i.e. $\alpha = \beta = \gamma = \delta = \frac{1}{\sqrt{2}}$, we have that:

$$\hat{B}\,|\psi\rangle_{AB} = \frac{\mathrm{i}}{8}\begin{cases} [|H_3H_3\rangle + |H_4H_4\rangle] \otimes [|-1,-1\rangle + |-1,+1\rangle + |+1,-1\rangle + |+1,+1\rangle] \\ + \\ [|V_3V_3\rangle + |V_4V_4\rangle] \otimes [-|-1,-1\rangle + |-1,+1\rangle + |+1,-1\rangle - |+1,+1\rangle] \\ + \\ 2\sqrt{2}\,[|H_3V_3\rangle + |H_4V_4\rangle] \otimes \frac{1}{\sqrt{2}}\,[|-1,-1\rangle - |+1,+1\rangle] \\ + \\ 2\sqrt{2}\,[|H_3V_4\rangle - |V_3H_4\rangle] \otimes \frac{1}{\sqrt{2}}\,[-|-1,+1\rangle + |+1,-1\rangle] \end{cases} \tag{5.5}$$

In case both detectors click on one side of the detecting scheme, we project the NV-center into the $|\Phi^-\rangle$ Bell state, in case the detectors click different sides we project the NV-center into the $|\Psi^-\rangle$ Bell state. Either of these Bell-state projections happens in 50% of the times. In case of a $|\Psi^-\rangle$ heralding by Charlie, either Alice or Bob needs to flip their NV-center spin in order to be fully positively correlated again.

The key is generated by first generating the $b_{A,B} = \{b_1, b_2, \cdots, b_N\}_{A,B}$, with N the number of successfully heralding events, containing the bases in which to measure the spin of the NV-center of Alice and Bob, respectively. After this, the actual measurements are performed and stored in the raw key strings $k_{A,B} = \{k_1, k_2, \cdots, k_N\}_{A,B}$. Finally, either Alice or Bob announces their string of bases and select the key string elements in which they used the same basis. As we have to measure an $S = 1$ system, the Hilbert space for measuring the spin state is of dimension three and typically, the sifted key will have a length $\frac{N}{9}$. A small portion of the key string is sacrificed to communicate and check for discrepancies, i.e. to estimate the error. If the error is sufficiently small, depending on the predicted quantum bit error rate Q, the key is restored using error correction and privacy amplification. Note that the procedure typically requires many NV-centers.

LIMITATIONS DUE TO STRAIN EFFECTS

Strain mixes a $|E_{1,2}\rangle$ state into the $|A_2\rangle$ state, lowering the strict optical selection rules so that we may take the following initial states:

$$|\psi\rangle_A = \frac{1}{\sqrt{2}}\,[|0\rangle \otimes |\sigma_+\rangle + |1\rangle \otimes |\sigma_-\rangle] \tag{5.6}$$

$$|\psi\rangle_B = \frac{1}{\sqrt{2}}\left[|0\rangle \otimes \left(\sqrt{\kappa\,(\delta)}\,|H\rangle + \mathrm{i}\sqrt{\lambda\,(\delta)}\,|V\rangle\right) + |1\rangle \otimes \left(\sqrt{\kappa\,(\delta)}\,|H\rangle - \mathrm{i}\sqrt{\lambda\,(\delta)}\,|V\rangle\right)\right] \tag{5.7}$$

with $\lim_{\delta\to 0}\kappa = \lim_{\delta\to 0}\lambda = \frac{1}{2}$, $\lim_{\delta\to\infty}\kappa = 0$ and $\lim_{\delta\to\infty}\lambda = 1$. Finally, we should always have that $\kappa + \lambda = 1$. For instance $\kappa\,(\delta) = \frac{\mathrm{e}^{-\delta}}{2}$ and $\lambda\,(\delta) = 1 - \frac{\mathrm{e}^{-\delta}}{2}$. Defining $\theta \equiv \sqrt{\kappa} + \sqrt{\lambda}$ and $\eta \equiv \sqrt{\kappa} - \sqrt{\lambda}$, we

find upon a successful heralding by Charlie the following states:

$$|\psi\rangle = \frac{\mathrm{i}}{2\sqrt{2}} \begin{cases} [\theta\,|00\rangle + \eta\,|01\rangle - \eta\,|10\rangle - \theta\,|11\rangle], & \text{in case of } |\Phi^-\rangle \text{ heralding} \\ [-\eta\,|00\rangle - \theta\,|01\rangle + \theta\,|10\rangle + \eta\,|11\rangle], & \text{in case of } |\Psi^-\rangle \text{ heralding} \end{cases} \tag{5.8}$$

yielding:

$$\boldsymbol{\rho} = \frac{1}{4}\begin{pmatrix} \theta^2 & \eta\theta & -\eta\theta & -\theta^2 \\ \eta\theta & \eta^2 & -\eta^2 & -\eta\theta \\ -\eta\theta & -\eta^2 & \eta^2 & \eta\theta \\ -\theta^2 & -\eta\theta & \eta\theta & \theta^2 \end{pmatrix} \tag{5.9}$$

for which we find that:

$$\mathrm{CHSH} = 2\sqrt{2}\left[\frac{1}{2} + \sqrt{\lambda\kappa}\right] \tag{5.10}$$

We thus have that as the strain factor $\delta > 2.4099$, the Bell equality is no longer violated and the entanglement loses its meaning.

DETECTING ENTANGLEMENT

Determining the CHSH value is not the only way to confirm entanglement between two states. We may generalize the detection of entanglement in a witness operator formalism, even though using a witness operator in this case does not seem to provide any direct advantage over determining the CHSH value. Defining the density operator:

$$\hat{\rho} \equiv p\,|\psi\rangle\langle\psi| + (1-p)\,\hat{\sigma}, \quad 0 \leq p \leq 1 \tag{5.11}$$

with $\hat{\rho}$ and $\hat{\sigma}$ density operators with the restriction that $\|\hat{\sigma} - \hat{\mathbb{1}}/4\| \leq d$. We now define that the state associated with the density matrix $\hat{\rho}$ is entangled if and only if there exists and operator $\hat{W}$ such that $\mathrm{Tr}\left(\hat{W}\hat{\rho}\right) < 0$, while for all density matrices $\hat{\rho}_{\mathrm{sep}}$, associated with separable states, it holds that $\mathrm{Tr}\left(\hat{W}\hat{\rho}_{\mathrm{sep}}\right) \geq 0$.

For states with a non positive partial transpose such an operator $\hat{W}$ may be easily constructed. Let $|e_-\rangle$ be the eigenstate of $\hat{\rho}^{\mathrm{T}_A}$ that corresponds to its minimal eigenvalue $\lambda_{\min} < 0$. The label T_A refers to the partial transpose taken with respect to the first subsystem. We then have that $\hat{W} = (|e_-\rangle\langle e_-|)^{\mathrm{T}_A}$ detects the entanglement of $\hat{\rho}$ as it can be seen that $\mathrm{Tr}\left[(|e_-\rangle\langle e_-|)^{\mathrm{T}_A}\hat{\rho}\right] = \mathrm{Tr}\left(|e_-\rangle\langle e_-|\,\hat{\rho}^{\mathrm{T}_A}\right) = \lambda_{\min} < 0$.

Let $|\psi\rangle \equiv a\,|01\rangle + b\,|10\rangle$, with $a, b \in \mathbb{R}^+$ and $a^2 + b^2 = 1$, yielding:

$$\hat{\rho} = a^2\,|01\rangle\langle 01| + ab\,(|01\rangle\langle 10| + |10\rangle\langle 01|) + b^2\,|10\rangle\langle 10| \tag{5.12}$$

Furthermore, let $d = 0$ so that $\hat{\sigma} = \hat{\mathbb{1}}/4$. We then find that $\lambda_{\min} = (1-p)/4 - pab$, for the eigenstate $|e_-\rangle = \frac{1}{\sqrt{2}}[|00\rangle - |11\rangle]$. We thus find that in the $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ basis, the matrix representation of $\hat{W}$ is the following:

$$\boldsymbol{W} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{5.13}$$

In conclusion, for any superposition of $|01\rangle$ and $|10\rangle$ and an experimental apparatus producing white noise, $\hat{W}$ is a suitable operator to detect this fact.

The witness operator as determined before turns out to be suitable for the scenario in which noise effects in the experimental setup are characterized by memory effects, or the case where $|\psi\rangle$ is generated perfectly and then sent through a channel with correlated noise. If the noise mechanisms acting on the state can be described as a depolarizing channel with some correlations of strength μ, then the resulting state will be of the form:

$$\hat{\rho} = \frac{1}{4}\left\{\hat{\mathbb{1}}\otimes\hat{\mathbb{1}} + \eta\left(a^2 - b^2\right)\left[\hat{\sigma}_z\otimes\hat{\mathbb{1}} - \hat{\mathbb{1}}\otimes\hat{\sigma}_z\right] + \left[\mu + (1-\mu)\,\eta^2\right]\left[-\hat{\sigma}_z\otimes\hat{\sigma}_z + 2ab\left(\hat{\sigma}_x\otimes\hat{\sigma}_x + \hat{\sigma}_y\otimes\hat{\sigma}_y\right)\right]\right\} \tag{5.14}$$

where η and μ determine the depolarization and degree of memory introduced by the noise process. Thus, this family of states is characterized by a, η, and μ.

It has been shown [36] that for any bipartite qubit state $|\phi\rangle = \alpha|00\rangle + \beta|11\rangle$ can be decomposed into a sum of projectors onto product vectors:

$$(|\phi\rangle\langle\phi|)^{T_A} = \frac{(\alpha+\beta)^2}{3}\sum_{i=1}^{3}|f_i f_i\rangle\langle f_i f_i| - \alpha\beta(|01\rangle\langle 01| + |10\rangle\langle 10|) \tag{5.15}$$

where:

$$|f_1\rangle \equiv e^{-i\pi/3}\cos\theta|0\rangle + e^{i\pi/3}\sin\theta|1\rangle \equiv |f_2^*\rangle \tag{5.16}$$

$$|f_3\rangle \equiv \cos\theta|0\rangle + \sin\theta|1\rangle = |f_1\rangle + |f_2\rangle \tag{5.17}$$

with:

$$\cos\theta \equiv \sqrt{\frac{\alpha}{\alpha+\beta}}, \quad \sin\theta \equiv \sqrt{\frac{\beta}{\alpha+\beta}} \tag{5.18}$$

Note that an optimum in the number of projection operators (ONP) does not necessarily imply an optimum in the number of device settings (ONS) and vice versa, which can be easily seen by expressing the operator $\hat{W}$ in terms of Pauli-operator eigenstates. Let $|z^+\rangle \equiv |0\rangle, |z^-\rangle \equiv |1\rangle$, $|x^\pm\rangle \equiv \frac{1}{\sqrt{2}}[|0\rangle \pm |1\rangle]$, and $|y^\pm\rangle \equiv \frac{1}{\sqrt{2}}[|0\rangle \pm i|1\rangle]$. Furthermore, let $\hat{P}_{ij} \equiv |ij\rangle\langle ij|$, so that:

$$(|\phi\rangle\langle\phi|)^{T_A} = \alpha^2\hat{P}_{z^+z^+} + \beta^2\hat{P}_{z^-z^-} + \alpha\beta\left(\hat{P}_{x^+x^+} + \hat{P}_{x^-x^-} - \hat{P}_{y^+y^-} - \hat{P}_{y^-y^+}\right) \tag{5.19}$$

Even though this expression has got six projection operators and is therefore not ONP, there are only three measurement settings involved, yielding the expression to be ONS, since impossible to decompose $(|\phi\rangle\langle\phi|)^{T_A}$ with less than three device settings.

Again regarding the case in which $|\psi\rangle \equiv a|01\rangle + b|10\rangle$, with $a, b > 0$ and $a^2 + b^2 = 1$, and $d = 0$, we find that:

$$\mathrm{Tr}\left(\hat{W}\hat{\rho}\right) = \lambda_{\min} = (1-p)/4 - pab \iff p = \frac{1 - 4\mathrm{Tr}\left(\hat{W}\hat{\rho}\right)}{1+4ab} \tag{5.20}$$

From now on, we will assume $a = b = \frac{1}{\sqrt{2}}$, i.e. we will investigate the maximally entangled state $|\Psi^+\rangle = \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle]$ which is mixed with some noise state $\hat{\sigma}$, such that $\|\hat{\sigma} - \hat{\mathbb{1}}/4\| \leq d$, according to some mixing parameter p:

$$\hat{\rho}(p,d) = p|\Psi^+\rangle\langle\Psi^+| + (1-p)\hat{\sigma} \tag{5.21}$$

We can imagine the state $\hat{\rho}(p,d)$ lying within a sphere $B_{p,d}$ with radius $(1-p)d$. If p is such that $B_{p,d} \subseteq \{\hat{\rho}_{\text{sep}}\} \wedge \{\hat{\rho}_{\text{ent}}\}$, then the operator $\hat{W}$ as given earlier is optimal and $\mathrm{sgn}\left[\mathrm{Tr}\left(\hat{W}\hat{\rho}\right)\right]$ provides a signature of entanglement versus separability. However, if $B_{p,d} \subseteq \{\hat{\rho}_{\text{sep}}\} \cup \{\hat{\rho}_{\text{ent}}\}$, we cannot be sure of this identity of $\hat{W}$ anymore. We can estimate a lower bound τ such that if $\mathrm{Tr}\left(\hat{W}\hat{\rho}\right) \geq \tau$, then $\hat{\rho}(p,d)$ is necessarily separable.We have that $\hat{\rho} \in \bigcup_{p\in[0,1]} B_{p,d}$, which we can regard as a convex cone originating in $|\Psi^+\rangle\langle\Psi^+|$ and terminating in in the sphere $B_{0,d}$ of radius d around the maximally mixed state $\hat{\mathbb{1}}/4$. There is a sphere $\mathcal{B}$ of separable states of maximal radius $\frac{1}{\sqrt{12}}$ around this maximally mixed state. The bigger $\mathrm{Tr}\left(\hat{W}\hat{\rho}\right)$, the closer $\hat{\rho}$ is to the sphere $B_{0,d} \subset \mathcal{B}$. If $\mathrm{Tr}\left(\hat{W}\hat{\rho}\right)$ is big enough, we have that $\hat{\rho} \in \mathcal{B}$. In this manner, we can determine τ to be:

$$\tau(d) = \frac{1}{4} - d^2 - \sqrt{\left(\frac{1}{12} - d^2\right)\left(\frac{3}{4} - d^2\right)} \tag{5.22}$$

For every τ' with $0 \leq \tau' < \tau$, there exists an entangled state $\hat{\rho}(p,d)$ with $\mathrm{Tr}\left(\hat{W}\hat{\rho}\right) = \tau'$.

If we assign $\mathrm{Tr}\left(\hat{W}\hat{\rho}\right) > 0 \iff \hat{\rho} \in \{\hat{\rho}_{\text{sep}}\}$, it is more favorable to use $\hat{W}_\epsilon \equiv \hat{W} - \epsilon\hat{\mathbb{1}}$, which is strictly not a witness operator but it requires the same measurement settings as $\hat{W}$.

The eigenvalues of $\hat{\rho}^{T_A}$ are λ, κ, and $\pm 2\sqrt{\lambda\kappa}$, with corresponding eigenstates:

$$\begin{gathered} \frac{1}{2}\left[-|00\rangle + |01\rangle - |10\rangle + |11\rangle\right], \quad \frac{1}{2}\left[-|00\rangle - |01\rangle + |10\rangle + |11\rangle\right] \\ \frac{1}{\sqrt{2}}\left[|01\rangle + |10\rangle\right], \quad \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right] \end{gathered} \tag{5.23}$$

We find the minimum eigenvalue of $\hat{\rho}^{T_A}$ to be $\lambda_{\min} = -2\sqrt{\lambda\kappa}$, corresponding to $|e_-\rangle \equiv \frac{1}{\sqrt{2}}\left[|01\rangle + |10\rangle\right]$, and so:

$$\hat{W} = \frac{1}{2}\left[|00\rangle\langle 11| + |11\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|\right] \tag{5.24}$$

Now to decompose $\hat{W}$ into a sum of projectors onto product states in the Pauli eigenstate basis:

$$\hat{W} = \hat{P}_{x^+x^+} + \hat{P}_{x^-x^-} + \hat{P}_{y^+y^-} + \hat{P}_{y^-y^+} - \hat{P}_{z^+z^+} - \hat{P}_{z^-z^-} \tag{5.25}$$

where $\hat{P}_{i^\pm j^\pm} \equiv |i^\pm j^\pm\rangle\langle i^\pm j^\pm|$, with $|x^\pm\rangle \equiv \frac{1}{\sqrt{2}}\left[|0\rangle \pm |1\rangle\right]$, $|y^\pm\rangle \equiv \frac{1}{\sqrt{2}}\left[|0\rangle \pm \mathrm{i}\,|1\rangle\right]$, and $|z^\pm\rangle \equiv |0/1\rangle$. which is obviously ONS. Note that in order to determine the expectation value of the witness operator we need six measurement settings in order to gather the proper statistics. It therefore is not necessarily a better or easier way to determine whether a state is entangled or not.

5.1.2. THE NV-CENTER AS A THREE LEVEL SYSTEM

We may summarize the energetically close triplet states $|^3A_{2+}\rangle$, $|^3A_{20}\rangle$, and $|^3A_{2-}\rangle$ into a general ground state $|g\rangle$, the singlet states $^1E_1$, $^1E_2$, and $^1A_1$ as the metastable state $|s\rangle$ and the triplet excited states ^3E as the general excited state $|e\rangle$. From experiment, we know that the zero phonon line between the state $|g\rangle$ and $|e\rangle$ is approximately 1.945 eV. The energy level of the state $|s\rangle$ is not exactly known. Having defined the states $|g\rangle$, $|e\rangle$, and $|s\rangle$, the feasibility of an NV-center to play the role of the three level atom in the model for a single photon transistor depends on the coherence time the state $|e\rangle$, which is preferably small, and the coherence time of the state $|s\rangle$, which is preferably large.

5.2. FUTURE WORK AND OUTLOOK

Regarding the NV-center analysis as done in chapter 2, a follow-up research may take into account the interaction of the electronic configuration with surrounding spins such as the nitrogen spin and the carbon spins. Also the effect of strain may be interesting to look into more as it may reveal additional features of the NV-center that can be used. Regarding the MDI-QKD studies as done in chapter 3, it may be interesting to investigate the influence of noise on the key generation rate and determine the conditions that need to be met in order to have an efficient protocol for secure key sharing. Furthermore, an alternative to determining the CHSH value might prove to be beneficial. The witness operator as introduced earlier does not seem to theoretically provide any added benefit to determining the CHSH value as it requires more measurement settings, but practically it might prove to be easier to implement. Finally, regarding solving the generalized single photon transistor model as derived in chapter 4 first the normalization issue needs to be resolved. Note that in spite of $|\psi(t)\rangle$ not being a normalized state because we limited our solution space we do require that:

$$|\beta_s(t)|^2 + |\beta_e(t)|^2 + |\beta_c(t)|^2 \leq 2\int_{-\infty}^{t} \left|\beta_{j\mathrm{in}}(t')\right|^2 \mathrm{d}t' \tag{5.26}$$

Regarding solving the system as written in equation (4.72), it may be interesting to look into more advanced numerical approaches. Once the system can be numerically solved, one might look into studying the system's behavior by varying the external fields $\Omega(t)$ and the input photon fields $\beta_{j\mathrm{in}}(t)$ and develop an optimization scheme within experimentally feasible limits.

A

BEAM-SPLITTER THEORY

In this appendix we took a closer look at the operation of a 50:50 beam splitter. The mode of operation is without any further derivation used in chapter 3.

A beam splitter may be modeled by a set of related creation operators. We model a beam splitter by having two input ports a_0 and a_1 and two output ports a_2 and a_3. We may model an incoming photon state as a product state of photons at the input gates by associating creation operators with each port: $a_0 \cong \hat{a}_0^\dagger$, $a_1 \cong \hat{a}_1^\dagger$, $a_2 \cong \hat{a}_2^\dagger$ and $a_3 \cong \hat{a}_3^\dagger$. A state in which n and m photons respectively enter the input ports is thus described by:

$$|n\rangle_{a_0} \otimes |m\rangle_{a_1} \equiv |nm\rangle_{01} = \frac{1}{\sqrt{n!}} \left(\hat{a}_0^\dagger\right)^n \frac{1}{\sqrt{m!}} \left(\hat{a}_1^\dagger\right)^m |00\rangle_{01} \tag{A.1}$$

The beam splitter operation may be described by the following set of output port operator relations [37]:

$$\hat{a}_2^\dagger = \mathrm{e}^{\mathrm{i}\phi_2} \left(\hat{a}_1^\dagger \sqrt{R}\, \mathrm{e}^{\mathrm{i}\alpha} + \hat{a}_0^\dagger \sqrt{T}\right), \quad \hat{a}_3^\dagger = \mathrm{e}^{\mathrm{i}\phi_3} \left(\hat{a}_1^\dagger \sqrt{T} + \hat{a}_0^\dagger \sqrt{R}\, \mathrm{e}^{\mathrm{i}(\pi-\alpha)}\right) \tag{A.2}$$

provided that $R + T = 1$. Note that the operator algebra is preserved, i.e. $\left[\hat{a}_i, \hat{a}_j^\dagger\right] = \delta_{ij}$. In a 50:50 beam splitter we have in the symmetric case that $\phi_2 = \phi_3 = 0$, $\alpha = \frac{\pi}{2}$, and $R = T = \frac{1}{2}$, so that:

$$\hat{a}_2^\dagger = \frac{1}{\sqrt{2}} \left(\mathrm{i}\hat{a}_1^\dagger + \hat{a}_0^\dagger\right), \quad \hat{a}_3^\dagger = \frac{1}{\sqrt{2}} \left(\hat{a}_1^\dagger + \mathrm{i}\hat{a}_0^\dagger\right) \tag{A.3}$$

Any input state may now be transformed by the beam splitter operation by means of transforming the input operators $\hat{a}_0^\dagger$ and $\hat{a}_1^\dagger$ and the input state $|00\rangle_{01}$ into the output operators $\hat{a}_2^\dagger$ and $\hat{a}_3^\dagger$ and the output state $|00\rangle_{23}$ accordingly. For a general input state $|nm\rangle_{01}$ we have:

$$|nm\rangle_{01} = \frac{1}{\sqrt{n!}} \left(\hat{a}_0^\dagger\right)^n \frac{1}{\sqrt{m!}} \left(\hat{a}_1^\dagger\right)^m |00\rangle_{01} \mapsto \frac{1}{\sqrt{2n!}} \left(-\mathrm{i}\hat{a}_3^\dagger + \hat{a}_2^\dagger\right)^n \frac{1}{\sqrt{2m!}} \left(\hat{a}_3^\dagger - \mathrm{i}\hat{a}_2^\dagger\right)^m |00\rangle_{23} \tag{A.4}$$

A specific example illustrates an important effect that arises from the beam splitter theory. Suppose there are two photons incident, each on a different input port, i.e. $|\psi\rangle_{\mathrm{in}} = |11\rangle_{01}$. The beam splitter then creates the following output state:

$$|11\rangle_{01} = \hat{a}_0^\dagger \hat{a}_1^\dagger |00\rangle_{01} \mapsto \frac{1}{2} \left(-\mathrm{i}\hat{a}_3^\dagger + \hat{a}_2^\dagger\right) \left(\hat{a}_3^\dagger - \mathrm{i}\hat{a}_2^\dagger\right) |00\rangle_{23} = -\frac{\mathrm{i}}{\sqrt{2}} \left(|02\rangle_{23} + |20\rangle_{23}\right) \tag{A.5}$$

This is the famous Hong-Ou-Mandel effect, which states that when two photons in the same state enter the beam splitter through different input ports, they are guaranteed to exit both through the same output port.

The relevant input states for our MDI-QKD model are the coherent states $|\psi\rangle_{\text{in}} = |\alpha\rangle_0 \otimes |\beta\rangle_1$. A coherent state $|\alpha\rangle_i$ can be expanded in the Fock state basis as follows:

$$|\alpha\rangle_i = \mathrm{e}^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle_i = \underbrace{\mathrm{e}^{\left(\alpha \hat{a}_i^\dagger - \alpha^* \hat{a}_i\right)}}_{D_i(\alpha)} |0\rangle_i \tag{A.6}$$

Upon beam splitter interaction we then readily find:

$$|\alpha\rangle_0 \otimes |\beta\rangle_1 \mapsto D_3\left(-\frac{\mathrm{i}\alpha}{\sqrt{2}}\right) D_3\left(\frac{\beta}{\sqrt{2}}\right) D_2\left(\frac{\alpha}{\sqrt{2}}\right) D_2\left(-\frac{\mathrm{i}\beta}{\sqrt{2}}\right) |00\rangle_{23} \tag{A.7}$$

Using the Baker-Campbell-Hausdorff formula we find that:

$$\begin{aligned} D_i(\alpha)\, D_i(\beta) &= \mathrm{e}^{\left(\alpha \hat{a}_i^\dagger - \alpha^* \hat{a}_i\right)} \mathrm{e}^{\left(\beta \hat{a}_i^\dagger - \beta^* \hat{a}_i\right)} && \text{(A.8)} \\ &= \mathrm{e}^{\left[(\alpha+\beta)\hat{a}_i^\dagger - (\alpha^*+\beta^*)\hat{a}_i\right]} \mathrm{e}^{\Im(\alpha\beta^*)} && \text{(A.9)} \\ &= D_i(\alpha+\beta)\, \mathrm{e}^{\Im(\alpha\beta^*)} && \text{(A.10)} \end{aligned}$$

and thus:

$$|\alpha\rangle_0 \otimes |\beta\rangle_1 \mapsto \left|\frac{\alpha - \mathrm{i}\beta}{\sqrt{2}}\right\rangle_2 \otimes \left|\frac{-\mathrm{i}\alpha + \beta}{\sqrt{2}}\right\rangle_3 \tag{A.11}$$

In our case, we have phase randomized, weak coherent input states, i.e. $|\psi\rangle_{\text{in}} = |\sqrt{\mu}\rangle_0 \otimes |\mathrm{e}^{\mathrm{i}\theta}\sqrt{\nu}\rangle_1$, yielding the following output state:

$$|\sqrt{\mu}\rangle_0 \otimes |\mathrm{e}^{\mathrm{i}\theta}\sqrt{\nu}\rangle_1 \mapsto \left|\frac{\sqrt{\mu} - \mathrm{i}\mathrm{e}^{\mathrm{i}\theta}\sqrt{\nu}}{\sqrt{2}}\right\rangle_2 \otimes \left|\frac{-\mathrm{i}\mathrm{e}^{\mathrm{i}\theta}\sqrt{\mu} + \sqrt{\nu}}{\sqrt{2}}\right\rangle_3 \tag{A.12}$$

We have now assumed the photons to be indistinguishable. However, in the MDI-QKD scheme the interacting photons carry polarizations that may be different on the different input ports of the beam splitter. Let's refine the model by specifying a polarization version of each creation operator, i.e. $\hat{a}_{iH}^\dagger$ and $\hat{a}_{iV}^\dagger$. Defining the Fock basis states $|n\rangle_{0H} \otimes |m\rangle_{0V} \otimes |k\rangle_{1H} \otimes |l\rangle_{1V} \equiv |nmkl\rangle_{0H0V1H1V}$, we have that in the general case that Alice sends a single $\alpha\,|1\rangle_{0H} + \beta\,|1\rangle_{0V}$ photon and Bob a single $\gamma\,|1\rangle_{1H} + \delta\,|1\rangle_{1V}$ photon:

$$\begin{aligned} |\psi\rangle = \alpha\gamma\,|1010\rangle + \alpha\delta\,|1001\rangle + \beta\gamma\,|0110\rangle + \beta\delta\,|0101\rangle \mapsto & -\frac{\mathrm{i}\alpha\gamma}{2}\left(|2000\rangle + |0020\rangle\right) && \text{(A.13)} \\ & -\frac{\mathrm{i}\beta\delta}{2}\left(|0200\rangle + |0002\rangle\right) && \text{(A.14)} \\ & +\frac{\alpha\delta + \beta\gamma}{2}\left(|1100\rangle + |0011\rangle\right) && \text{(A.15)} \\ & +\frac{\alpha\delta - \beta\gamma}{2}\left(|1001\rangle - |0110\rangle\right) && \text{(A.16)} \end{aligned}$$

Upon Alice and Bob sending a correlated state in the HV basis, i.e. either $\alpha = \gamma$ and $\beta = \delta$, we have that due to the Hong-Ou-Mandel effect both input photons end up in the same detector. Events where only one detector clicks are discarded. However, if one detects a click at two detectors, the initial state becomes indistinguishable from the two anti correlated Bell input states, i.e.:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|1001\rangle - |0110\rangle\right) \mapsto \frac{1}{\sqrt{2}}\left(|1001\rangle - |0110\rangle\right) \tag{A.17}$$

or:

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|1001\rangle + |0110\rangle\right) \mapsto \frac{1}{\sqrt{2}}\left(|1100\rangle + |0011\rangle\right) \tag{A.18}$$

implying that if one detects both a $|H\rangle$ and a $|V\rangle$ photon at either the left or the right measurement setup, the initial state is indistinguishable from a $|\Psi^+\rangle$ state. Furthermore, if one detects the $|H\rangle$ state

on either the left or the right side and the $|V\rangle$ state on the other side, the initial state is indistinguishable from a $|\Psi^-\rangle$ state. In both cases, Alice (or Bob) needs to flip her bit to have it fully correlated to Bob's bit.

Likewise, upon Alice and Bob sending a correlated state in the AD basis we find, again discarding events in which only one detector clicks, if one detects both a $|H\rangle$ and a $|V\rangle$ photon at either the left or the right measurement setup, which is only possible to obtain if Alice and Bob send the same state, the initial state is indistinguishable from a $|\Psi^+\rangle$ state. Alice (or Bob) does not need to apply a bit flip in this case. Furthermore, if one detects the $|H\rangle$ state on either the left or the right side and the $|V\rangle$ state on the other side, the initial state is indistinguishable from a $|\Psi^-\rangle$ state. In both cases, Alice (or Bob) needs to flip her bit to have it fully correlated to Bob's bit.

B

Quantum Error Correction and Privacy Amplification

In this appendix we will briefly discuss the principle of quantum error correction by introducing the error correction code for bit flip errors and the error correction code for phase flip errors, after which we will combine the two using the Shor code [38].

B.1. Quantum Error Correction

Examples of single qubit quantum noise are for instance a bit flip error, which flips a state $|0\rangle$ to $|1\rangle$ and vice versa. A bit flip error is equivalent to a pauli-X operation, i.e. for a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ we have:

$$|\psi\rangle \mapsto \hat{X}|\psi\rangle = \alpha\hat{X}|0\rangle + \beta\hat{X}|1\rangle = \alpha|1\rangle + \beta|0\rangle \tag{B.1}$$

A rotation error leaves the $|0\rangle$ state untouched but adds a phase θ to the $|1\rangle$ state. The general rotation operator $\hat{R}_\theta$ is equivalent to such an operation, i.e.:

$$|\psi\rangle \mapsto \hat{R}_\theta|\psi\rangle = \alpha|0\rangle + \beta\hat{R}_\theta|1\rangle = \alpha|0\rangle + \beta e^{i\theta}|1\rangle \tag{B.2}$$

A special case of the rotation operation is the π-phase rotation, known as a phase flip error. The pauli-Z operation is equivalent to this error, i.e.:

$$|\psi\rangle \mapsto \hat{Z}|\psi\rangle = \alpha|0\rangle + \beta\hat{Z}|1\rangle = \alpha|0\rangle - \beta|1\rangle \tag{B.3}$$

Another example of quantum noise is dephasing, in which $\hat{\rho} \mapsto \frac{1}{2}\left(\hat{\rho} + \hat{Z}\hat{\rho}\hat{Z}^\dagger\right)$. This situation corresponds to complete decoherence, in which all phase information on the state is lost, i.e.:

$$\hat{\rho} \mapsto \frac{1}{2}\left(\hat{\rho} + \hat{Z}\hat{\rho}\hat{Z}^\dagger\right) = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| \tag{B.4}$$

A general error applied by sending a state through some quantum channel subject to some quantum noise, which might or might not be Eve interfering, maps the original state to an erroneous state, i.e.:

$$\hat{\rho} \mapsto \mathcal{E}(\hat{\rho}) \equiv \sum_i \hat{E}_i\hat{\rho}\hat{E}_i^\dagger \tag{B.5}$$

The challenge lies with the detection and the correction of these general errors. We wish to preserve superpositions of states which would be destroyed by a direct measurement, so we need to come up with something more clever. The no cloning theorem keeps us from copying a quantum, but there is the option of encoding a physical qubit in a number of logical bits.

B.1.1. CODING FOR CORRECTING BIT FLIP ERRORS

We may encode a single qubit state $a|0\rangle + b|1\rangle$ in three qubits as $a|000\rangle + b|111\rangle$ by means of a simple quantum circuit as shown in figure B.1. As we have that a quantum channel has a noise element to it in the sense that there is a probability p for a bit to undergo a bit-flip operation, there is a probability of $(1-p)^3 + 3p(1-p)^2$ that the three-qubit state suffers from at most one bit-flip. This bit-flip can be determined and recovered as we may utilize the error diagnosis projection operators:

$$\hat{P}_0 = |000\rangle\langle 000| + |111\rangle\langle 111| \quad \text{(no error)} \tag{B.6}$$

$$\hat{P}_1 = |100\rangle\langle 100| + |011\rangle\langle 011| \quad \text{(bit-flip on qubit 1)} \tag{B.7}$$

$$\hat{P}_2 = |010\rangle\langle 010| + |101\rangle\langle 101| \quad \text{(bit-flip on qubit 2)} \tag{B.8}$$

$$\hat{P}_3 = |001\rangle\langle 001| + |110\rangle\langle 110| \quad \text{(bit-flip on qubit 3)} \tag{B.9}$$

The error correction is then done by, based on the error syndrome outcome, i.e. the parity measurement outcomes of qubit 1 and 2 and qubit 1 and 3, to flip the errored bit once more. The fidelity between a

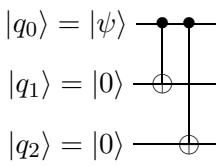

Figure B.1: Encoding of a single qubit into three qubits.

pure and a mixed state is a measure of how much pure state $|\psi\rangle$ there is in some mixture $\hat{\rho}$. It is defined as:

$$F(|\psi\rangle, \hat{\rho}) = \sqrt{\langle\psi|\hat{\rho}|\psi\rangle} \tag{B.10}$$

Without error correction, the mixed state after passing through the quantum channel is:

$$\hat{\rho} = (1-p)|\psi\rangle\langle\psi| + p\hat{X}|\psi\rangle\langle\psi|\hat{X} \tag{B.11}$$

with $\hat{X}$ the Pauli-X operator. We then find for the fidelity:

$$F = \sqrt{1 - p + p\langle\psi|\hat{X}|\psi\rangle^2} \tag{B.12}$$

As $\langle\psi|\hat{X}|\psi\rangle^2 > 0$, we have that the lower bound of the fidelity is $F_{\min} = \sqrt{1-p}$.

With error correction, the mixed state after passing through the quantum channel and being error-corrected is:

$$\hat{\rho} = (1-p)^3|\psi\rangle\langle\psi| + 3p(1-p)^2|\psi\rangle\langle\psi| + \cdots \tag{B.13}$$

We then find for the lower bound of the fidelity:

$$F_{\min} = \sqrt{(1-p)^3 + 3p(1-p)^2} \tag{B.14}$$

Given that $p < 1/2$, the fidelity has thus improved.

B.1.2. CODING FOR CORRECTING PHASE FLIP ERRORS

By performing the Hadamard transform we switch the basis of our state, i.e.:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \mapsto \hat{H}|\psi\rangle = \frac{\alpha}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{\beta}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv \alpha|+\rangle + \beta|-\rangle \tag{B.15}$$

Note that:

$$\hat{X}|+\rangle = |+\rangle, \quad \hat{X}|-\rangle = -|-\rangle \tag{B.16}$$

and:

$$\hat{Z}|+\rangle = |-\rangle, \quad \hat{Z}|-\rangle = |+\rangle \tag{B.17}$$

which shows that we have that in the Hadamard basis the Pauli-X operation is equivalent to a phase flip and the Pauli-Z operation is equivalent to a bit flip. We can thus use the exact same approach as for the bit-flip error correction, provided that we first switch to the Hadamard basis, i.e. $P_i \mapsto \hat{H}^{\otimes 3} P_i \hat{H}^{\otimes 3}$.

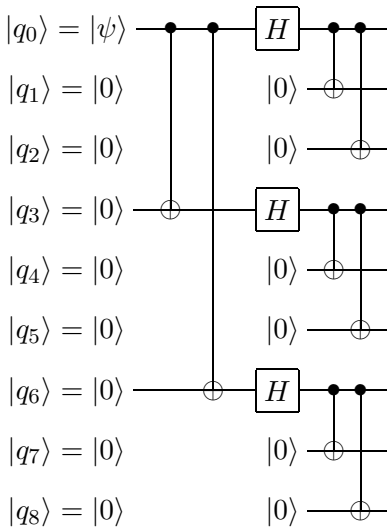

Figure B.2: Encoding of a single qubit into nine qubits.

B.1.3. THE SHOR CODE: CORRECTING BOTH

With the Shor Code we use nine qubits: one physical qubit and eight control qubits. By first utilizing the phase flip code:

$$|0\rangle \mapsto |+++\rangle\,, \quad |1\rangle \mapsto |---\rangle \tag{B.18}$$

and next encoding each of these qubits using the three qubit bit flip code:

$$|+\rangle \mapsto \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right), \quad |-\rangle \mapsto \frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right) \tag{B.19}$$

the codewords are given by:

$$|0\rangle \mapsto |0_L\rangle \equiv \frac{\left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)\left(|000\rangle + |111\rangle\right)}{2\sqrt{2}} \tag{B.20}$$

$$|1\rangle \mapsto |1_L\rangle \equiv \frac{\left(|000\rangle - |111\rangle\right)\left(|000\rangle - |111\rangle\right)\left(|000\rangle - |111\rangle\right)}{2\sqrt{2}} \tag{B.21}$$

A quantum circuit that establishes this encoding is displayed in figure B.2. The Shor code is able to protect against both phase flip and bit flip errors on any qubit. For detecting a bit flip error we simply perform a measurement $\hat{Z}_i\hat{Z}_{i+1}$, comparing the ith and the $(i+1)$th qubit. If we find that if these are different and the outcome is negative, we may conclude that a bit flip error occurred on either the ith or the $(i+1)$th qubit. By consecutively performing a $\hat{Z}_{i-1}\hat{Z}_i$ or a $\hat{Z}_{i+1}\hat{Z}_{i+2}$ measurement we find that in case of a negative outcome we may conclude that it was the ith or the $(i+1)$th qubit, respectively, which flipped. We may recover from the error by flipping said qubit again.

For coping with a phase flip error we look at blocks of qubits rather than individual qubits. Note that a phase flip error on any of the three qubits in a block results in a sign flip: $|000\rangle + |111\rangle \mapsto |000\rangle - |111\rangle$. Similar to the bit flip error detection, we may check for sign differences in blocks: when a phase flip occurs in one of the first three qubits we find that the signs of the first and the second block are different. By comparing the sign of the second and the third block we then find equal signs, indicating that the phase flip error must have occurred in one of the three first qubits. The original state is then recovered by applying a phase flip to the first block of qubits.

Note that in case of both a phase flip error and a bit flip error on the ith qubit, i.e. the operator $\hat{Z}_i\hat{X}_i$ is applied to the ith qubit, the first procedure recovers the bit flip error and the second recovers the phase shift error. The Shor code provides a means to recover both from a bit flip error and a phase flip error. We may even go one step further as to generalize the type of the error the Shor code can recover from, provided that the error is occurring on a single qubit. To show this, we introduce a

general trace-preserving noise operator $\hat{\mathcal{E}}$. It is convenient to express the operator $\hat{\mathcal{E}}$ in an operator sum representation with operation elements $\{\hat{E}_i\}$. For an initial state $|\psi\rangle$ we may thus write:

$$\hat{\mathcal{E}}\,|\psi\rangle\,\langle\psi| = \sum_i \hat{E}_i\,|\psi\rangle\,\langle\psi|\,\hat{E}_i^\dagger \tag{B.22}$$

In order to analyze the effects of error-correction we focus on a single term, say $\hat{E}_i\,|\psi\rangle\,\langle\psi|\,\hat{E}_i^\dagger$ and expand the operator $\hat{E}_i$ as a linear combination of the identity $\hat{\mathbb{1}}$, the bit flip $\hat{X}_j$, the phase flip $\hat{Z}_j$ and the combined bit and phase flip $\hat{X}_j\hat{Z}_j$, all acting on the jth qubit, as follows:

$$\hat{E}_i = e_{i0}\hat{\mathbb{1}} + e_{i1}\hat{X}_j + e_{i2}\hat{Z}_j + e_{i3}\hat{X}_j\hat{Z}_j \tag{B.23}$$

We may thus write the quantum state $\hat{E}_i\,|\psi\rangle$ as a superposition of four terms. Measuring the error syndrome collapses this superposition into one of theses four states $|\psi\rangle$, $\hat{X}_j\,|\psi\rangle$, $\hat{Z}_j\,|\psi\rangle$, and $\hat{X}_j\hat{Z}_j\,|\psi\rangle$. From each of these states the original state $|\psi\rangle$ may be recovered by applying the appropriate inversion operation.

B.2. PRIVACY AMPLIFICATION

Let Alice and Bob have a random variable W, which is for instance an n-bit string, while Eve learns a correlated random variable V, providing at most $t < n$ bits of information on W, i.e. $H(W|V) \geq n - t$. In general, the details on the distribution P_{VW} are unknown to both Alice and Bob. Alice and Bob wish to publicly choose a compression function $g : \{0,1\}^n \to \{0,1\}^r$ such that Eve's partial information on W and her complete information on g give her arbitrarily little information on $K = g(W)$. K can then be used safely as a cryptographic key.

Eve may have obtained:

1. t arbitrary bits of W
2. t arbitrary parity checks of W
3. the result of an arbitrary function mapping n-bit strings to t-bit strings
4. the string W transmitted through a binary symmetric channel with bit error probability ϵ satisfying $h(\epsilon) = 1 - n/t$ and hence with a capacity t/n, where $h(\cdot)$ denotes the binary entropy function

In a more general sense, of which all described possibilities are a special case, we allow Eve sto specify an arbitrary distribution P_{VW} (unknown to Alice and Bob) subject to the only constraint that $R(W|V = v) \geq n - t$ with high probability (over values v), where $R(W|V = v)$ the second-order conditional Rényi entropy [39] of W, given $V = v$.

BIBLIOGRAPHY

[1] R. P. Feynman, *Simulating physics with computers*, International Journal of Theoretical Physics **21**, 467 (1982).

[2] L. K. Grover, *A fast quantum mechanical algorithm for database search*, in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96* (ACM Press, New York, New York, USA, 1996) pp. 212–219, arXiv:9605043 [quant-ph] .

[3] P. Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, in *Proceedings 35th Annual Symposium on Foundations of Computer Science* (IEEE Comput. Soc. Press, 1994) pp. 124–134.

[4] MagiQ Technologies, *MagiQ,* (2014).

[5] D-Wave Systems Inc., *D-Wave,* (2014).

[6] W. Pfaff, B. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, and R. Hanson, *Unconditional quantum teleportation between distant solid-state quantum bits*, Science , 1 (2014).

[7] J. E. Mooij, *Josephson Persistent-Current Qubit*, Science **285**, 1036 (1999).

[8] H. J. Kimble, *The quantum internet.* Nature **453**, 1023 (2008).

[9] J. H. N. Loubser and J. A. van Wyk, *Electron spin resonance in the study of diamond*, Reports on Progress in Physics **41**, 1201 (1978).

[10] M. Tinkham, *Group Theory and Quantum Mechanics* (Dover Publications, 2003).

[11] N. Manson, J. Harrison, and M. Sellars, *Nitrogen-vacancy center in diamond: Model of the electronic structure and associated dynamics*, Physical Review B **74**, 104303 (2006).

[12] Y. Ma, M. Rohlfing, and A. Gali, *Excited states of the negatively charged nitrogen-vacancy color center in diamond*, Physical Review B **81**, 041204 (2010).

[13] J. R. Maze, A. Gali, E. Togan, Y. Chu, A. Trifonov, E. Kaxiras, and M. D. Lukin, *Properties of nitrogen-vacancy centers in diamond: the group theoretic approach*, New Journal of Physics **13**, 025025 (2011).

[14] L. Pauling, *The Nature of the Chemical Bond. Application of Results Obtained from the Quantum Mechanics and from a Theory of Paramagnetic Susceptibility to the Structure of Molecules*, Journal of the American Chemical Society **53**, 1367 (1931).

[15] M. Lannoo, G. Baraff, and M. Schlüter, *Self-consistent second-order perturbation treatment of multiplet structures using local-density theory*, Physical Review B **24**, 943 (1981).

[16] J. Sakurai, *Modern Quantum Mechanics*, revised ed. (Addison Wesley, 1994).

[17] A. Lenef and S. Rand, *Electronic structure of the N-V center in diamond: Theory*, Physical Review B **53**, 13441 (1996).

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

[19] C. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984) pp. 175–179.

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

[21] I. Quantique, *Swiss Quantum*, (2009).

[22] J. Clauser, M. Horne, A. Shimony, and R. Holt, *Proposed Experiment to Test Local Hidden-Variable Theories*, Physical Review Letters **23**, 880 (1969).

[23] M. Pawłowski and N. Brunner, *Semi-device-independent security of one-way quantum key distribution*, Physical Review A **84**, 010302 (2011).

[24] M. Pawłowski, *Security proof for cryptographic protocols based only on the monogamy of Bell's inequality violations*, Physical Review A **82**, 032313 (2010).

[25] M. Pawłowski and v. Brukner, *Monogamy of Bell's Inequality Violations in Nonsignaling Theories*, Physical Review Letters **102**, 030403 (2009).

[26] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, *Device-Independent Quantum Key Distribution with Local Bell Test*, Physical Review X **3**, 031006 (2013).

[27] R. Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, Swiss Federal Institute of Technology (2005), arXiv:0512258v2 [arXiv:quant-ph] .

[28] M. Tomamichel and E. Hänggi, *The link between entropic uncertainty and nonlocality*, Journal of Physics A: Mathematical and Theoretical **46**, 055301 (2013), arXiv:arXiv:1108.5349v2 .

[29] H.-K. Lo, X. Ma, and K. Chen, *Decoy State Quantum Key Distribution*, Physical Review Letters **94**, 230504 (2005).

[30] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, *Security of quantum key distribution with imperfect devices*, Quantum Information and Computation **4**, 22 (2002), arXiv:0212066 [quant-ph] .

[31] V. Giovannetti, S. Lloyd, and L. Maccone, *Quantum Random Access Memory*, Physical Review Letters **100**, 160501 (2008).

[32] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics*, 1st ed. (Cambridge University Press, 1995).

[33] E. Jaynes and F. Cummings, *Comparison of quantum and semiclassical radiation theories with application to the beam maser*, Proceedings of the IEEE **51**, 89 (1963).

[34] M. Scully and M. Zubairy, *Quantum Optics*, 1st ed. (Cambridge University Press, 1997).

[35] B. Dayan, A. S. Parkins, T. Aoki, E. P. Ostby, K. J. Vahala, and H. J. Kimble, *A photon turnstile dynamically regulated by one atom*. Science (New York, N.Y.) **319**, 1062 (2008).

[36] A. Sanpera, R. Tarrach, and G. Vidal, *Local description of quantum inseparability*, Physical Review A **58**, 826 (1998).

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

[38] M. Nielsen and I. Chuang, *Quantum Computation and Quantum Information*, 1st ed. (Cambridge University Press, 2010).

[39] A. Rényi, *Observability of Rényi's entropy*, in *Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability* (1960) pp. 547–561.