Atomic-Ensemble-based Quantum Repeaters

Numerical investigation of the effect of hardware parameters on atomic-ensemble-based repeater protocols

W.A. Stevense

TUDelft QuTech

Atomic-Ensemble-based Quantum Repeaters

Numerical investigation of the effect of hardware parameters on atomic-ensemble-based repeater protocols

by

W.A. Stevense

T̃UDelft   **QuTech**

Abstract

We perform a numerical optimisation of the hardware parameters of an atomic-ensemble-based single repeater setup. The setup operates on a real-life fiber network connecting the cities Delft and Eindhoven. Besides this network, the setup encompasses photon pair sources, quantum memories, single photon detectors, and 50:50 beam splitters. The corresponding hardware parameters we consider are the following;

- The detector efficiency, η_d, defined as the probability the photon detector correctly registers an incident photon.
- The detector dark count probability, p_d, defined as the probability that a detector registers a false detection event.
- The memory efficiency, $\eta_{m,0}$, defined as the maximum probability that an excitation is not lost in the quantum memory.
- The memory coherence time, T_c, defined as the characteristic time after which an excitation is lost in the quantum memory.
- The Hong-Ou-Mandel visibilty, v, which is a measure of the indistinguishability of the photons in the setup.

Additionally, the setup has the ability to be multiplexed. This means that the probabilistic processes essential for executing the repeater protocol are initiated M times in parallel. This increases the performance of the protocol.

To achieve the optimisation, we introduce absolute minimal hardware requirements and minimal hardware requirements. An absolute minimal hardware requirement is defined as the least favourable hardware parameter that still allows the setup to reach a given target metric. This implies that all other hardware parameters are at their optimal value. Minimal hardware requirements are defined as the least favourable set of hardware parameters that still allow the setup to reach a given target metric.

To evaluate the aforementioned target metric we conduct a numerical analysis. This analysis is based on the entanglement based version of quantum key distribution. We use Netsquid, a discrete event simulator for quantum networks, to carry out the numerical analysis. Utilising this, we formulate an optimisation problem that allows us to find absolute minimal hardware requirements and minimal hardware requirements for an atomic-ensemble-based single repeater setup.
We develop a method to solve this optimisation problem. This allows us to find absolute minimal hardware requirements and minimal hardware requirements for the hardware parameters listed above. We do this for different number M of multiplexing modes, and different node placements on the existing fiber network. We consider both perfect photon pair sources and a model of a photon pair source based on Spontaneous Parametric Down Conversion (SPDC).

This work serves as a guide for further experimental progress. Consequently, we highlight the merit of increasing multiplexing capabilities. Moreover, we recognise the importance of improving current state-of-the art quantum memories. We additionally remark the negative effect of asymmetry in the setup on the performance of the repeater. We identify that multi-photon emission inherent in SPDC sources is a major bottleneck to the performance of atomic-ensemble-based repeater setups.

Preface

Here we are. Delivering this thesis feels like closing the book on my formal education journey. Looking back, I am grateful for the opportunity to dive into the world of Applied Physics. Going for a Master's degree has been a mix of challenges and rewards, and I have truely enjoyed the whole ride. My education was not just about the theoretical concepts; it was about the thrill of discovery, the "aha" moments when concepts click, and the satisfaction of overcoming challenges. This thesis is the magnum opus of my education, and represents almost a year of research, coding, and hard work.

As with everything in life, this work is not the product of my efforts alone. There are many people I could not have done it without, and I want to express my gratitude to them. First and foremost, my daily supervisor, Francisco. Thank you for your support, invaluable guidance, and the numerous discussions we had. Even after you graduated and were on holiday you took the time to proofread and provide feedback to my thesis, for which I cannot thank you enough. You have been a great supervisor. More importantly, I learned a lot from you in terms of research, problem-solving, and project organisation.

Furthermore, I would like to thank Stephanie Wehner and all other people from the Wehner group for allowing me to do this project, and making me feel so welcome in the group. You have provided a very inspirational environment. I am certain that if one day we will make a quantum internet, the Wehner group will (have) play(ed) a major role in this.

I would also like to thank David, the original author of much of the code I used for this project. Whenever we were stuck, you were always willing to help. The many discussions I had with you, especially at the beginning of the project, really helped me to complete my thesis.

Then there are my parents, who have supported me since the day I was born. As a child, I was always curious about science. My parents bought me science books, took me to museums, and allowed me to experiment on their computer. Then in high school, puberty hit and I became rebellious. I decided following management courses rather than science courses would be my ticket to the riches. During my final year of high school my passion for science reemerged and I came across the Applied Physics programme. Many people deemed catching up on the physics courses impossible, but my parents and some of my high school teachers believed in me, and supported me to pull this off anyways. The rest is history. Therefore, I want to say to my parents; thank you for always standing behind me no matter what. I would have never been where I am today if it were not for you.

Last but not least, I want to thank my loving girlfriend; Qiqi. Your belief in me has been a constant source of strength. In the process of writing this thesis, you were probably the only person to ever notice when I was stressed if things were not going my way. Thank you for always standing by my side. Looking forward to a future with you makes me genuinely excited, and is one of the driving forces behind my motivation.

Contents

1

Introduction

On October 29th 1969 Prof. Leonard Kleinrock sent the very first message ever over the internet from the University of California, Los Angeles to Stanford University [1]. Today, approximately 50 years later, life without the internet is almost unimaginable. It is unlikely that Prof. Kleinrock would have known the impact the internet would have in the future when he first sent the message 'Login'. Today, we stand at the beginning of a similar revolution with the quantum internet. The quantum internet is believed by many to possess the potential to revolutionise the world in the same way the regular internet has in the past decades. A quantum internet makes use of quantum bits (qubits). Whereas the value of a classical bit is binary (0 or 1), a qubit can be in a superposition of 0 and 1 at the same time. Qubits can also be entangled with each other, leading to much larger correlations than possible classically. Finally, the laws of quantum mechanics do not allow a qubit to be copied [2, 3, 4]. Whereas this latter property enables great opportunities for secure communication, it also poses a challenge to the distribution of qubits over large distances, as qubits cannot be amplified in order to overcome signal losses and other imperfections [5]. Quantum repeaters are devices that aim to overcome this challenge [6].

The Quantum Internet Alliance (QIA) is on a moonshot mission to create such a quantum internet. QIA is a collective of universities, research institutions, and companies throughout Europe cooperating to create a European made quantum internet. In 2022 a 7 year program funded by the European Union aiming to build a full-stack prototype network commenced. The goal of this program is to "build two metropolitan scale networks containing quantum processors and photonic clients, connected by a long-distance fiber backbone using quantum repeaters [7]".

An important part of this objective is thus a long-distance fiber backbone using quantum repeaters. The long-distance backbone will serve to generate entanglement over a long distance. Establishing entanglement over this distance enables the execution of quantum applications between devices in the in the two distant metropolitan-scale quantum networks. A quantum repeater protocol aims to break the long distance over which entanglement is desired up into smaller, easier to bridge, segments [6]. Proof-of-concept experiments have been successfully conducted but realisation of a scalable quantum repeater is yet to be achieved. One of the most promising candidates for realisation of scalable quantum repeaters are atomic-ensembles, yielding several successful experiments in the past few years both locally in the lab and at several-kilometre range [8, 9]. Hardware with sufficient quality to realise large-scale quantum repeaters as desired for the QIA prototype is yet to be developed. A lot about the exact hardware requirements for atomic-ensembles running protocols on large scale remains unclear and developing such hardware is resource intensive [10, 11]. Hence, it is imperative to develop simulations analysing the performance of atomic-ensembles with different hardware parameters. Earlier efforts by D. Maier and J. Rabbie [12, 13] at QuTech have already produced working simulations of atomic-ensembles using the Netsquid discrete-event quantum-network simulator [14]. The main goal of this thesis is to build on and extend those simulations so that hardware parameter scans for large-scale atomic-ensemble-based repeaters can be performed. The simulations are then used to optimise the said hardware parameters in order to answer the question of which hardware parameters need to be improved in order to realise the long-distance fibre backbone of QIA's 2029 full stack prototype.

In order to enact the previously mentioned hardware parameter scans, we make the following contributions:

- We complete the integration of a code snippet containing models to simulate atomic-ensemble-based hardware [15] into NLblueprint, which is a repository that allows general simulation of quantum networks. Before the initialisation of this thesis project, David Maier authored code for this purpose. We make substantial efforts to ensure this code is error-free and complete. The foundation of all this rests on Netsquid [14]. We subsequently validate the results of simulations leveraging this integration. To conclude this validation, we juxtapose simulated outcomes against analytical results obtained in [16].
- We develop a novel methodology to employ Bayesian optimisation [17] to optimise the hardware parameters of the aforementioned integrated simulations. We develop code to enable the execution of this optimisation.
- We utilise a methodology developed by the authors of [10] and [11] to optimise the hardware parameters of the newly integrated simulations. To fulfil this, we slightly adapt previously written code [18].
- We carry out the previously mentioned optimisations. We compare the result to current state-of-the art experimental results and analyse the effect of design choices regarding the repeater on the results. From this, we infer conclusions and devise suggestions for further research undertakings.

The structure of this thesis is the following. We discuss all relevant background theory in Chapter 2. Building on this background, we introduce a methodology to perform the aforementioned optimisation in Chapter 3. To this end, we introduce code snippets that allow us to perform simulations of an atomic-ensemble-based repeater setup. Moreover, we formulate the aforementioned task of optimising hardware parameters as a mathematical problem. This mathematical formulation will bring about the definitions of absolute minimal hardware requirements and minimal hardware requirements. These are defined as the least favourable hardware parameter that still allows the setup to reach a given target metric, given all other hardware parameters are at their optimal value, and the least favourable set of hardware parameters that still allows the setup to reach a given target metric respectively. In Chapter 4, we perform a validation of the simulations. In Chapter 5, we introduce a real-life fiber network based on which we design the simulated setup. We solve the optimisation problems on this setup finding both absolute minimal hardware requirements and minimal hardware requirements. In Chapter 6, we present and discuss the absolute minimal hardware requirements. In Chapter 7, we present and discuss the minimal hardware requirements. Finally, in Chapter 8, we draw final conclusions and give suggestions for future research endeavours.

<div style="text-align: right; font-size: 3em;">2</div>

Background

In this chapter we present the theoretical background used over the course of this thesis. In Section 2.1 we discuss what repeaters are. In Section 2.2 we introduce quantum key distribution which will provide a measure for the performance of a repeater scheme. In Section 2.3 we introduce a first physical implementation of a repeater scheme: the DLCZ protocol. In section we 2.4 introduce multiplexing. In Section 2.5 we discuss a modification to the DLCZ protocol that makes is more practical to implement. Finally, in Section 2.6 we discuss physical implementations of the components that are used in the protocol.

2.1. Repeaters

2.1.1. Why repeaters?

The quantum internet aims to distribute quantum information over long distances. In order to do so, carriers of quantum information that can be sent over long distances are required. The best candidates for those carriers are, like with the classical internet, photons sent over an optical fiber. When sending photons over an optical fiber they can get lost. The probability to lose a photon scales exponentially with the distance, L, covered by the photon [6]. The transmittance, η_t, is given by

$$\eta_t(L) = 10^{-\alpha L/10}. \tag{2.1}$$

η_t denotes the probability of successfully transmitting a photon and α is the attenuation, which is a parameter of the optical fiber.
A typical value for the attenuation of a commercial optical fiber recorded at telecom wavelength (1550 nm) is 0.2 dB/km [19]. Consequently, this means that when sending a message from Amsterdam to Paris (430 km), on average approximately $4 \cdot 10^8$ photons have to be sent for one to be transmitted successfully. Practically, this makes communication over a direct optical fiber at large distances impossible. Classically, this issue is solved by amplifying the signal at midpoint stations distributed along the to be bridged distance. For quantum information, however, the no-cloning theorem [4] forbids copying a quantum state rendering amplifying quantum information impossible. For the quantum internet another protocol is thus needed.

2.1.2. General repeater protocol

This is where repeater protocols enter the picture. Originally proposed by Briegel et al. (1998) in [6], repeaters make use of entanglement to split the distance to be bridged into smaller segments. Entanglement is a property of quantum mechanics where two quantum systems share a single state. This has the counter-intuitive result that even though all information is known about the combined system, nothing is known about the individual particles [2, 3, 20]. Once entanglement between two distant nodes has been established, different applications like Quantum Key Distribution (QKD) [21, 22], Blind Quantum Computing (BQC) [23, 24] or quantum teleportation [25, 26] can be performed. The main goal of the quantum internet is therefore the ability to generate entanglement between remote nodes, enabling them to execute quantum applications.
A quantum repeater scheme hence aims to generate entanglement between two distant nodes. A schematic overview of the workings of a repeater scheme is in Figure 2.1. In the scheme, the

communication channel is cut into $N = 2^n$ different segments called elementary links. n is called the nesting level. In a general repeater scheme, first entanglement is generated between all elementary links. After entanglement has been generated between all nearest neighbour nodes, the entanglement gets swapped until the two end nodes are entangled. Three requirements for a quantum repeater are identified [27]

1. The ability to establish entanglement between the elementary links in a heralded way. This means that even though entanglement generation between the two nodes can be probabilistic, success has to be heralded when entanglement is actually generated. This is essential as the repeater protocol needs to know when entanglement is successfully established. There is a variety of methods to generate entanglement in a heralded fashion [28]. Heralded entanglement generation in atomic-ensemble-based quantum repeaters is discussed in Section 2.3.2. We emphasise that this requirement entails the need for back-and-forth communication between the nodes of the repeater.

2. The ability to swap entanglement. Concretely this means that if A and B are entangled, and C and D are entangled, after performing the entanglement swap, A and D are entangled. The concept of such an entanglement swap is validated in [29]. The physical implementation of an entanglement swap in atomic-ensemble-based quantum repeaters is discussed in Section 2.3.3.

3. The ability to store entanglement once it has been generated. This is necessary as once entanglement has been generated in one of the links, the repeater protocol can only proceed to entanglement swapping once all links have successfully generated entanglement. Therefore, unless entanglement is always generated simultaneously, a repeater scheme needs a so called quantum memory [30]. Concretely, a quantum memory enables the storage of a quantum state over a period of time.

The repeater protocol described above is known as a first generation repeater [31]. First generation repeater protocols sometimes make use of entanglement purification, which is the process of turning a number of generated instances of end-to-end entanglement into a single instance of better (i.e. less noisy) entanglement [32, 33, 34, 35, 36].

A second generation repeater has the additional ability to perform quantum error correction to correct errors in the protocol [31]. In simple terms, quantum error correction accomplishes its task by encoding a single logical qubit using multiple physical qubits. By employing error-detection and error-correcting codes [37, 38, 39, 40] the logical qubit can be decoded, decreasing the likelihood of errors in the sent quantum information. Propositions for such second generation quantum repeaters include [41], [42], and [43].

A third generation repeater relies solely on quantum error correction to correct all losses and errors in the protocol [31]. As a result, this removes the requirement on a repeater to establish entanglement in a heralded fashion and would require only one-way communication. This increases possible communication rates drastically. Propositions for such second generation quantum repeaters include [44], [45], [46], and [47].

In this thesis we focus on a first generation repeater protocol that does not make use of entanglement purification.

2.2. Quantum Key Distribution

Now that the general working of a repeater scheme has been outlined it is imperative to discuss metrics that can be used to assess the performance of a repeater scheme. A good way to evaluate performance of hardware is to look at how well it executes desired applications. For this reason we introduce the application Quantum Key Distribution (QKD) in the form of the BB84 protocol, originally proposed by C.H. Benett and G. Bassard in [21]. We make use of the entanglement based version of this protocol introduced in [22]. This protocol is a good fit as it does not require that the entangled end nodes are processing nodes (i.e. have the ability to perform quantum gates on the qubits they have stored in their memories), which atomic-ensemble-based nodes researched in this thesis are not [27, 28]. We use the Secret Key Rate (SKR) that arises from this protocol as a general measure of the performance of a repeater scheme throughout this thesis.
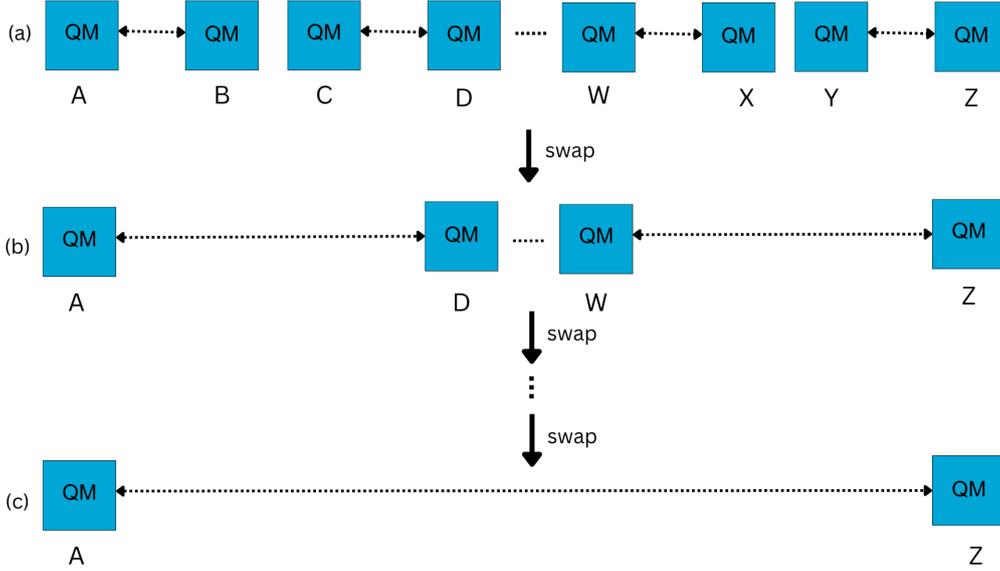
Figure 2.1: Schematic depiction of the working of a repeater scheme. **a)** entanglement is created between the elementary links. Consequently, this means that all nearest neighbour nodes are entangled. **b)** Entanglement is swapped between the neighbouring links. **c)** Iterations of entanglement swaps take place. After the last entanglement swap the two end nodes are entangled. QM = Quantum Memory.

2.2.1. The entanglement-based BB84 protocol

As the aim of this thesis is to analyse the hardware performance of a repeater scheme, we present an entanglement-based version of the BB84 protocol in the absence of an eavesdropper in this section. For a more detailed discussion on the BB84 protocol, and its security when an eavesdropper is involved the reader is referred to [20], [21], [22], and [48]. Say Alice (A) and Bob (B) want to generate a secret key. The protocol used to assess the performance of a repeater scheme throughout this report works as follows for a single bit of secure key:

1. An entangled state is distributed between A and B.
2. A and B measure their respective qubits in either the Z or the X basis at random.
3. If bases A and B measured in are not the same, the resulting measurement result is discarded.
4. If the bases A and B measured in are the same, the measurement outcomes are either correlated or anti-correlated as A and B shared an entangled state, hence generating a bit of secure key.

2.2.2. Secret Key Rate

The speed of light imposes a ceiling on the rate at which the protocol outlined above can be executed, because each round of communication by A and B takes a finite amount of time due to the finite nature of the speed of light. Furthermore, hardware imperfections can also effect this rate, as the signal can be lost somewhere in the protocol, further increasing the average time it takes to get a successful round. The rate at which successful rounds occur is defined as the success rate, R_{succ}. Hardware imperfections might also lead to false successes. The ratio of false successes is defined as the Quantum Bit Error Rate (QBER). The QBER is computed as the fraction of measurement outcomes that should be (anti-)correlated but are not. Note that the QBER is not necessarily the same in the Z and X basis. It differs for example when distinct kinds of hardware are needed to perform measurement in the Z and X basis, involving different errors. All this leads to the SKR, R_{SK},

$$R_{SK} = R_{succ} \cdot \mathsf{max}(0, 1 - h(Q_Z) - h(Q_X)). \tag{2.2}$$

Here Q_Z and Q_X are the QBER in the Z and X basis respectively and h is the binary entropy function defined by

$$h(p) = -p\log_2(p) - (1-p)\log_2(1-p).$$

(2.3)

2.2.3. Error analysis of QKD

If n bits are generated, with bit i being generated at time t_i, the mean generation time, $\bar{t}$, time is simply given by

$$\bar{t} = \frac{1}{n}\sum_{i=1}^{n} t_i.$$

(2.4)

We compute the error in this quantity by the standard error [49]

$$\epsilon_x = \sqrt{\frac{\sum_{i=1}^{n}(x_i - \bar{x})^2}{n}}.$$

(2.5)

From this, the error in the success rate is given by

$$\epsilon_{R_{succ}} = \frac{\epsilon_t}{\bar{t}^2}.$$

(2.6)

Furthermore, using Equation 2.2 the error in the SKR can be seen to be [50]

$$\epsilon_{SKR} = R_{succ}\epsilon_{R_{succ}} + [1 + \text{logit}_2(Q_z)]\epsilon_{Q_z} + [1 + \text{logit}_2(Q_x)]\epsilon_{Q_x}.$$

(2.7)

Here ϵ_{Q_z} and ϵ_{Q_x} are the QBER for the Z and X basis respectively, and are also computed by the standard error, and $\text{logit}_2(p)$ is the logit function defined as

$$\text{logit}_2(p) = \log_2\left(\frac{p}{1-p}\right).$$

(2.8)

2.3. Atomic-ensembles: the DLCZ protocol

In this section we discuss the physical workings of the most simple form of an atomic-ensemble-based repeater scheme: the Duan, Lukin, Cirac, Zoller (DLCZ) protocol originally proposed in [51]. Despite its simplicity, it fulfils all the requirements discussed in Section 2.1.2.

2.3.1. Information storage

The DLCZ protocol is based on a collection of N_A three-level atoms. A graphical representation of the energy levels and the read and write process is in Figure 2.2. The energy levels of each atom are denoted as two ground states $|g_1\rangle$ and $|g_2\rangle$, with the energy of $|g_2\rangle$ being slightly higher than that of $|g_1\rangle$, and an excited state $|e\rangle$, which has an energy much higher than both the ground states. The initial state of the atomic ensemble is defined as all atoms being in $|g_1\rangle$. This state is defined as the logical 0 of the qubit [27, 51]

$$|0\rangle = \prod_{k=1}^{N_A} |g_1\rangle_k.$$

(2.9)

To excite the $|0\rangle$ state to the logical one state $|1\rangle$ the write pulse is used. The write pulse is a laser pulse that is off resonant with the three level atom. With low probability the write pulse will excite a single atom in the ensemble from the $|g_1\rangle$ state to the $|e\rangle$ state. Note that although the probability to excite a single atom is small, the big number of atoms inside the ensemble makes the probability to excite an atom more significant. Once in the $|e\rangle$ state the system will spontaneously decay to the $|g_2\rangle$ state, in the process emitting a photon known in literature as the Stokes photon. Detection of the Stokes photon at a large enough distance to ensure that all information about where in the atomic-ensemble the Stokes photon originates from is lost, projects the state of the atomic-ensemble
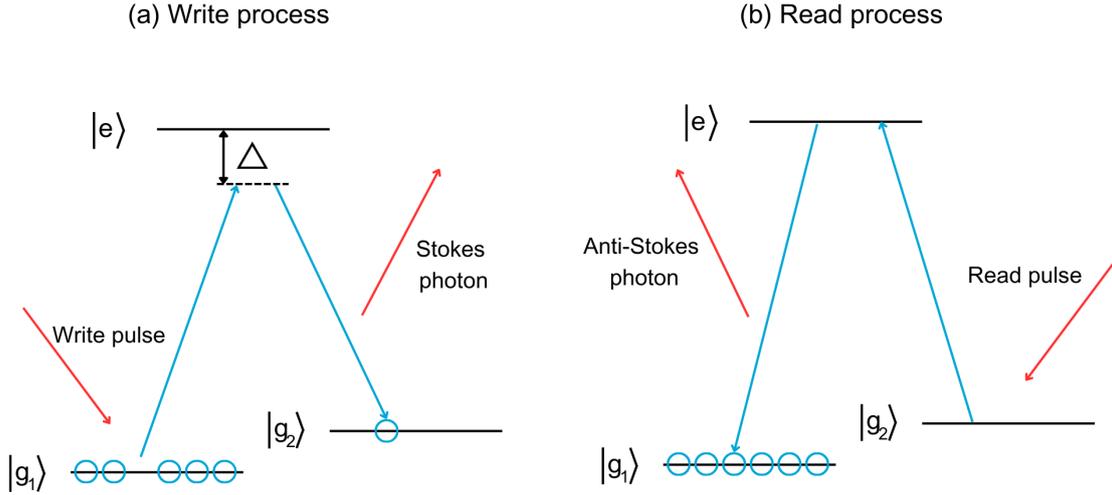
Figure 2.2: Schematic depiction of the energy levels of an atom as proposed in the DLCZ scheme. **a)** In the write process an off resonant write pulse induces a transition from $|g_1\rangle$ to $|e\rangle$. The $|e\rangle$ state then spontaneously decays to $|g_2\rangle$, emitting a Stokes photon in the process. This state, where there is one atom in $|g_2\rangle$, represents the logical $|1\rangle$ of the stored qubit. The initial state, where all atoms are in $|g_1\rangle$, represents the logical $|0\rangle$ of the stored qubit. **b)** In the read process a resonant read pulse induces a transition form the $|g_2\rangle$ to the $|e\rangle$ state which then spontaneously decays back to the $|g_1\rangle$ state, emitting an Anti-Stokes photon in the process.

into a coherent superposition of all the states where there is one atom in the $|g_2\rangle$ state and all other $N_A - 1$ atoms are in the $|g_1\rangle$ state. This state is defined as the logical 1 of the qubit [27, 51]

$$|1\rangle = \frac{1}{\sqrt{N_A}} \sum_{k=1}^{N_A} e^{i(\mathbf{k_w}-\mathbf{k_s})\mathbf{x_k}} |g_1\rangle_1 |g_1\rangle_2 \dots |g_2\rangle_k \dots |g_1\rangle_{N_A-1} |g_1\rangle_{N_A} . \tag{2.10}$$

Here $\mathbf{k_w}$ and $\mathbf{k_s}$ are the wavevectors of the write pulse and Stokes photon respectively, and $\mathbf{x_k}$ is the position of the k-th atom in the ensemble at the time of the write process.
At this point it is worth noting that exciting more than one atom, and therefore emitting more than one Stokes photons, induces an error in the process of writing the qubit to the logical 1 state. This is the reason excitation from the $|g_1\rangle$ to the $|e\rangle$ state has to happen with low probability and hence an off-resonant laser pulse is used.
The advantage of the protocol is that the qubits can be read out very efficiently. In the read process the atom in the $|g_2\rangle$ state is excited to the $|e\rangle$ state using a resonant laser pulse. The atom in the $|e\rangle$ state then spontaneously decays back to the $|g_1\rangle$ state, in the process emitting an Anti-Stokes photon. The atomic ensemble is now back in the $|0\rangle$ state, having accumulated an additional phase given by [27, 51]

$$\sum_{k=1}^{N_A} e^{i(\mathbf{k_w}-\mathbf{k_s})\mathbf{x_k}} e^{i(\mathbf{k_r}-\mathbf{k_{AS}})\mathbf{x_k'}}. \tag{2.11}$$

Here $\mathbf{k_r}$ and $\mathbf{k_{AS}}$ are the wavevectors of the read pulse and Stokes photon respectively, and $\mathbf{x_k'}$ is the position of the k-th atom in the ensemble at the time of readout. If $\mathbf{x_k} = \mathbf{x_k'}$, $\forall k$ (i.e. the atoms in the ensemble are not moving), constructive interference happens whenever $\mathbf{k_S} + \mathbf{k_{AS}} = \mathbf{k_w} + \mathbf{k_r}$. This means that if N_A is sufficiently large emission of the Anti-Stokes photon in the direction $\mathbf{k_w} + \mathbf{k_r} - \mathbf{k_S}$ dominates emission in other directions, allowing for very efficient collection of the Anti-Stokes photon. If $\mathbf{x_k} \neq \mathbf{x_k'}$, $\forall k$, constructive interference is still possible if $\mathbf{k_S} = \mathbf{k_w}$ and $\mathbf{k_{AS}} = \mathbf{k_r}$ [27].

2.3.2. Heralded entanglement generation

In the DLCZ protocol entanglement is generated in the elementary links by deleting all which-way information. This method to generate entanglement was first proposed in [52] and [53]. A schematic representation of how this is done is in Figure 2.3. The entanglement is generated between two atomic-ensembles (denoted by A and B), as described in Section 2.3.1. The Stokes photons that each of the ensembles probabilistically emits are collected in optical fibres, which both lead to the same heralding station. The heralding station consists of a 50:50 beam splitter and two detectors, and is responsible for heralding success upon entanglement generation.

The ensembles are prepared such that a Stokes photon is emitted with probability p. The state of the ensembles is given by [27, 51]

$$|\psi_{a,b}\rangle = \left(1 + \sqrt{p}\left(\hat{s}_a^\dagger \hat{a}^\dagger e^{i\phi_a} + \hat{s}_b^\dagger \hat{b}^\dagger e^{i\phi_b}\right) + \mathcal{O}(p)\right)|0\rangle. \tag{2.12}$$

Here $\hat{s}_a^\dagger$ and $\hat{s}_b^\dagger$ are the bosonic creation operators for an atomic excitation in A and B respectively. $\hat{a}^\dagger$ and $\hat{b}^\dagger$ are the bosonic creation operators for a Stokes photon in the optical fibers of A and B respectively. ϕ_a and ϕ_b are the phases of the write laser at A and B respectively. Finally, $\mathcal{O}(p)$ is the aforementioned error due to multi-photon emission.

At the heralding station the modes of the optical fibers are sent into a 50:50 beam splitter. The exact mechanics of a beam splitter are discussed in Section 2.6.3. However, what is important at this point is that when a single photon enters a 50:50 beam splitter, it has a 50% probability to come out of either end. This implies that when a single click in one of the detectors of the beam splitter is observed, all information on which of the ensembles the Stokes photon originated from is lost, hence entangling the ensembles. The shared state of the ensembles after this measurement is given by [27]

$$|\psi_{ab}\rangle = \frac{1}{\sqrt{2}}\left(\hat{s}_a^\dagger e^{i\phi_a + \xi_a} \pm \hat{s}_b^\dagger e^{i\phi_b + \xi_b}\right)|00\rangle. \tag{2.13}$$

Using the definitions from Equation 2.9 and 2.10 we recognise $|\psi_{ab}\rangle = \frac{1}{\sqrt{2}}(|10\rangle_{AB} \pm |01\rangle_{AB} \, e^{i\theta_{ab}})$ where, $\theta_{ab} = \phi_b - \phi_a + \xi_a - \xi_b$, which is a maximally entangled state.

It is noteworthy to observe that this process can also be seen as an entanglement swap between two pairs of entangled atomic-ensembles with Stoke photons. The swap that happens at the heralding station is known in literature as an optical Bell State Measurement (BSM). The success probability of an optical BSM, p_{BSM}, cannot be higher than $\frac{1}{2}$, even with perfect hardware [54, 55, 56].

2.3.3. Entanglement swapping

Now that it is clear how entanglement is generated in a heralded fashion and how this entanglement is stored in the DLCZ protocol, the only of the requirements on a quantum repeater introduced in Section 2.1.2 left to fulfil is the ability to perform an entanglement swap. Figure 2.4 depicts how this is done in the DLCZ protocol. The entanglement swap is performed between two entangled links (denoted by AB and CD) which share the state $|\psi_{ab}\rangle \otimes |\psi_{cd}\rangle$, where both $|\psi_{ab}\rangle$ and $|\psi_{cd}\rangle$ are in the form of Equation 2.13. The atomic excitations on nodes B and C are read out with a resonant read pulse, once more emitting an anti-Stokes photon in case of an excitation. The modes of the anti-Stokes photons are collected in the arms of a beam splitter and another optical BSM is performed, thus erasing all which way information again. This projects the shared state to [27, 51]

$$\left|\psi_{ad}^\phi\right\rangle = \frac{1}{\sqrt{2}}(\hat{s}_a^\dagger \pm \hat{s}_d^\dagger e^{i\phi})|00\rangle. \tag{2.14}$$

Here ϕ is the complete phase shift gained in the left and right channel, i.e. $\phi = \theta_{ab} + \theta_{cd}$. This state can again be recognised as a maximally entangled state.

We remark that hardware imperfections can have an effect on this process. As such we introduce the detector efficiency, η_d, which is defined as the probability that a detector successfully detects an incident photon, the detector dark count probability, p_d, which is defined as the probability that a detector has a false detection event, and the quantum memory efficiency, η_m, which is defined as the probability that an excitation is not lost in the memory. Non perfect values of these hardware
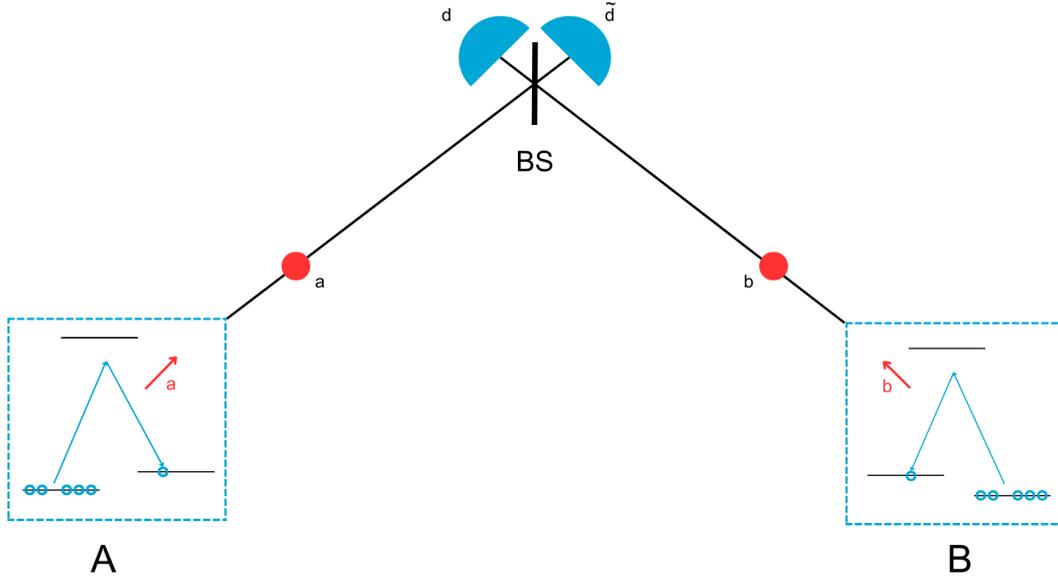
8

Figure 2.3: Schematic depiction of heralded entanglement generation in an elementary link in the DLCZ protocol between atomic-ensembles A and B. The Stokes photons that are emitted when one of the ensembles is excited probabilistically, are collected into optical fibers. The optical fibres lead to a 50:50 beam splitter. Detecting a single click in either of the detector ends, means all which-way information is deleted, entangling A and B. The entanglement encompasses a superposition between one of the atomic-ensembles containing an excited atom (i.e. the $|1\rangle$ state), and the other atomic-ensemble not containing an excited atom (i.e. the $|0\rangle$ state).

parameters result in the final state, ρ_{ad}^{ϕ}, not being a pure maximally entangled state but containing an additional vacuum component [27, 51]

$$\rho_{ad}^{\phi} = \alpha \left| \psi_{ad}^{\phi} \right\rangle\!\!\left\langle \psi_{ad}^{\phi} \right| + \beta \left| 00 \right\rangle\!\!\left\langle 00 \right|. \tag{2.15}$$

Here α and β are defined as the entangled component and the vacuum component respectively. Furthermore, hardware imperfections can result in the probability of the entanglement swap being less than p_{BSM}. The success probability of the first swap (i.e. the entanglement swap between two instances of elementary entanglement), P_1, is given by [27]

$$P_1 = \eta_m \eta_d \left(1 - \frac{\eta_m \eta_d}{2} \right). \tag{2.16}$$

2.3.4. Postselection

Now that all requirements on a quantum repeater as posed in Section 2.3.1 are met, one problem still remains; a qubit can be measured in an arbitrary basis whereas the DLCZ protocol only seems to allow measuring in a single basis. This basis is the one in which we define no atomic excitation as a logical 0, and we define one atomic excitation as a logical 1. We define this basis as the Z basis throughout this thesis.

The solution to performing measurements in other bases comes in the form of postselection. Figure 2.5 displays a postselected scheme. The setup consists of two entangled chains (denoted by $A_1 Z_1$ and $A_2 Z_2$). The two ends of the chains Λ_1 and Λ_2 ($\Lambda = A$ or Z) are optically connected to the input arms of a 50:50 beam splitter and to one of the ends Λ_2 an additional phase ϕ_Λ is added. The output ends of the beam splitter are connected to detectors D_{Λ_1} and D_{Λ_2}. Provided that the two states are established over identical channels, the vacuum coefficients and ϕ-parameters of the initial state of two chains are the same. The shared state is therefore denoted by $\rho_{A_1 Z_1}^{\phi} \otimes \rho_{A_2 Z_2}^{\phi}$. Here $\rho_{\Lambda_1 \Lambda_2}^{\phi}$ is given by Equation 2.15.
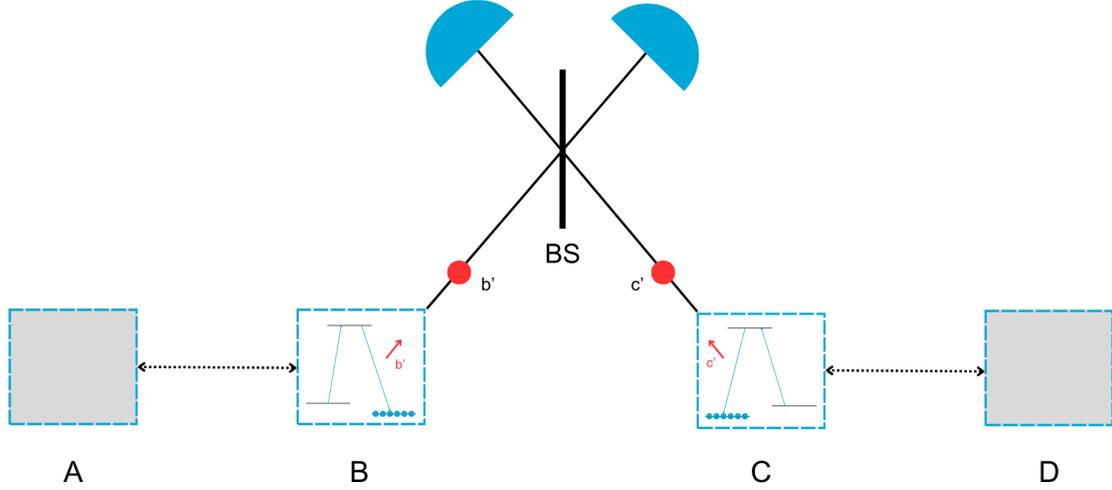
9

Figure 2.4: Schematic depiction of an entanglement swap in the DLCZ protocol. Nodes B and C are read out with a resonant read pulse. The modes of the resulting Anti-Stokes photons are collected into the arms of a beam splitter in order to delete the which-way information entangling node A and D.

The objective of the setup is to convert the created two instances of excitation-entanglement into one instance of more directly useful two-photon entanglement. This is done by reading out all nodes with a coherent read pulse. The shared state of the two links after readout but before collection into the beam splitter or adding the extra phase is then [27, 51]

$$\frac{1}{2}\left(\hat{a}_1'^\dagger + e^{i\phi}\hat{z}_1'^\dagger\right)\left(\hat{a}_2'^\dagger + e^{i\phi}\hat{z}_2'^\dagger\right)|0000\rangle_{A_1' A_2' Z_1' Z_2'}. \tag{2.17}$$

The projection of this state onto the subspace where there is one photon at each location (i.e. a photon at a_1' and at z_2' or a photon at a_2' and z_1'), heralded by measuring exactly one detector click form the set $\{D_{\Lambda_1}, D_{\Lambda_2}\}$ is given by [27, 51]

$$|\Psi_{az}\rangle = \frac{1}{\sqrt{2}}\left(\hat{a}_1'^\dagger \hat{z}_2'^\dagger + \hat{a}_2'^\dagger \hat{z}_1'^\dagger\right)|0000\rangle_{A_1' A_2' Z_1' Z_2'}. \tag{2.18}$$

This state is similar to conventional polarisation or time-bin entangled photon states and can thus be used to perform the desired measurements.

It can be seen that the combined action of the beam splitter and the phase shift is equivalent to a single-bit rotation with angle $\phi_\Lambda/2$ in the basis $\left\{|0\rangle_\Lambda \equiv \hat{\lambda}_1^\dagger |00\rangle_{\Lambda_1 \Lambda_2}, |1\rangle_\Lambda \equiv \hat{\lambda}_2^\dagger |00\rangle_{\Lambda_1 \Lambda_2}\right\}, \left(\hat{\lambda} = \hat{a}', \hat{z}'\right)$ [51, 57]. As a result, for certain phase shifts the cases where photons of the two distance node hit different detectors destructively interfere. The rate of coincidences between a pair of opposite detectors (one at each node) is proportional to [57]

$$\left\langle \hat{a}_1'^\dagger \hat{z}_2'^\dagger \right\rangle = \left\langle \hat{a}_2'^\dagger \hat{z}_1'^\dagger \right\rangle = \frac{1}{4}\left[1 - \cos(\phi_A - \phi_Z)\right]. \tag{2.19}$$

From this, it can be seen that if $\phi_A = \phi_Z$ the detector clicks should be perfectly correlated (in the absence of hardware imperfections).

Using this, definitions used throughout this thesis for X and Y measurements can be deduced. X measurements are defined as a measurement with beam splitter and no added phase ($\phi = 0$). Y measurements are defined as a measurement with beams splitter and added phase of $\pi/2$ ($\phi = \pi/2$). Now, a scheme to perform QKD for Alice and Bob can be designed:

1. Two atomic-ensemble-based instances of entanglement are generated using the explained method.
2. Measurements are done by both Alice and Bob using the postselection protocol, randomly choosing a basis from the set $\{X, Z\}$.
3. Measurements where Alice and Bob did not measure in the same basis are discarded.
4. If Alice and Bob measured in the same basis the detector clicks have to be correlated. A click in detector D_{Λ_1} is registered as a logical 0 in the secret key, A click in detector D_{Λ_2} is registered as a logical 1 in the secret key.

Hardware imperfections also lead to a non unit probability with which the postselection succeeds, P_{ps}. At nesting level n, the probability to successfully postselect is given by [27]

$$P_{ps} = \frac{\alpha_n^2 \eta_m^2 \eta_d^2}{2}.$$

(2.20)

2.4. Multiplexing

One of the features that make atomic-ensembles such great candidates for a future quantum internet is their ability to be multiplexed [9, 27, 58, 59, 60]. As discussed in Section 2.3.2, heralded entanglement generation is a probabilistic process. When mulitiplexing, entanglement generation is attempted multiple times simultaneously, and the instance where success occurs is stored [27, 42]. For simplicity, we assume that only one successful event is stored. As the probability of success when multiplexing is the probability that at least one event succeeds, this probability is given by the geometric distribution [27, 61]. We define M as the number of multiplexing modes, and p_{single} as the probability that one mode succeeds. The multiplexed success probability, p_{mp}, is given by

$$p_{mp} = 1 - (1 - p_{single})^M.$$

(2.21)

There are several ways to perform multiplexing [27];

- **Spatial multiplexing**: Attempting the entanglement generation over different physical links simultaneously [61].
- **Temporal multiplexing**: Attempting the entanglement generation simultaneously in multiple time-bins. That is, say the heralding station is at a distance L and the speed of light in the optical fiber is c. It will therefore take L/c for a photon to arrive at the heralding station. With temporal multiplexing, multiple photons are sent in the interval L/c [9, 58, 62].
- **Spectral multiplexing**: Attempting the entanglement generation simultaneously at different frequencies. That is, instead of sending a single photon a pulse containing multiple frequencies is sent to the heralding station [59, 60]. This is the approach used in [59], whose proposed setup is also the inspiration for the setup simulated in this thesis.

In the lab successful setups with 26 [59], 30 [60], and 62 [9] multiplexing modes have already been demonstrated. The hardware used to yield the results in [9] holds the promise of 10^3 multiplexing modes in the near future by combining spatial, temporal, and spectral multiplexing techniques. Furthermore, by combining e.g. 10 spatial modes, 400 temporal modes and 500 spectral modes, 10^6 multiplexing could theoretically be realised [59].

2.5. Modifying the DLCZ protocol

2.5.1. Separation of source and memory

In the DLCZ protocol as discussed in Section 2.3 the Stokes photon plays a crucial role in heralded entanglement generation process. As this Stokes photon has to travel over a long distance through an optical fiber to the heralding station, its wavelength is ideally of telecom wavelength. This results in a strong constraint on the operating wavelength of the quantum memory. In practice, this constraint

a) Z basis
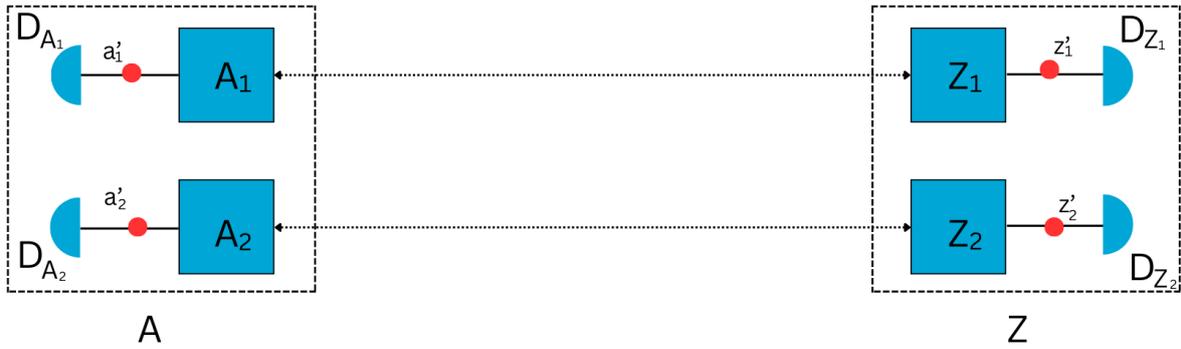
b) X basis and Y basis
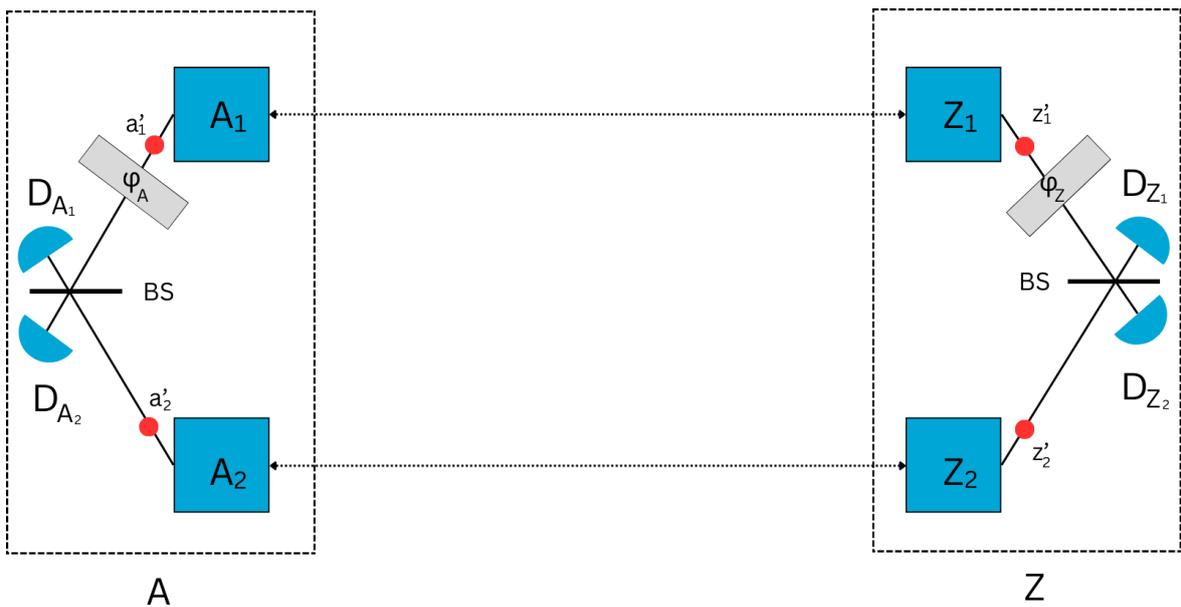
Figure 2.5: Schematic depiction of a setup including postselection in the DLCZ protocol. Two nodes are entangled between the location independently. The nodes are then read out and the Anti-Stokes photons are combined into a beam splitter. The desired subspace where the useful two-photon entanglement lives results when both locations measure one photon. **a)** Measurement in the Z basis can be done directly. **b)** Measurements in the X basis are done by interfering the photons using a 50:50 beam splitter and measurements in the Y basis are done by adding an extra phase to one of the photons and then interfering them using a 50:50 beam splitter.
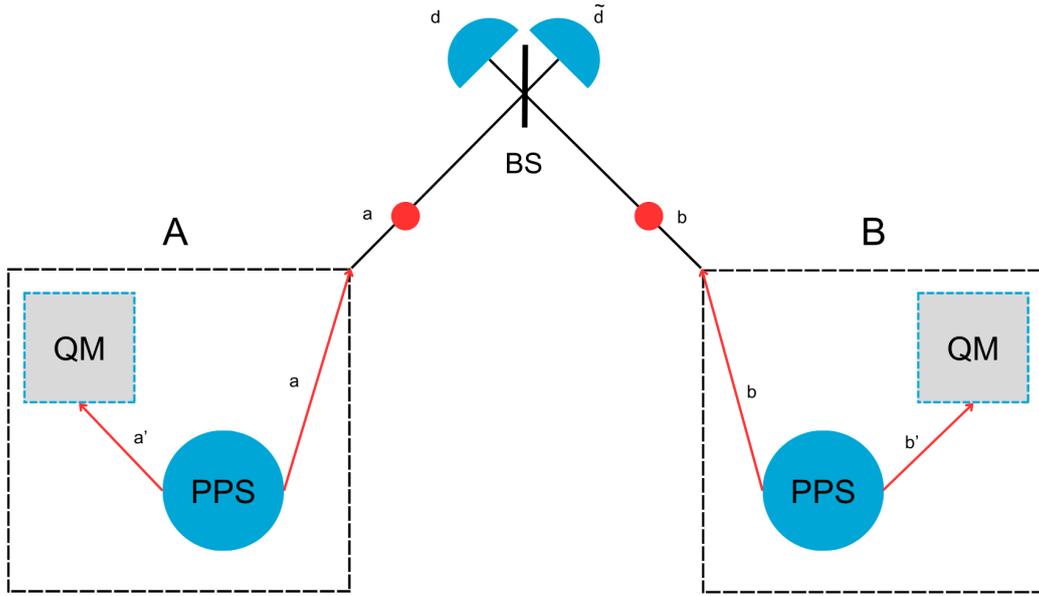
Figure 2.6: Schematic depiction of the seperation of source and memory. Each node (A and B) has a photon pair source and a quantum memory. One of the output modes of the photon pair source is connected to memory of the corresponding node and the other one is sent to a 50:50 beam splitter. A single click at one of the detectors of the beam splitter heralds entanglement between the quantum memories.

proves to be a major problem, as none of the quantum memories that have been successfully operated in the lab with sufficient performance to potentially perform the DLCZ protocol operate at telecom wavelength [59].

To tackle this issue the authors of [62] propose a different setup. This setup is depicted in Figure 2.6. In the setup, each node has both a photon pair source and a quantum memory. One output mode of the photon pair source is connected to the corresponding node's quantum memory, whereas the other one is connected to the heralding station. Note that the two photons can have different frequencies, so that the photon used for the heralding can be of telecom wavelength, whereas the one connected to the quantum memory can be in the frequency range the quantum memory operates in.

When simultaneously and coherently exciting the photon pair sources, such that each of them has a probability p to emit a pair of photons, the resulting state is [27, 62]

$$\left(1 + \sqrt{p}(\hat{a}^\dagger \hat{a}'^\dagger + \hat{b}^\dagger \hat{b}'^\dagger) + \mathcal{O}(p)\right)|0\rangle . \tag{2.22}$$

Here a (b) is the mode connected to the heralding station and a' (b') is the mode connected to the quantum memory of node A (B). Note that here the multi-photon emission, $\mathcal{O}(p)$, also plays a role. The remainder of the protocol is similar to the original DLCZ protocol. The photons used for the heralding are collected into a 50:50 beam splitter with the objective of deleting which way information. Observing a single click on one of the detectors at the output arms of the beam splitter projects the state onto a similar state to the one in Equation 2.13. The final state can be recognised as $\frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ where one of the quantum memories stores an excitation and the other one does not. Where in the original DLCZ protocol one is restricted to presence-absence encoding of the qubit (i.e. defining the $|0\rangle$ as no excitation and the $|1\rangle$ as a single excitation) the separation of source and memory gives more freedom. A pulse of two photons can be created by the photon pair source. A photon in the early time-bin is then defined as the $|0\rangle$ and one in the late time-bin is defined as the $|1\rangle$ [63, 64, 65]. This removes the necessity to postselect.

2.5.2. Double click protocol

In this section we introduce a repeater protocol with separated photon pair sources and quantum memories that make use of time-bin encoded qubits. In [59], the authors put forth this protocol. We denote this protocol as the double click protocol, and it will serve as the protocol we will use throughout this thesis to implement an atomic-ensemble-based repeater. In this section we discuss a single repeater setup, but this can naturally be extended to more repeaters. We illustrate the setup in Figure 2.7. Each end node contains a single photon pair source and quantum memory. The repeater node contains two photon pair sources, two quantum memories, and a beam splitter that can be used to perform an entanglement swap.

When attempting elementary entanglement generation, the photon pair sources probabilistically emit a photon pair in the early time-bin, e, or in the late time-bin, l [63, 64, 65]. We discuss how these probabilities emerge in Section 2.6.1. The photons are sent to the heralding stations, which is a given distance away. Note that these distances are not necessarily equal across the chain, resulting in the possibility to have asymmetric repeater setups. At the heralding station, which way information is deleted using a 50:50 beam splitter. Success is heralded when there is a single click in each of the time-bins, hence the name double click protocol. When there is a single click in each time-bin the state of the system is projected onto the state where either of the PPS emitted a photon in the early time-bin and either emitted in the late time-bin. Using the definition of the logical 0 and 1 of the time-bin encoded qubits from Section 2.5.1 one can see this is exactly the maximally entangled state. Upon success the entanglement gets stored in the quantum memories. The quantum memories thus needs the ability to store an excitation in the early and in the late time-bin. Once entanglement is established in both elementary links, the quantum memories in the repeater node are read out. The outcoming photons are then sent to the beam splitter in order to perform an entanglement swap. Once again, success is heralded when there is a single click in each of the time-bins. Upon success the quantum memories in the end nodes are entangled.

When using the time-bin encoding the necessity for postselection no longer applies and a single case of end to end entanglement is sufficient to perform measurements in all bases. We define measurement in the Z basis as directly measuring the modes of the photons in both time-bins. We define measurement in the X basis as interfering the modes of the photons before the measurement [12]. We remark on the similarity to the protocol discussed in Section 2.3.4.

2.6. Physical components

Now that the setup we will simulated is understood it is imperative to review physical implementations of components that can be used for the setup. In [59], the authors propose a setup consisting of Spontaneous Parametric Down Conversion (SPDC) crystals as photon pair sources and Atomic Frequency Combs (AFCs) as quantum memories. Furthermore, in this section we discuss beam splitters and single photon detectors, which in the context of quantum applications are typically Superconducting Nanowire Single Photon Detectors (SNSPDs).

2.6.1. Spontaneous Parametric Down Conversion

SPDC is a process in which a single photon known as the pump photon splits into two photons known as the signal and idler photon. This process is a well known example of nonlinear optics and it occurs when the pump photon is shot at a nonlinear crystal. Its working is displayed in Figure 2.8. SPDC is a phenomenon that can only be explained and understood within the framework of quantum mechanics. As such, it is very suitable for quantum applications [66] and can be used for implementation of a photon pair source in the setup discussed in Section 2.5.2.

The states resulting from the SPDC process are known to be two mode squeezed states [67, 68, 69]. The two mode squeezed states for a single idler (i) and a single signal (s) photon are given by [68]

$$|\Psi\rangle_{TMS}^{PA} = \frac{1}{\cosh(r)} \sum_{n=0}^{\infty} \tanh^n(r) |nn\rangle_{si}.$$

(2.23)

Here we define r as the squeeze parameter. The probability for the SPDC to emit n photon pairs,

14
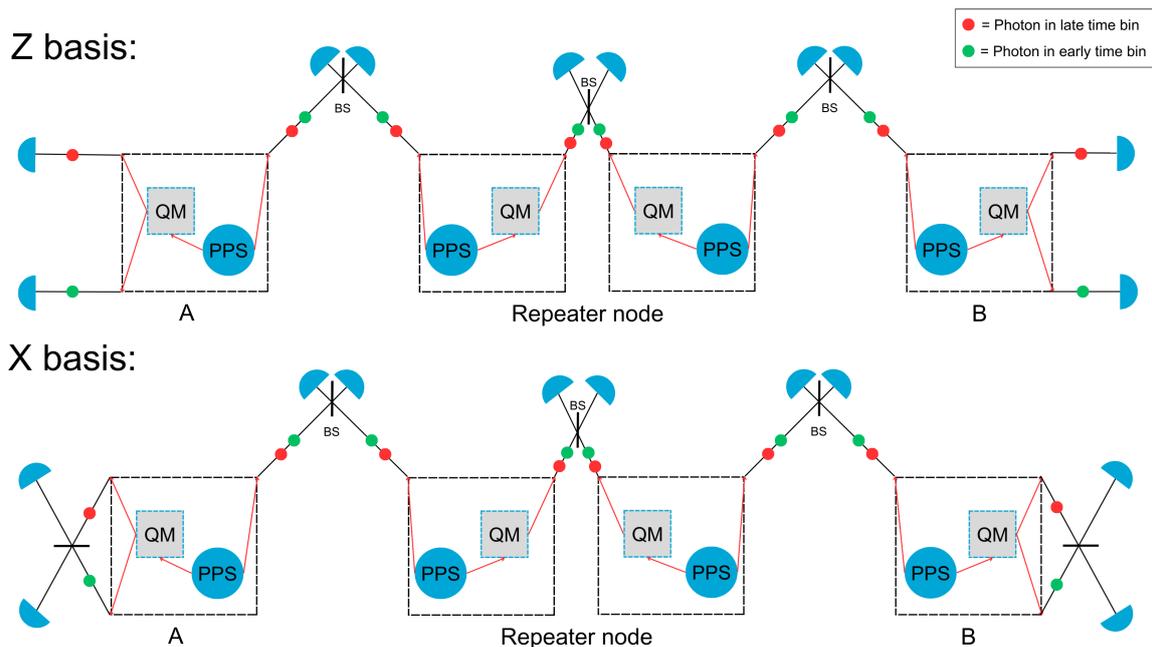
Figure 2.7: Schematic depiction of a setup for a single repeater setup of a double click protocol. Each node has a Photon Pair Source (PPS) and a Quantum Memory (QM). The PPS emits photons that correspond to a qubit encoded in two time-bins, early (red) and late (green). We define the logical $|0\rangle$ of the qubit as having a photon in the early time-bin, and the logical $|1\rangle$ of the qubit as having a photon in the late time-bin. One of the qubits emitted by each PPS is sent to the heralding station with the objective to entangle the two nodes. The other qubit gets stored in the QM. The heralding station contains a 50:50 beam splitter and two detectors. Success occurs when exactly one detection event occurs in both time-bins (i.e. two detection events happen, in separate time-bins). As a result, the QMs of the nodes are entangled. The QMs at the repeater node are then read out to perform a BSM with the aim to do an entanglement swap. The BSM once again succeeds in the case there is exactly one detection event in both of the time-bins. At the end photons can be measured by either measuring directly (Z basis) or interfering the photons in the early and late time-bin (X basis).

$p^{PA}_{SPDC}(n)$, can be directly seen to be [68, 70]

$$p^{PA}_{SPDC}(n) = \frac{\tanh^{2n}(r)}{\cosh^2(r)}.\qquad(2.24)$$

In order to utilise SPDC to execute the setup introduced in Section 2.5.2 an implementation of SPDC operating in two time-bins is required. Such an implementation, with corresponding two mode squeezed states, exists [69]. Said two mode squeezed state is given by [69]

$$|\Psi\rangle^{TB}_{TMS} = \sum_{n=0}^{\infty} \lambda_n |\Psi_n\rangle^{TB}_{TMS},\qquad(2.25)$$

$$\lambda_n = \sqrt{n+1}\frac{\tanh^n(r)}{\cosh^2(r)},\qquad(2.26)$$

$$|\Psi_n\rangle^{TB}_{TMS} = \frac{1}{\sqrt{n+1}}\sum_{m=0}^{n}(-1)^m |n-m,m;n-m,m\rangle_{se,sl;ie,il}.\qquad(2.27)$$

Here the notation of the state is $|se,sl;ie,il\rangle$ where se denotes the signal photon in the early time-bin, sl denotes the signal photon in the late time-bin, ie denotes the idler photon in the early time-bin, and il denotes the idler photon in the late time-bin. The probability to emit n photon pairs, $p^{TB}_{SPDC}(n)$, can be obtained from the probability amplitude of the state λ_n

$$p^{TB}_{SPDC}(n) = (n+1)\frac{\tanh^{2n}(r)}{\cosh^4(r)}.\qquad(2.28)$$

The intuition behind Equation 2.27 is the following; the number of photon pairs emitted is governed by the distribution specified in Equation 2.28. The photon pairs are distributed over the early and late time-bins as an equal superposition of all possible combinations.
We now introduce the mean photon number, μ. The mean photon number is related to the squeeze parameter by

$$\mu = \sinh^2(r).\qquad(2.29)$$

In terms of the mean photon number, the earlier found probabilities become [70]

$$p^{PA}_{SPDC}(n) = \frac{\mu^n}{(\mu+1)^{n+1}},\qquad(2.30)$$

$$p^{TB}_{SPDC}(n) = (n+1)\frac{\mu^n}{(\mu+1)^{n+2}}.\qquad(2.31)$$

Note that ideally $p_{SPDC}(n > 1) = 0$. If this is not the case, this will lead to a multi-photon emission error $\mathcal{O}(p)$ as seen in equations 2.12 and 2.22. Equations 2.30 and 2.31 form the basis on how we model multi-photon emission throughout this thesis.

2.6.2. Atomic Frequency Comb

An AFC is a quantum information storage device that shows resemblance to how information storage works in the original DLCZ protocol. The principles of the AFC are depicted in Figure 2.9. The device consists of an ensemble of atoms with ground states $|g\rangle$ and $|s\rangle$, and an excited state $|e\rangle$ (note the similarity to the DLCZ protocol). The states $|g\rangle$ and $|s\rangle$ are optically connected to $|e\rangle$ and the transition $|g\rangle - |e\rangle$ has a narrow homogeneous linewidth, γ_h, and a large inhomogeneous broadening, Γ [58]. Also the transition is spectrally shaped such that the atomic density function is a train of peaks in a large frequency range. We define the spacing between these peaks as Δ. For more details on the physical workings the reader is referred to [58].
A single input photon can be totally absorbed by the AFC in spite of the spectral density of the atoms being concentrated to narrow peaks. This is a consequence of the Heisenberg energy-time uncertainty relation. The time scale of the absorption will be of the order of the input pulse duration, which is very small. This results in a large uncertainty of the optical $|g\rangle - |e\rangle$ transition, which causes
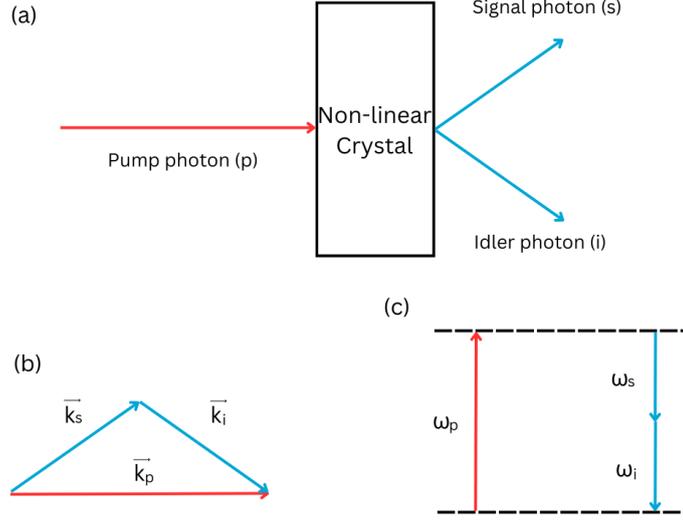
Figure 2.8: Schematic depiction of the workings of a SPDC source. **a)** Non-linear process in which the pump photon (p) is split into a signal photon (s) and an idler photon (i). **b)** Conservation of momentum. **b)** Conservation of energy.

an averaging of the sharp AFC structure to a smooth distribution which allows for uniform absorption of the photon [58].

Say the absorption occurs at time $t = 0$. The photon is then stored as a single excitation de-localised over each of the atoms that are in resonance with the photon resulting in the state of the ensemble [58]

$$|\psi\rangle = \sum_{j=1}^{N_A} c_j e^{i\delta_j t} e^{-ikz_j} |g_1...e_j...g_{N_A}\rangle. \qquad (2.32)$$

Here c_j is a coefficient that depends on the particular atom j, δ_j is the detuning of the atom with respect to the laser frequency, k is the wave vector of the photon, and z_j is the position of atom j inside the ensemble. This state can be understood as a coherent superposition of a large number of excited atomic modes as a result of a single photon. We once more remark on the similarity to the DLCZ protocol. After time $2\pi/\Delta$, re-emission of the photon spontaneously occurs [58].

Thus far, a quantum memory that re-emits the photon after a fixed time has been described. In the context of the protocol described in Section 2.5.2, this quantum memory would be useless as these protocols require storage of the quantum information for extended periods of time, until readout is requested. In order to realise this, the single collective excitation in $|e\rangle$ is stored in the ground state spin level $|s\rangle$.

This is done by applying an optical control field on the $|e\rangle - |s\rangle$ transmission. The excitation is then stored as a collective spin wave, which allows for long lived storage as spin coherence lifetimes are generally longer than optical coherence lifetimes [58, 71, 72]. A typical value for an optical coherence time is 1 ms [73], whereas current state-of-the art spin coherence lifetimes are 530 ms [72]. Furthermore, the spin wave state does not spontaneously re-emit a stored excitation. Instead, it only re-emits stored quantum information once the optical control field is applied once more, resulting in the desired on-demand readout. If the excitation has been stored for a duration T_s the photon will be re-emitted at time $T_s + 2\pi/\Delta$.

A reason to use AFC memories in the protocols is their excellent multiplexing possibilities [62]. On one hand there is the ability to perform temporal multiplexing. Say there are a given number of temporally multiplexed modes within a certain input duration. The length of the input duration is bound by the time to re-emit the photon $2\pi/\Delta$, whereas the length of a single mode is only limited by the total frequency bandwith which is proportional to $1/(N_p\Delta)$ with N_p being the number of peaks in the comb. The total number of allowed modes is thus proportional to N_p [58]. The number of temporal multiplexing modes can thus be increased by adding more peaks to the comb. On the other hand, there is the ability to perform spectral multiplexing. Spectral multiplexing requires applying adjustable frequency shifts and spectral filtering [59]. Both temporal and spectral multiplexing using AFC
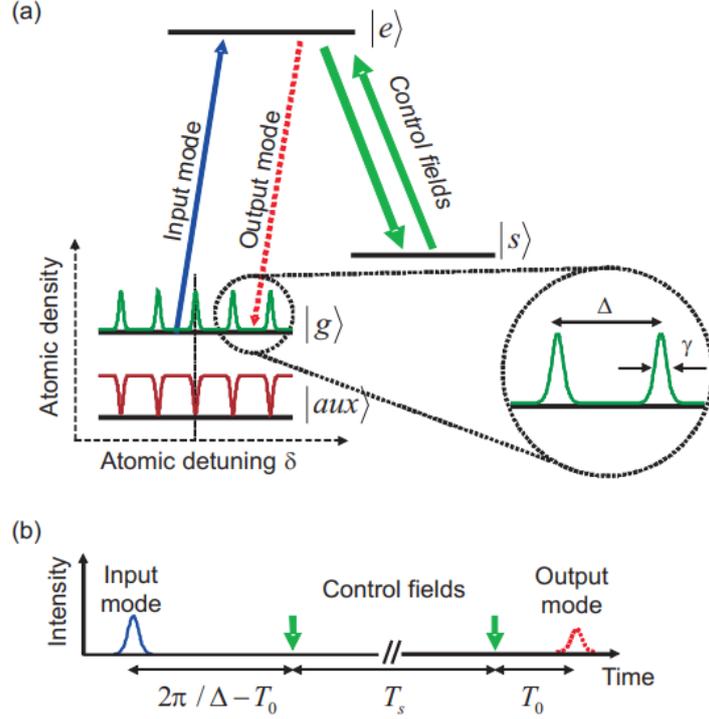
Figure 2.9: Schematic depiction of the workings of an AFC memory. **a)** A photon is stored as an excitation on the $|g\rangle - |e\rangle$ transition. The excitation will be re-emitted after time $2\pi/\Delta$. To allow for longer storage times and better decoherence times the excitation is transferred to the $|s\rangle$ state by applying a control field. The comb structure is created by transfering atoms from $|g\rangle$ to an auxiliary state $|aux\rangle$. **b)** A photon is absorbed by the AFC at time $t = 0$, after time $(2\pi/\Delta) - T_0$ the control field is applied. The excitation is then stored in the $|s\rangle$ state for time T_s. After this the memory is read out by applying another control field, causing a re-emission of the photon after time T_0. Retrieved from [58]

memories have already been successfully demonstrated in the lab [9, 59, 60].
Finally, the memory's maximum retrieval efficiency is given by [74]

$$\eta_0^{AFC} = \left(\frac{d_1}{F}\right)^2 e^{-\frac{d_1}{F}} e^{-\frac{7}{F^2}} e^{-d_0}. \tag{2.33}$$

Here d_1 denotes the optical depth (i.e. the number of atoms participating in the AFC structure), d_0 denotes the background optical depth (i.e. the number of atoms not participating in the AFC structure) and $F = \Delta/\gamma_h$ is defined as the finesse of the AFC. The first term in the efficiency describes the collective re-emission, the second term describes re-absorption of the emitted photon, the third term describes de-phasing and the last term describes the impact of background optical depth.
As mentioned before the stored quantum information also has a finite coherence time T_c. As a result of this, the probability to lose an excitation in the AFC memory is not only defined by $1 - \eta_0^{AFC}$, but also increases with time. We will further elaborate how this is modelled in Section 3.1.2.

2.6.3. Beam splitter

A graphical depiction of a beam splitter is shown in Figure 2.10. The beam splitter has two incoming photon modes associated with bosonic annihilation operators $\hat{a}$ and $\hat{b}$ and two outgoing photon modes associated with bosonic annihilation operators $\hat{c}$ and $\hat{d}$. The action of a beam splitter with transmittance $|\tau|^2$ and reflectance $|\rho|^2$ on the two incoming modes is characterised by [75, 76]

$$\begin{bmatrix} \hat{a} \\ \hat{b} \end{bmatrix} = \begin{bmatrix} \tau_1 & \rho_2 \\ \rho_1 & \tau_2 \end{bmatrix} \begin{bmatrix} \hat{c} \\ \hat{d} \end{bmatrix}. \tag{2.34}$$
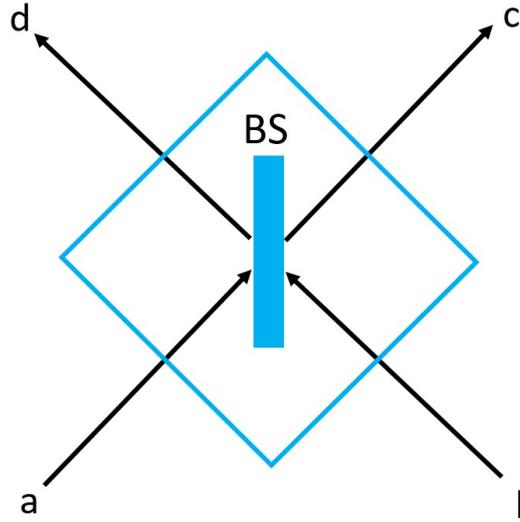
18

Figure 2.10: Schematic depiction of a beam splitter with input modes a and b and output modes c and d

Here τ_1, τ_2, ρ_1, and ρ_2 are complex parameters with $|\tau_1| = |\tau_2| = |\tau|$, $|\rho_1| = |\rho_2| = |\rho|$, and $|\tau|^2 + |\rho|^2 = 1$. In the case of a 50:50 beam splitter, which plays a crucial role in the protocol from Section 2.5.2, $|\tau|^2 = |\rho|^2 = \frac{1}{2}$. The action of such a beam splitter is characterised by [77, 78]

$$
\begin{cases}
\hat{a}^\dagger \xrightarrow{\text{50:50 beam splitter}} \frac{1}{\sqrt{2}}(\hat{c}^\dagger + \hat{d}^\dagger) \\
\hat{b}^\dagger \xrightarrow{\text{50:50 beam splitter}} \frac{1}{\sqrt{2}}(\hat{c}^\dagger - \hat{d}^\dagger)
\end{cases}
. \tag{2.35}
$$

Note the difference in signs is a requirement as any quantum operation has to be unitary. The action of a 50:50 beam splitter on a state with a photon in both the input arms $\hat{a}^\dagger \hat{b}^\dagger |0\rangle$ is thus the following

$$
\hat{a}^\dagger \hat{b}^\dagger |0\rangle \to \frac{1}{2}(\hat{c}^\dagger + \hat{d}^\dagger)(\hat{c}^\dagger - \hat{d}^\dagger)|0\rangle = \frac{1}{2}\left((\hat{c}^\dagger)^2 - (\hat{d}^\dagger)^2\right)|0\rangle. \tag{2.36}
$$

Here we use the commutation rule $[\hat{c}^\dagger, \hat{d}^\dagger] = 0$.

Equation 2.36 unveils the remarkable fact that when two photons enter the beam splitter in two different arms they always come out together. This is known as the Hong-Ou-Mandel effect and was first discovered in [79]. At the heart of the Hong-Ou-Mandel effect is that the photonic modes where the photons come out of different arms of the beam splitter interfere destructively as the photons are indistinguishable. A measure of the indistinguishability of photons is the Hong-Ou-Mandel visibility v. v is defined by [78]

$$
v = \frac{C_{max} - C_{min}}{C_{max}}. \tag{2.37}
$$

Here C_{max} is the probability that two photons entering the input arms of a 50:50 beam splitter come out of both arms when the photons are made distinguishable. C_{min} is the same probability when the photons are as indistinguishable as possible for the hardware used. Ideally, photons are perfectly indistinguishable and thus $v = 1$. Realistically however, hardware imperfections lead to non-unit visibility. This can thus lead to photons coming out of the two different arms of the beam splitter, regardless of the Hong-Ou-Mandel effect.

2.6.4. Superconducting Nanowire Single Photon Detector

Devices that can detect single photons usually work by the principle that they convert a single incoming photon to a readable electric pulse. Current state-of-the art devices that realise this are SPNSPDs. The working of a SPNSPD is depicted in Figure 2.11.

SPNSPDs operate by maintaining the wires well below the critical temperature and just below the critical current density at which super conduction is destroyed. When a photon incides on the wire this

19
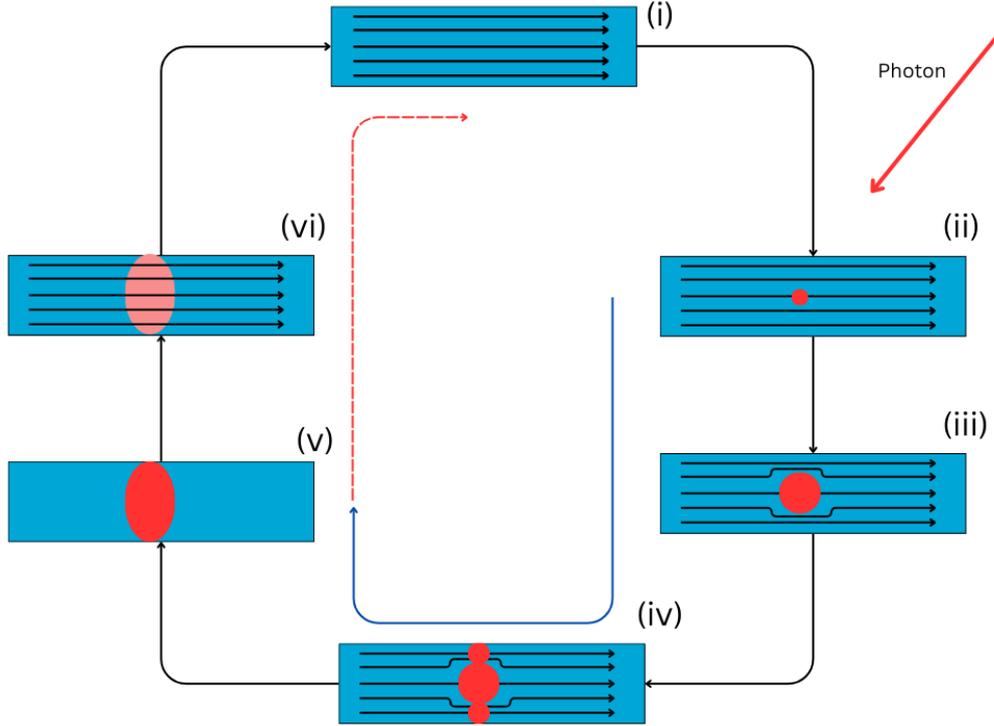
Figure 2.11: Schematic depiction of the working of a Superconducting Nanowire Single Photon Detector. **(i)** A supercurrent flows through the nanowire. **(ii)** An incident photon disturbs the superconduction forming a hotspot. **(iii)** The current is forced to flow around the hotspot. **(iv)** The current density around the hotspot is driven above the critical current above which superconduction no longer occurs. **(v)** The resistance across the wire increases form 0 to a finite value resulting in a measurable voltage peak across the wire **(vi)** The nanowire recovers returning to its original state. The blue arrow denotes the time it takes from incidence of the photon to measurement signal. The red (dashed) line denotes the time it takes for the SPNSPD to recover.

disturbs the Cooper pairs in a certain area, forming a hotspot that is not large enough to span the width of the nanowire. As a result, the current is forced to flow around the hotspot. This drives the current density towards the critical current density across the width of the wire. The resulting sudden increase in resistance from 0 to a finite value leads to a strong peaked measurable voltage peak across the wire [80].

The efficiency of a SPNSPD can be divided into 3 parts [80]

$$\eta_{SPNSPD} = \eta_{coupling} \cdot \eta_{absorption} \cdot \eta_{registering}. \tag{2.38}$$

$\eta_{coupling}$ denotes the efficiency with which a photon is collected from the fiber and is correctly aimed at the nanowire. $\eta_{absorption}$ denotes the efficiency with which the incident photon is absorbed into the nanowire as opposed to being reflected or being transmitted through the wire. $\eta_{registering}$ denotes the efficiency with which the process that leads from absorbing a photon to registering a click happens. $\eta_{registering}$ can for example be improved by making the nanowire thinner.

Photons in the environment and noise in electrical components can potentially mimic the output signal that denotes a click. This results in another imperfection of SPNSPD in the form of a dark count probability (p_{dark}) [80].

<div style="text-align: right">3</div>

Methodology

In this chapter we introduce the methodology that is used to optimise the hardware parameters of the physical components of the protocol in Section 2.5.2. In Section 3.1 we introduce how the simulations are done. In Section 3.2 we introduce how simulations are used to evaluate the performance of the setup with imperfect hardware. Here we introduce the concepts of absolute minimal hardware requirements and minimal hardware requirements. Furthermore, we define the task of finding those as an optimisation problem. Finally, in Section 3.3 we introduce the methodology that is used to solve the aforementioned optimisation problem.

3.1. Simulation methodology

3.1.1. Simulations

Netsquid
The main aim of this thesis is to perform optimisation of hardware parameters of an atomic-ensemble-based single repeater chain setup. To do this we use a numerical method to evaluate the performance of the setup in the form of. Hence, it is crucial to have a simulator that can execute simulations of such setups. For this, we utilise Netsquid. Netsquid is a "discrete-event based platform for simulating all aspects of quantum networks and modular quantum computing systems", introduced in [14]. Netsquid simulations are generally performed in three steps [14]. The first step is to model the network using components based on physical models. In this step, we define a combination of these components that perform a certain operation together at one location in the network as a node. In the second step, protocols are assigned to network nodes that make them perform the intended operations. The details of the components and protocols used for atomic-ensemble-based simulations are described in Section 3.1.2. The final step is to perform a simulation for the network for a given number of runs, n, to collect statistics with which the performance of the network can be assessed.

Netsquid-AE
The components used for simulation of atomic-ensemble-based repeater chains are organised in the code snippet Netsquid-AE [15]. Netsquid-AE contains code for components based on physical models that can be used to make both end nodes and repeater nodes. Among this are a model of a photon pair source, a model of a quantum memory, a model of a detector to perform a measurement in the QKD protocol, and a physical model of a detector to perform a BSM. Furthermore, Netsquid-AE contains code for a heralded connection between its nodes. Again, how all physical components are modelled is described in Section 3.1.2. The components in Netsquid-AE have been developed and verified mostly by the authors of [12] and [13].

NLblueprint
NLblueprint is a code snippet containing tools to run realistic quantum network simulations with the goal to analyse the performance of different design aspects of a quantum internet. It contains, among other things, code for protocols that generate entanglement between nodes, protocols that make end nodes execute a QKD protocol, and protocols that keep track of entanglement within the chain. Furthermore, it contains scripts that perform the simulations, collect data from them, and process this

into analysable data. To do this, the script uses the NetSquid-NetConf [81] snippet to generate physical networks that Netsquid can simulate, and the NetSquid-SimulationTools [82] snippet to perform data analysis. NLblueprint has already yielded a lot of interesting research such as [10], [11], [83], and [84]. Here the authors perform optimisation of various aspects of repeater chains that are as realistic as possible using numerical methods. It would be valuable to include Netsquid-AE simulations in NLblueprint in order to enable the possibility to have atomic-ensemble-based repeater chains in similar research. This is important as in the vision of QIA atomic-ensemble-based repeater chains are used to distribute the entanglement in the longest length scale. One of the results of this thesis is to have Netsquid-AE simulations using NLblueprint.

3.1.2. Components and protocols

Photon pair source
The first component we discuss is the photon pair source. The component is a physical model of an SPDC source as discussed in Section 2.6.1. Both presence-absence or time-bin encoding are supported. The working principle of the source is the following: the source has a specified probability to emit a given number of photon pairs. For each emission event the number of emitted photons is thus sampled using these probabilities. Multi-photon emission of up to three photons is modelled. The choice to model three photons is made by the author of [12], whom found this was the best trade-off between accuracy and required compute power. We found that opting for this was a favourable decision. Generally, for a repeater protocol to be feasible, the likelihood of emitting three photons should already be extremely low . This implies that the likelihood of emitting four photons should be smaller still. Numerical benefits reaped from this would thus be minimal. The required compute power, however, would increase exponentially.
The probability to emit a number of photons can be specified as a list $\{p(0), p(1), p(2), p(3)\}$, where $\sum_{n=0}^{3} p(n) = 1$. In the presence-absence encoding each entry of this list simply denotes the probability to emit the given number of photons, whereas for the time-bin encoding each entry of this list denotes the probability to emit that number of photon pairs distributed over the time-bins with equal probability. Alternatively, the mean photon number, μ, can be specified in which case the probabilities will be computed as per Equation 2.30 or Equation 2.31. In this case thus a more realistic SPDC source is modelled.
Netsquid does not natively support multi-photon states such as the two mode squeezed states. Therefore, an encoding is used. The photon state is encoded as two Netsquid qubits. $|00\rangle$ encodes a mode with no photons, $|01\rangle$ encodes a mode with 1 photon, $|10\rangle$ encodes a mode with 2 photons, and $|11\rangle$ encodes a mode with 3 photons. Using this encoding, the two mode squeezed states of Equations 2.23 and 2.25 can be modelled. For the presence-absence encoding the output state of the photon pair source is modelled as [12]

$$|\Psi\rangle_{TMS,Netsquid}^{PA} = \sqrt{p(0)}\,|00,00\rangle_{L,R} + \sqrt{p(1)}\,|01,01\rangle_{L,R} + \sqrt{p(2)}\,|10,10\rangle_{L,R} + \sqrt{p(3)}\,|11,11\rangle_{L,R}. \quad (3.1)$$

Where L denotes a photon to the left and R denotes a photon to the right. To realise a repeater protocol, such as investigated throughout this thesis, one of the photons (either L or R) is usually stored in a quantum memory. The other photon is then used for the heralded entanglement generation. Note that in total 4 Netsquid qubits are used to model the state.
As the protocol from Section 2.5.2 makes use of time-bin-encoded qubits, it is essential for the photon pair source to support a time-bin-encoded implementation. In the time-bin encoding, the output state

of the photon pair source is modelled as [12]

$$|\Psi\rangle_{TMS,Netsquid}^{TB} = \sqrt{p(0)}\,|00,00;00,00\rangle_{Le,Ll;Re,Rl} +$$

$$\sqrt{\frac{p(1)}{2}}\left(|01,00;01,00\rangle_{Le,Ll;Re,Rl} + |00,01;00,01\rangle_{Le,Ll;Re,Rl}\right) +$$

$$\sqrt{\frac{p(2)}{3}}\left(|10,00;10,00\rangle_{Le,Ll;Re,Rl} - |01,01;01,01\rangle_{Le,Ll;Re,Rl} + |00,10;00,10\rangle_{Le,Ll;Re,Rl}\right) +$$

$$\frac{\sqrt{p(3)}}{2}\left(|11,00;11,00\rangle_{Le,Ll;Re,Rl} - |10,01;10,01\rangle_{Le,Ll;Re,Rl} +\right.$$

$$\left.|01,10;01,10\rangle_{Le,Ll;Re,Rl} - |00,11;00,11\rangle_{Le,Ll;Re,Rl}\right). \quad (3.2)$$

Here Le denotes a photon to the left in the early time-bin, Ll denotes a photon to the left in the late time-bin, Re denotes a photon to the right in the early time-bin, and Rl denotes a photon to the right in the late time-bin. Note that in total 8 Netsquid qubits are used to model the state.

Amplitude damping model
Netsquid-AE models photon loss both in the quantum memories and in the fiber. The quantum memory component is a physical model inspired by the discussion on atomic frequency combs in Section 2.6.2. The parameters that affect photon loss in this model are the memory efficiency, $\eta_{m,0}$, and the coherence time T_c. We model the probability of losing an excitation that has been in the memory for a time t as [12]

$$\gamma = 1 - \eta_{m,0}e^{-t/T_c}. \quad (3.3)$$

We model the probability of losing a photon in the fibre as

$$\gamma = 1 - \eta_t. \quad (3.4)$$

Here the photon transmittance, η_t, is given by Equation 2.1.
The amplitude damping model is used to model photon loss from these probabilities. It describes evolution of the density matrix of the system ρ to ρ' over time t as a linear transformation

$$\rho' = \sum_k A_k \rho A_k^\dagger. \quad (3.5)$$

Here A_k are positive linear operators known as Kraus operators, and in the Hilbert space of the system alone are given by [85]

$$A_k = \sum_{n>k} \sqrt{\binom{n}{k}}\sqrt{(1-\gamma)^{n-k}\gamma^k}\,|n-k\rangle\langle n|. \quad (3.6)$$

Generally, k describes the number of photons lost and n describes the number of photons initially in the system. As in the simulations the highest number of photons considered is 3 it suffices to sum k from 0 to 3 and consider no n greater than 3.

Detectors
For the entanglement swap, the QKD measurements, and the heralded entanglement creation measurements ought to be done. All detector components in Netsquid-AE that are considered throughout this thesis perform their measurements on two photons simultaneously. The detector component that performs the QKD measurement measures both photons directly if it measures in the Z basis. The detector component that performs the BSM and the detector component that performs the QKD measurement, given that it measures in the X basis, interfere the two incoming photons before detection. This interference is modelled by the mechanics of a 50:50 beam splitter. The detectors are furthermore assumed to have a flat frequency response, meaning they show the same behaviour for photons of all frequencies, and can be either number resolving (i.e. the ability to

distinguish between number of photons incident) or non number resolving. Furthermore, detectors are assumed to have no device recovery time after a measurement and to have no timing jitter, meaning that their behaviour does not vary over time.

At this component the hardware parameters of interest that are modelled are thus the detector efficiency, η_d, detector dark counts, p_d, and the Hong-Ou-Mandel visibility, v. When measuring photons directly the behaviour of the detectors is trivial. With probability p_d one detection event is added to the measurement outcome and with probability $1 - \eta_d$ there is no detection event. Note that in the case of non number resolving detectors, accordingly there is no detection event when n photons incide with probability $1 - \eta_d$. In the case of a number resolving detector, the probability to have one less detection event is $1 - \eta_d$, meaning the probability to get no detection event is $(1 - \eta_d)^n$. As the photons are not interfered the visibility v does not have an effect here.

When interfering the photons before detection the situation becomes increasingly intricate. Interfering the photons is modelled by means of the action of a beam splitter as described in Section 2.6.3. The detectors are modelled in the following way:

- A photon in input arm a of the beam splitter is modelled by

$$\int \phi(\omega)\hat{a}^\dagger(\omega)d\omega \ket{0}_a.$$

(3.7)

A photon in input arm b of the beam splitter is modelled by

$$\int \psi(\omega)\hat{b}^\dagger(\omega)d\omega \ket{0}_b.$$

(3.8)

Here $\phi(\omega)$ and $\psi(\omega)$ are the spectral amplitude functions in input arm a and b respectively. The visibility is then given by [86]

$$v = \left| \int \phi^*(\omega)\psi(\omega)d\omega \right|^2.$$

(3.9)

- The action of the beam splitter is as characterised in Equation 2.35. Applying this to Equations 3.7 and 3.8 analytical expressions for projections of all the possible detector outcomes can be found. It turns out these can be expressed in terms of the visibility, v, as defined in Equation 3.9 [86]. For the form of these analytical expressions the reader is referred to [12] and the appendix of [86]. In Netsquid-AE these analytical expressions are evaluated using QuAlg [87].

- After the interference the detector efficiency, η_d, and the detector dark counts, p_d, are applied classically to obtain the final baheviour, equivalent to the case where there is no interference of the photons.

The measurements themselves are modelled by means of Positive Operator-Valued Measures (POVMs), M_{kl}, that capture the behaviour of the detectors as highlighted above. Here kl denotes the POVM element corresponding to k detection events in one detector and l detection events in the other detector. From the POVMs, a Kraus operator can be defined as

$$A_{kl} = \sqrt{M_{kl}}.$$

(3.10)

The probability p_{kl} of measuring k photons are at one detector and l photons at the other detector when measuring a quantum state ρ (which is the combined state of both the photons measured) is then given by

$$p_{kl} = \mathsf{Tr}\left(A_{kl}^\dagger A_{kl}\rho\right) = \mathsf{Tr}(M_{kl}\rho).$$

(3.11)

The corresponding post measurement state, $\rho_{|kl}$, is given by [88]

$$\rho_{|kl} = \frac{A_{kl}\rho A_{kl}^\dagger}{\mathsf{Tr}\left(A_{kl}^\dagger A_{kl}\rho\right)}.$$

(3.12)

The component that performs the QKD measurement then registers detection events according to the probability distribution given in Equation 3.11. These detection events are the raw data with which the

datacollector of Nlblueprint, which we will introduce later in this section, performs the data analysis of a QKD based simulation. After measurement by this component the state of the qubits are discarded. The components that perform the BSM also register detection events according to the probability distribution given in Equation 3.11. They herald success if there is exactly one detection event in one of the detectors and herald failure otherwise. When heralding success, the shared state of the qubits that are measured is set according to Equation 3.12.

Magic

When simulating setups that make use of heralded entanglement generation, simulating each individual event becomes unfeasible. This can be attributed to the fact that we are only interested in the events where entanglement generation is successful. These interesting events comprise only a fraction of the total events. To resolve this, magic is introduced. The concept of magic is that the elementary links of a setup are not fully simulated but that the quantum states that result from the elementary link are inserted into the corresponding quantum memories of the elementary link 'magically'.

Concretely, this is achieved by knowing the probabilities of each successful BSM outcome and the corresponding resulting states before running the actual simulation. From the known probability of success, the time it takes to generate entanglement is sampled from a geometric distribution. After this time, the system assigns the beforehand known shared state to the two memories that ought to be entangled. Magic is organised into the code snippet NetSquid-Magic [89]. Because the atomic-ensemble-based simulations have some special requirements on the states in the quantum memories (i.e. the abiliy to store photon states encoded into multiple Netsquid qubits) some parts of the magic for those is organised in the Netsquid-AE [15] snippet.

Throughout this thesis, a specific kind of magic known as forced magic is used. This means that each elementary link is simulated once to obtain the relevant states and probabilities. The two photon pair sources in the elementary links send one of their photons to the heralding station and the other one to its corresponding quantum memory. From the states of the photons at the heralding station the probability of each measurement outcome that corresponds to a successfully BSM is computed using Equation 3.11. The resulting state is computed using Equation 3.12. This state and its probability is stored permanently so that every time a setup containing an elementary link with similar parameters is simulated, those can be used to enhance the performance of the simulations.

Services and protocols

To run realistic quantum network simulations NLblueprint utilises services. A service is defined by an input, a function it aims to perform, and an output. We provide an example of this in the form of a service that measures a qubit. The input to this service would be the request to measure a qubit, the function it aims to perform would be the measurement of the qubit, and the output would be the measurement outcome. The execution of the function, known as a protocol, is thus separated from the service itself. The protocol is responsible for ensuring that the intended functionality is accomplished and the outcome is yielded [10].

This separation of services and protocols brings about some advantages. Firstly it allows to us to easily execute similar protocols on different types of hardware. To exemplify, a repeater protocol might require an entanglement swap. To do so, it will place a request on the local entanglement swap service. The protocol then does not need to know any specifics regarding how the swap is implemented. This allows us to easily use existing code from the NLblueprint to run simulations using models in Netsquid-AE. Secondly, it facilitates a modular stack of protocols, enabling the seamless interchangeability of protocols that implement a specific service. This way new implementations can be made more efficiently, since many portions of the code can be repurposed.

We will now elucidate the implementation of services and protocols to generate one bit of secret key used throughout this thesis. Entanglement generation across the repeater chain is in itself defined by a service. This service is known as a link-layer service [86, 90]. Request to this service should be put on the end-nodes of the repeater, which activates a messaging service. This messaging service then sends messages across the repeater chain to initiate the entanglement generation. An agreement service is then responsible for reaching agreement on when elementary links start generating entanglement. Once this agreement has been reached, a protocol that uses the physical models in Netsquid-AE to start the elementary entanglement generation is initiated. We point out that this

elementary entanglement generation happens magically, as described in the previous subsection. To this end, the protocol sends a request to a magic service. A separate service keeps track of where entanglement exists across the repeater. As soon as a repeater node established entanglement with both its neighbours the corresponding swap service receives a request to perform the entanglement swap. As we consider a single repeater setup in this thesis this means end-to-end entanglement is established. The protocol can however easily be extended to an arbitrary number of repeaters. When end-to-end entanglement is established both of the measure services located at the end nodes receive a request to measure the qubit in their memory. The measure service subsequently forwards its output to the datacollector, which is the focus of the following section. We note that for atomic-ensemble-based simulations specifically there is a possibility that the measurement fails. This can for example be a consequence of having more than one excitation in a memory at any given time (due to multi-photon emission). In this case, the detector could detect more than one photon. This cannot be seen as a logical one or zero and thus is considered a 'failure'. The simulation is repeated until n bits of secret key are generated successfully.

Datacollector

The datacollector converts the measurement outcomes of the QKD detectors to analysable data. To do this, the datacollector keeps track of the time in the simulation. Once it receives the measurement outcomes from both the end nodes, it stores the time it took to generate the bit of secret key. Once it collected the n bits of secret key from both the nodes, it can compute the average rate it took to generate one bit of successful key. From the measurement results it can also compute the QBER as the fraction where the measurement outcomes of the two end nodes are not (anti-)correlated. Finally, it uses Equation 2.2 to compute the secret key rate. For more details on the computations the datacollector performs and how it computes the errors we refer the reader back to Section 2.2.2 and Section 2.2.3

3.2. Optimisation problem

We now formulate the task of optimising hardware parameters as a mathematical problem. We define the solutions of these previously indicated problems as absolute minimal hardware requirements and minimal hardware requirements. To solve this problem, we formulate a cost function that reaches its minimum for the parameters that solve the problem. The hardware parameters that this cost function should take as an input are discussed in Section 3.2.1. Thereafter, absolute minimal hardware requirements and minimal hardware parameters are elaborated upon in Section 3.2.2 and Section 3.2.3 respectively. Besides, cost functions are specified in the mentioned sections.

3.2.1. Simulated hardware parameters

The hardware parameters and their corresponding current state-of-the art baseline values are tabularised in Table 3.1. Parameters for the detectors are those of the commercially available ID281 Superconducting Nanowire Series manufactured by IDQuantique [91]. Baseline values for the quantum memories are results of AFC memories realised in the lab [92, 72].
One of the unique attributes of the simulations used is its ability to simulate multi-photon emission. As explained in Section 3.1.2 this is done by simulating SPDC sources with mean photon number μ. Since the simulated setups are not symmetric the values for the mean photon numbers are not necessarily equal for all photon pair sources. Each simulated elementary link has two photon pair sources, of which the outgoing photons have to travel over different distances to arrive at the respective heralding stations they are sent to. Thus, in accordance with Equation 2.1, the photons have different probabilities to get lost in the fiber.
Combining this with the fact that the ideal photon numbers potentially are also dependent on the other hardware parameters, the search space for the minimal hardware requirements of this setup would become very expensive to optimise. In order to reduce the search space a heuristic introduced in [93] is used. The heuristic states that the probability that a single photon arrives at the heralding station, which we define as p_{surv}, is equal across the setup. Note that for the single repeater setup this thesis aims to optimise this means the four parameters needed to describe the multi-photon emission are reduced to a single parameter (p_{surv}).

Table 3.1: Simulated hardware parameters and their baseline values. Baseline values correspond to current state-of-the art values that have been realised in practice. This is either in an experimental setup or in a commercially available product.

Hardware parameter	Baseline value
detector efficiency (η_d)	0.8 [91]
detector dark count probability (p_d)	$1 \cdot 10^{-5}$ [91]
max. memory efficiency ($\eta_{m,0}$)	0.52 [92]
memory coherence time (T_c)	0.5 s [72]
visibility (v)	0.9 [12]

3.2.2. Absolute minimal hardware requirements

To evaluate the performance of the setup with imperfect hardware we introduce the concept of absolute minimal hardware requirements. The conceptual question an absolute minimal hardware requirement answers is "Say all other parameters are perfect, what would be the minimal hardware parameter value that makes the performance of the setup good enough?". From this formulation it is natural to ask what "good enough" means. As mentioned in Section 2.2 the SKR associated with QKD is used to assess the performance of a simulated repeater chain. To find the absolute minimal hardware requirement a target SKR, $R_{sk,target}$, is introduced. The hardware parameter value that makes the performance of the setup good enough is then the value for which the simulated SKR, $R_{sk,simulated}$, is exactly equal to the target SKR $R_{sk,target}$. We thus formally define absolute minimal hardware requirements as the least favourable value of a hardware parameter that still allows us to reach the SKR, $R_{sk,target}$, given the only other imperfection considered is photon loss in the fibers. To translate the problem formulation of absolute minimal hardware requirements to a mathematical optimisation problem we introduce the cost function. The cost function is minimised exactly when its input is the parameter value corresponding to the absolute minimal hardware requirement.

The simplest form of the cost function is one that can be used to find minimal hardware parameters for a setup with a perfect photon pair source. A perfect photon pair source means a source without multi-photon emission. Having no multi-photon emission means the p_{surv} parameter introduced above is redundant. As in this case improving the hardware parameter always increases the SKR an adequate cost function, $C_{AMR,perf}$, that optimises hardware parameter x is

$$C_{AMR,perf}(x) = |R_{sk,simulated}(x) - R_{sk,target}|. \tag{3.13}$$

When looking at setups with multi-photon emission, and hence using the parameter p_{surv}, this simple cost function no longer suffices. This is due to the fact that there might be an entire subspace in (x, p_{surv})-space that minimises the cost function, whereas the cost function that solves the problem formulation of absolute minimal requirements is only the solution where the hardware parameter value is the lowest. We illustrate this by giving an example. If $R_{sk,simulated}(x = 0.7, p_{surv} = 0.002) = R_{sk,target}$ and $R_{sk,simulated}(x = 0.6, p_{surv} = 0.005) = R_{sk,target}$ (and bigger x indicates better hardware) the cost function in Equation 3.13 will not be able to distinguish between the solutions $\{x = 0.7, p_{surv} = 0.002\}$ and $\{x = 0.6, p_{surv} = 0.005\}$. An optimisation technique might then very well converge to the solution that indicates $x = 0.7$ is the absolute minimal requirement for our setup. We are however interested in the solution $x = 0.6$, as this is an even lower hardware parameter value that still allows us to reach the target we set. Hence, a penalty for better hardware parameter values is needed in the cost function.

To this end we introduce the no-error probability p_{ne}. This is simply the probability that a given hardware parameter does not result in an imperfection. For the detector efficiency this is $p_{ne}(\eta_d) = \eta_d$, for the detector dark count probability this is $p_{ne}(p_d) = 1 - p_d$, for the maximum efficiency of the memory this is $p_{ne}(\eta_{m,0}) = \eta_{m,0}$, for the memory coherence time this is $p_{ne}(T_c) = \exp(-1/T_c)$, and for the visibility this is $p_{ne}(v) = v$ [10].

Using this, we design an adequate cost function, C_{AMR},

$$C_{AMR}(x, p_{surv}) = wu\left[R_{sk,target} - R_{sk,simulated}(x, p_{surv})\right] + p_{ne}(x). \tag{3.14}$$

Here w is a factor to ensure the cost for not meeting the target is more than the cost for having better

hardware which we have set to 10 and u is the heaviside step function defined by

$$u(x) = \begin{cases} 0 & \text{if } x \leq 0 \\ 1 & \text{if } x > 0 \end{cases}. \tag{3.15}$$

3.2.3. Minimal hardware requirements

In reality, no hardware parameters can be considered perfect. Consequently, relying only on the absolute minimum hardware requirements provides only a partial understanding of the overall hardware requirements of a setup. It's important to note that imperfections in some hardware parameters may also lead to stronger requirements in other hardware parameters. For this reason the absolute minimal hardware requirement value poses an absolute minimum for the hardware parameter to meet its target, but do not necessarily contain information about a set of hardware parameters that make the setup meet its target. To answer this question, we introduce minimal hardware requirements.

Conceptually minimal hardware requirements are very similar to absolute minimal hardware requirements. We define minimal hardware requirements as the least favourable set of hardware parameters that make the performance of the setup good enough. Good enough is again the value for which the simulated SKR, $R_{sk,simulated}$, is exactly equal to a target SKR, $R_{sk,target}$. We furthermore define the least favourable set of hardware parameters as the hardware parameters that in total need to be improved the least when comparing to the baseline values (and thus have worse performance than a 'more favourable' set of hardware parameters).

For this problem formulating a cost function is slightly more difficult. This is due to the fact that the further a hardware parameter is increased, the higher this should be penalised. To account for this, we introduce the improvement factor, k. The behaviour of the improvement factor is described by [10, 11]

$$p_{ne}(x) = p_{ne}(b)^{1/k}. \tag{3.16}$$

This can be read as: the no-error probability of the baseline value, b, is improved by a factor k to get hardware value x. Note that the improvement factor k being 1 denotes a hardware parameter not improving, and as the improvement factor k goes to infinity the no-error probability of the hardware parameter goes to 1 (i.e. the hardware parameter goes to perfection).

The cost associated with improving the hardware, H_c, is then simply given as the sum of the improvement factor for all the hardware parameters

$$H_C(\vec{x}) = \sum_{i=1}^{N} \frac{\ln\{p_{ne}(b_i)\}}{\ln\{p_{ne}(x_i)\}}. \tag{3.17}$$

Here $\vec{x}$ is a vector of length N containing all hardware parameters and b_i is the baseline value of parameter x_i. The baseline values used are those in Table 3.1.

Using this, a suitable cost function, C_{MR}, that solves the problem of finding minimal hardware requirements is designed [10]

$$C_{MR}(\vec{x}, p_{surv}) = w_1 \left(1 + [R_{sk,target} - R_{sk,simulated}(\vec{x}, p_{surv})]^2\right) \cdot$$
$$u\left[R_{sk,target} - R_{sk,simulated}(\vec{x}, p_{surv})\right] + w_2 H_C(\vec{x}). \tag{3.18}$$

Here w_1 and w_2 are hyperparameters that are set to $1 \cdot 10^{20}$ and 1 respectively. u is the heaviside step function defined by Equation 3.15. Note that this cost function is appropriate both for setups with a perfect photon pair source and setups with multi-photon emission included. The only difference being that when having a perfect photon pair source the probability p_{surv} that a photon arrives at the heralding station is redundant.

3.3. Optimisation methodology

The final puzzle piece needed are methods to optimise the cost functions introduced above. As such, we introduce Bayesian optimisation and genetic algorithms in Section 3.3.1 and Section 3.3.2 respectively.

3.3.1. Bayesian optimisation

Bayesian optimisation is a suitable optimisation technique if C is a black box function of which no closed form nor its gradients are known, C is computationally expensive to evaluate, and evaluations of C contain noise [17, 94]. As evaluation of all the cost functions introduced in Section 3.2 require performing a simulation and thus have no closed form, are computationally expensive, and contain noise, Bayesian optimisation is a good fit.

Algorithm 1 describes Bayesian optimisation. It involves making a statistical estimate of C based on a given number of data points, also known as Gaussian process regression. This statistical estimate of C will be a probability distribution over all possible functions. Gaussian process regression postulates that this probability distribution is a so called Gaussian process. Such a Gaussian process can be understood as a (infinite dimensional, i.e. the ability to generate an outcome for all continuous $\vec{x}$) multivariate normal distribution and is thus characterised by a mean function $\mu(\vec{x})$ and a variance function $\sigma^2(\vec{x})$ [94, 95, 96]. $\mu(\vec{x})$ and $\sigma^2(\vec{x})$ can be used to find the expected improvement, $EI(\vec{x})$. The expected improvement is defined as [17, 94, 97]

$$EI(\vec{x}) = E\left[\max\{C^* - C(\vec{x}), 0\}\right]. \tag{3.19}$$

Here C^* is the lowest function evaluation thus far. The expected improvement can thus be interpreted as the expected value of the difference between the function value at entry $\vec{x}$ and the best evaluation thus far, given that there is an improvement at entry $\vec{x}$.

The entry with the highest expected improvement is then evaluated next, resulting in an extra data point and a new statistical model for C. This process is repeated until N data points are evaluated. It turns out that for making a statistical model of C based on available data points all that is needed is a so called kernel function [94, 96]. This kernel function should be a measure of the covariance between the available data points. Moreover, it should be chosen such that two inputs that are close to each other in the input space have a larger correlation, in order to ensure their function values ought to be more similar. A commonly used kernel that is also used in the implementation in this thesis is the Matérn kernel Σ [94, 96]

$$\Sigma(\vec{x_1}, \vec{x_2}) = \alpha_0 \frac{2^{1-\nu}}{\Gamma(\nu)} \left(\sqrt{2\nu}|\vec{x_1} - \vec{x_2}|\right)^{\nu} \mathcal{K}_{\nu}\left(|\vec{x_1} - \vec{x_2}|\right). \tag{3.20}$$

Here Γ is the gamma function, $\mathcal{K}_{\nu}$ is the modified Bessel function, and α_0 and ν are parameters that in the implementation used throughout this thesis are 1 and 2.5 respectively. Literature verifies the Matérn kernel is suitable to serve as a kernel for virtually any optimisation problem [94, 96].

Using the kernel function $\mu(\vec{x})$ and $\sigma^2(\vec{x})$ can be computed. Say there are n data points at input $\{\vec{x_1}, ..., \vec{x_n}\}$ with function evaluation $\{C_1, ..., C_n\}$ available. We define **k** as the vector $[\Sigma(\vec{x}, \vec{x_1}), ..., \Sigma(\vec{x}, \vec{x_n})]^T$. We define **S** as the $n \times n$ matrix with entries $\mathbf{S}_{k,l} = \Sigma(\vec{x_k}, \vec{x_l})$. We define **C** as the vector $[C_1, ..., C_n]^T$. $\mu(\vec{x})$ and $\sigma^2(\vec{x})$ can be computed as [94, 95, 96]

$$\mu(\vec{x}) = \mathbf{k}^T \mathbf{S}^{-1} \mathbf{C} \tag{3.21}$$

$$\sigma^2(\vec{x}) = \Sigma(\vec{x}, \vec{x}) - \mathbf{k}^T \mathbf{S}^{-1} \mathbf{k}. \tag{3.22}$$

From this, the expected improvement can be computed as [94, 97]

$$EI(\vec{x}) = \max\{C^* - \mu(\vec{x}), 0\} + \sigma(\vec{x})\phi\left(\frac{C^* - \mu(\vec{x})}{\sigma(\vec{x})}\right) - |C^* - \mu(\vec{x})|\Phi\left(\frac{C^* - \mu(\vec{x})}{\sigma(\vec{x})}\right). \tag{3.23}$$

Here ϕ denotes the standard normal density function and Φ denotes the standard normal distribution function.

For a more detailed description of Bayesian optimisation and derivations the reader is referred to [94], [95], [96], and [97]. We use Scikit-optimize [17] to develop the code that performs Bayesian optimisation in this thesis.

3.3.2. Genetic Algorithm

The genetic algorithm we introduce here is another method for optimisation of a cost function C. Genetic algorithms are known to be suitable when the search space in which the solution that

---
Algorithm 1 Pseudo code for Bayesian optimisation

Evaluate C at n_0 randomly sampled entries

Using observations $\{(\vec{x}_1, C(\vec{x}_1)), ..., (\vec{x}_{n_0}, C(\vec{x}_{n_0}))\}$ build a probabilistic model for C using Gaussian Process Regression

Set $n = n_0$

while $n \leq N$ **do**

    Optimise the expected improvement based on the probabilistic model for f to sample a new entry point $\vec{x}_{n+1}$

      Evaluate $C(\vec{x}_{n+1})$

      Update the probabilistic model for C using Gaussian Process Regression

      Increment n

end while

Return the $\vec{x}$ with the lowest evaluation

---

optimises C lives is not well known [98]. We note that this specifically applies well to cost functions of the form of Equation 3.18.

Genetic algorithms are inspired by evolution theory and natural selection. In the context of genetic algorithms a single parameter value is known as a gene. A gene is typically encoded in the [0,1] range. A set of genes forming a possible solution to the optimisation problem is known as a chromosome. A set of chromosomes is known as a population.

Algorithm 2 describes genetic algorithms. A genetic algorithm is an iterative process. Each iteration is known as a generation. A generation consists of N_{pop} chromosomes. Each generation will produce an offspring which is a new generation consisting new chromosomes based on the previous generation. The first generation will consist of a set of random possible solutions [98].

For each chromosome in a generation the cost function C is evaluated. The $N_{elitism}$ chromosomes with the lowest C value are directly added to the offspring. The mating pool is a set of chromosomes that is used to produce the $N_{pop} - N_{elitism}$ remaining chromosomes. The mating pool consists of the $N_{parents}$ chromosomes with the lowest C value.

New chromosomes are generated from the mating pool as follows. First two parents are randomly sampled from the mating pool with a lower cost function corresponding to a higher probability to be sampled. There exist multiple methods to perform this sampling. In this thesis, roulette wheel selection is used, which means the probability of a parent, i, to be selected, $p_{select,i}$, is proportional to the inverse of its cost [99]

$$p_{select,i} = \frac{1/C_i}{\sum_{j=1}^{N_{parents}}(1/C_j)}. \tag{3.24}$$

With probability $p_{crossover}$ a new chromosome is created by combining the two parents at a random crossover point. For example if the parents are $\{a_1, a_2, a_3\}$ and $\{b_1, b_2, b_3\}$ and the crossover is 2, the created chromosome is $\{a_1, a_2, b_3\}$. With probability $1 - p_{crossover}$ the parent with the lowest C value is copied directly. The newly created chromosome then undergoes a mutation process with probability $p_{mutation}$, meaning one of the genes of the chromosome is randomly altered [98, 100]. Once there are N_{pop} in the offspring, the offspring forms the new generation and which will in the same way produce its own offspring. This process is repeated for a total of N_{gen} generations. The chromosome in the last generation with the lowest C value is the final solution.

Note there are a couple of hyperparameters involved in the process that affect the algorithm that need to be tuned. N_{pop} in theory gives more accurate results but increases the required compute power. $N_{elitism}$ ensures that the best few solutions stay in the generation, but setting it too high will result in too little new solutions being explored [101]. Increasing $p_{crossover}$ and $p_{mutaion}$ result in more exploring of new solutions but overdoing this may disregard all the information that is already in the existing solutions [100]. From earlier work using Netsquid simulations to optimise over different setups [10, 11] and general literature on genetic algorithms [99, 100, 102] it has been concluded that a good value for N_{pop} lays between 100 and 200, a good value for $p_{crossover}$ lays between 0.6 and 0.8, a good value for $p_{mutation}$ lays between 0 and 0.1, and a good value for $N_{elitism}$ is around 5% of the total population.

For N_{gen}, work using Netsquid simulations to optimise over different setups [10, 11] has shown that

the algorithm converges for at around 50 generations. Two possible methods are distinguished to asure convergence of the algorithm [10]. The first one is to simply let the algorithm run for N_{gen} generations. The second one is a more sophisticated method requiring a bigger number of N_{gen}. Convergence is then defined as the cost function of the best chromosome in the population of each generation not varying for a given number of generations within a certain relative tolerance. Typical number for this are 10 generations with a tolerance of 1%.

We use PyGAD [98] to implement genetic algorithms. We implement PyGAD through YOTSE [18], a comprehensive tool to optimise scientific experiments.

Algorithm 2 Pseudo code for Genetic Algorithms

Randomly generate a population consisting of N_{pop} chromosomes

Set $generations = 0$

while $generations \leq N_{gen}$ **do**

    Evaluate the cost function C for each chromosome in the population

    Select the $N_{parents}$ chromosomes with the lowest C value to be in the mating pool

    Add the $N_{elitism}$ chromosomes with the lowest C value to the offspring

    while number of chromosomes in offspring $\leq N_{pop}$ **do**

        Randomly sample two parents from the mating pool

        With probability $p_{crossover}$: create a new chromosome by combining the two parents at a random crossover point

        Else: copy the chromosome of the first parent

        With probability $p_{mutation}$: let the created chromosome undergo a mutation process

        Add the newly created chromosome to the offspring

    end while

    Set the new population to the offspring

    Increment $generations$

end while

Return the chromosome in the last generation with the lowest C value

---

Validation

As explained in Section 3.1.1, one of the achievements of this thesis is to have working atomic-ensemble-based using NLblueprint. The components of Netsquid-AE are mostly verified in [12] and [13]. It is valuable to have a validation of an atomic-ensemble-based simulation making use of NLblueprint. More specifically, we aim to validate that the code authored to integrate Netsquid-AE into NLblueprint. That is, we want to confirm that simulations utilising this integration work as expected. To do this, we validate a simulation of an elementary link against analytical results obtained by the authors of [16] in this chapter.

4.1. Setup

The setup we use for the simulation is shown in Figure 4.1. All parameters used in the simulation are in Table 4.1. The setup consists of a symmetric elementary link between two nodes that contain a photon pair source emitting photons in time-bin encoding, a quantum memory and a detector. The detector measures the photons coming from the quantum memory directly if it measures in the Z basis, or interferes them first if it measures in the X basis. The nodes are connected through optical fibers with attenuation factor $\alpha = 0.2$ dB/km (commercial grade fiber [19]) of length L to a heralding station.

All detectors in the setup (both those used in the BSM and those used for the measurements) have detector efficiency, $\eta_d = 0.9$, and dark count probability, $p_d = 3 \cdot 10^{-4}$. The quantum memory has a efficiency $\eta_{m,0} = 0.9$. We use these parameters as the decrease they yield in the SKR is significant. However, this decrease is not sizeable enough to nullify the SKR for these parameters. Moreover, these parameters are also used by the authors of [16] to display the analytical results. The authors of [16] assume the memory efficiency does not decay over time (i.e. $T_c = \infty$) to obtain the analytical results. Furthermore, they assume that the photon pair source is perfect, meaning it always emits exactly one photon with equal probability in each time-bin. Additionally, we use $M = 10^3$ multiplexing modes. We make this choice to be consistent with [16] once more.

We vary the distance L from 10 km to 140 km in steps of 10 km. We make this choice for two reasons. The first is that in this way all distances in the network which we will use to optimise hardware parameters, which we will further discuss in Chapter 5, are covered. The second is that this way both the regime where the effect of photon loss in the fiber is negligible and the regime where it has a very dominant effect on the performance of the setup are covered.

4.2. Method

In order to validate the simulation framework we compare the results of simulating QKD on an elementary link against results from [16]. We simulate entanglement based QKD using the protocols and components highlighted in Section 3.1.2. In [16], the authors perform an analytical analysis of the effect of memory efficiency, $\eta_{m,0}$, detector efficiency, η_d, and detector dark counts, p_d, on the SKR of a repeater architecture with a perfect photon pair source with photons encoded in time-bin encoding. The analytical results are quite involved and are summarised in Appendix A.

The protocol used in [16] for entanglement generation is, however, different than the protocol explained in Section 3.1.2. The authors of [16] assume the photon pair sources emit a photon pair each time T_q. The two end nodes measure in each attempt (so each T_q) and only at the very end of
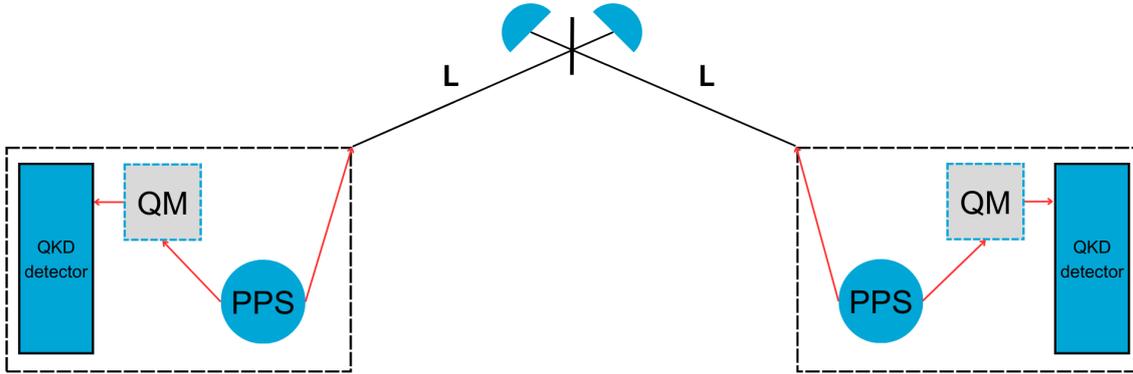
Figure 4.1: Schematic depiction of the setup simulated for validation against the results in [16]. The setup consists of an elementary link with both end nodes at a distance L away from the heralding station. The end nodes contain a Photon Pair Source (PPS), that emits photons corresponding to a time-bin-encoded qubit. Furthermore they contain a Quantum Memory (QM), and a QKD detector. The QKD detector measures two photons that correspond to a time-bin-encoded qubit. It measures the photons directly if it measures in the Z basis, or interferes them first if it measures in the X basis. The heralding station creates elementary entanglement by performing a BSM using two detectors and a 50:50 beam splitter. Section 3.1.2 contains additional information on the modelling of individual components.

the protocol discard all instances where the BSM for either the entanglement generation or the entanglement swap heralded as a failure. This is in contrast with the protocol we use, where a measurement is only done once entanglement between the end nodes is established.

As a result, the protocol used in [16] will have a higher SKR as this protocol is not limited by the cycle time, i.e. there is no need to wait for a result from the heralding station before starting a new attempt. Note that despite the fact that the protocol introduced in [16] achieves much higher SKR, it would likely not be feasible as an architecture for a possible quantum internet. The protocol requires entangled pairs to be measured immediately, limiting the number of possible quantum applications that can be executed drastically. Furthermore it would require keeping track of which measurement corresponds to which successful heralding signal, which in practise would be a complex ordeal.

To compare the results obtained from the simulation to those presented in [16] we convert the simulated SKR to a number of attempts per bit after initiating trying to generate entanglement. To do this we use the beforehand known cycle time $2L/c$. We then present the results as the converted SKR that would result from attempting each $T_q = 5 \cdot 10^{-7}$ s (again consistent with [16]) and compare this directly to results from [16].

4.3. Results

We perform simulations of setup in Figure 4.1 with the parameters in Table 4.1 for L ranging from 10 km to 140 km. The results are in Figure 4.2. For each L the simulations are run until 10^3 successful measurements have occurred in each measurement basis (i.e. $2 \cdot 10^3$ measurements in total). It can be seen that the simulated data is in agreement with the analysis in [16]. This agreement is demonstrated along a wide range of distances L. There is a regime, $L < 70$ km, where the high number of multiplexing modes ensures entanglement generation is almost deterministic and all imperfections can thus be accounted to hardware parameters in the nodes themselves. There is also a regime, $L \geq 70$ km, where due to the large distance photon loss in the fiber happens with high probability and this becomes the main reason the SKR decreases.

From this, it is concluded that enough confidence in the simulations generate useful results regarding

the hardware parameters of repeater chains is built. We have only verified results with perfect photon pair sources as analytical results that take into account multi-photon emission do not exist to the best of our knowledge.
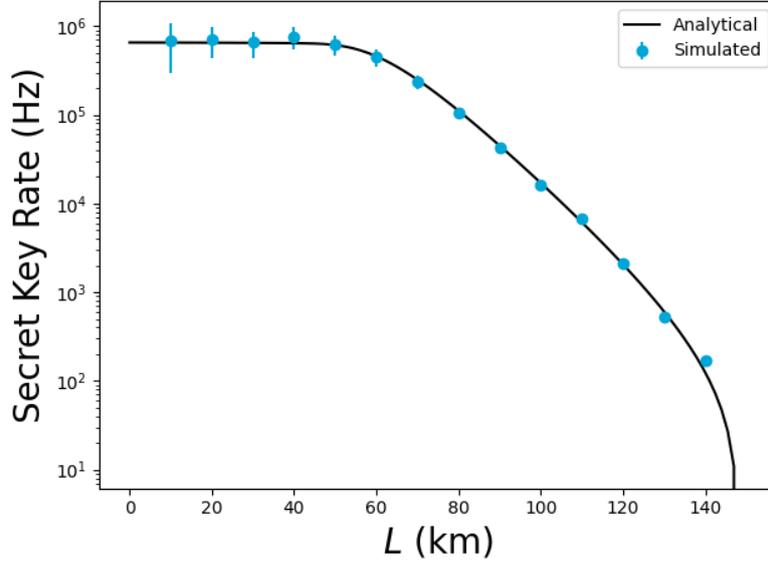

Figure 4.2: Results of running simulations for a symmetric atomic-ensemble-based elementary link, as depicted in Figure 4.1. The simulated results are obtained using code from NLblueprint and Netsquid-AE [15]. Simulated results are converted to attempts it takes to generate one bit of secret key and then multiplied by $1/T_q$ where $T_q = 5 \cdot 10^{-7}$ s for consistency with [16]. Furthermore, we consider the following hardware parameters: detector dark count probability, $p_{dark} = 3 \cdot 10^{-4}$, detector efficiency, $\eta_d = 0.9$, memory efficiency, $\eta_{m,0} = 0.9$, number of multiplexing modes, $M = 10^3$, fiber attenuation factor, $\alpha = 0.2$ dB/km. We vary L, which denotes the distance from both the nodes to the heralding station, from 10 km to 140 km. All other parameters are considered to be perfect. Errorbars are obtained using Equation 2.6. The simulated results are juxtaposed against analytical results from [16].

Table 4.1: Parameters used to validate the simulation against analytical results from [16]

Parameter		Value
Attenuation	α	0.2 dB/km
Memory efficiency	$\eta_{m,0}$	0.9
Memory coherence time	T_c	∞
Detector efficiency	η_d	0.9
Detector dark count probability	p_d	$3 \cdot 10^{-4}$
Detector visibility	v	1
Multiplexing modes	M	10^3
PPS emission probabilities	$\{p(0), p(1), p(2), p(3)\}$	$\{0, 1, 0, 0\}$
Number resolving detectors		True

<div style="text-align: right; font-size: 3em;">5</div>

Setup: the Delft-Eindhoven network

5.1. Network

In order to evaluate the effect of hardware parameters on a single repeater chain by the method presented in Chapter 3.1 a network on which the repeater chain operates is needed. As it is likely that deployment of repeaters will make use of existing fiber networks [103], we choose to consider a real-life fiber network. To this end we introduce a network based on SURF's fiber infrastructure, connecting the Dutch cities of Delft and Eindhoven. This network is also used in [10]. We present this network in Figure 5.1.

The usage of this network brings about some consequences. Using this network places restrictions on the locations where end nodes, repeater nodes, and heralding stations can be placed. For these locations we restrict ourselves to hubs in SURF's network with the facilities to realise quantum hardware [104]. As a result, heralding stations for the elementary entanglement generation cannot be placed equidistantly from both nodes. It is known that this asymmetry has a negative effect on the performance of a repeater [84, 93].

SURF has such hubs in Rotterdam, Utrecht, Nieuwegein and Den Bosch. At these intermediate cities a repeater node or heralding station can be placed. Since we consider a single repeater setup this leaves freedom in the placement of the repeater node and heralding station when connecting Delft and Eindhoven.

Making use of these locations, two repeater configurations are possible. We show these configurations in Figure 5.2. We define setup N as the setup with a repeater in Nieuwegein and heralding stations in Utrecht and Den Bosch. We define setup U as the setup with a repeater in Utrecht and heralding stations in Rotterdam and Nieuwegein. Furthermore, we define $L_{1,l}$ as the distance from Delft to the first heralding station, we define $L_{1,r}$ as the distance from the first heralding station to the repeater node, we define $L_{2,l}$ as the distance from the repeater node to the second heralding station and we define $L_{2,r}$ as the distance from the second heralding station to Eindhoven. Using this, the asymmetry of elementary link i in setup S is defined as [84, 93]

$$A_{S,i} = \frac{|L_{i,l} - L_{i,r}|}{L_{i,l} + L_{i,r}}. \tag{5.1}$$

As a result $A_{N,1} = 0.627..., A_{N,2} = 0.2, A_{U,1} = 0.638...,$ and $A_{U,2} = 0.736....$ We thus conclude that setup N is more symmetric than setup U. Hence, we hypothesise that setup N will have better performance than setup U [84, 93].

For completeness, we show the contents of each kind of node in Figure 5.3. The end nodes contain a photon pair source, a quantum memory, and a QKD detector that can measure the quantum memory of the end node when end-to-end entanglement is established in the Z and X basis. The repeater node contains two photon pair sources, two quantum memories, and has the ability to swap entanglement when both its quantum memories are entangled with the end nodes. The heralding station contains a 50:50 beam splitter and detectors that perform a Bell state measurement. We remind the reader that since we deploy a double click protocol, as introduced in Section 2.5.2, all components operate in the time-bin encoding. For more details on the modelling of the individual components, we refer the reader back to Section 3.1.2.

Figure 5.1: Schematic depiction of a network based on SURF's fiber infrastructure. The blue circles represent the locations of hubs in the network that possess the facilities to realise quantum hardware. The placement of end nodes, repeater nodes and heralding stations is restricted to these hubs. Distances are in kilometres.
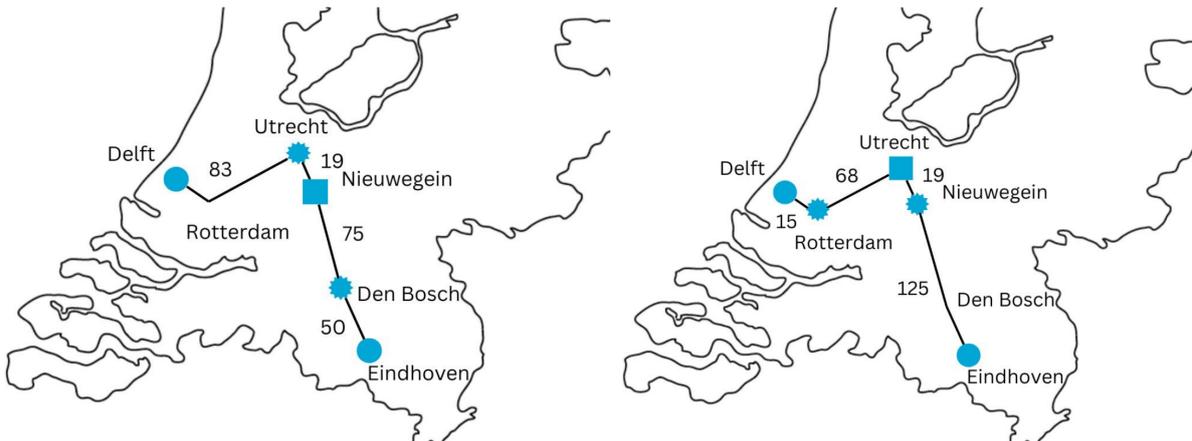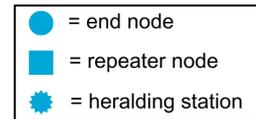
Figure 5.2: Schematic depiction of the two possible setups to implement a single-repeater setup making use of SURF's fiber infrastructure to connect the cities Delft and Eindhoven. The placement of end nodes, repeater nodes and heralding stations is restricted to hubs with the facilities to realise quantum hardware. The contents of all respective types of node are in Figure 5.3. **a)** Setup N, the repeater node is located in Nieuwegein and heralding stations are located in Utrecht and Den Bosch. **b)** Setup U, the repeater node is located in Utrecht and heralding stations are located in Rotterdam and Nieuwegein. Distances are in kilometres.
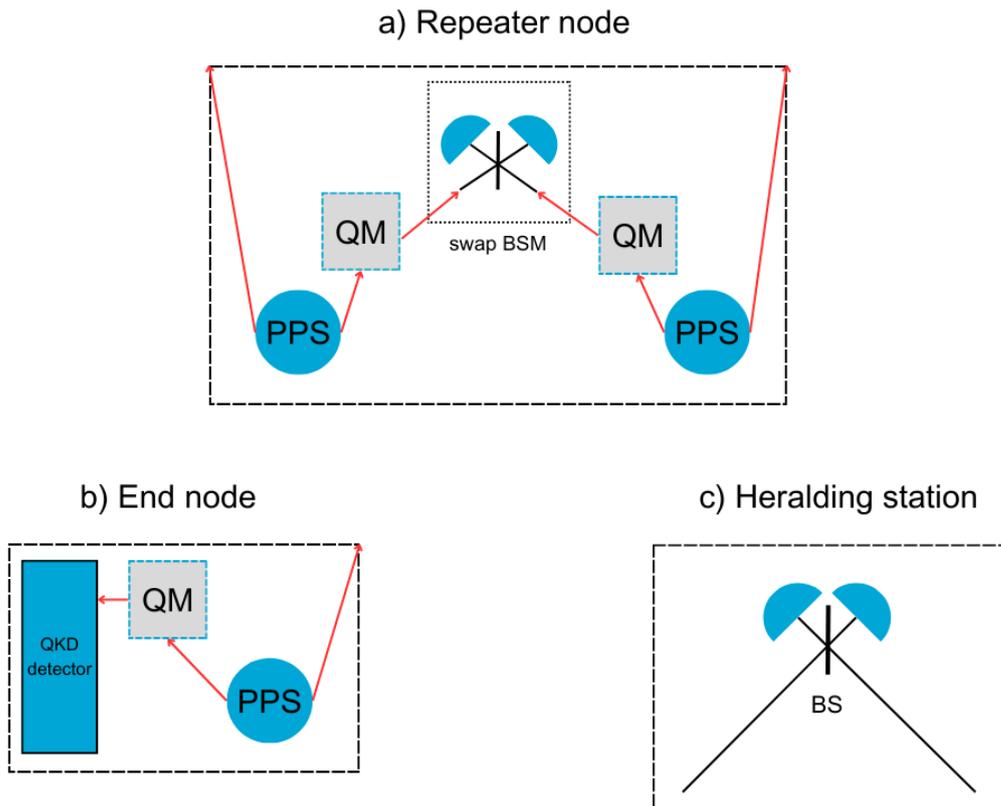
Figure 5.3: Schematic depiction of the nodes within the SURF network and the components encapsulated within them. **a)** The repeater node contains two Photon Pair Sources (PPS), that emit photons corresponding to a time-bin-encoded qubit, as defined by Equation 3.2. Furthermore, it contains two Quantum Memories (QM). The quantum memories can be read out, after which a BSM is done to perform an entanglement swap. **b)** The end node contains one QM, one PPS, and a QKD detector. The QKD detector measures two photons that correspond to a time-bin-encoded qubit. It measures the photons directly if it measures in the Z basis, or interferes them first if it measures in the X basis. **c)** The heralding station creates elementary entanglement by performing a BSM using two detectors and a 50:50 Beam Splitter (BS). Section 3.1.2 contains additional information on the modelling of individual components.

5.2. Simulations

Scenarios
On this network we optimise the hardware parameters discussed in Section 3.2.1. To this end, we simulate entanglement based QKD using the protocols and components highlighted in Section 3.1.2. We assume that the fibers throughout the network all have an attenuation factor $\alpha = 0.2$ dB/km, similar to a commercial grade fiber [19]. Moreover, we assume that the detectors are non number resolving. We make this decision guided by details about SNSPDs, which as introduced in Section 2.6.4 we base the detectors on. Making an SNSPD number resolving requires connecting multiple individual SNSPD pixels in parallel [105]. This is thus inherently more resource intensive. As a future quantum network would require many of such detectors, employing number resolving detectors would be suboptimal.

We distinguish between setups with perfect photon pair sources and photon pair sources with multi-photon emission. We define a perfect photon pair source as a source that always emits exactly one photon, and does this with equal probability in the early or late time-bin. Consequently, this means the corresponding emission probabilities of the photon pair source, as introduced in Section 3.1.2, are $\{p(0), p(1), p(2), p(3)\} = \{0, 1, 0, 0\}$. We define a photon pair sources with multi-photon emission as a photon pair source that is modelled after a SPDC source introduced in Section 2.6.1. Conctretely, this means we specify the mean photon number, μ, of the photon pair sources. As explained we introduce a parameter denoting the probability a photon arrives at the heralding station, p_{surv}, to deal with the value of μ of the photon pair sources across the asymmetric setup. Now that the network is known we can formulate a concrete equation for p_{surv},

$$p_{surv} = \mu_{1,l}\eta_t(L_{1,l}) = \mu_{1,r}\eta_t(L_{1,r}) = \mu_{2,l}\eta_t(L_{2,l}) = \mu_{2,r}\eta_t(L_{2,r}). \tag{5.2}$$

Here the transmittance of the photons in the fibers, η_t, is once again given by Equation 2.1. As all the η_t values are constant, p_{surv} provides a single parameter to tune all mean photon numbers. Moreover, we remark that dealing with the mean photon numbers of the photon pair sources by setting p_{surv} is not the only challenge associated with multi-photon emission. As characterised by Equation 3.2, multi-photon emission is modelled by multiple Netsquid qubits. This results in a major upswing in required compute power when multi-photon emission occurs. The optimisation with multi-photon emission thus takes considerably longer.

Furthermore, the number of multiplexing modes of the network, M, needs a special treatment, as there is no perfect value for number of multiplexing modes. Increasing multiplexing capabilities will always lead to an increase in performance until the point where elementary link entanglement generation would happen deterministically. To also be able to analyse the effect of multiplexing on the performance of a single repeater setup, we choose to simulate 3 distinct values for the number of multiplexing modes, $M = 62$, $M = 10^3$, and $M = 10^6$. These values are based on current state-of-the-art for quantum memories [9], a possible future scenario that can be achieved by combining multiplexing methods, and a theoretical far-future scenario [59] respectively.

Absolute minimal hardware requirements
We find absolute minimal hardware requirements for an atomic-ensemble-based single repeater setup by optimising the cost function in Equation 3.13 and Equation 3.14. We thus find a set of absolute minimal requirements when the photon pair sources are perfect and with multi-photon emission taken into account. We do this to be able to compare the results. Evaluation of the cost function requires executing a simulation to find a SKR. We perform this simulation using the components and protocols in Section 3.1.2. Optimisations are done both on setup N and setup U in order to analyse the effect of node placement on performance on the repeater setup. To perform the optimisation we use Bayesian optimisation introduced in Section 3.3.1. This choice is motivated by the fact that Bayesian optimisation requires relatively little data points compared to other optimisation methods [95]. As each data point requires doing a simulation Bayesian optimisation will save compute time.

Minimal hardware requirements
We find minimal hardware requirements for an atomic-ensemble-based single repeater setup by optimising the cost functions in Equation 3.18. We find a set of absolute minimal requirements considering perfect photon pair sources. Similar to the absolute minimal hardware requirements we

Table 5.1: Table containing all hyperparameters used for the genetic algorithm to find minimal hardware requirements. As a reminder we include a short description of each hyperparameter in the table. For a more elaborate discussion the reader is referred to Section 3.3.2.

Hyperparameter	Short description	Value
N_{pop}	Total number of chromosomes in each generation	108
$N_{elitism}$	Number of chromosomes with the best evaluation that are immediately added to the offspring	15
$p_{crossover}$	Probability that a new chromosome is created by combining two parents	0.75
$p_{mutation}$	Probability that a newly created chromosome is randomly mutated	0.07

evaluate the cost function using both simulations on setup N and U to analyse the effect of repeater placement. To perform the optimisation we use a genetic algorithm introduced in Section 3.3.2. The reasoning for using genetic algorithms is the following; the search space increases exponentially with the number of parameters optimised over. The search space for minimal hardware requirements is thus much larger than that of absolute minimal hardware requirements. This means Bayesian optimisation will have a hard time to make a good statistical model over the entire search space without having many data points. Furthermore, as making the statistical model requires matrix multiplications which matrix sizes that are proportional to the number of data points, the Bayesian optimisation itself might get very computationally expensive as the number of data points grows. Genetic algorithms are more suitable for exploring large search spaces.

Hyperparameters

Finally we discuss the hyperparameters of the Bayesian optimisation and genetic algorithm. For the number of initial guesses used in the Bayesian optimisation, n_0, we choose 4 and 10 for the case with perfect photon pair sources and multi-photon emission respectively. This parameter is chosen big enough to ensure a sufficient coverage of the search space. In this way the algorithm can make a good enough statistical model to make a first choice of which datapoint to evaluate next. We validated the convergence of the Bayesian optimisation by confirming that the SKR of the final solutions are within 2% of the target set. We empirically found that aiming for a 2% margin is a good trade-off between accuracy and required compute time.

All hyperparameters used with the genetic algorithm are in Table 5.1. For a more elaborate discussion on these hyperparameters the reader is referred to Section 3.3.2. We validate the convergence of the genetic algorithm using the stopping criterion introduced in Section 3.3.2. The genetic algorithm is terminated once the lowest cost function in the generation has not changed with more than 1% for 10 generations. The authors of [10] found this is a good criterion for convergence.

$$6$$

Absolute minimal hardware requirements

In this chapter we present the results for the optimisation of absolute minimal hardware requirements for an atomic-ensemble-based single repeater setup. In Section 6.1 we present the results obtained when considering perfect photon pair sources. In section 6.2 we present the results obtained when considering multi-photon emission.

6.1. Perfect photon pair source

6.1.1. Results

We remind the reader that we defined absolute minimal hardware requirements as the least favourable hardware parameter that still allows the setup to reach a given target SKR, $R_{sk,target}$, given all other hardware parameters are at their optimal value, in Section 3.2.2. We furthermore remind the reader that we consider two different setups for the repeater chain, setup N and setup U, as defined in Figure 5.2. We remarked that setup N is more symmetric than setup U.

We determine a good value for the target SKR, $R_{sk,target}$, for the setups in empirical fashion. Concretely, we performed a simulation for all combinations of number of multiplexing modes, $M \in \{62, 10^3, 10^6\}$, and setups $\in \{N, U\}$. We run this simulation with perfect parameters, meaning the only imperfection comes from the photon loss in the fibers of the network. From these simulations we determined that a good value for the target SKR, $R_{sk,target}$, for setups with a perfect photon pair source is 5 Hz. A good value means all combinations can reach this SKR with perfect parameters. We also notice that for $M = 62$, setup N is capable of reaching a significantly higher SKR than setup U. We thus decide it is worthwhile to perform an optimisation requiring a target SKR, $R_{sk,target} = 20$ Hz, on setup N, to investigate the effect of setting a higher target on absolute minimal hardware requirements.

We present the results for the optimisation using target SKR, $R_{sk,target} = 5$ Hz, in Figure 6.1. The figure contains a table with all values of the absolute minimal hardware requirements. Furthermore, it contains a unitless comparison showcasing the effect of choosing a different number M of multiplexing modes and different setups respectively. These comparisons are elaborated upon in Section 6.1.2 and Section 6.1.3. We observationally established that a good trade off between statistically significant results and compute time is achieved for $n = 500$ successful measurements in both measurement bases.

We remark that the current state-of-the art values ($M = 62$ and the baseline hardware parameters from Table 3.1) are not yet sufficient to reach the target we set. This is mainly due to the low baseline value for the maximum efficiency of the quantum memories, $\eta_{m,0}$. We can thus conclude that the efficiency $\eta_{m,0}$, of the quantum memories, requires extra improvement compared to the other hardware parameters. Also remarkable is the low requirement for the coherence time, T_c, of the quantum memories, compared to its baseline value. This can be explained by the fact that we use QKD to evaluate the performance of the repeater chain. As QKD only requires to have one entangled qubit at any given time, requirements for coherence time are naturally lower than other potential applications of interest. This is also highlighted by results obtained by the authors of [83], whom using a different model find that blind quantum computing puts stronger requirements on coherence time by a factor of around 2.5.

To draw conclusions on realistic repeater chain setups it is imperative to analyse results with realistic

photon pair sources to analyse the effect of multi-photon emission, and to find the minimal hardware requirements to see how hardware parameters interconnect. Furthermore, we would like to look at the effect of the number of multiplexing modes, M, and the node placement, as defined by setup N and setup U, which is the focus of the next two sections.

6.1.2. Effect of number of multiplexing modes

In b) of Figure 6.1 we plot a unitless comparison of the results by number of multiplexing modes, M. We notice that the effect improving the number of multiplexing modes from current state-of-the art ($M = 62$) to $M = 10^3$ is large. For example, the detector efficiency, η_d, has to be better approximately by a factor 2.5 when considering $M = 62$ compared to $M = 10^3$ when looking at setup N. Improving multiplexing capabilities even further to $M = 10^6$ has only limited effect. For example, the detector efficiency, η_d, has to be better approximately by a factor 1.2 when considering $M = 10^3$ compared to $M = 10^6$ when looking at setup N. For other parameters, such as the Hong-Ou-Mandel visibility of the photons, v, the dark count probability of the detectors, p_d, and the maximum efficiency of the memories, $\eta_{m,0}$, the absolute minimal hardware requirements are even practically identical when looking at setup N.

This can be explained by the fact that multiplexing affects only the probability with which elementary entanglement generation succeeds. As we overcome the constraints the time with which elementary entanglement generation poses on the SKR, the SKR is primarily influenced by hardware imperfections related to the entanglement swap and QKD measurement.

Two important lessons can be learned from these results.

1. Improving the number of multiplexing modes is key to the feasibility of atomic-ensemble-based repeater chains as it can drastically reduce requirements on the hardware used. This confirms that efforts to improve number of multiplexing modes such as the work done in [9], [59], and [60] are along the right track and should be continued.
2. In addition to improving the number of multiplexing modes hardware also needs to be improved further. For atomic-ensemble-based repeater chains specifically especially the quantum memory needs to be improved. This validates the merit of efforts to improve AFC memories such as the work done in [92].

6.1.3. Effect of node placement

In c) of Figure 6.1 we plot a unitless comparison between the results of the different setups. We conclude that, as hypothesised in Section 5.1, setup N generally performs better than setup U, resulting in lower absolute hardware requirements. We remark that the effect on the hardware requirements of having an inefficient repeater placement decreases as multiplexing capabilities. These results are to be expected as having asymmetry in the setup should only affect elementary entanglement generation. For a larger number M of multiplexing modes, the probability of successful heralded elementary entanglement generation gets close to unity. Therefore, imperfections that do not have to do with elementary entanglement generation become dominant.

There are two notable exception to this. The most notable one is the dark count probability p_d corresponding to the detectors. As stated before, increasing multiplexing capabilities only affects the time it takes to have successful entanglement generation. Nonzero dark count probability, however, leads to false successes in the BSM, which affects the fidelity of the entangled state. Increasing M cannot correct for this. The more asymmetric a setup is, the higher the relative probability that heralded success from the BSM stems from (a) false detection event(s).

The second exception is the coherence time T_c, corresponding to the memories. We notice that even for high multiplexing capabilities, $M = 10^6$, even though relatively closer, there is still a gap between the requirement found using setup U compared to using setup N. Even as the probability of successful heralded elementary entanglement generation gets close to unity, the time the qubits spend in the quantum memories is proportional to the cycle time of the setup. Because the cycle time will always be bigger for more asymmetric setups, stronger demands on coherence time are necessary.

a)

	N			U			Baseline
	$M = 62$	$M = 10^3$	$M = 10^6$	$M = 62$	$M = 10^3$	$M = 10^6$	
T_c (ns)	8.94×10^6	1.41×10^6	1.21×10^6	2.44×10^8	2.72×10^6	1.44×10^6	5.00×10^8
η_d	0.75	0.50	0.40	0.93	0.60	0.41	0.8
$\eta_{m,0}$	0.66	0.42	0.40	0.90	0.50	0.41	0.52
p_d	5.43×10^{-4}	7.60×10^{-4}	7.74×10^{-4}	6.13×10^{-5}	1.98×10^{-4}	1.61×10^{-4}	1.00×10^{-5}
v	0.79	0.56	0.60	0.94	0.66	0.59	0.9

b)

Setup = N   Setup = U

Comparing $M=62$ to $M=10^3$

Comparing $M=10^3$ to $M=10^6$

c)
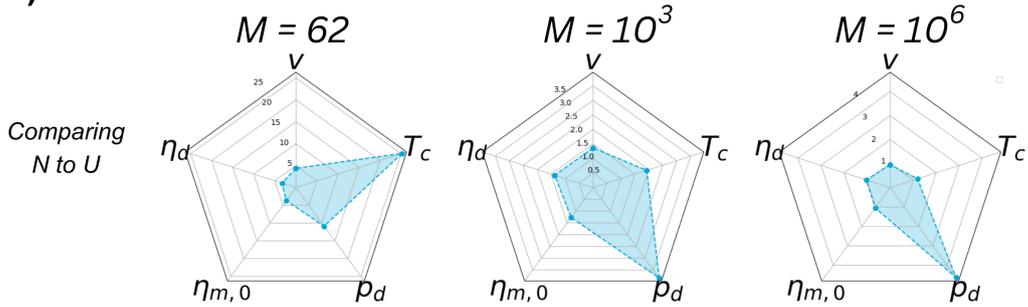
$M = 62$ $M = 10^3$ $M = 10^6$

Comparing N to U
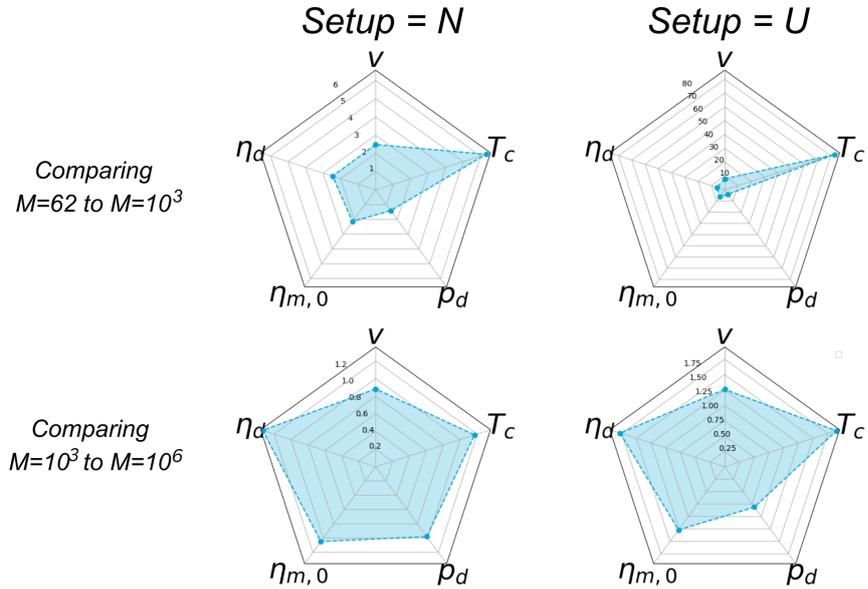
Figure 6.1: Absolute minimal hardware requirements to reach the target SKR $R_{sk,target} = 5$ Hz. Parameters: T_c = memory coherence time, η_d = detector efficiency, $\eta_{m,0}$ = maximum efficiency of the memory, p_d = detector dark count probability , v = visibility of the photons. To obtain the results we evaluate an atomic-ensemble-based single repeater setup connecting the cities of Delft and Eindhoven by setup N and U, defined in Figure 5.2. These setups deploy a double click protocol. Furthermore, we assume that the photon pair sources are perfect and the detectors are non number resolving. Results denote the least favourable value of the hardware parameter that allows us to reach SKR $R_{sk,target}$, given that the only other imperfection is photon loss in the fibers of the network. Moreover, we obtain the results by optimising the cost function in Equation 3.13 using Bayesian optimisation introduced in Section 3.3.1. Different number of multiplexing modes, M, are considered. **a)** Table containing the results for the absolute minimal hardware requirements. Besides, we show the baseline values of the hardware parameters. Baseline values correspond to current state-of-the art values [12, 72, 91, 92]. **b)** Unitless comparison of absolute minimal hardware requirements to analyse the effect of number of multiplexing modes using the definition of the improvement factor in Equation 3.16. Top: comparison of the absolute minimal hardware requirements with $M = 62$ and $M = 10^3$ multiplexing modes. Bottom: comparison of the absolute minimal hardware requirements with $M = 10^3$ and $M = 10^6$ multiplexing modes. **c)** Unitless comparison of absolute minimal hardware requirements to analyse the effect of the placement of the repeater node (i.e. setup N or U) using the definition of the improvement factor in Equation 3.16.

6.1.4. Effect of setting a higher target

We now investigate the effect of setting a higher target SKR. To this end, we perform the optimisation for the absolute minimal hardware requirements using a target SKR $R_{sk,target} = 20$ Hz. Only setup N is considered, as setup U is unable to reach the target for low multiplexing modes, even with perfect hardware parameters. The results of this optimisation are in Figure 6.2.

To examine the impact of the higher target SKR we plot a unitless comparison between the two targets we set. We observe that when going current state-of-the art multiplexing capabilities to $M = 10^3$, additional requirements on the hardware to reach the higher SKR decrease. When increasing multiplexing capabilities further this effect is again only limited. We thus conclude that additional number of multiplexing modes do not only serve a valuable function in relaxing hardware requirements, but are also instrumental in increasing the performance of a repeater chain.

6.2. Multi-photon emission

6.2.1. Results

Similar to the case with perfect photon pair sources, we determined a value for the target SKR, $R_{sk,target}$, in empirical fashion, by performing some baseline simulations. We remark on the big effect of multi-photon emission on the simulated SKR. We find that performance of the repeater chain is substantially worse. As a result, we decide on a target of 10^{-3} Hz. Furthermore, the setup is unable to reach any significant SKR for configuration U with the lowest number of multiplexing modes, $M = 62$, hence for setup U only $M = 10^3$ and $M = 10^6$ are considered. We present the results for the absolute minimal hardware requirements in Figure 6.3.

To find the absolute minimal hardware requirements with multi-photon emission considered we also need an optimal value for p_{surv}. We remind the reader that p_{surv} is defined by the heuristic we use to determine the mean photon number of the photon pair sources in Equation 5.2. p_{surv} denotes the probability an emitted photon successfully arrives at the heralding station. The optimal values of p_{surv} that are found using the Bayesian optimisation for each hardware parameter are in Figure 6.4. We notice a trend that more multiplexing modes seem to favour a lower p_{surv}. This can be explained as a higher p_{surv} increases the probability that the photon pair sources emit a photon. This corresponds to a higher probability for the heralding station to herald success, which means an increase of success rate, R_{succ}, in Equation 2.2. This however comes at the cost of more multi-photon emission and as a result the entangled states having a lower fidelity and thus a higher QBER (Q_Z and Q_X in Equation 2.2). When the number M of multiplexing modes is 10^6, the probability of success heralded will anyways be very high, so decreasing multi-photon emission proves efficient. For lower M, this is however not the case and a higher QBER must be taken for granted.

We conclude by emphasising once more that multi-photon emission is detrimental to the performance of a repeater setup. We thus identify multi-photon emission as a major barrier to realising atomic-ensemble-based repeaters.

6.2.2. Effect of number of multiplexing modes

We compare the absolute minimal hardware requirements in Figure 6.3 by number of multiplexing modes. We notice the effect of adding multiplexing modes is even bigger when considering multi-photon emission compared to perfect photon pair sources. This is to be expected as the mean photon numbers of the photon pair sources typically must be low to limit multi-photon emission. Therefore, more multiplexing modes are required to get the probability for heralded entanglement to succeed close to unity. We thus conclude that when using SPDC sources multiplexing modes are particularly crucial.

6.2.3. Effect of node placement

We compare the absolute minimal hardware requirements in Figure 6.3 by repeater placement. We again notice the effect of repeater placement is even bigger when considering multi-photon emission

a)

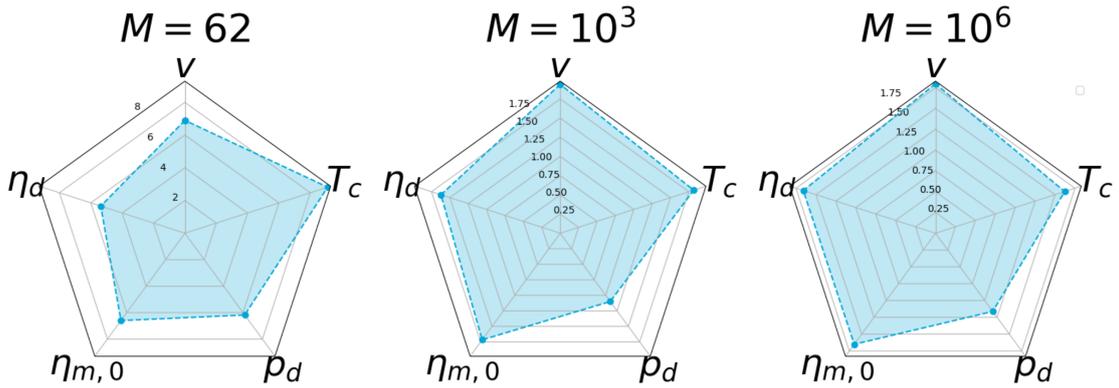|	M = 62	M = 10³	M = 10⁶	Baseline
T_c (ns)	8.14×10⁷	2.57×10⁶	1.96×10⁶	5.00×10⁸
η_d	0.95	0.65	0.57	0.8
$\eta_{m,0}$	0.94	0.60	0.57	0.52
p_d	8.79×10⁻⁵	6.91×10⁻⁴	6.40×10⁻⁴	1.00×10⁻⁵
v	0.97	0.74	0.76	0.9

b)

Figure 6.2: Absolute minimal hardware requirements to reach the target SKR $R_{sk,target} = 20$ Hz. Parameters: T_c = memory coherence time, η_d = detector efficiency, $\eta_{m,0}$ = maximum efficiency of the memory, p_d = detector dark count probability , v = visibility of the photons. To obtain the results we evaluate an atomic-ensemble-based single repeater setup connecting the cities of Delft and Eindhoven by setup N, defined in Figure 5.2. This setup deploys a double click protocol. Furthermore, we assume that the photon pair sources are perfect and the detectors are non number resolving. Results denote the least favourable value of the hardware parameter that allows us to reach SKR $R_{sk,target}$, given that the only other imperfection is photon loss in the fibers of the network. Moreover, we obtain the results by optimising the cost function in Equation 3.13 using Bayesian optimisation introduced in Section 3.3.1. Different number of multiplexing modes, M, are considered. **a)** Table containing the results for the absolute minimal hardware requirements. Besides, we show the baseline values of the hardware parameters. Baseline values correspond to current state-of-the art values [12, 72, 91, 92]. **b)** Unitless comparison to analyse the effect of setting a higher target SKR, $R_{sk,target}$, on absolute minimal hardware requirements. Plotted values comprise a comparison between absolute minimal hardware requirements for reaching $R_{sk,target} = 20$ Hz and $R_{sk,target} = 5$ Hz on setup N. The results are compared using the definition of the improvement factor in Equation 3.16. Comparison is done for different number of multiplexing modes, M.

compared to perfect photon pair sources. More asymmetric setups by definition must contain longer fibers. As per the heuristic defined by Equation 5.2, the mean photon number of the photon pair sources sending their photon through this long fiber must be higher. More asymmetric setups thus inherently have more multi-photon emission and their performance is as a result worse, regardless of the probability of success of the heralded entanglement generation. We also notice that this has an effect on the optimal values of the probability p_{surv} of a photon arriving at the heralding station in Figure 6.4. We observe that setup N generally allows for higher photon survival probability p_{surv} than setup U. As setup U inherently results in more multi-photon emission it is more sensitive to the negative effects of a higher photon survival probability p_{surv}. These might be a consequence of the heuristic we choose to implement, and by choosing the mean photon numbers differently it may be possible to mitigate this. We however suspect asymmetry will always have a negative effect on the fidelity of the state.

a)

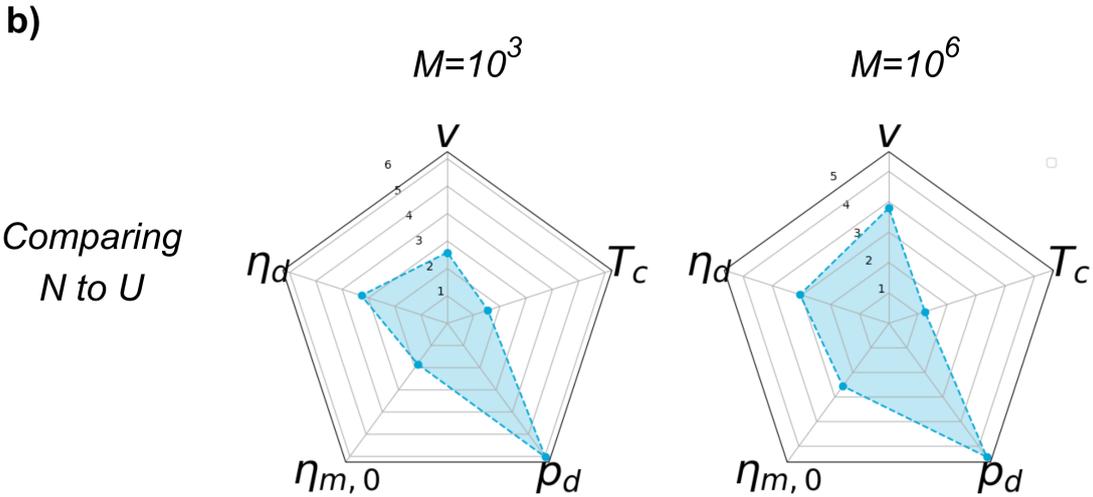|	N			U		Baseline
	$M = 62$	$M = 10^3$	$M = 10^6$	$M = 10^3$	$M = 10^6$	
T_c (ns)	1.67×10^9	7.01×10^8	6.29×10^6	1.08×10^9	7.79×10^6	5.00×10^8
η_d	0.98	0.69	0.22	0.89	0.61	0.8
$\eta_{m,0}$	0.97	0.75	0.29	0.86	0.62	0.52
p_d	1.76×10^{-4}	2.44×10^{-4}	2.43×10^{-4}	4.03×10^{-5}	4.48×10^{-5}	1.00×10^{-5}
v	0.90	0.83	0.20	0.93	0.65	0.9

b)

Figure 6.3: Absolute minimal hardware requirements to reach the SKR $R_{sk,target} = 10^{-3}$ Hz. Parameters: T_c = memory coherence time, η_d = detector efficiency, $\eta_{m,0}$ = maximum efficiency of the memory, p_d = detector dark count probability , v = visibility of the photons. To obtain the results we evaluate an atomic-ensemble-based single repeater setup connecting the cities of Delft and Eindhoven by setup N and U, defined in Figure 5.2. These setups deploy a double click protocol. Furthermore, we model photon pair sources after SPDC sources using the heuristic defined by Equation 5.2 to set the mean photon number of each respective photon pair source. The heuristic encapsulates that the probability p_{surv} that a single photon reaches the heralding station is equal across the setup. Results denote the least favourable value of the hardware parameter that allows us to reach SKR $R_{sk,target}$, given that the only other imperfection is photon loss in the fibers of the network. We obtain the results by optimising the cost function in Equation 3.14 using Bayesian optimisation introduced in Section 3.3.1. We present results for different number of multiplexing modes, M. **a)** Table containing the results for the absolute minimal hardware requirements. Besides, we show the baseline values of the hardware parameters. Baseline values correspond to current state-of-the art values [12, 72, 91, 92]. **b)** Unitless comparison of absolute minimal hardware requirements to analyse the effect of the placement of the repeater node using the definition of the improvement factor in Equation 3.16. For the node placement defined by configuration N and configuration U, as defined in Figure 5.2, are considered.
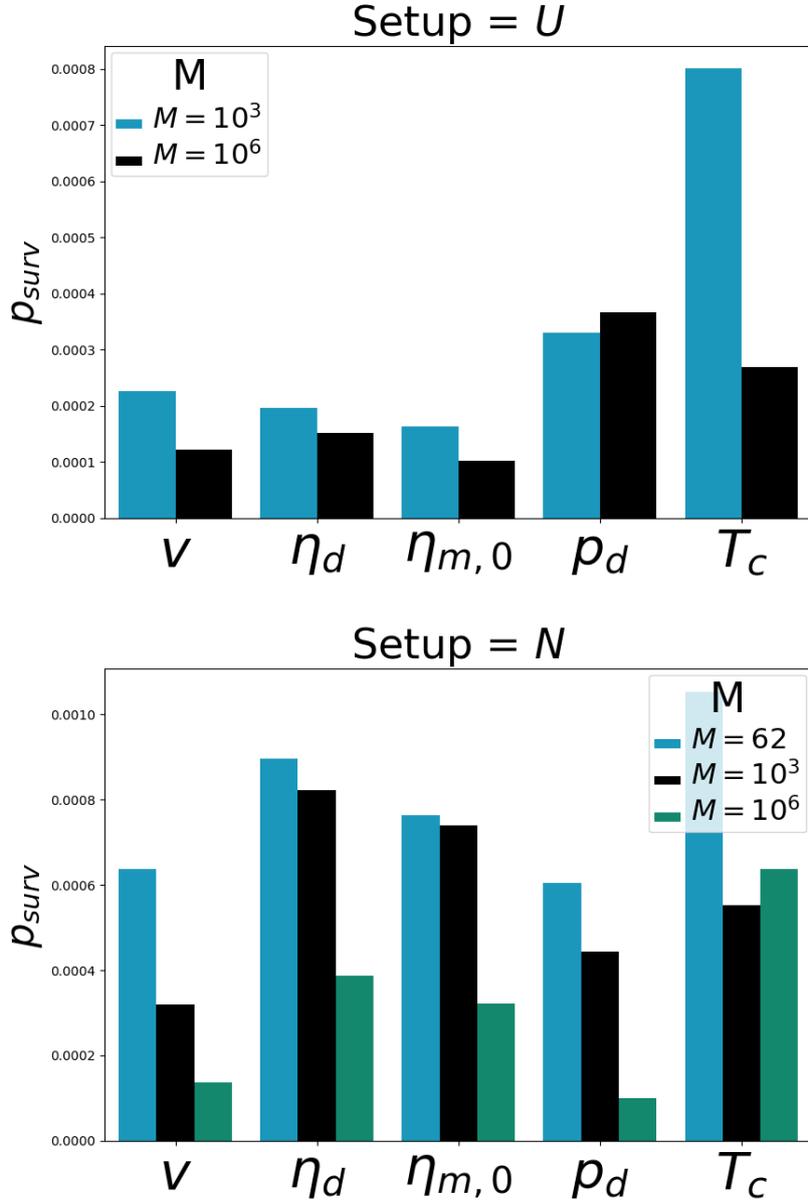
Figure 6.4: Optimal value of the probability p_{surv} that a photon arrives at the heralding station, corresponding to the absolute minimal hardware requirements to reach the target SKR $R_{sk,target} = 10^{-3}$ Hz. To obtain the results we evaluate an atomic-ensemble-based single repeater setup connecting the cities of Delft and Eindhoven by setup N and U, defined in Figure 5.2. These setups deploy a double click protocol. We use p_{surv} as a parameter to set the mean photon number of the photon pair sources in setup N and U, as defined by the heuristic in Equation 5.2. The heuristic encapsulates that the probability p_{surv} that a single photon reaches the heralding station is equal across the setup. Parameters: T_c = memory coherence time, η_d = detector efficiency, $\eta_{m,0}$ = maximum efficiency of the memory, p_d = detector dark count probability , v = visibility of the photons. We obtain the results by optimising the cost function in Equation 3.14 using Bayesian optimisation introduced in Section 3.3.1. Furthermore, we present results for different number of multiplexing modes, M. We remark a trend that a higher number of multiplexing modes results in a lower optimal value for p_{surv}.

Minimal hardware requirements

In this chapter we present the results for the optimisation of minimal hardware requirements.

7.1. Results

We remind the reader that we defined minimal hardware requirements as the least favourable set of hardware parameter that still allows the setup to reach a given target SKR, $R_{sk,target}$, in Section 3.2.3. We furthermore remind the reader that we consider two different setups for the repeater chain, setup N and setup U, as defined in Figure 5.2. We remarked that setup N is more symmetric than setup U. To allow for comparison we naturally choose to consider the same target SKR as in Chapter 6. Concretely, we perform an optimisation using a target SKR $R_{sk,target} = 5$ Hz and an optimisation using a target SKR $R_{sk,target} = 20$ Hz.

We present the results for minimal hardware requirements to reach target SKR $R_{sk,target} = 5$ Hz using perfect photon pair sources in Table 7.1. The table contains the results, the absolute minimal hardware requirements from Chapter 6, and the baseline values from Table 3.1. The baseline values correspond to current state-of-the art. To perform the optimisation, we empirically established that a good trade off between statistically significant results and compute time is achieved for $n = 200$ successful measurements in both measurement bases (i.e. 400 successful measurements in total). In line with the expectations, we observe an increase in hardware parameter values when comparing the results to the absolute minimal hardware requirements from Section 6.1. We point out that this increase is similar to results found in [10], where the authors perform a similar optimisation on different types of hardware.

We furthermore observe that current state-of-the art hardware is not sufficient to reach the target we set, even when considering perfect photon pair sources and multiplexing capabilities such that elementary entanglement generation becomes deterministic for practical purposes. We remark that once more especially the memory efficiency requires further improvement.

We also highlight that solutions illustrated in Table 7.1 are not unique solutions to the optimisation problem posed. Other solutions that optimise the setup might exist. For this reason we compare the effect of multiplexing and node placement not by the values of the hardware parameters, but rather by the value of cost function defined by Equation 3.18, corresponding to the solution. Moreover, we remark on the seemingly high requirements on memory coherence time, T_c, compared to the absolute minimal hardware requirements. These high requirements are a consequence of the baseline value presented in Table 3.1 already being sufficient, and the fact that the cost function defined by Equation 3.18 depends on the baseline values in a way that cost is added based on how much current state-of-the art hardware parameters are improved.

7.2. Effect of number of multiplexing modes and node placement

The values of the cost function of the solution are also in Table 7.1. We note that similar conclusions as those drawn from the absolute minimal requirements in Section 6.1.2 and Section 6.1.3 hold. Improving multiplexing capabilities from $M = 62$ to $M = 10^3$ leads to a big relaxation of hardware requirements. When further improving multiplexing capabilities from $M = 10^3$ to $M = 10^6$ the effect is significantly less. Additionally, setup N generally performs better than setup U, and increasing the number M of multiplexing modes mitigates the negative effect of the added asymmetry.

Table 7.1: Minimal hardware requirements (**MR**) to reach the target SKR $R_{sk,target} = 5$ Hz. To obtain the results we evaluate an atomic-ensemble-based single repeater setup connecting the cities of Delft and Eindhoven by setup N and U, defined in Figure 5.2. These setups deploy a double click protocol. Furthermore, we assume that the photon pair sources are perfect and the detectors are non number resolving. Results denote the least favourable set of hardware parameters that still allows us the reach SKR $R_{sk,target}$. Moreover, we obtain the results by optimising the cost function, C, in Equation 3.18 using the genetic algorithm introduced in Section 3.3.2. We present results for different different number of multiplexing modes, M. In addition to the results, we display the value of the cost function C of the solution. To allow for easy comparison, the table contains baseline values (**B**) [12, 72, 91, 92], which are current state-of-the art values. The table additionally contains the absolute minimal hardware requirements (**AMR**) from Figure 6.1

		N			**U**		
		$M = 62$	$M = 10^3$	$M = 10^6$	$M = 62$	$M = 10^3$	$M = 10^6$
Memory coherence time T_c (ns)	B				5.00×10^8		
	AMR	8.94×10^6	1.41×10^6	1.21×10^6	2.44×10^8	2.72×10^6	1.44×10^6
	MR	8.53×10^8	5.06×10^8	5.10×10^8	8.08×10^8	6.07×10^8	2.19×10^8
Detector efficiency η_d	B				0.8		
	AMR	0.75	0.50	0.40	0.93	0.60	0.41
	MR	0.91	0.73	0.78	0.99	0.75	0.70
Maximum memory efficiency $\eta_{m,0}$	B				0.52		
	AMR	0.66	0.42	0.40	0.90	0.50	0.41
	MR	0.86	0.78	0.60	0.93	0.84	0.73
Detector dark count probability p_d	B				1.00×10^{-5}		
	AMR	5.43×10^{-4}	7.60×10^{-4}	7.74×10^{-4}	6.13×10^{-5}	1.98×10^{-4}	1.61×10^{-4}
	MR	1.97×10^{-5}	1.89×10^{-5}	2.70×10^{-5}	9.01×10^{-7}	1.55×10^{-5}	2.95×10^{-5}
Photon visibility v	B				0.9		
	AMR	0.79	0.56	0.60	0.94	0.66	0.59
	MR	0.90	0.83	0.85	0.97	0.88	0.90
Total cost C	MR	9.95	5.37	4.22	50.1	7.15	4.46

7.3. Effect of setting a higher target

We now investigate the effect of setting a higher target SKR. To this end, we perform the optimisation for the minimal hardware requirements using a target SKR $R_{sk,target} = 20$ Hz. The results of this optimisation are in Figure 7.1.

A unitless comparison of the results between the minimal hardware requirements, one aiming for for target SKR $R_{sk,target} = 5$ Hz and the other for target SKR $R_{sk,target} = 20$ Hz is in b) of Figure 7.1. Once more, we see similar behaviour as with the absolute minimal requirements in Section 6.1.4. For current state-of-the art number of multiplexing modes $M = 62$ the required increase in hardware parameters is substantial when comparing to $M = 10^3$. When examining $M = 10^6$ afterwards, this required increase is lower.

We again stress that solutions found by solving the optimisation problem are not necessarily unique solutions. Thus, we verify our claims by looking at the values of the cost function as defined by equation 3.18. For the number of multiplexing modes $M = 62$ the cost function value of the solution increases from 9.95 to 68.3 when aiming for $R_{sk,target} = 5$ Hz compared to $R_{sk,target} = 20$ Hz. For the number of multiplexing modes $M = 10^3$ the cost function values are 5.37 and 7.66 respectively. For the number of multiplexing modes $M = 10^6$ they are 7.15 and 4.22. In conclusion, the results validate the claims made in Section 6.1.4.
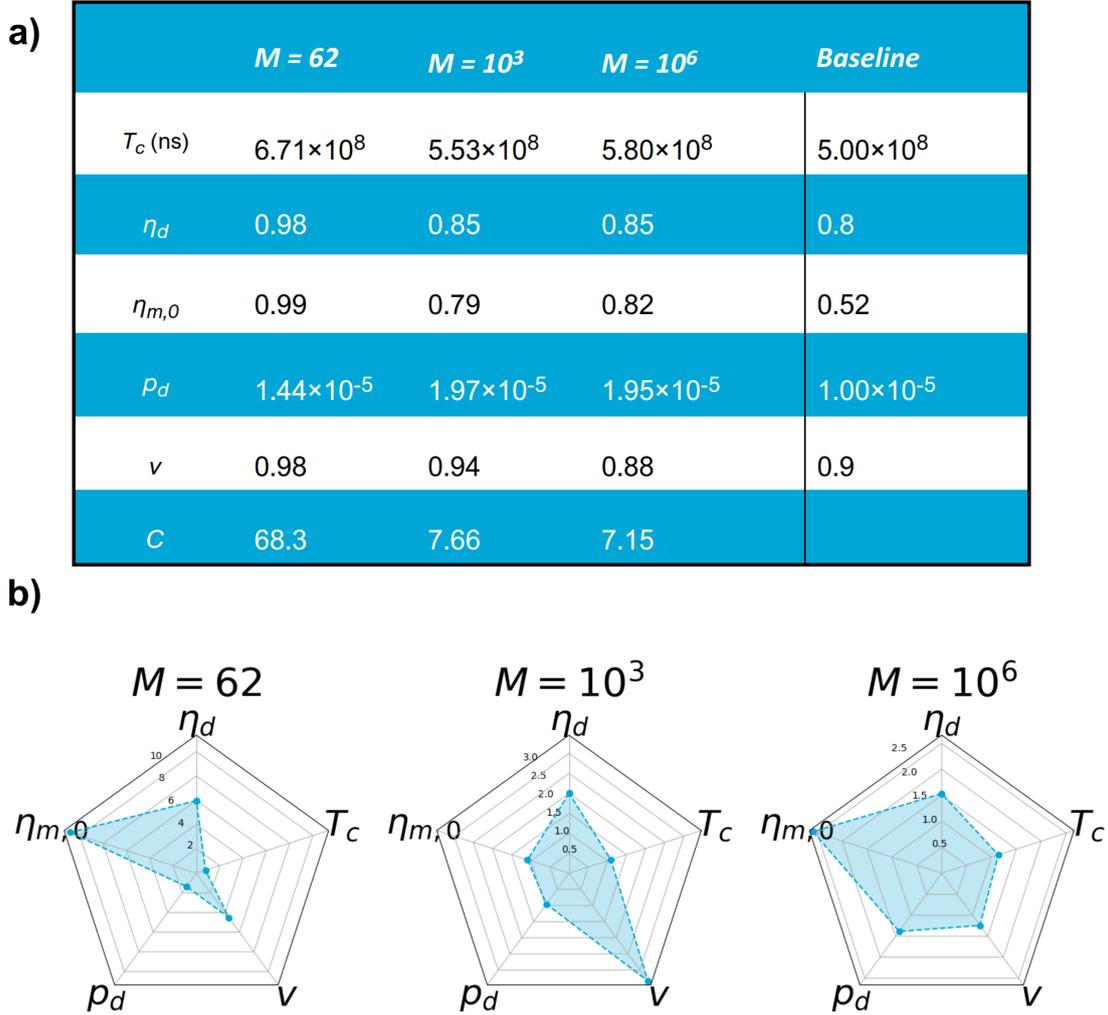
a)

	M = 62	M = 10³	M = 10⁶	Baseline
T_c (ns)	6.71×10^8	5.53×10^8	5.80×10^8	5.00×10^8
η_d	0.98	0.85	0.85	0.8
$\eta_{m,0}$	0.99	0.79	0.82	0.52
p_d	1.44×10^{-5}	1.97×10^{-5}	1.95×10^{-5}	1.00×10^{-5}
v	0.98	0.94	0.88	0.9
C	68.3	7.66	7.15	

b)

Figure 7.1: Minimal hardware requirements to reach the SKR $R_{sk,target} = 20$ Hz. Parameters: T_c = memory coherence time, η_d = detector efficiency, $\eta_{m,0}$ = maximum efficiency of the memory, p_d = detector dark count probability , v = visibility of the photons. To obtain the results we evaluate an atomic-ensemble-based single repeater setup connecting the cities of Delft and Eindhoven by setup N, defined in Figure 5.2. This setup deploys a double click protocol. Furthermore, we assume that the photon pair sources are perfect and the detectors are non number resolving. Results denote the least favourable set of hardware parameters that still allows us the reach SKR $R_{sk,target}$. Moreover, we obtain the results by optimising the cost function, C, in Equation 3.18 using the genetic algorithm introduced in Section 3.3.2. We present results for different number of multiplexing modes, M. **a)** Table containing the results for the minimal hardware requirements including the value of C corresponding to the solution. In addition to the results, the table contains baseline values. Baseline values correspond to current state-of-the art [12, 72, 91, 92]. **b)** Unitless comparison to analyse the effect of setting a higher target SKR, $R_{sk,target}$, on minimal hardware requirements. Plotted values comprise a comparison between minimal hardware requirements for reaching $R_{sk,target} = 20$ Hz and $R_{sk,target} = 5$ Hz on setup N. The results are compared using the definition of the improvement factor in Equation 3.16. Comparison is done for different number of multiplexing modes, M.

<div style="text-align: right; font-size: 3em;">8</div>
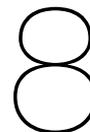
Conclusions and future research

8.1. Conclusions

The main objective of this thesis was to find (absolute) minimal hardware requirements of an atomic-ensemble-based repeater setup. Our purpose in doing this is to offer insights into improvements that are needed to realise a large-scale atomic-ensemble-based repeater. To achieve this, we enabled atomic-ensemble-based simulations making use of Netsquid-AE [15] and NLblueprint, as introduced in Section 3.1.2. We validated the working of these simulations by juxtaposing simulated outcomes with analytical results in Chapter 4. Subsequently, we developed code to enable Bayesian optimisation of hardware parameters using these simulations. Additionally, we modified code designed to perform a genetic algorithm. Initially the code was tailored for other kinds of Netsquid simulations [10, 18]. Following the customisation, our code also accommodates performing genetic algorithms on the atomic-ensemble-based simulations. Using this code absolute minimal hardware requirements and minimal hardware requirements have been found.

We infer conclusions from the absolute minimal hardware requirements in Chapter 6 and minimal hardware requirements in Chapter 7. To start with, we highlight the importance of multiplexing. Increasing multiplexing capabilities can lead both to relaxation in hardware parameters and increase in performance of the repeater setup. However, benefits reaped from multiplexing are saturated after a certain point. After this point increasing the number of multiplexing modes M provides only a limited impact.

Secondly, we note that the results obtained confirm that asymmetry in the setup has a negative effect on the performance of the repeater setup and results in stronger hardware requirements. This negative effect can be neutralised by increasing the number of multiplexing modes M, but as discussed in Section 6.1.3, stronger requirements on the coherence time T_c of the quantum memories will always remain with the protocol considered in this thesis.

Moreover, we remark that multi-photon emission proves a major challenge to the feasibility of atomic-ensemble-based repeater setups. The difficulties arising from multi-photon emission intensify when the setup is asymmetric. As a result of this, a high number M of multiplexing modes are necessary to mitigate the effect of multi-photon emission. Furthermore, we found that multi-photon emission will always hamper the performance of atomic-ensemble-based repeater chains. As such, a workaround to bypass multi-photon emission might offer merit. We provide a suggestion for this in Section 8.2.

We now further elaborate on the feasibility of atomic-ensemble-based quantum repeaters with the aim to provide direction to experimental progress. Firstly, we recommend increasing multiplexing capabilities. Results in this thesis suggest 10^3 multiplexing modes are a good target to aim for to allow for executing quantum applications. Furthermore we notice that current state-of-the art SNSPDs, such as [91], are quite satisfactory. We remark that implementation of a viable atomic-ensemble-based repeater setup requires improvement of the quantum memories. This highlights the importance of work such as [9], [60], and [72].

Additionally, we assess the potential real world performance of repeater setup, such as those considered, by delving into its potential to facilitate execution of the quantum application considered throughout this thesis; QKD. To this end, we compare the performance of the simulated setup to recent experimental results realising QKD. In this work, QKD was performed over a repeater-less ultra low-loss fiber. Here, a SKR of 6.5 Hz has been achieved over a distance of 421 km [106]. As the total distance covered by the fiber network considered in this thesis encompasses only 227 km, and

results in this thesis shown that even when considering perfect photon pair sources hardware needs to be improved to reach a SKR of 5 Hz, we conclude matching results form [106] will be challenging. We however also recognise that authors of [106] do not use the entanglement based version of QKD, and the used method is thus exclusive to QKD and unable to perform other quantum applications of interest. Experimental realisation of a setup such as the one considered in this thesis would thus be invaluable as proof-of-concept even if its performance is practically fruitless.

On top of this, reaching practically viable performance becomes an even more formidable task when considering realistic photon pair sources based on SPDC. Our results show that in this case reaching a SKR of 10^{-3} Hz already require improvement of current state-of-the art hardware. Reaching SKR on the order of Hz would require a huge increase in multiplexing capabilities. We thus conclude multi-photon emission emerging from considering SPDC sources proves a barrier to atomic-ensemble-based repeater setups.

This thesis highlights the viability of using optimisation techniques such as developed in [10], [11], and [83] to help realise a large-scale proof-of-concept quantum network. We recognise that to achieve such a proof-of-concept additional experimental effort is required and optimisation problems are beneficial to assist in making trade-offs regarding design choices of the network.

8.2. Future research

It would be worthwhile to compare the results of the optimisation of atomic-ensemble-based repeaters acquired in this thesis against results in [10], where the authors perform similar optimisation of the hardware parameters of color-center-based repeater schemes and nitrogen-vacancy-based repeater schemes. However, in [10] the authors use blind quantum computing to evaluate the performance of the repeater rather than QKD. We thus conclude that optimisation of atomic-ensemble-based repeater based on blind quantum computing would be of great use. We note that an additional challenge to realise this optimisation is the fact that atomic-ensemble-based nodes are not processing nodes, which means they do not possess the capability to perform quantum operations on the qubits they store in their memory [27, 28]. As this is a requirement for performing blind quantum computing [24], optimisation of atomic-ensemble-based repeater based on blind quantum computing requires the generated entanglement to be transferred to a processing node. As a first step to realise this optimisation we suggest considering this transfer to be perfect. This way comparisons can already be made. To improve on those results, more realistic transfer protocols could be considered. Furthermore, we highlight the merit of evaluating the performance of atomic-ensemble-based repeaters by noting that the objectives of the QIA program introduced in the introduction aims to perform blind quantum computing and not QKD.

What is more, the Netsquid-AE snippet also contains code to perform protocols that are more similar to the postselected one introduced in Section 2.3.4, known as single click protocols. Single click protocols generally produce higher entanglement generation rates, but produce states with lower fidelity [107]. This lower fidelity is amplified when considering setups that are asymmetric, such as the fiber network considered throughout this thesis. We thus deemed the double click protocol introduced in Section 2.5.2 more fit for the optimisation problem considered in this thesis. Investigating if single click protocols might result in higher performance on more symmetric setups might be rewarding. Furthermore, as we noted in Section 6.2.3 a more optimal way to deal with mean photon number of the photon pair sources might exist. More investigation in this direction might be advantageous.

To circumvent the issue regarding multi-photon emission the authors of [108] propose a setup based on single photon sources. This setup is shown in figure 8.1. The single photon source deterministically emits a photon that is sent to a 50:50 beam splitter. The photon is then with equal probability transmitted and collected into a fiber or collected into a quantum memory. Consequently, the photon collected into the fiber can then be sent to a heralding station enabling DLCZ-like protocols. We propose that investigation on the possible implementation of such setups might be fruitful. For the single photon pair sources we suggest to consider using quantum dots. Implementations of single photons sources using quantum dots have experimentally been shown [109, 110]. If everything is perfect, we expect implementation of the setup proposed to lead to a performance of the repeater chain similar to the case we defined as perfect photon pair sources. It would be interesting to incorporate a model of a single photon pair source in the numerical analysis and review the effect of possible hardware imperfections in this process on the performance. Results
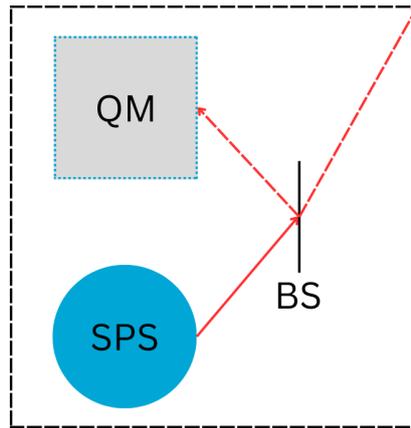
Figure 8.1: Proposition for a setup for a node using a Single Photon Source (SPS). The SPS deterministically emits a photon that is sent to a 50:50 Beam Splitter (BS). The photon is then either transmitted and collected into a fiber to be sent to a heralding station or collected in a Quantum Memory (QM). This would allow for DLCZ like protocols.

could then be compared to results obtained in this thesis to help decide whether investigating such using single photon sources might be fruitful.

We conclude this thesis by remarking that the integration that is a product of this thesis in principle allows to perform analysis of heterogeneous repeater chains including atomic-ensemble nodes. To illustrate, a repeater chain consisting of processing nodes, such as color-center nodes or nitrogen-vacancy nodes, and atomic-ensemble nodes could be made. In theory this allows for investigation of more complex quantum networks, hopefully helping to pave the way towards a future quantum internet.

Bibliography

[1] Barry M Leiner et al. "A brief history of the Internet". In: *ACM SIGCOMM computer communication review* 39.5 (2009), pp. 22–31.

[2] David J Griffiths and Darrell F Schroeter. *Introduction to quantum mechanics*. Cambridge university press, 2018.

[3] L. Susskind and A. Friedman. *Quantum Mechanics: The Theoretical Minimum*. The Theoretical Minimum. Basic Books, 2014. ISBN: 9780465080618.

[4] WK Wootters and WH Zurek. "A single quantum cannot be cloned". In: *Nature* 299.5886 (1982), pp. 802–803. DOI: `10.1038/299802a0`.

[5] Stephanie Wehner, David Elkouss, and Ronald Hanson. "Quantum internet: A vision for the road ahead". In: *Science* 362 (Oct. 2018).

[6] H-J Briegel et al. "Quantum repeaters: the role of imperfect local operations in quantum communication". In: *Physical Review Letters* 81.26 (1998), p. 5932.

[7] Stephanie Wehner. *The Quantum Internet Alliance will build an advanced European Quantum Internet ecosystem*. Oct. 2022. URL: `https://quantuminternetalliance.org/2022/10/14/the-quantum-internet-alliance-will-build-an-advanced-european-quantum-internet-ecosystem/`.

[8] Yong Yu et al. "Entanglement of two quantum memories via fibres over dozens of kilometres". In: *Nature* 578.7794 (2020), pp. 240–245.

[9] Dario Lago-Rivera et al. "Telecom-heralded entanglement between multimode solid-state quantum memories". In: *Nature* 594.7861 (2021), pp. 37–40.

[10] Guus Avis et al. "Requirements for a processing-node quantum repeater on a real-world fiber grid". In: *NPJ Quantum Information* 9.1 (2023), p. 100.

[11] Francisco Ferreira Da Silva et al. "Optimizing entanglement generation and distribution using genetic algorithms". In: *Quantum Science and Technology* 6.3 (2021), p. 035007.

[12] David Maier. "Investigating the scalability of Quantum repeater protocols based on atomic ensembles". QuTech, 2020.

[13] Julian Rabbie. "Simulation Model for Atomic Ensemble based Quantum Repeaters and the Optimization of their Positioning". QuTech, 2020.

[14] Tim Coopmans et al. "Netsquid, a network simulator for quantum information using discrete events". In: *Communications Physics* 4.1 (2021), p. 164.

[15] QuTech. *NetSquid-AE*. GitHub. 2023. URL: `https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-ae`.

[16] Saikat Guha et al. "Rate-loss analysis of an efficient quantum repeater architecture". In: *Physical Review A* 92.2 (2015), p. 022357.

[17] Tim Head et al. *scikit-optimize/scikit-optimize*. Version v0.9.0. Oct. 2021. DOI: `10.5281/zenodo.5565057`. URL: `https://doi.org/10.5281/zenodo.5565057`.

[18] SURFQuantum. *YOTSE: Your Optimization Tool for Scientific Experiments*. GitHub. 2023. URL: `https://github.com/SURFQuantum/yotse#yotse---your-optimization-tool-for-scientific-experiments`.

[19] Corning. *Corning®TXF®Optical fiber product information*. Brochure. 2023. URL: `https://www.corning.com/media/worldwide/coc/documents/Fiber/PI-1433-AEN.pdf`.

[20] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000. ISBN: 9780521635035.

[21] C.H. Benett and G. Bassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing". In: *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (1984), pp. 175–179.

[22] Artur K Ekert. "Quantum cryptography based on Bell's theorem". In: *Physical review letters* 67.6 (1991), p. 661.

[23] Dorit Aharonov, Michael Ben-Or, and Elad Eban. *Interactive Proofs For Quantum Computations*. 2008. arXiv: 0810.5375 [quant-ph].

[24] Joseph F Fitzsimons. "Private quantum computation: an introduction to blind quantum computing and related protocols". In: *npj Quantum Information* 3.1 (2017), p. 23.

[25] Charles H Bennett et al. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". In: *Physical review letters* 70.13 (1993), p. 1895.

[26] Dik Bouwmeester et al. "Experimental quantum teleportation". In: *Nature* 390.6660 (1997), pp. 575–579.

[27] Nicolas Sangouard et al. "Quantum repeaters based on atomic ensembles and linear optics". In: *Reviews of Modern Physics* 83.1 (2011), p. 33.

[28] William J Munro et al. "Inside quantum repeaters". In: *IEEE Journal of Selected Topics in Quantum Electronics* 21.3 (2015), pp. 78–90.

[29] Marek Zukowski et al. "" Event-ready-detectors" Bell experiment via entanglement swapping." In: *Physical review letters* 71.26 (1993).

[30] W. Tittel et al. "Photon-echo quantum memory in solid state systems". In: *Laser & Photonics Reviews* 4.2 (2010), pp. 244–267. DOI: https://doi.org/10.1002/lpor.200810056.

[31] Sreraman Muralidharan et al. "Optimal architectures for long distance quantum communication". In: *Scientific reports* 6.1 (2016), p. 20463.

[32] David Deutsch et al. "Quantum privacy amplification and the security of quantum cryptography over noisy channels". In: *Physical review letters* 77.13 (1996), p. 2818.

[33] Earl T Campbell and Simon C Benjamin. "Measurement-based entanglement under conditions of extreme photon loss". In: *Physical review letters* 101.13 (2008), p. 130502.

[34] Naomi H Nickerson, Joseph F Fitzsimons, and Simon C Benjamin. "Freely scalable quantum technologies using cells of 5-to-50 qubits with very lossy and noisy photonic links". In: *Physical Review X* 4.4 (2014), p. 041041.

[35] Charles H Bennett et al. "Purification of noisy entanglement and faithful teleportation via noisy channels". In: *Physical review letters* 76.5 (1996), p. 722.

[36] Dong Pyo Chi, Taewan Kim, and Soojoon Lee. "Efficient three-to-one entanglement purification protocol". In: *Physics Letters A* 376.3 (2012), pp. 143–146.

[37] Peter W Shor. "Scheme for reducing decoherence in quantum computer memory". In: *Physical review A* 52.4 (1995), R2493.

[38] Andrew M Steane. "Error correcting codes in quantum theory". In: *Physical Review Letters* 77.5 (1996), p. 793.

[39] Charles H Bennett et al. "Mixed-state entanglement and quantum error correction". In: *Physical Review A* 54.5 (1996), p. 3824.

[40] Raymond Laflamme et al. "Perfect quantum error correcting code". In: *Physical Review Letters* 77.1 (1996), p. 198.

[41] Liang Jiang et al. "Quantum repeater with encoding". In: *Physical Review A* 79.3 (2009), p. 032325.

[42] WJ Munro et al. "From quantum multiplexing to high-performance quantum networking". In: *Nature Photonics* 4.11 (2010), pp. 792–796.

[43] M Zwerger, HJ Briegel, and W Dür. "Hybrid architecture for encoded measurement-based quantum computation". In: *Scientific reports* 4.1 (2014), p. 5364.

[44] Austin G Fowler et al. "Surface code quantum communication". In: *Physical review letters* 104.18 (2010), p. 180503.

[45] Sreraman Muralidharan et al. "Ultrafast and fault-tolerant quantum communication across long distances". In: *Physical review letters* 112.25 (2014), p. 250501.

[46] William J Munro et al. "Quantum communication without the necessity of quantum memories". In: *Nature Photonics* 6.11 (2012), pp. 777–781.

[47] Filip Rozpędek et al. "Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes". In: *npj Quantum Information* 7.1 (2021), p. 102.

[48] Peter W. Shor and John Preskill. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol". In: *Physical Review Letters* 85.2 (July 2000), pp. 441–444. DOI: `10.1103/physrevlett.85.441`.

[49] Frederik Michel Dekking et al. *A Modern Introduction to Probability and Statistics: Understanding why and how*. Vol. 488. Springer, 2005.

[50] I.G. Hughes and T.P.A. Hase. *Measurements and their uncertainties*. Oxford, UK: Oxford University Press, 2010.

[51] L-M Duan et al. "Long-distance quantum communication with atomic ensembles and linear optics". In: *Nature* 414.6862 (2001), pp. 413–418.

[52] Carlos Cabrillo et al. "Creation of entangled states of distant atoms by interference". In: *Physical Review A* 59.2 (1999), p. 1025.

[53] S Bose et al. "Proposal for teleportation of an atomic state via cavity decay". In: *Physical Review Letters* 83.24 (1999), p. 5158.

[54] Lev Vaidman and Nadav Yoran. "Methods for reliable teleportation". In: *Physical Review A* 59.1 (1999), p. 116.

[55] Norbert Lütkenhaus, John Calsamiglia, and K-A Suominen. "Bell measurements for teleportation". In: *Physical Review A* 59.5 (1999), p. 3295.

[56] Stephen Wein et al. "Efficiency of an enhanced linear optical Bell-state measurement scheme with realistic imperfections". In: *Physical Review A* 94.3 (2016), p. 032332.

[57] Chin-Wen Chou. "Towards a quantum network with atomic ensembles". PhD thesis. California Institute of Technology, 2006. DOI: `10.7907/ANAH-0961`.

[58] Mikael Afzelius et al. "Multimode quantum memory based on atomic frequency combs". In: *Physical Review A* 79.5 (2009), p. 052329.

[59] Neil Sinclair et al. "Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control". In: *Physical review letters* 113.5 (2014), p. 053603.

[60] Antariksha Das et al. "A long-lived spectrally multiplexed solid-state optical quantum memory for high-rate quantum repeaters". In: *Proceedings of SPIE - The International Society for Optical Engineering* 12133 (2022). DOI: `10.1117/12.2620943`.

[61] OA Collins et al. "Multiplexed memory-insensitive quantum repeaters". In: *Physical review letters* 98.6 (2007), p. 060502.

[62] Christoph Simon et al. "Quantum repeaters with photon pair sources and multimode memories". In: *Physical review letters* 98.19 (2007), p. 190503.

[63] Ivan Marcikic et al. "Distribution of time-bin entangled qubits over 50 km of optical fiber". In: *Physical Review Letters* 93.18 (2004), p. 180502.

[64] Peter C Humphreys et al. "Linear optical quantum computing in a single spatial mode". In: *Physical review letters* 111.15 (2013), p. 150501.

[65] John M Donohue et al. "Coherent ultrafast measurement of time-bin encoded photons". In: *Physical Review Letters* 111.15 (2013), p. 153602.

[66] Robert W. Boyd. *Nonlinear Optics*. 3rd. USA: Academic Press, Inc., 2008. ISBN: 0123694701.

[67] Christophe Couteau. "Spontaneous parametric down-conversion". In: *Contemporary Physics* 59.3 (2018), pp. 291–304.

[68] Carlton M Caves et al. "Photon statistics of two-mode squeezed states and interference in four-dimensional phase space". In: *Physical Review A* 43.7 (1991), pp. 38–54.

[69] Cezary Śliwa and Konrad Banaszek. "Conditional preparation of maximal polarization entanglement". In: *Physical Review A* 67.3 (2003), p. 030101.

[70] Antia Lamas-Linares, John C Howell, and Dik Bouwmeester. "Stimulated emission of polarization-entangled photons". In: *Nature* 412.6850 (2001), pp. 887–890.

[71] Sacha Welinski et al. "Coherence time extension by large-scale optical spin polarization in a rare-earth doped crystal". In: *Physical Review X* 10.3 (2020), p. 031060.

[72] Adrian Holzäpfel et al. "Optical storage for 0.53 s in a solid-state atomic frequency comb memory using dynamical decoupling". In: *New Journal of Physics* 22.6 (2020), p. 063009.

[73] Y-W Cho et al. "Highly efficient optical quantum memory with long coherence time in cold atoms". In: *Optica* 3.1 (2016), pp. 100–107.

[74] Mohsen Falamarzi Askarani. "Telecom-wavelength quantum memories in rare earth ion-doped materials for quantum repeaters". PhD thesis. Delft Institute of Technology, 2019. DOI: `https://doi.org/10.4233/uuid:d418a98b-f2aa-4af3-b0e0-864875fcad2b`.

[75] A Luis and LL Sanchez-Soto. "A quantum description of the beam splitter". In: *Quantum and Semiclassical Optics: Journal of the European Optical Society Part B* 7.2 (1995), p. 153.

[76] H Fearn and R Loudon. "Quantum theory of the lossless beam splitter". In: *Optics communications* 64.6 (1987), pp. 485–490.

[77] Si Wang et al. "Research on the Hong-Ou-Mandel interference with two independent sources". In: *Scientific Reports* 9.1 (2019), p. 3854.

[78] Frédéric Bouchard et al. "Two-photon interference: the Hong–Ou–Mandel effect". In: *Reports on Progress in Physics* 84.1 (2020), p. 012402.

[79] Chong-Ki Hong, Zhe-Yu Ou, and Leonard Mandel. "Measurement of subpicosecond time intervals between two photons by interference". In: *Physical review letters* 59.18 (1987), p. 2044.

[80] Chandra M Natarajan, Michael G Tanner, and Robert H Hadfield. "Superconducting nanowire single-photon detectors: physics and applications". In: *Superconductor Science and Technology* 25.6 (Apr. 2012), p. 063001. DOI: `10.1088/0953-2048/25/6/063001`. URL: `https://dx.doi.org/10.1088/0953-2048/25/6/063001`.

[81] QuTech. *NetSquid-NetConf*. GitHub. 2023. URL: `https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-netconf`.

[82] QuTtech. *NetSquid-SimulationTools*. GitHub. 2023. URL: `https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-simulationtools`.

[83] Francisco Ferreira da Silva et al. "Requirements for upgrading trusted nodes to a repeater chain over 900 km of optical fiber". In: *arXiv preprint arXiv:2303.03234* (2023).

[84] Guus Avis et al. "Asymmetric node placement in fiber-based quantum networks". In: *arXiv preprint arXiv:2305.09635* (2023).

[85] Isaac L Chuang, Debbie W Leung, and Yoshihisa Yamamoto. "Bosonic quantum codes for amplitude damping". In: *Physical Review A* 56.2 (1997), pp. 11–14.

[86] Axel Dahlberg et al. "A link layer protocol for quantum networks". In: *Proceedings of the ACM special interest group on data communication*. 2019, pp. 159–173.

[87] Axel Dahlberg. "QuAlg–A symbolic algebra package for quantum information". In: *arXiv preprint arXiv:2008.06467* (2020).

[88] Stephanie Wehner, Nelly Ng, and Thomas Vidick. *Lecture notes Quantum Cryptography Week 1: Quantum tools and a first protocol*.

[89] QuTech. *NetSquid-Magic*. GitHub. 2023. URL: `https://gitlab.com/softwarequtech/netsquid-snippets/netsquid-magic`.

[90] Matteo Pompili et al. "Experimental demonstration of entanglement delivery using a quantum network stack". In: *npj Quantum Information* 8.1 (2022), p. 121.

[91] IDQuantique. *ID281 Superconductiong Nanowire Series*. Brochure. 2023. URL: `https://marketing.idquantique.com/acton/attachment/11868/f-023b/1/-/-/-/-/ID281_Brochure.pdf`.

[92] Stefano Duranti et al. "Efficient cavity-assisted storage of photonic qubits in a solid-state quantum memory". In: *arXiv preprint arXiv:2307.03509* (2023).

[93] Hana Jirovská. "Analysing the Effect of Asymmetry on the Performance of Atomic Ensemble Based Repeater Protocols". QuTech, TUDelft, 2021.

[94] Peter I Frazier. "A tutorial on Bayesian optimization". In: *arXiv preprint arXiv:1807.02811* (2018).

[95] Christopher M Bishop and Nasser M Nasrabadi. *Pattern recognition and machine learning*. Vol. 4. 4. Springer, 2006.

[96] Carl Edward Rasmussen, Christopher KI Williams, et al. *Gaussian processes for machine learning*. Vol. 1. Springer, 2006.

[97] Donald R Jones, Matthias Schonlau, and William J Welch. "Efficient global optimization of expensive black-box functions". In: *Journal of Global optimization* 13 (1998), pp. 455–492.

[98] Ahmed Fawzy Gad. "Pygad: An intuitive genetic algorithm python library". In: *arXiv preprint arXiv:2106.06158* (2021).

[99] Khalid Jebari, Mohammed Madiafi, et al. "Selection methods for genetic algorithms". In: *International Journal of Emerging Sciences* 3.4 (2013), pp. 333–344.

[100] Ahmad Hassanat et al. "Choosing Mutation and Crossover Ratios for Genetic Algorithms—A Review with a New Dynamic Approach". In: *Information* 10.12 (2019). ISSN: 2078-2489. DOI: `10.3390/info10120390`.

[101] Shengxiang Yang. "Genetic algorithms with elitism-based immigrants for changing optimization problems". In: *Workshops on Applications of Evolutionary Computation*. Springer. 2007, pp. 627–636.

[102] VP Patil and DD Pawar. "The optimal crossover or mutation rates in genetic algorithm: A review". In: *International Journal of Applied Engineering and Technology* 5.3 (2015), pp. 38–41.

[103] G. Avis. "Shortcuts towards fiber-based quantum networks". English. PhD thesis. Delft University of Technology, 2023. ISBN: 978-94-6483-200-6. DOI: `10.4233/uuid:d5548689-2e68-4960-ae7c-b475d82c7cd7`.

[104] Julian Rabbie et al. "Designing quantum networks using preexisting infrastructure". In: *npj Quantum Information* 8.1 (2022), p. 5.

[105] Lorenzo Stasi et al. "High-efficiency and fast photon-number resolving parallel superconducting nanowire single-photon detector". In: *arXiv preprint arXiv:2207.14538* (2022).

[106] Alberto Boaron et al. "Secure quantum key distribution over 421 km of optical fiber". In: *Physical review letters* 121.19 (2018), p. 190502.

[107] Adrià Labay-Mora, Francisco Ferreira da Silva, and Stephanie Wehner. "Reducing hardware requirements for entanglement distribution via joint hardware-protocol optimization". In: *arXiv preprint arXiv:2309.11448* (2023).

[108] Nicolas Sangouard et al. "Long-distance entanglement distribution with single-photon sources". In: *Physical Review A* 76.5 (2007), p. 050301.

[109] Natasha Tomm et al. "A bright and fast source of coherent single photons". In: *Nature Nanotechnology* 16.4 (2021), pp. 399–403.

[110] T Müller et al. "A quantum light-emitting diode for the standard telecom window around 1,550 nm". In: *Nature communications* 9.1 (2018), p. 862.

A

Analytical results for validation

The following is a summary of the analytical results for the Secret Key Rate and the Quantum Bit Error Rate obtained in [16] in terms of detector dark counts p_d, detector efficiency η_d, memory efficiency $\eta_{0,m}$, and transmittance of the fibers η_t. For further derivations and details the reader is referred to [16].

The overall success probability at nesting level n is given by

$$P_{succ} = \frac{1}{4s} \left[4s(1 - (1 - 4s_1)^M) \right]^{2^n}. \tag{A.1}$$

$4s$ and $4s_1$ are the success probability of a successful swap and successful link respectively and are given by

$$s = a + b + 2c, \tag{A.2}$$

$$s_1 = a_e + b_e + 2c_e. \tag{A.3}$$

a, b, c, a_e, b_e, and c_e are coefficients related to the quantum state of interest and are defined in terms of the noise parameters by

$$a = \frac{1}{8} \left[p_d^2(1 - A_r)^2 + A_r^2(1 - p_d)^2 \right], \tag{A.4}$$

$$b = \frac{1}{8} \left[2A_r p_d(1 - A_r)(1 - p_d) \right], \tag{A.5}$$

$$c = P_d(1 - p_d) \left[p_d(1 - B_r) + B_r(1 - p_d) \right]. \tag{A.6}$$

Here

$$A_r = \eta_d \eta_{m,0} + p_d(\eta_{m,0}\eta_d), \tag{A.7}$$

$$B_r = 1 - (1 - p_d)(1 - \eta_d\eta_{m,0})^2. \tag{A.8}$$

Furthermore,

$$a_e = \frac{1}{8} \left[p_d^2(1 - A_e)^2 + A_e^2(1 - p_d)^2 \right], \tag{A.9}$$

$$b_e = \frac{1}{8} \left[2A_e p_d(1 - A_e)(1 - p_d) \right], \tag{A.10}$$

$$c_e = P_d(1 - p_d) \left[p_d(1 - B_e) + B_e(1 - p_d) \right]. \tag{A.11}$$

Here

$$A_e = \eta_d \eta_{m,0} \eta_t + p_d(\eta_{m,0}\eta_d\eta_t), \tag{A.12}$$

$$B_e = 1 - (1 - p_d)(1 - \eta_d\eta_{m,0}\eta_t)^2. \tag{A.13}$$

A_d is defined as

$$A_d = \eta_d\eta_{0,m} + (1 - \eta_d\eta_{0,m})p_d. \tag{A.14}$$

Using A_d the sift probability P_1 can be computed as

$$P_1 = (q_1 + q_2 + q_3)^2 \tag{A.15}$$

where

$$q_1 = (1 - p_d)A_d, \tag{A.16}$$
$$q_2 = (1 - A_d)p_d, \tag{A.17}$$
$$q_3 = p_d A_d. \tag{A.18}$$

Finally, the overall success rate R_{succ} can be computed

$$R_{succ} = \frac{P_{succ}P_1}{2T_q}. \tag{A.19}$$

Furthermore, the QBER is given by

$$QBER = \frac{1}{2}\left(1 - \frac{t_d}{t_r}(t_r t_e)^{2^n}\right). \tag{A.20}$$

Here

$$t_e = \frac{1 - 2w_1}{1 + 2w_1}, \tag{A.21}$$
$$t_r = \frac{1 - 2w_2}{1 + 2w_2}, \tag{A.22}$$
$$t_d = \frac{q_1 - q_2}{(q_1 + q_2 + q_3)^2}, \tag{A.23}$$
$$w_1 = \frac{c_e}{a_e + b_e}, \tag{A.24}$$
$$w_2 = \frac{c}{a + b}. \tag{A.25}$$