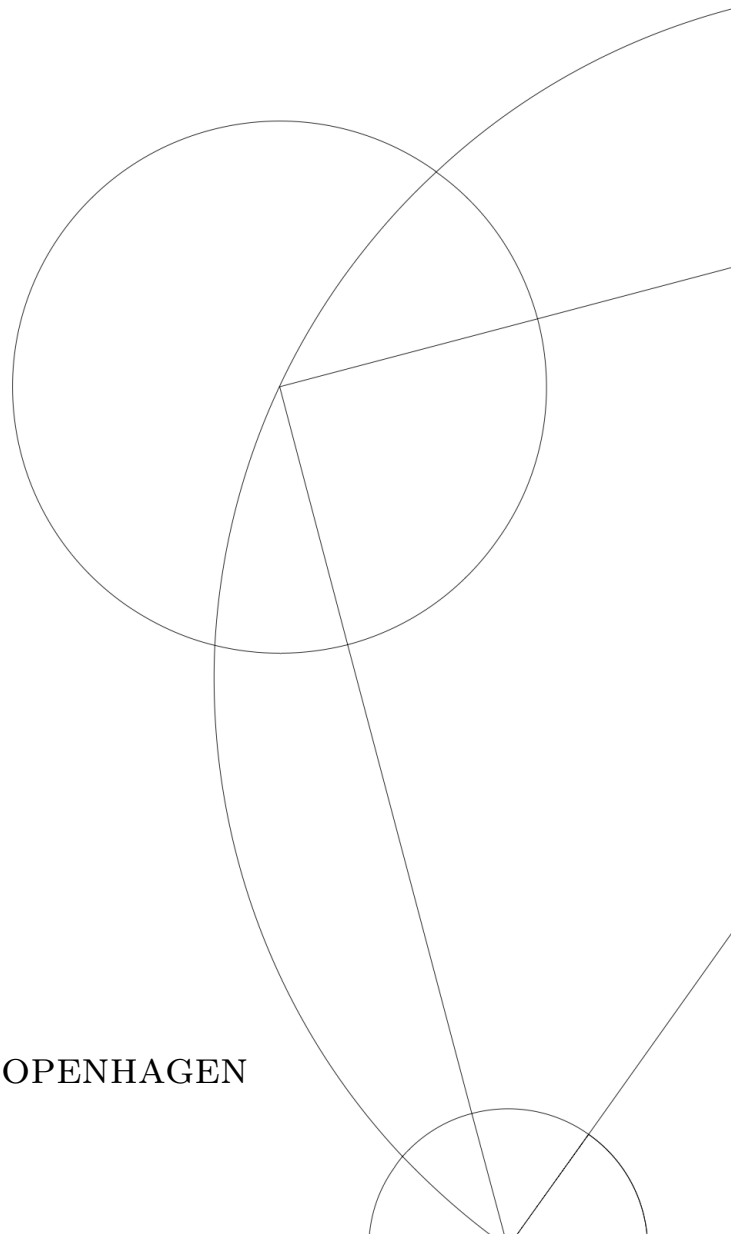
Quantum Key Distribution and Entanglement Distribution with Satellite Links

Master's Thesis

Written by *Anton Lauenborg Andersen*

30th September 2020

Supervised by
Anders Søndberg Sørensen



University of Copenhagen

This page is intentionally left blank.

Abstract

The efficient distribution of quantum states over global distances constitutes a key challenge in the implementation of quantum communication protocols. While direct transmission through optical fibres allows for quantum key distribution up to a few hundred kilometres [1], achieving truly global distances remains impossible due to the exponential decay of photon transmission in fibres. To overcome this, satellite links have been proposed, and demonstrated to distribute entangled pairs of photons between two parties separated by more than 1100 km [2, 3]. However, the two photon count rate at the ground stations is limited due to the two-photon transmission being 56 to 71 dB. To overcome this, we study the inclusion of quantum memories to the satellite, which will make the rate depend on the one-photon transmission instead, thereby potentially increasing the rate by three orders of magnitude. For quantum key distribution, we find that the implementation of state-of-the-art quantum memories allows us to reach the same rate as the current satellites [2, 3]. We suggest an uplink protocol requiring two memory qubits in the satellite with a coherence time of 0.2 s, in order to reach a two photon count rate of 1.1 Hz. For the distribution of entanglement, we find the setup without memories in the satellite to yield the highest rate of entangled memories, requiring two orders of magnitude less memory qubits at the ground than the proposals with quantum memories in the satellite, in order to reach the same rate.

Acknowledgments

First and foremost I should thank Anders, the little more than a year that I have spent on this masters' project have, without comparison, been the most enjoyable part of my education. I very much appreciate the chance that I have gotten to be part of his group. And I should thank him for the time he has spent on our weekly meetings and for, during a meeting last fall, telling me: *"Kan du ikke bare for én gangs skyld vise noget entusiasme?"*

I should also thank Bastian, Svend, Maria and Caroline for patiently listening to me explain my project and for proofreading parts of the thesis. I particularly owe a great deal of the project to Eva who have helped me countless times, both in understanding the physics behind this thesis and for helping me refine the structure of the thesis.

Finally, I think it would be fun to thank my mom and dad, partially because they will probably never read this. They both provide me with their excellent guidance when I need it the most.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter introduces quantum cryptography by explaining the BB84 protocol for quantum key distribution. We then move on to introduce the Einstein–Podolsky–Rosen protocols and measurement-device-independent quantum key distribution. Furthermore we introduce the challenge of performing quantum key distribution over global distances, and consider how satellite links can be employed to overcome the limitations posed by fibre links. Finally we present the main proposal of this thesis, by considering the addition of quantum memories to the satellite and see how that affects the rate of communication.

1.1 Quantum Cryptography

Secure communication between two parties is of upmost importance. From bank transactions to war planning, there is a global need for communication without unwanted parties listening in. However, the advances made on quantum computing [4], and Peter Shor's algorithm for prime factorisation [5] poses a serious threat to classical cryptography. Fortunately, quantum mechanics also provides a solution for safe communication in the form of quantum cryptography.

In order to explain quantum cryptography we will consider the classical story of the two communicating parties Alice and Bob [6]. Suppose that Alice have a secret message m in the form of a bit-string that she would like Bob to have. Furthermore we assume that Alice and Bob share a random bit-string k of the same length as m, that only they know. For Alice to send the secret message to Bob she will create a new bit-string $s = m \oplus k$ ($\oplus$ is the binary addition modulo 2 without carry), which she send to Bob via a public channel. When Bob receives s he will simply add the key to it again, $s \oplus k = m \oplus k \oplus k = m$, thereby recovering the message. In this way Alice has effectively shared the information in m with Bob. The secrecy of the message is secured by k being completely random such that no useful information can be inferred from s without the knowledge of k, and by the fact that only Alice and Bob knows k. We will now explore a few proposals for how to use the fundamental principles of quantum mechanics to generate a key satisfying these criteria in a process known as quantum key distribution (QKD).

1.1.1 The BB84 Protocol

The first protocol for QKD was proposed by Bennet and Brassard in 1984 [7], thereby acquiring the name BB84. It provides a way for Alice and Bob to establish a shared secret key k, thereby

Alice	Bit-string	0	1	0	1	0	1	1	1	1	1	0	1	1
	Basis	X	X	X	X	Z	X	Z	X	Z	X	X	Z	Z
	Polarisation	$\nearrow$	$\searrow$	$\nearrow$	$\searrow$	$\uparrow$	$\searrow$	$\rightarrow$	$\searrow$	$\rightarrow$	$\searrow$	$\nearrow$	$\rightarrow$	$\rightarrow$
Bob	Basis	X	Z	Z	X	X	X	X	X	Z	X	Z	Z	Z
	Measurement	$\nearrow$	$\uparrow$	$\rightarrow$	$\searrow$	$\searrow$	$\searrow$	$\nearrow$	$\searrow$	$\rightarrow$	$\searrow$	$\uparrow$	$\rightarrow$	$\rightarrow$
	Bit-string	0	0	1	1	1	1	0	1	1	1	0	1	1
Comparing basis		✔	✘	✘	✔	✘	✔	✘	✔	✔	✔	✘	✔	✔
Check of random bits							1			1	1			1
Sifted Key		0			1				1				1	

Table 1.1: Overview of the different steps of the BB84 protocol.

allowing them to encrypt a message in the way described above. We will explain the protocol using polarisation encoded photons as qubits, but it should become clear that the principles behind the protocol are far more general than this specific choice that we have made. The protocol assumes that Alice has some way of generating a random bit-string.

Furthermore it assumes that Alice is able to knowingly able to create four different quantum states belonging to two different bases. Here we use polarisation of a photon such that the four states are $|\uparrow\rangle$ and $|\rightarrow\rangle$ for the vertical and horizontal polarisation states respectively (which constitutes the Z basis), and $|\nearrow\rangle$ and $|\searrow\rangle$ for the $+45°$ and $-45°$ polarisation states respectively (which constitutes the X basis). Alice and Bob should also beforehand have agreed on assigning value 0 to the states $|\uparrow\rangle$ and $|\nearrow\rangle$ and the value 1 to the states $|\rightarrow\rangle$ or $|\searrow\rangle$. For each bit in her bit-string Alice will chose at random a basis to encoded it in, and send the a photon with the corresponding polarisation to Bob. When the photons arrive at Bob, he will at random choose a basis to measure the state that he receives, and convert it back to a bit. If Bob randomly chooses the basis in which Alice had encoded the photon, then Bob will get the correct bit in his bit-string. If on the other hand Bob measures in the wrong basis the outcome will be completely random and there will be a 50% chance that he gets the correct bit. After Alice and Bob are done exchanging photons, they will compare basis via a public classical channel and keep only the parts of the bit-string where Alice encoded in the same basis that Bob measured in. We should note that this step does not comprise the security of the protocol, as anyone listening in on this conversation will not be able to infer the outcome of Bob's measurements, only the basis. An overview of the steps of the BB84 protocol can be seen in table 1.1.

At this point it might not be apparent why Alice and Bob need to have two different basis, after all they seem to only lower the speed at which they are able to communicate. To understand this part of the protocol we should consider what an eavesdropper, who we will refer to as Eve, could gain by intercepting the photons as they travel from Alice to Bob. One tactic Eve might employ is to measure the polarisation of the photons. This will not work as any measured photon will not arrive at Bob, meaning that in the comparison phase of the protocol Alice and Bob will simply not select those bits to be part of the final bit-string. Another tactic Eve might employ is to try to make a copy of the photon as it passes her by. Let $|\psi\rangle_A$ be the state of the photon from Alice, and $|i\rangle_E$ be the initial state which Eve wishes to be a copy of $|\psi\rangle_A$. To copy the sate Eve then needs to perform the transformation $|\psi\rangle_A |i\rangle_E \rightarrow |\psi\rangle_A |\psi\rangle_E$, however the *no-cloning theorem* [8] states

that such a transformation is not possible to perform.[1] Therefore Eve can not simply copy the state in transfer from Alice to Bob. Finally we will consider the *intercept-resend strategy* where Eve measures each qubit in either the X or Z basis, and sends a photon similar to the outcome of her measurement. This will however reveal her presence, as this will lead to a 25% error rate in the final key, which may be discovered if Alice and Bob check random bits of the key [6].

1.1.2 The EPR Protocols

We will now discuss another type of QKD protocol utilising the Einstein–Podolsky–Rosen paradox [9]. For these protocols a third party, creates a maximally entangled state, for example the singlet state,

$$\left|\psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|H\right\rangle_a\left|V\right\rangle_b - \left|V\right\rangle_a\left|H\right\rangle_b\right), \tag{1.1}$$

where we have used $|H\rangle$ for horizontal polarisation and $|V\rangle$ for vertical polarisation. One photon is sent to Alice while the other is sent to Bob. Like in BB84, they both at random choose to measure their photon in either the Z or X basis, after which they compare their choice of basis via a public calssical channel and keep their measurement outcome if their choice of basis matches. The first protocol of this type, commonly referred to as Ekert91, was proposed by Ekert in 1991 [10]. He connected the security of the protocol with the violation of the CHSH inequality [11]. The following year Bennett, Brassard and Mermin criticised Ekert's proposal and highlighted its similarity with the BB84 protocol, by making an EPR version of this protocol known as BBM92 [12].

Recent developments of this type of protocols include the device-independent quantum key distribution protocol (DI-QKD)[13, 14], so called because Alice and Bob are completely agnostic about how the quantum apparatuses involved operate. DI-QKD makes the fewest possible assumptions on Alice and Bob's trust in their experimental devices, and security relies on violation of Bell's inequality (See [15] for a more complete overview of DI-QKD).

1.1.3 Measurement-Device-Independent Quantum Key Distribution

Finally we will discuss the the measurement-device-independent quantum key distribution (MDI-QKD) protocol [16]. This protocol may be thought of as an EPR protocol flipped on its head. Alice and Bob independantly prepare at random one of the four polarisation states $|H\rangle, |V\rangle, |+\rangle$ or $|-\rangle$, where we have defined the X eigenstates $|\pm\rangle = (|H\rangle \pm |V\rangle)\sqrt{2}$. Then they will send their states to a central station Charlie, who will measure the states in the Bell state basis $\{|\phi^{+}\rangle, |\phi^{-}\rangle, |\psi^{+}\rangle, |\psi^{-}\rangle\}$,

[1] Specifically the operator U copying the state by $U\left|\psi\right\rangle_A\left|0\right\rangle_E = \left|\psi\right\rangle_A\left|\psi\right\rangle_E$, for all $|\psi\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$ is not unitary.

where the four Bell states are the four maximally entangled states:

$$\begin{aligned}
\left|\phi^{+}\right\rangle_{a,b} &= \frac{1}{\sqrt{2}}\left(|H\rangle_a |H\rangle_b + |V\rangle_a |V\rangle_b\right) = \frac{1}{\sqrt{2}}\left(|+\rangle_a |+\rangle_b + |-\rangle_a |-\rangle_b\right), \\
\left|\phi^{-}\right\rangle_{a,b} &= \frac{1}{\sqrt{2}}\left(|H\rangle_a |H\rangle_b - |V\rangle_a |V\rangle_b\right) = \frac{1}{\sqrt{2}}\left(|+\rangle_a |-\rangle_b + |-\rangle_a |+\rangle_b\right), \\
\left|\psi^{+}\right\rangle_{a,b} &= \frac{1}{\sqrt{2}}\left(|H\rangle_a |V\rangle_b + |V\rangle_a |H\rangle_b\right) = \frac{1}{\sqrt{2}}\left(|+\rangle_a |+\rangle_b - |-\rangle_a |-\rangle_b\right), \\
\left|\psi^{-}\right\rangle_{a,b} &= \frac{1}{\sqrt{2}}\left(|H\rangle_a |V\rangle_b - |V\rangle_a |H\rangle_b\right) = \frac{1}{\sqrt{2}}\left(|+\rangle_a |-\rangle_b - |-\rangle_a |+\rangle_b\right).
\end{aligned} \tag{1.2}$$

Charlie will announce the result and Alice and Bob will compare their basis of encoding to discard the events where they chose different bases. From the measurement announced by Charlie and their knowledge of their own photon, Alice and Bob are thus able to deduce the state sent by the other part. For the specific implementation of Bell state measurement (BSM) that we will consider in this thesis, only detection of the odd parity sates $|\psi^{\pm}\rangle$ is possible (this will be covered in section 2.3.2), but this in not a problem for the operation of the protocol [16].

1.2 Global Distance QKD and Satellites

Common to the protocols described above is a reliance on the transport of qubits. Specifically we have considered qubits encoded in the form of the polarisation of single photons.[2] With the introduction of single photons we should also consider the ubiquitous influence of photon loss. Transmission through optical fibres is an obvious choice for intra- and inter-city distances, and while MDI-QKD using a 404 km long coiled fibre has been done at short distances [1], implementing QKD over global distances ($>$ 1000 km) by direct fibre links becomes impossible due to the exponential decay in photon transmission as a function of length. With state-of-the-art optical fibres having a loss of 0.16 dB/km (as was used in [1]), a 1000 km long fibre would mean 160 dB loss. If Alice used a single photon source emitting photons at with a 10 GHz rate, through such a fibre, Bob would get one photon on average every 11.5 days, making any practical communication utterly infeasible. To overcome this limitation two main venues have been proposed: quantum repeaters and satellite links. This thesis will mainly be concerned with the satellite link proposal, but quantum repeaters will briefly be revisited in chapter 4.

The satellite link QKD in its simplest form implements a EPR protocol, wherein the satellite sends entangled photon pairs from space down to Alice and Bob on the ground. The advantage of utilising satellite links, is that loss predominantly occurs in the lower parts of the atmosphere [2], whit the loss in the upper parts of the atmosphere will be dominated by diffraction. In 2016 the *Micius* satellite was launched to an altitude of $\sim$ 500 km, carrying a source of polarisation entangled photons [2, 3]. A violation of the CHSH type of Bell inequality was first reported in 2017, by achieving the CHSH parameter $S = 2.37 \pm 0.09$ with a ground separation of 1203 km [2]. With the source onboard the satellite emitting 5.9 million entangled photons pairs per second, and a two photon loss of 64 dB to 82 dB, an average two photon count rate at the ground stations of 1.1 Hz was measured. In 2020 the satellite was used to implement the BBM92 protocol

[2] If Alice, in order to combat loss, chooses to send two or more photons per bit of her bit-string, she compromises the security of the protocol. In this case Eve might take one of the photons, store it and measure it after Alice and Bob have compared basis. This type of attack is known as a photon-number-splitting attack and can be combated by decoy-state techniques [17], but the average photon number per bit form Alice still needs to be close to one.

[12], to perform QKD to ground stations separated by 1120 km [3]. With various improvements the two photon loss was lowered to 56 dB to 71 dB, thereby increasing the average two photon count rate to 2.2 Hz. Again the CHSH inequality was violated with $S = 2.56 \pm 0.07$ being reported.

We may understand the two-count photon rate of the experiment through classical probability calculations. We let R_s denote the source brightness, i.e. the number of emitted photon pairs per second. Assuming for simplicity that the probability of photon transmission to the ground p_d is the same for the two stations we may calculate the two-photon count rate as,

$$R = p_d^2 R_s. \tag{1.3}$$

From the reported numbers in [3] of $R_s = 5.9 \times 10^6$ Hz and using $p_d^2 = 10^{-6.35}$ as the average two photon transmission we get $R = 2.6$ Hz, without taking detector efficiency into account, which is reasonably close to the achieved rate. While the ability for two parties separated by more than 1000 km to perform QKD is a major technological achievement, the rate at which they are able to do it is still low, thereby limiting the practical use of the QKD. The main topic of this thesis will be to explore how to improve the performance for satellite based QKD.

1.3 Beating Quadratic Scaling

One way of overcoming the poor rate of the protocol, is by adding memories to the satellite. With the addition of memories to the satellite it becomes possible to circumvent the requirement of needing two photons to arrive at the ground at the same time. This is done by having the satellite talk independently to Alice and Bob. A way of implementing this can be seen in figure 1.1. The satellite now has two photon sources, each producing the bell state $|\psi^+\rangle$, but this time sending only one photon to the ground while the other is loaded into the memory.

Let a be the mode which is loaded onto the memory and α the mode sent to Alice for detection. She will then at random choose to measure the polarisation of the photon in the Z- or the X-basis thereby determining the polarisation of the photon in the memory of the satellite according to table 1.2. Upon the arrival of a photon to Alice she will send a signal to the satellite with the information of the time of arrival of the photon, thereby letting it know which photon in the memory corresponds to the one that reached Alice. The procedure for Bob is the same and occurs simultaneous. Once both Alice and Bob have received a photon from the satellite, the satellite will perform a Bell state measurement on the two qubits in the memories corresponding to the transmitted photons, and announce the result. Alice and Bob are then able to construct their shared key in a manner similar to MDI-QKD.[3]

By now it might not be obvious why this should lead to a higher rate than the other protocol. To see this we will calculate the rate of the protocol. We start by discretising time and considering the photon sources as sources emitting an entangled pair of photons with probability p_s per time step. Then we calculate the expectation value of the number of attempts needed for the protocol

[3] Although the logic for Alice and Bob to construct their keys is similar to MDI-QKD, the protocol used is actually an EPR-protocol. This is because the state which Alice and Bob performs measurements on is created in the satellite.

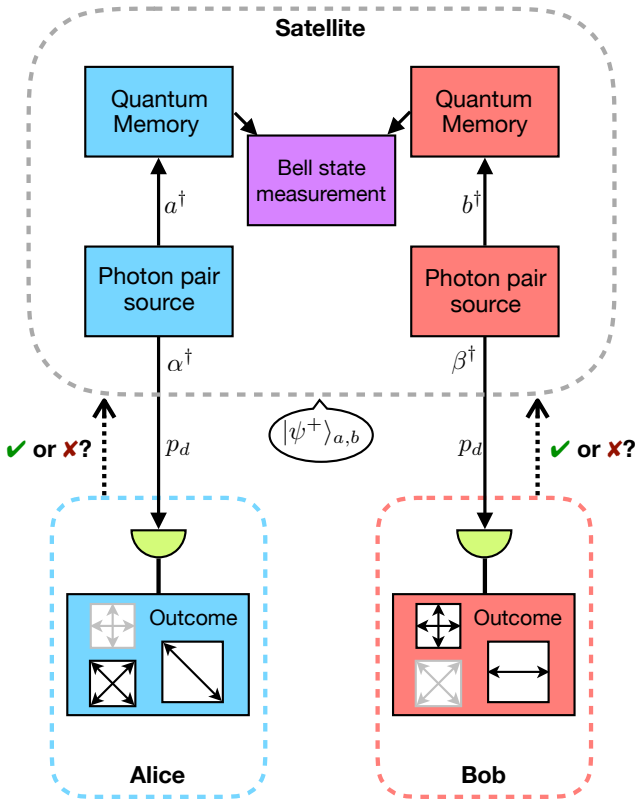


Figure 1.1: Satellite QKD with memory in the satellite. Alice and Bob will again have the choice to measure in the X or Z basis, and report back to the satellite if they received a photon or not. After both Alice and Bob have detected a photon the satellite will perform a Bell state measurement on the corresponding qubits stored in the memory and announce the result.

to succeed $\langle n \rangle$. Once this is done we may find the rate as the inverse of this,

$$R = \frac{1}{\langle n \rangle} \eta_{swap} r_{rep}, \tag{1.4}$$

where η_{swap} is the efficiency of the Bell state measurement in the satellite and r_{rep} is the rate of attempts i.e. the inverse of the discretised time step.

The expected number of attempts can be calculated as a weighted average,

$$\langle n \rangle = \sum_{n=1}^{\infty} n\, p(n), \tag{1.5}$$

where $p(n)$ is the probability of the protocol being successful on attempt n. When memories are added to the satellite the protocol succeeds if both Alice and Bob have created entanglement with the satellite. Let n_a (n_b) be the attempt in which Alice (Bob) creates entanglement, an example of which is shown in figure 1.2. The expected number of attempts needed for both Alice and Bob

Basis	Measurement	State in memory
X	$\|+\rangle_\alpha$ $\|-\rangle_\alpha$	$\|+\rangle_a$ $\|-\rangle_a$
Z	$\|H\rangle_\alpha$ $\|V\rangle_\alpha$	$\|V\rangle_a$ $\|H\rangle_a$

Table 1.2: By measuring the polarisation of the photon which reaches Alice, she determines the polarisation of the photon loaded onto the memory in the satellite. The table assumes that the photons are entangled in the state $\left|\psi^+\right\rangle = \left(|H,V\rangle + |V,H\rangle\right)/\sqrt{2}$.

Attempt	1	2	3	4	5	6	7
Alice	✘	✘	✔				
Bob	✘	✘	✘	✘	✘	✘	✔

Figure 1.2: Example of a single run of the protocol where $n_a = 3$, $n_b = 7$, $n_{min} = \min(n_a, n_b) = 3$ and $\Delta = |n_a - n_b| = 4$. Check marks indicate successful entanglement generation while crosses indicate failure. The inclusion of a memory in the satellite allows Alice to store her qubit while she waits for Bob to create entanglement with the satellite.

to create entanglement with the satellite is then given by,

$$\langle n \rangle = \sum_{n=1}^{\infty} \max\left(n_a, n_b\right) p(n_a, n_b), \qquad \text{where,} \qquad p(n_a, n_b) = p_e^2 \left(1 - p_e\right)^{n_a + n_b - 2}, \tag{1.6}$$

where we have introduced $p_e = p_s p_d$ the probability that Alice receives a photon per attempt. To evaluate the sum it is convenient to rewrite this in terms of the attempt of the first entanglement creation $n_{min} = \min\{n_a, n_b\}$ and the number of attempts between entanglement is created for Alice and Bob $\Delta = |n_a - n_b|$. This yields,

$$p(n_{min}, \Delta) = \begin{cases} p_e^2 \left(1 - p_e\right)^{2n_{min} - 2} & \text{if } \Delta = 0 \\ 2p_e^2 \left(1 - p_e\right)^{2n_{min} + \Delta - 2} & \text{if } \Delta \neq 0 \end{cases} \tag{1.7}$$

which when plugged into equation 1.6 and evaluating the resulting geometric series gives,

$$\langle n \rangle = \sum_{n_{min}=1}^{\infty} \sum_{\Delta=0}^{\infty} p(n_{min}, \Delta)(n_{min} + \Delta) = \frac{3 - 2p_e}{p_e(2 - p_e)}. \tag{1.8}$$

As mentioned in the previous section the probability of transmission of a photon form the satellite to the ground and vice versa is small meaning that $p_e \ll 1$. Expanding $\langle n \rangle$ is this regime yields,

$$\langle n \rangle = \frac{3}{2p_e}. \tag{1.9}$$

This is the expected number of attempts it takes for Alice and Bob both to share entanglement with the satellite. In order for Alice and Bob to share entangled qubits a Bell state measurement should be made on the two bits in the satellite, thereby performing an entanglement swap that results in Alice's and Bob's qubits being entangled. As we will see in the next chapter this swap

can be done using linear optics with an efficiency of $\eta_{swap} = 1/2$, thus giving the entanglement generation rate between Alice and Bob of,

$$R = \frac{1}{3} p_d p_s r_{rep}, \tag{1.10}$$

which is linear in p_d as opposed to the rate without memories as given by equation 1.3. Thus by implementing memories into the satellite we unlock the potential to increase the rate by several orders of magnitude. We will pursue this increase in rate in the next chapter where we will consider different implementations involving quantum memories in the satellite.

Chapter 2

Quantum Key Distribution

In this chapter we will cover different proposed schemes for satellite QKD. Specifically we will consider different implementations of satellites with imperfect quantum memories, and compare them to the direct downlink scenario without memory. The goal of the chapter is to state the specific requirements of the memories used, in order to achieve greater rates than the direct downlink scenario.

2.1 Introduction

Before we turn to the analysis of the different satellite QKD schemes, we will go over some of the assumptions common to all the proposals. Firstly we will assume that the geometry of Alice, Bob and the satellite is constant in time. Specifically that they form an isosceles triangle, such that the distance L from Alice and Bob to the satellite is the same. This in turn allows us to use the same probability p_d, p_u for the transmission of photons for Alice and Bob.

To compare the different proposed schemes, we will calculate the effective two-photon count rate. This rate tells us how many entangled pairs of photons Alice and Bob will have available to them to perform QKD with. Going forward we will just use rate to refer to the of effective two-photon count rate.

Loss is an inevitable part of real world implementations of QKD schemes, as mentioned in the previous chapter. Loss is however not the only process which can occur and lead to errors in the operation of the protocols. To quantify the errors we will calculate the resulting state $\rho^{(a,b)}$, that Alice and Bob will have available to them to perform QKD with, and calculate the fidelity with the ideal state $|\psi_{ideal}\rangle$ in use for the protocol,

$$F = \frac{\langle\psi_{ideal}|\,\rho^{(a,b)}\,|\psi_{ideal}\rangle}{\mathrm{Tr}\left[\rho^{(a,b)}\right]}. \tag{2.1}$$

The trace in the denominator is there in order to ensure the normalisation of $\rho^{(a,b)}$, as we generally will adopt a laissez-faire approach to the normalisation of the states during our calculations, only reinstating it at the end.

Finally we will assume all photon detectors to be non-photon-number-resolving photon detectors with unit detection efficiency.

2.2 Direct Downlink

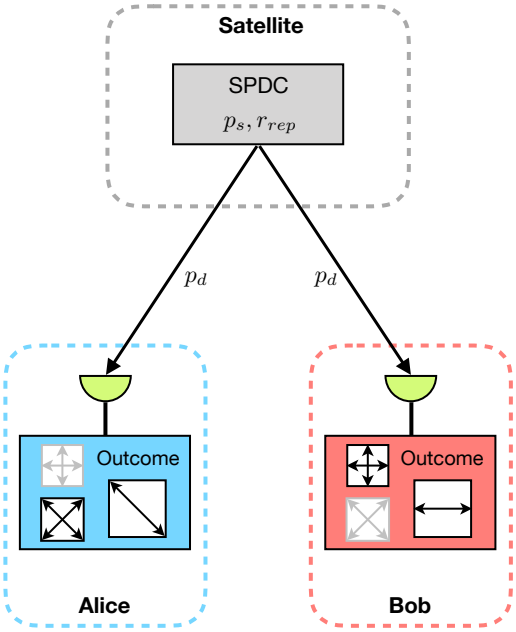


Figure 2.1: The direct downlink scheme. The photon source in the satellite produces entangled photons with probability p_s and repetition rate r_{rep}. Alice and Bob randomly measures the polarisation of the incoming photons, thereby implementing an EPR QKD protocol as described in 1.1.2

The direct downlink scheme, as implemented in the Micius satellite will be the first scheme we will consider. As mentioned in the introduction, the scheme works by having the satellite produce two polarisation entangled photons,

$$\left|\psi^+\right\rangle_{a,b} = \frac{1}{\sqrt{2}}(\left|H\right\rangle_a \left|V\right\rangle_b + \left|V\right\rangle_a \left|H\right\rangle_b). \tag{2.2}$$

The photons are then sent to Alice and Bob, who will measure the the polarisation of the received photon in either the X or Z basis, chosen at random. A schematic view of the direct downlink scheme can be found in figure 2.1. If we view the photon source as emitting a Bell state with probability p_s per repetition of the protocol, we acquire the rate by multiplying the rate of bell state generation with the probability that both photons reach the ground,

$$R = p_d^2 p_s r_{rep} \tag{2.3}$$

where r_{rep} is the repetition rate.

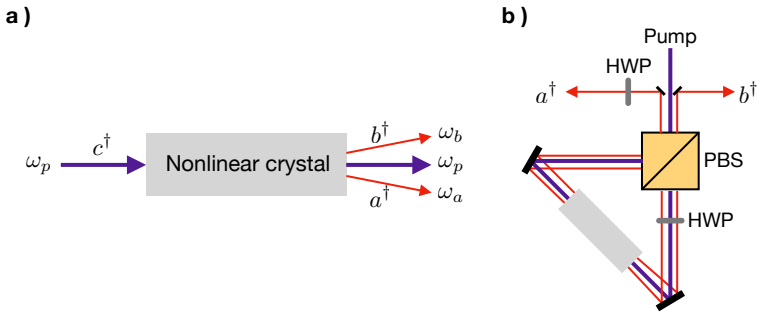


Figure 2.2: a) The nonlinear crystal used for spontaneous parametric downconversion (SPDC). **b)** The Sagnac interferometer with the nonlinear crystal inside. This setup allows for the generation of polarisation entangled photons in the two modes $a^\dagger$ and $b^\dagger$.

2.2.1 Spontaneous Parametric Downconversion as a Bell State Source

We will now take a closer look at how spontaneous parametric downconversion (SPDC) is being used to generate entangled photon pairs in the satellite. In SPDC photons from a pump laser are being converted into pairs of lower energy photons in a nonlinear medium. A pump laser with frequency ω_p is being used to drive a nonlinear crystal with the hamiltonian [18, p. 186-187],

$$H = \omega_a a^\dagger a + \omega_b b^\dagger b + \omega_p c^\dagger c + i\chi^{(2)}\left(abc^\dagger - a^\dagger b^\dagger c\right) \tag{2.4}$$

where $c^\dagger$ is the creation operator of the pump field, $a^\dagger$ and $b^\dagger$ the modes of the two photons being created with frequency ω_a and ω_b and $\chi^{(2)}$ is the second order susceptibility. The two modes generated are spatially separated as seen in figure 2.2a and with $\omega_a = \omega_b = \omega_p/2$. Assuming the the pump laser to be a strong coherent field with mean photon number $|\gamma|^2$, we may apply the parametric approximation and switch to the interaction picture to get the Hamiltonian,

$$H_I = i(\zeta^* ab - \zeta a^\dagger b^\dagger), \tag{2.5}$$

where $\zeta = \chi^{(2)}\gamma$. To see how this can be used to generate Bell states we follow the lead of [19]. Consider a Sagnac interferometer with the nonlinear crystal placed inside as seen in figure 2.2b. The pump field is polarised in the $+45°$ direction and being send to the polarising beam splitter (PBS), splitting the field into two by transmitting the horizontal polarised light and reflecting the vertical polarised light. Let us first follow the clockwise (CW) path around the interferometer. The Half-wave plate (HWP) rotates the polarisation of the light by $90°$ such that the light becomes vertically polarised. The field then pumps the crystal thereby invoking the Hamiltonian $H_{CW} = i(\zeta^* a_V b_V - \zeta a_V^\dagger b_V^\dagger)$, with the subscript indicating the polarisation of the photons. At the PBS the vertically polarised photons are reflected and thus being send back in the direction of the pump. For the counterclockwise path, the HWP comes after the crystal meaning that the polarisation is rotated before escaping the interferometer. The effective hamiltonian is thus $H_{CCW} = i(\zeta^* a_H b_H - \zeta a_H^\dagger b_H^\dagger)$. Finally after the CW and CCW path are merged at the BSM, the a modes are led through another HWP thereby flipping the rotation.[1] The full Hamiltonian governing the output modes a and b is,

$$H_{SPDC} = i\left[\zeta^*\left(a_H b_V + a_V b_H\right) - \zeta\left(a_H^\dagger b_V^\dagger + a_V^\dagger b_H^\dagger\right)\right]. \tag{2.6}$$

[1] Without this final HWP, the photons would be entangled in the state $\left|\phi^+\right\rangle_{a,b}$, which also is usable for QKD purposes.

The associated time evolution operator is $U(\Delta t) = e^{-iH_{SPDC}\Delta t}$, which in the weak coupling regime $|\zeta|\Delta T \ll 1$ produces the state

$$\begin{aligned}|\psi\rangle &\approx \left(1 - iH_{SPDC}\Delta t - \frac{1}{2}H_{SPDC}^2\Delta t^2\right)|\varnothing\rangle \\ &\approx |\varnothing\rangle + \sqrt{\frac{p_s}{2}}\left(|H,V\rangle_{a,b} + |V,H\rangle_{a,b}\right) + \frac{p_s}{2}\left(|2H,2V\rangle_{a,b} + |2V,2H\rangle_{a,b} + |HV,HV\rangle_{a,b}\right)\end{aligned} \tag{2.7}$$

where we have defined the Bell state probability $p_s = 2\zeta^2\Delta t^2$. We now see that we have effectively created a probabilistic Bell state source producing Bell states with probability p_s. Furthermore we see that to suppress the term involving four photon states we unfortunately need to keep $p_s \ll 1$, which will lead to lower rate of the scheme. In the next section we will explore this last point further by showing how the four photon contributions to the Bell state influences the fidelity of the protocol.

2.2.2 Fidelity

To characterise the fidelity of the scheme we start with the state generated by the SPDC,

$$|\psi\rangle_{a,b} = |\varnothing\rangle + \sqrt{\frac{p_1}{2}}\left(|H,V\rangle_{a,b} + |V,H\rangle_{a,b}\right) - \sqrt{\frac{p_2}{3}}\left(|2H,2V\rangle_{a,b} + |2V,2H\rangle_{a,b} + |HV,HV\rangle_{a,b}\right). \tag{2.8}$$

The loss in the atmosphere will be modelled by a beam splitter with transmittance $\sqrt{p_d}$,

$$c_\sigma^\dagger \to \sqrt{1-p_d}\, l_{c_\sigma}^\dagger + \sqrt{p_d}c_\sigma^\dagger, \tag{2.9}$$

for $c \in \{a,b\}$, $\sigma \in \{H,V\}$ and with l_{c_σ} being the loss mode for c_σ. Therefore using $\sqrt{1-p_d} \approx 1$ and keeping only terms up to order $\mathcal{O}(p_d)$ the state becomes,

$$\begin{aligned}|\psi\rangle_{a,b} \xrightarrow{\text{loss}} |\psi'\rangle_{a,b,l_a,l_b} = {} & |\varnothing,\varnothing,\varnothing,\varnothing\rangle + \sqrt{\frac{p_1p_d^2}{2}}\Big(|H,V,\varnothing,\varnothing\rangle + |V,H,\varnothing,\varnothing\rangle\Big) \\ & + \sqrt{\frac{p_1p_d}{2}}\Big(|H,\varnothing,\varnothing,V\rangle + |\varnothing,V,H,\varnothing\rangle + |V,\varnothing,\varnothing,H\rangle + |\varnothing,H,V,\varnothing\rangle\Big) \\ & + \sqrt{\frac{p_1}{2}}\Big(|\varnothing,\varnothing,H,V\rangle + |\varnothing,\varnothing,V,H\rangle\Big) - \sqrt{\frac{4p_2p_d^2}{3}}(|H,V,H,V\rangle + |V,H,V,H\rangle\Big) \\ & - \sqrt{\frac{p_2p_d^2}{3}}\Big(|2H,\varnothing,\varnothing,2V\rangle + |\varnothing,2V,2H,\varnothing\rangle + |2V,\varnothing,\varnothing,2H\rangle + |\varnothing,2H,2V,\varnothing\rangle \\ & + |HV,\varnothing,\varnothing,HV\rangle + |H,H,V,V\rangle + |H,V,V,H\rangle + |V,H,H,V\rangle + |V,V,H,H\rangle \\ & + |\varnothing,HV,HV,\varnothing\rangle\Big) - \sqrt{\frac{2p_2p_d}{3}}\Big(|H,\varnothing,H,2V\rangle + |\varnothing,V,2H,V\rangle + |V,\varnothing,V,2H\rangle \\ & + |\varnothing,H,2V,H\rangle\Big) - \sqrt{\frac{p_2p_d}{3}}\Big(|H,\varnothing,V,HV\rangle + |V,\varnothing,H,HV\rangle + |\varnothing,H,HV,V\rangle \\ & + |\varnothing,V,HV,H\rangle\Big) - \sqrt{\frac{p_2}{3}}\Big(|\varnothing,\varnothing,2H,2V\rangle + |\varnothing,\varnothing,2V,2H\rangle + |\varnothing,\varnothing,HV,HV\rangle\Big),\end{aligned} \tag{2.10}$$

where the subscripts have been omitted, but are all in order a, b, l_a, l_b. We then trace out the loss modes, to get the density matrix of the mixed state reaching Alice and Bob,

$$\begin{aligned}
\rho^{(a,b)} &= \mathrm{Tr}_{l_a,l_b}\left[|\psi'\rangle\langle\psi'|\right] \\
&= \left(|\varnothing,\varnothing\rangle + \sqrt{\frac{p_1 p_d^2}{2}}\Big(|H,V\rangle + |V,H\rangle\Big)\right)\left(\langle\varnothing,\varnothing| + \sqrt{\frac{p_1 p_d^2}{2}}\Big(\langle H,V| + \langle V,H|\Big)\right) \\
&+ \left(\frac{p_1 p_d}{2} + p_2 p_d\right)\Big(|H,\varnothing\rangle\langle H,\varnothing| + |V,\varnothing\rangle\langle V,\varnothing| + |\varnothing,H\rangle\langle\varnothing,H| + |\varnothing,V\rangle\langle\varnothing,V|\Big) \\
&+ \left(\sqrt{\frac{p_1}{2}}\,|\varnothing,\varnothing\rangle - \sqrt{\frac{4p_2p_d^2}{3}}\,|H,V\rangle - \sqrt{\frac{p_2p_d^2}{3}}\,|V,H\rangle\right)\left(\sqrt{\frac{p_1}{2}}\,\langle\varnothing,\varnothing| - \sqrt{\frac{4p_2p_d^2}{3}}\,\langle H,V| - \sqrt{\frac{p_2p_d^2}{3}}\,\langle V,H|\right) \\
&+ \left(\sqrt{\frac{p_1}{2}}\,|\varnothing,\varnothing\rangle - \sqrt{\frac{4p_2p_d^2}{3}}\,|V,H\rangle - \sqrt{\frac{p_2p_d^2}{3}}\,|H,V\rangle\right)\left(\sqrt{\frac{p_1}{2}}\,\langle\varnothing,\varnothing| - \sqrt{\frac{4p_2p_d^2}{3}}\,\langle V,H| - \sqrt{\frac{p_2p_d^2}{3}}\,\langle H,V|\right) \\
&+ \frac{p_2p_d^2}{3}\Big(|2H,\varnothing\rangle\langle 2H,\varnothing| + |2V,\varnothing\rangle\langle 2V,\varnothing| + |\varnothing,2H\rangle\langle\varnothing,2H| + |\varnothing,2V\rangle\langle\varnothing,2V| + |HV,\varnothing\rangle\langle HV,\varnothing| \\
&+ |\varnothing,HV\rangle\langle\varnothing,HV| + |H,H\rangle\langle H,H| + |V,V\rangle\langle V,V|\Big) + p_2\,|\varnothing\rangle\langle\varnothing|\,.
\end{aligned} \tag{2.11}$$

Finally Alice and Bob may post-select only the events where they both receive a photon from the satellite. This is modelled by projecting onto $\mathbb{P}_{PS} = \mathbb{1} - |\varnothing\rangle\langle\varnothing|$, giving the final state,

$$\begin{aligned}
\rho_{PS}^{(a,b)} &= \mathbb{P}_{PS}\,\rho^{(a,b)}\,\mathbb{P}_{PS} \\
&= \left(p_1p_d^2 + \frac{8}{3}p_2p_d^2\right)|\psi^+\rangle\langle\psi^+| + \frac{p_2p_d^2}{3}\mathbb{P}_1^{(a)}\otimes\mathbb{P}_1^{(b)},
\end{aligned} \tag{2.12}$$

where $\mathbb{P}_1^{(a)} = |H\rangle_a\langle H| + |V\rangle_a\langle V|$ is the projection operator onto the one photon Fock space. With the ideal state $|\psi_{ideal}\rangle = |\psi^+\rangle$, we are now ready to calculate the fidelity,

$$F = \frac{\langle\psi^+|\,\rho_{PS}^{(a,b)}\,|\psi^+\rangle}{\mathrm{Tr}\left[\rho_{PS}^{(a,b)}\right]} = \frac{1+3p_2^*}{1+4p_2^*} \approx 1 - p_2^*, \tag{2.13}$$

where $p_2^* = p_2/p_1$ and the approximation being valid for $p_2^* \ll 1$ which is necessary for achieving a fidelity close to unity. When using SPDC as a photon source $p_2^* = 3p_s/4$ such that the fidelity is given by,

$$F = 1 - \frac{3}{4}p_s. \tag{2.14}$$

2.2.3 Performance

The infidelity, as seen by equation 2.14, is being caused by the four photon production from the SPDC. Alice and Bob are able to increase the fidelity of the protocol by lowering p_s, however doing so will also decrease the rate of the protocol. Therefore supposing Alice and Bob desire some specific fidelity F_0 of the incoming photons, they will thus limit the rate to be,

$$R = \frac{4}{3}\left(1 - F_0\right)p_d^2 r_{rep}. \tag{2.15}$$

As discussed in the introduction the rate achieved with the Micius satellite is $R = 2.2$ Hz with an estimated fidelity of $F = 0.910 \pm 0.007$ [3]. We will use the rate of $R = 1$ Hz as a benchmark in order to compare the proposed schemes with the direct downlink scheme.

2.3 Downlink and Memory Scheme

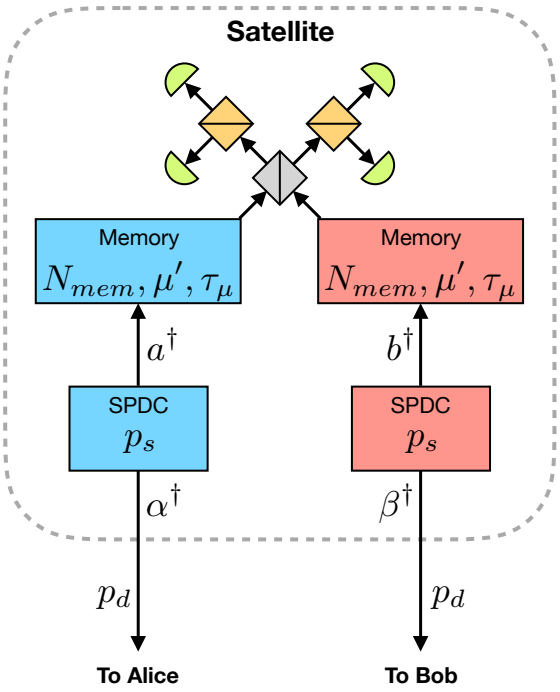


Figure 2.3: Schematic view of the satellite with quantum memories.

We will now expand further upon the alternative scheme proposed in section 1.3 of this thesis and seen in figure 2.3. We will analyse the scheme with realistic components, and see what limitations they will impose. The procedure for Alice and Bob to use this satellite was discussed in section 1.3, we will therefore just consider the performance in this section.

Realistic quantum memories are only able to store a limited amount of qubits. Let N_{mem} be the multimode capacity of the memories in the protocol. This imposes a limit on the repetition rate of the photon sources, as one qubit in the memory is occupied in the time between creation of an entangled photon pair, until a signal comes back from the ground indicating whether or not the photon arrived. We will call this time the communication time and it is given by,

$$T_{com}^{S\leftrightarrow G} = \frac{2L}{c}, \tag{2.16}$$

where L is the distance from the satellite to Alice and Bob and c is the speed of light.[2] As it turns out it will be beneficial to fill up the memory as rapidly as possible instead of spreading the

[2]For simplicity we have assumed that the geometry of the Alice-Bob-Satellite system is an isosceles triangle.

creation of photons out over the period $T_{com}^{S\leftrightarrow G}$. In the limit where $N_{mem}p_s p_d \ll 1$, the probability of at least one photon reaching the ground station for each burst of photons is,

$$\begin{aligned} p_e &= 1 - (1 - p_s p_d)^{N_{mem}} \\ &\approx N_{mem} p_s p_d. \end{aligned} \tag{2.17}$$

Assuming that the time it takes to fill up the memory in negligible compared to the communication time, the effective repetition rate of the protocol becomes,

$$r_{rep}^{eff} = \frac{1}{T_{com}^{S\leftrightarrow G}}. \tag{2.18}$$

2.3.1 Ensemble memories

As seen in equation 2.17 the probability of entanglement, and thus the rate of the protocol, is highly reliant on having memories with great multimode storage. As a candidate for the choice of memory in the satellite we are going to consider the atomic frequency comb protocol (AFC) as described in [20]. This protocol relies on an ensemble of atoms, with an inhomogeneously broadened transition from a ground state $|g\rangle$ to an excited state $|e\rangle$. By employing spectral hole burning the atomic density of the state $|g\rangle$ is prepared in a frequency comb, with Δ being the distance between the teeth of the comb. An incoming photon with spectral width larger than Δ, but narrower than the broadening of the transition $|g\rangle$-$|e\rangle$, will be absorbed at time $t = 0$ and leave the atoms in the state,

$$|\psi(t)\rangle = \sum_{j=1}^{N} c_j e^{-i(kz_j - \delta_j t)} |g_1 \cdots e_j \cdots g_N\rangle, \tag{2.19}$$

where the sum is over the N atoms in the comb, z_j being the position of the j'th atom, k being the wave number of the light, δ_j the detuning of the light with respect to the $j'th$ atom and the amplitude c_j being dependant on the detuning and position of the atom. For $t > 0$ the atoms containing the excitations will evolve out of phase due to different detuning δ_j, stemming from the excitation being spread out over multiple teeth of the comb. This will suppress re-emission of the photon. If the peaks of the AFC are much narrower than the spacing between them Δ, the phases will realign after time $2\pi/\Delta$ and the photon will be reemitted from the ensemble. For storage times longer than $2\pi/\Delta$, transfer from state $|e\rangle$ to another stable state $|s\rangle$ can be performed.

The multimode capabilities of the AFC memory is achieved by sending in multiple temporally distinguishable modes. The number of modes the memory is able to store, is limited by the width of the pulse τ and the time before reemission of the first photon absorbed $2\pi/\Delta$. We should note that the width of the photon is limited by the total width of the of the comb; $\tau \sim 1/N_p\Delta$ where N_p is the number of peaks in the comb, such that the number of modes storable is $N_{mem} \sim N_p$ [20]. The need for all the excitations to be loaded into the memory before the reemission of the first photon, such that the excitations can be stored in the state $|s\rangle$, is a reason to create the photons in bursts as described above.

As a model for the storage efficiency we will assume exponential decay $\mu(t) = \mu' e^{-t/\tau_\mu}$, where t is the storage time, μ' is the zero-time efficiency and τ_μ is the coherence time of the memory. In the original paper [20], europium-doped Y_2SiO_5 crystals are proposed as the medium of the memory.

There it is estimated that storage of 100 modes with an efficiency of $\mu' = 0.9$ is within technical reach. Recent experiments with the same crystals, shows storage of a classical light pulse including transfer to a meta-stable spin-wave state $|s\rangle$, with a coherence time of $\tau_\mu = 530$ ms and efficiency $\mu' = 0.035$ [21]. Storage of states with a mean photon number of 1, including employing spin-echo techniques, has also been demonstrated with storage time of 0.5 ms and $5.1 \pm 0.4\%$ efficiency [22]. Finally storage of up to 50 (100) modes for on demand readout (fixed storage time) has been demonstrated for 0.541 ms (51 μs) with an efficiency of $1.6 \pm 0.2\%$ ($8.5 \pm 0.5\%$) [23].

2.3.2 Bell state measurement

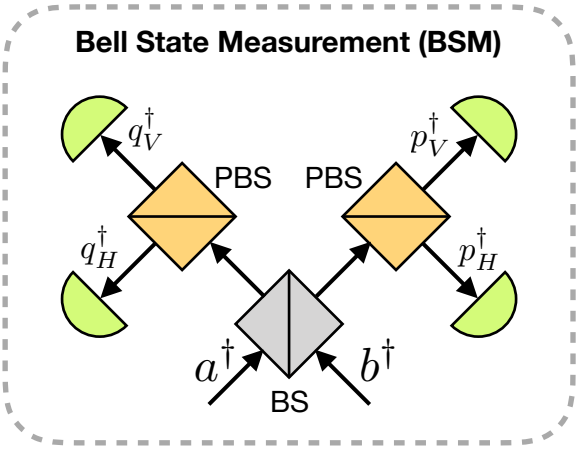


Figure 2.4: Setup used for performing bell state measurements of polarisation entangled photons.

For this schemes with ensemble based memories, we will consider Bell state detection using linear optics as depicted in figure 2.4. Let $a_\sigma^\dagger$ ($b_\sigma^\dagger$) be the creation operator of the photon leaving the memory corresponding Alice (Bob), with σ describing the polarisation. The two photons will be mixed on a 50:50 beamsplitter, according to

$$\begin{aligned} a_\sigma^\dagger &= \frac{1}{\sqrt{2}}\left(p_\sigma^\dagger + q_\sigma^\dagger\right) \\ b_\sigma^\dagger &= \frac{1}{\sqrt{2}}\left(p_\sigma^\dagger - q_\sigma^\dagger\right), \end{aligned} \tag{2.20}$$

thereby erasing the which-path information. This transforms the four Bell states into,

$$\begin{aligned} \left|\psi^+\right\rangle_{a,b} &= \frac{1}{\sqrt{2}}\left(p_H^\dagger p_V^\dagger - q_V^\dagger q_H^\dagger\right)|\varnothing\rangle \\ \left|\psi^-\right\rangle_{a,b} &= \frac{1}{\sqrt{2}}\left(q_H^\dagger p_V^\dagger - q_V^\dagger p_H^\dagger\right)|\varnothing\rangle \\ \left|\phi^+\right\rangle_{a,b} &= \frac{1}{2\sqrt{2}}\left(p_H^{\dagger\,2} - q_H^{\dagger\,2} + p_V^{\dagger\,2} - q_V^{\dagger\,2}\right)|\varnothing\rangle \\ \left|\phi^-\right\rangle_{a,b} &= \frac{1}{2\sqrt{2}}\left(p_H^{\dagger\,2} - q_H^{\dagger\,2} - p_V^{\dagger\,2} + q_V^{\dagger\,2}\right)|\varnothing\rangle \end{aligned} \tag{2.21}$$

Each of the modes p and q are sent to a polarising beamsplitter, after which detection occurs. Assuming detectors which can not differentiate between one and two incoming photons, we are

thus able to measure $|\psi^+\rangle$ and $|\psi^-\rangle$. It is not possible to detect the two remaining Bell states $|\phi^+\rangle$ and $|\phi^-\rangle$ due Hong–Ou–Mandel effect [24], where two incoming photons of same polarisation bunch after the beamsplitter. Therefore by detecting half the Bell states we perform the entanglement swap with efficiency $\eta_{swap} = 1/2$.

2.3.3 Rate

Let us now consider the rate of the scheme. With the inclusion of imperfect memories the rate will differ from the one calculated in the introduction. In the ensemble based memories there is a chance of loosing a photon from the memory, this will lead to the protocol failing as the Bell state detection will fail. We will use $p_{load}(\Delta)$ to describe the time dependant probability of successfully loading both photons from the memories. It turns out that it is beneficial to limit the maximum storage time. We introduce the parameter N_{max} as the maximum number of repetitions allowed for a qubit to be stores in the memory, after which it is erased and the memory reset. Let $p_{N_{max}}(n_{min})$ be the probability of this occurring, when the first successful qubit arrived at attempt n_{min}. Finally we have $p(n_{min}, \Delta)$ being the probability of the first memory being ready at attempt n_{min} and the second Δ attempts after. Taking these imperfect memory modifications into account, the equation for $\langle n \rangle$ becomes,

$$\begin{aligned}\langle n \rangle = \sum_{n_{min}=1}^{\infty} \Bigg[&\sum_{\Delta=0}^{N_{max}} p(n_{min}, \Delta)\,(n_{min} + \Delta) + p_{N_{max}}(n_{min})\,(n_{min} + N_{max} + \langle n \rangle) \\ &+ \sum_{\Delta=0}^{N_{max}} p(n_{min}, \Delta)\,(1 - p_{load}(\Delta))\,(n_{min} + \Delta + \langle n \rangle) \Bigg].\end{aligned} \tag{2.22}$$

Where the first term is the same as in equation 1.8, except this time Δ is limited by N_{max}, and accounts for the protocol being successful. The second term corresponds to the cases where the maximum storage time is reached, and the third term corresponds to a failure of retrieval of both qubits from memory. Solving for $\langle n \rangle$ yields,

$$\langle n \rangle = \frac{\sum_n \left[\sum_\Delta p(n, \Delta)\,(n + \Delta) + p_{N_{max}}(n)\,(n + N_{max})\right]}{\sum_{n,\Delta} p(n, \Delta)\,p_{load}(\Delta)} \tag{2.23}$$

We may interpret this result in a rather intuitive way. The numerator in the above fraction, is the average number of repetitions before the protocol is reset, either because entanglement were successfully generated in both arms, or because entanglement was generated in one arm but the other took too long, meaning that the good memory had to be reset. The denominator is the probability of the protocol succeeding before it is reset. The average number of repetitions before success is therefore just the average number of repetitions per reset of the protocol, divided by the probability of success within one reset of the protocol. Hence minimising $\langle n \rangle$, and thereby maximising the rate is a question of balancing the numerator and denominator, but more on this later.

We will now turn to the evaluation of equation 2.23. As in the introduction we have the probability of having both arms ready,

$$p(n_{min}, \Delta) = \begin{cases} p_e^2\,(1 - p_e)^{2n_{min}-2} & \text{if } \Delta = 0 \\ 2p_e^2\,(1 - p_e)^{2n_{min}+\Delta-2} & \text{if } \Delta \neq 0 \end{cases} \tag{2.24}$$

We can use this to find $p_{N_{max}}(n_{min})$ by summing up all the probabilities $p(n_{min}, \Delta)$ where $\Delta > N_{max}$,

$$p_{N_{max}}(n) = \sum_{\Delta=N_{max}+1}^{\infty} p(n_{min}, \Delta) = 2p_e \left(1-p_e\right)^{2n+N_{max}-1}. \tag{2.25}$$

With the efficiency of the memories being $\mu(t) = \mu' e^{-t/\tau_\mu}$, we have

$$p_{load}(\Delta) = \mu_{com}^2 e^{-\Delta/\Delta_m}, \tag{2.26}$$

where $\mu_{com} = \mu(T_{com})$ and $\Delta_m = \tau_\mu / r_{rep}$. With this the sums in equation 2.23 becomes nothing more than geometric series, which are readily evaluated,

$$\langle n \rangle^{-1} = \mu_{com}^2 p_e^2 \frac{e^{\frac{1}{\Delta_m}} \left(1 + (1-p_e)\, e^{-\frac{1}{\Delta_m}} - 2e^{-\frac{N_{max}+1}{\Delta_m}} \left(1-p_e\right)^{N_{max}+1}\right)}{\left(e^{\frac{1}{\Delta_m}} - 1 + p_e\right)\left(3 - 2p_e - 2\left(1-p_e\right)^{N_{max}+1}\right)}. \tag{2.27}$$

We will consider this in a good memory limit and a bad memory limit. Let us start by considering the good memory limit. This regime is defined by the lifetime of the memory $\tau = \Delta_m / r_{rep}$, being much greater than the average entanglement creation time in one arm of the setup $\langle T_e \rangle = p_e^{-1} r_{rep}^{-1}$. When this is the case, $\langle n \rangle$ will reduce to that of the perfect memory scenario,

$$\langle n \rangle^{-1} = \frac{2}{3} \mu_{com}^2 p_e, \quad \text{when,} \quad \Delta_m \gg \frac{1}{p_e} \gg 1. \tag{2.28}$$

In the bad memory limit we define $\alpha = (N_{max}+1)/\Delta_m$ roughly being the maximum storage time in terms of the lifetime of the memory. With this we get,

$$\langle n \rangle^{-1} = 2\Delta_m \left(1 - e^{-\alpha}\right) \mu_{com}^2 p_e^2, \quad \text{when,} \quad p_e \ll \frac{1}{\Delta_m} \ll 1. \tag{2.29}$$

Inclusion of the entanglement swap and the repetition rate, as described above, thus leads to the following rate of the protocol,

$$R = \Delta_m N_{mem}^2 p_s^2 p_d^2 \mu_{com}^2 \left(1 - e^{-\alpha}\right) r_{rep}, \qquad \text{for} \quad N_{mem} p_s p_d \ll \frac{T_{com}}{\tau} \tag{2.30}$$

$$R = \frac{1}{3} N_{mem} p_s p_d \mu_{com}^2 r_{rep}, \qquad \text{for} \quad N_{mem} p_s p_d \gg \frac{T_{com}}{\tau} \tag{2.31}$$

where $r_{rep} = \frac{1}{T_{com}^{S \leftrightarrow G}}$.

2.3.4 Fidelity

In a try to increase the rate of the protocol, one might naively try to increase the rate of the protocol by increasing p_s. While this would increase the rate of Bell state generation, it would also lead to an increased amount of four photons being produced, thereby potentially introducing errors in the distilled key of Alice and Bob. To get an estimate of the optimal value of p_s and memory cutoff N_{max}, which will increase the rate while keeping the errors down, we will calculate the fidelity of the effective state at Alice and Bob and use that as a measure of the fidelity of the protocol.

We start out by considering the evolution of the sate in one arm of the protocol. The state produced by the SPDC is,

$$|\psi\rangle_{a,\alpha} = |\varnothing\rangle + \sqrt{\frac{p_1}{2}}\left(|H,V\rangle_{a,\alpha} + |V,H\rangle_{a,\alpha}\right) - \sqrt{\frac{p_2}{3}}\left(|2H,2V\rangle_{a,\alpha} + |2V,2H\rangle_{a,\alpha} + |HV,HV\rangle_{a,\alpha}\right). \tag{2.32}$$

As before we will model the loss in the atmosphere by the beamsplitter $\alpha_\sigma^\dagger \to l_{\alpha_\sigma}^\dagger + \sqrt{p_d}\alpha_\sigma^\dagger$, where $\sigma \in \{H,V\}$ and we will use that $\sqrt{1-p_d} \approx 1$. Similarly the loss in the memory we will model by $a_\sigma^\dagger \to \sqrt{1-\mu_a}\, l_{a_\sigma}^\dagger + \sqrt{\mu_a}\, a_\sigma^\dagger$, where $\mu_a = \mu(t_a)$ is the efficiency of the memory after the qubit has been stored for time t_a. After tracing out the losses and conditioning on a photon reaching Alice, the shared state between Alice and the memory in the satellite is,

$$\begin{aligned}
\rho^{(a,\alpha)} = {} & \mu_a p_d p_1 \left|\psi^+\right\rangle\!\left\langle\psi^+\right| + (1-\mu_a)\, p_d p_1 \left|\varnothing\right\rangle_a \left\langle\varnothing\right| \otimes \frac{\mathbb{P}_1^{(\alpha)}}{2} \\
& + \frac{p_d p_2}{3}\mu_a^2 \left(\sqrt{2}\left|2V,H\right\rangle + \left|HV,V\right\rangle\right)\left(\sqrt{2}\left\langle 2V,H\right| + \left\langle HV,V\right|\right) \\
& + \frac{p_d p_2}{3}\mu_a^2 \left(\sqrt{2}\left|2H,V\right\rangle + \left|HV,H\right\rangle\right)\left(\sqrt{2}\left\langle 2H,V\right| + \left\langle HV,H\right|\right) \\
& + p_d p_2 \mu_a (1-\mu_a)\frac{4}{3}\left(|H,V\rangle + |V,H\rangle\right)\left(\langle H,V| + \langle V,H|\right) \\
& + \frac{p_d p_2}{3}\mu_a(1-\mu_a)\mathbb{P}_1^{(a)} \otimes \mathbb{P}_1^{(\alpha)}
\end{aligned} \tag{2.33}$$

where we have neglected terms where two photons reach Alice and vacuum terms in α proportional to p_2. Following this, a Bell state measurement will be carried out on the a and b modes of the product state $\rho^{(a,\alpha)} \otimes \rho^{(b,\beta)}$ as described above, where $\rho^{(b,\beta)}$ is the state in Bob's half of the system. For the BSM to work at least two photons of different polarisations should reach the central beam splitter. This means that we may disregard some terms in $\rho^{(a,\alpha)} \otimes \rho^{(b,\beta)}$, that corresponds to events in the protocol which can be post-selected away, because of wrong combinations of detector clicks. Moreover we discard the terms proportional to p_2^2 as these are small compared to the other terms leading to infidelity. In table 2.1 an overview of which combination of states we will lead to the right detector clicks, and with what probability they will occur.

	$\|\varnothing\rangle_a$	$\|H\rangle_a$	$\|V\rangle_a$	$\|2H\rangle_a$	$\|2V\rangle_a$	$\|HV\rangle_a$
$\|\varnothing\rangle_b$	No photons	Only one photon	Only one photon	Only one polarisation	Only one polarisation	$p=1$
$\|H\rangle_b$	Only one photon	Only one polarisation	$p=1$	Only one polarisation	$p=\frac{1}{2}$	$p=1$
$\|V\rangle_b$	Only one photon	$p=1$	Only one polarisation	$p=\frac{1}{2}$	Only one polarisation	$p=1$
$\|2H\rangle_b$	Only one polarisation	Only one polarisation	$p=\frac{1}{2}$	Probabillity $\propto p_2^2$		
$\|2V\rangle_b$	Only one polarisation	$p=\frac{1}{2}$	Only one polarisation			
$\|HV\rangle_b$	$p=1$	$p=1$	$p=1$			

Table 2.1: Overview of what combination of states will lead to the correct pattern of detector clicks. Measurement of either $\left|\psi^+\right\rangle$ or $\left|\psi^-\right\rangle$ requires at least two photons of opposite polarisation. The combinations with $|2H\rangle$ or $|2V\rangle$ may be postselected half of the times when the two photons travel down different paths after the beam splitter.

Keeping only the terms that produces the right detector pattern we have,

$$
\begin{aligned}
\rho^{(a,\alpha)}\otimes\rho^{(b,\beta)} = &\left(\mu_a p_d p_1+\frac{8}{3}p_d p_2\mu_a(1-\mu_a)\right)\left(\mu_b p_d p_1+\frac{8}{3}p_d p_2\mu_b(1-\mu_b)\right)\left|\psi^+\right\rangle_{a,\alpha}\left\langle\psi^+\right|\otimes\left|\psi^+\right\rangle_{b,\beta}\left\langle\psi^+\right| \\
&+\frac{\mu_a\mu_b^2p_d^2p_1p_2}{3}\left[\left|\psi^+\right\rangle_{a,\alpha}\left\langle\psi^+\right|\otimes\left(\sqrt{2}\left|2V,H\right\rangle_{b,\beta}+\left|HV,V\right\rangle_{b,\beta}\right)\left(\sqrt{2}\left\langle 2V,H\right|+\left\langle HV,V\right|\right)\right] \\
&+\frac{\mu_a\mu_b^2p_d^2p_1p_2}{3}\left[\left|\psi^+\right\rangle_{a,\alpha}\left\langle\psi^+\right|\otimes\left(\sqrt{2}\left|2H,V\right\rangle_{b,\beta}+\left|HV,H\right\rangle_{b,\beta}\right)\left(\sqrt{2}\left\langle 2H,V\right|+\left\langle HV,H\right|\right)\right] \\
&+\frac{\mu_a^2\mu_bp_d^2p_1p_2}{3}\left[\left(\sqrt{2}\left|2V,H\right\rangle_{a,\alpha}+\left|HV,V\right\rangle_{a,\alpha}\right)\left(\sqrt{2}\left\langle 2V,H\right|+\left\langle HV,V\right|\right)\otimes\left|\psi^+\right\rangle_{b,\beta}\left\langle\psi^+\right|\right] \\
&+\frac{\mu_a^2\mu_bp_d^2p_1p_2}{3}\left[\left(\sqrt{2}\left|2H,V\right\rangle_{a,\alpha}+\left|HV,H\right\rangle_{a,\alpha}\right)\left(\sqrt{2}\left\langle 2H,V\right|+\left\langle HV,H\right|\right)\otimes\left|\psi^+\right\rangle_{b,\beta}\left\langle\psi^+\right|\right] \\
&+\frac{\mu_a\mu_bp_d^2p_1p_2}{3}\left[(1-\mu_b)\left|\psi^+\right\rangle_{a,\alpha}\left\langle\psi^+\right|\otimes\mathbb{P}_1^{(b)}\otimes\mathbb{P}_1^{(\beta)}+(1-\mu_a)\mathbb{P}_1^{(a)}\otimes\mathbb{P}_1^{(\alpha)}\otimes\left|\psi^+\right\rangle_{b,\beta}\left\langle\psi^+\right|\right] \\
&+\frac{\mu_b^2(1-\mu_a)p_d^2p_1p_2}{6}\left[\left|\varnothing\right\rangle_a\left\langle\varnothing\right|\otimes\mathbb{P}_1^{(\alpha)}\otimes\left(\sqrt{2}\left|2V,H\right\rangle_{b,\beta}+\left|HV,V\right\rangle_{b,\beta}\right)\left(\sqrt{2}\left\langle 2V,H\right|+\left\langle HV,V\right|\right)\right] \\
&+\frac{\mu_b^2(1-\mu_a)p_d^2p_1p_2}{6}\left[\left|\varnothing\right\rangle_a\left\langle\varnothing\right|\otimes\mathbb{P}_1^{(\alpha)}\otimes\left(\sqrt{2}\left|2H,V\right\rangle_{b,\beta}+\left|HV,H\right\rangle_{b,\beta}\right)\left(\sqrt{2}\left\langle 2H,V\right|+\left\langle HV,H\right|\right)\right] \\
&+\frac{\mu_a^2(1-\mu_b)p_d^2p_1p_2}{6}\left[\left(\sqrt{2}\left|2V,H\right\rangle_{a,\alpha}+\left|HV,V\right\rangle_{a,\alpha}\right)\left(\sqrt{2}\left\langle 2V,H\right|+\left\langle HV,V\right|\right)\otimes\left|\varnothing\right\rangle_b\left\langle\varnothing\right|\otimes\mathbb{P}_1^{(\beta)}\right] \\
&+\frac{\mu_a^2(1-\mu_b)p_d^2p_1p_2}{6}\left[\left(\sqrt{2}\left|2H,V\right\rangle_{a,\alpha}+\left|HV,H\right\rangle_{a,\alpha}\right)\left(\sqrt{2}\left\langle 2H,V\right|+\left\langle HV,H\right|\right)\otimes\left|\varnothing\right\rangle_b\left\langle\varnothing\right|\otimes\mathbb{P}_1^{(\beta)}\right].
\end{aligned}
\tag{2.34}
$$

Without loss of generality we assume a clicks on detectors corresponding to the p_H and p_V modes, this collapses the state into,

$$\begin{aligned}\rho_{PS}^{(\alpha,\beta)} &= \frac{1}{8}\left(\mu_a p_d p_1 + \frac{8}{3}p_d p_2 \mu_a(1-\mu_a)\right)\left(\mu_b p_d p_1 + \frac{8}{3}p_d p_2 \mu_b(1-\mu_b)\right)|\psi^+\rangle_{\alpha,\beta}\langle\psi^+| \\ &+ \frac{p_d^2 p_1 p_2}{24}\mu_a\mu_b(\mu_a+\mu_b)\Big[(|V,H\rangle_{\alpha,\beta}+|V,V\rangle_{\alpha,\beta}+|H,V\rangle_{\alpha,\beta})(\langle V,H|+\langle V,V|+\langle H,V|) \\ &+ (|V,H\rangle_{\alpha,\beta}+|H,H\rangle_{\alpha,\beta}+|H,V\rangle_{\alpha,\beta})(\langle V,H|+\langle H,H|+\langle H,V|)\Big] \\ &+ \frac{p_d^2 p_1 p_2}{24}\left(\mu_a\mu_b(2-\mu_a-\mu_b)+\mu_a^2(1-\mu_b)+\mu_b^2(1-\mu_a)\right)\mathbb{P}_1^{(\alpha)}\otimes\mathbb{P}_1^{(\beta)}.\end{aligned} \tag{2.35}$$

We can pick out the ideal state by noting that the ideal state should happen with probability $p_d^2 p_1^2 \mu_a\mu_b$, therefore $|\psi_{ideal}\rangle = |\psi^+\rangle$. We are now able to calculate the fidelity as a function of the memory efficiencies μ_a and μ_b,

$$\begin{aligned}f(\mu_a,\mu_b) &= \frac{\langle\psi^+|\,\rho_{PS}^{(\alpha,\beta)}\,|\psi^+\rangle}{\mathrm{Tr}\left[\rho_{PS}^{(\alpha,\beta)}\right]} \\ &= \frac{\mu_a\mu_b + \frac{1}{3}p_2^*\left(\mu_a^2+\mu_b^2+18\mu_a\mu_b-6\mu_a^2\mu_b-6\mu_a\mu_b^2\right)}{\mu_a\mu_b+\frac{2}{3}p_2^*\left(2\mu_a^2+2\mu_b^2+12\mu_a\mu_b-5\mu_a^2\mu_b-5\mu_a\mu_b^2\right)},\end{aligned} \tag{2.36}$$

where we have again introduced $p_2^* = p_2/p_1$. For high fidelity operation we expect $\mu_a, \mu_b \sim 1$ and $p_2^* \ll 1$, meaning that we may expand $f(\mu_a,\mu_b)$ in the limit $2p_2^*/(3\mu_a\mu_b) \ll 1$ to get,

$$f(\mu_a,\mu_b) = 1 - p_2^*\left(2+\frac{\mu_a}{\mu_b}+\frac{\mu_b}{\mu_a}-\frac{4}{3}\mu_a-\frac{4}{3}\mu_b\right). \tag{2.37}$$

To get the average fidelity F we need to average over the memory efficiencies, which can be accomplished by exploiting the symmetry of μ_a and μ_b, and that the swap occurs immediately after the second entanglement is created. Setting $\mu_b = \mu_{com}$ and $\mu_a = \mu(\Delta) = \mu_{com}e^{-\Delta/\Delta_m}$, we may take the average in the following way,

$$F = \sum_{\Delta=0}^{N_{max}} p_\Delta f(\mu(\Delta),\mu_{com}), \tag{2.38}$$

where p_Δ is the probability of waiting Δ repetitions between the two setups being ready and can be calculated with equation 2.24,

$$p_\Delta = \frac{\sum_{n_{min}} p(n_{min},\Delta)}{\sum_{n_{min},\Delta} p(n_{min},\Delta)} = \frac{(2-\delta_{\Delta,0})\,p_e\,(1-p_e)^\Delta}{2-p_e-2\,(1-p_e)^{N_{max+1}}}, \tag{2.39}$$

where $\delta_{\Delta,0}$ is the Kronecker delta. Evaluation of equation 2.38, reduces to the evaluation of the following type of sums,

$$S_\pm = \sum_{\Delta=0}^{N_{max}} p_\Delta e^{\pm\frac{\Delta}{\Delta_m}} = \frac{p_e}{1-e^{\pm\frac{1}{\Delta_m}}(1-p_e)}\,\frac{1+e^{\pm\frac{1}{\Delta_m}}(1-p_e)-2e^{\pm\frac{N_{max}+1}{\Delta_m}}(1-p_e)^{N_{max}+1}}{2-p_e-2(1-p_e)^{N_{max}+1}}. \tag{2.40}$$

such that,

$$F = 1 - p_2^*\left(2+S_+ + S_- - \frac{4}{3}\mu_{com}\,(1+S_-)\right). \tag{2.41}$$

In the good memory limit $\Delta_m \gg 1/p_e$,[3] we get $S_\pm \approx 1$, such that

$$F = 1 - 4p_2^* \left(1 - \frac{2}{3}\mu_{com}\right). \tag{2.42}$$

On the other hand, in the bad memory limit $1 \ll \Delta_m \ll 1/p_e$,[4] we expect $N_{max} \sim \Delta_m$ such that $S_\pm \approx \mp(1 - e^{\pm\alpha})/\alpha$, where $\alpha = (N_{max} + 1)/\Delta_m$, and the fidelity becomes,

$$F = 1 - 4p_2^* \left(1 + \frac{\sinh(\alpha)}{2\alpha} - \frac{1}{3}\mu_{com}(1 + e^{-\frac{\alpha}{2}})\right). \tag{2.43}$$

Substituting the reduced four photon probability of the SPDC $p_2^* = 3p_s/4$, we arrive at

$$F = 1 - 3p_s \left(1 + \frac{\sinh(\alpha)}{2\alpha} - \frac{1}{3}\mu_{com}(1 + e^{-\frac{\alpha}{2}})\right), \qquad \text{for} \quad N_{mem}p_s p_d \ll \frac{T_{com}}{\tau_\mu} \tag{2.44}$$

$$F = 1 - 3p_s \left(1 - \frac{2}{3}\mu_{com}\right), \qquad \text{for} \quad N_{mem}p_s p_d \gg \frac{T_{com}}{\tau_\mu} \tag{2.45}$$

2.3.5 Optimisation

We now turn to the task posed at the start of the previous section; what values of N_{max} and p_s will maximise the rate of the protocol, while keeping the errors down? Specifically we will consider the rate and fidelity as functions of α and p_s, and impose a condition stating that the protocol should produce states with some desired fidelity F_0.

In the bad memory regime, we will for simplicity treat α as a continuous variable. Solving equation 2.44 for p_s gives,

$$p_s(\alpha, F_0) = \frac{1 - F_0}{3\left(1 + \frac{\sinh(\alpha)}{2\alpha} - \frac{1}{3}\mu_{com}(1 + e^{-\frac{\alpha}{2}})\right)}. \tag{2.46}$$

Plugging this into equation 2.30 to get $R(\alpha, p_s(\alpha, F_0))$, we may find α giving the maximum rate,

$$0 = \frac{\mathrm{d}}{\mathrm{d}\alpha} R(\alpha, p_s(\alpha, F_0)) \tag{2.47}$$

$$\Rightarrow \frac{e^{-\alpha}}{1 - e^{-\alpha}} = \frac{\frac{1}{3}\mu_{com}e^{-\frac{\alpha}{2}} + \frac{\cosh(\alpha)}{\alpha} - \frac{\sinh(\alpha)}{\alpha^2}}{1 - \frac{1}{3}\mu_{com}\left(1 + e^{-\frac{\alpha}{2}}\right) + \frac{\sinh(\alpha)}{2\alpha}}. \tag{2.48}$$

A nice feature of this result is that the choice of α is independent of the desired fidelity F_0.[5] In figure 2.5 equation 2.48 is solved numerically, showing the optimal choice of α in the bad regime. Once α has been found, finding p_s and R is straightforward.

[3] The approximation used in the good memory regime is essentially the same as saying that the memory efficiency is constant.

[4] In the bad memory regime, the approximation is the same as saying that p_Δ is constant, i.e. the probability of the second memory being ready is the same for all $\Delta \leq N_{max}$.

[5] This turns out to always be the case if $R(p_s, \alpha) = p_s^c h(\alpha)$ and $F(p_s, \alpha) = 1 - p_s g(\alpha)$, for some constant $c \neq 0$ and differentiable functions $h(\alpha), g(\alpha) \neq 0$. In this case equation 2.48 becomes $cg'(\alpha)/g(\alpha) = h'(\alpha)/h(\alpha)$.

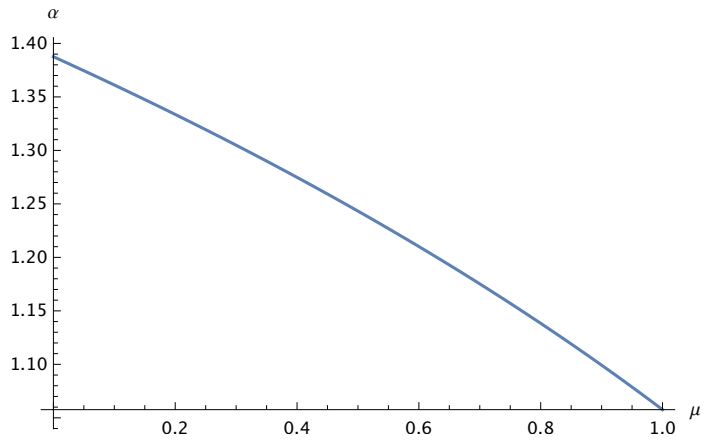


Figure 2.5: Plot of equation 2.48.

In the good memory regime optimisation is trivially done by solving equation 2.45 for p_s and substituting it into equation 2.31,

$$R = \frac{1 - F_0}{9\left(1 - \frac{2}{3}\mu_{com}\right)} N_{mem} p_d \mu_{com}^2 r_{rep}, \quad \text{for} \quad N_{mem} p_s p_d \gg \frac{T_{com}}{\tau}. \tag{2.49}$$

2.3.6 Performance

Finally we will look at the performance of the scheme proposed in this section. We assume satellite height of $L = 1000$ km leading to an effective repetition rate of $R \approx 150$ Hz, and the satellite-ground transmission of $p_d = 10^{-3}$. Furthermore we will require a fidelity of $F_0 = 0.95$.[6] Using the state-of-the-art parameters for the memory as described previously of $N_{mem} = 50$, $\tau_\mu = 0.53$ s and $\mu' = 0.05$, we get the rate $R = 9.9 \times 10^{-6}$ Hz after optimisation, which is quite far from the benchmark of $R = 1$ Hz set by the direct link satellite. In order to beat this benchmark $N_{mem} \gtrsim 1000$, $\mu' \sim 1$ and $\tau_\mu \gtrsim 0.5$s is needed. Figure 2.6 shows how the rate varies as the coherence time of the memory increases for $\mu' = 0.9$ and $N_{mem} = 200$ and 1000.

The scheme proposed in this chapter with the current available memory is still quite far from beating the *Micius* satellite in performance. However, the performance ceiling of the protocol is higher, meaning that in the future it might still be an appealing alternative.

2.4 Emitter and Downlink Scheme

A major factor limiting the rate of the protocol in the previous section is the combination of needing to store each mode for a minimum time of T_{com} with the choice of a probabilistic photon source. With probability $1 - p_s$ the SPDC produces vacuum which takes up a memory slot, thereby severely limiting the rate of the protocol. In this section we will explore an alternative approach to adding memories to the satellite, which avoids the probabilistic photon sources. The trick is to let the memory act as a photon source, by sending out a photon entangled with the state of the

[6] This is chosen higher than the 0.907 ± 0.007 achieved in [2], to make room for errors unaccounted for.

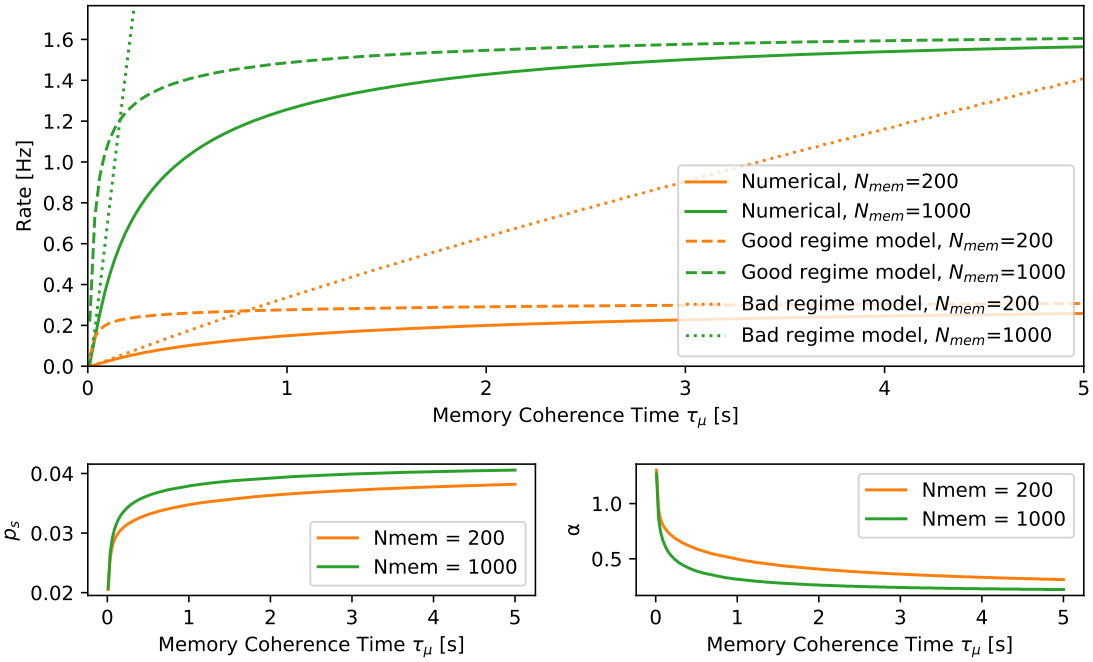


Figure 2.6: (Upper) Optimised rate as a function of the memory coherence time with $F = 0.95$, $\mu' = 0.9$, $L = 1000$ km and $p_d = 10^{-3}$. Solid lines are the result of numerical optimisation with the exact rate and fidelity. The dashed (dotted) lines stems from equation 2.31 (2.30) with p_s (and α) from the numerical optimisation. (Lower right) The optimised values of p_s. (Lower left) Optimised values of α. As $\tau_\mu \to 0$ we see that $\alpha \to 1.39$ as predicted in figure 2.5.

emitter,

$$|\psi\rangle_{a,A} = \sqrt{\frac{\eta_c}{2}} \left(|0\rangle_a |0\rangle_A + |1\rangle_a |1\rangle_A \right), \tag{2.50}$$

where η_c is the collection efficiency of the emitted photon, $|\cdot\rangle_a$ denotes the state of photon and $|\cdot\rangle_A$ denotes the state of the emitter. As opposed to the SPDC we may acheive $\eta_c \sim 1$.

A possible choice of emitter is the Nitrogen-vacancy (NV) centre defect in diamonds. The defect occurs when two neighbouring carbon atoms of a diamond, are replaced by an nitrogen atom and a vacancy. These emitters have been employed to do a loophole free violation of Bell's inequality [25], where the electronic spin associated with the NV centre was entangled with the time-bin encoded emitted photons. By employing nearby nuclear nuclear spins as memory spins, it becomes possible to store several qubits in the same NV centre, which has been used to distill entanglement between two NV centres [26]. The coupling of the electronic spin to nuclear spins is particularly useful as it allows us to use the same NV centre to communicate with both Alice and Bob. This can be done by first emitting a photonic qubit entangled with the electronic spin to Alice, and then transfer the qubit stored in the electronic spin to the nuclear spin, such that the electronic spin may be used to emit another photonic qubit to Bob. This allows us to perform the Bell state measurement directly on the NV-centre, which allows us to achieve a swapping efficiency

greater than 50%. Unfortunately this also limits the BSM to be performed on the same NV centre, which will lead to greater coherence time requirements.[7]

Finally we will model loss in the emitters considered as depolarisation of the qubit. This also means that, when performing the BSM the satellite will not be able to tell if the qubit stored in one of the memories has been lost. This is unlike, the previous schemes where photon loss, most of the times is heralded by a failing BSM.

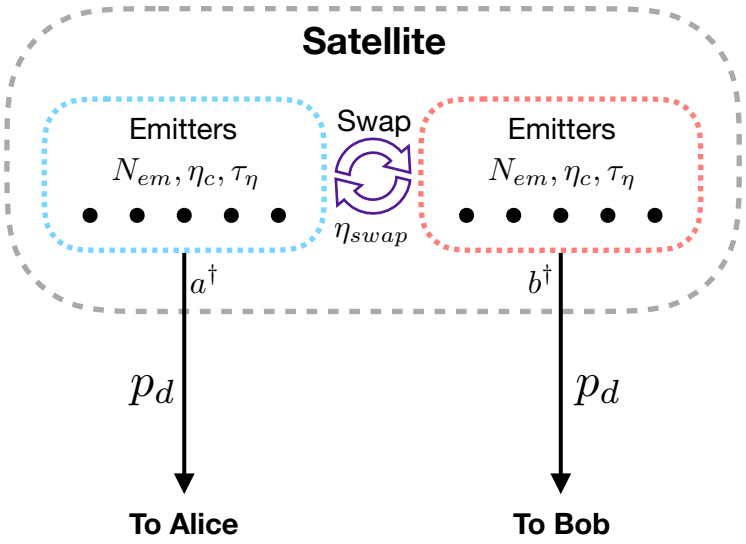


Figure 2.7: Overview of the setup used for the emitter downlink QKD scheme.

2.4.1 Rate

When changing the type of memory in the protocol we also need to modify our expression for the rate of the protocol. Let us start with the expression for $\langle n \rangle$ as given by equation 2.23, but as the swap is done internally and that a decohered qubit only will reduce the fidelity and not lead to an inconclusive BSM we have $p_{load} = 1$,

$$\langle n \rangle = \frac{\sum_n \left[\sum_\Delta p(n,\Delta)\,(n+\Delta) + p_{N_{max}}(n)\,(n+N_{max})\right]}{\sum_{n,\Delta} p(n,\Delta)}, \tag{2.51}$$

where $p(n,\Delta)$ is given by equation 2.24 and $p_{N_{max}}(n)$ by equation 2.25. Evaluating the sums yields,

$$\langle n \rangle^{-1} = p_e \frac{2 - p_e - 2(1-p_e)^{N_{max}+1}}{3 - 2p_e - 2(1-p_e)^{N_{max}+1}}. \tag{2.52}$$

[7] We skipped right past this point when considering ensemble based memories in the previous section. But the fact that being able to perform a BSM on an arbitrary pair of qubits leads to a lower requirement on the memory coherence time, was a significant discovery first made in [27].

We may consider this in two different regimes,

$$\langle n \rangle^{-1} = \frac{2}{3} p_e, \qquad \text{when} \quad \frac{1}{N_{max}} \ll p_e, \tag{2.53}$$

$$\langle n \rangle^{-1} = (1 + 2N_{max}) p_e^2, \qquad \text{when} \quad \frac{1}{N_{max}} \gg p_e. \tag{2.54}$$

As opposed to before, it is not at first apparent when we will be in each regime. The parameter N_{max} is really just a *knob in the lab*, meaning that we have full control over its value. Thus we are in principle always able to reach the good regime of equation 2.53. However increasing the value of N_{max} comes at a cost of lowering the fidelity of the protocol, meaning that it is not always favorable to do so. What value of N_{max} provides a suitable choice will be discussed in section 2.4.3, after we have calculated the fidelity.

With $p_e = p_d \eta_c$ being the probability of entanglement in one arm, η_{swap} being the efficiency of the swap and considering N_{em} emitters, each possessing two memory qubits, in the satellite we acquire the expressions for the rate of the scheme,

$$R = (1 + 2N_{max}) \eta_c^2 p_d^2 \eta_{swap} N_{em} r_{rep}, \qquad \text{when} \quad \frac{1}{N_{max}} \gg p_d \eta_c, \tag{2.55}$$

$$R = \frac{2}{3} \eta_c p_d \eta_{swap} N_{em} r_{rep}, \qquad \text{when} \quad \frac{1}{N_{max}} \ll p_d \eta_c, \tag{2.56}$$

where $r_{rep} = \frac{1}{T_{com}^{S \leftrightarrow G}}$.

2.4.2 Fidelity

We will now characterise the fidelity of the protocol. We start out by considering one half of the system, which starts out in the sate given by equation 2.50,

$$|\psi\rangle_{a,A} = \sqrt{\frac{\eta_c}{2}} \left(|H\rangle_a |0\rangle_A + |V\rangle_a |1\rangle_A \right), \tag{2.57}$$

where a is a photonic mode and A is the sate of the emitter, and we have considered polarisation encoded photonic qubits. After loss in the atmosphere the state is,

$$\rho_{\mathrm{I}}^{(a,A)} = \frac{p_d \eta_c}{2} \left(|H,0\rangle + |V,1\rangle \right) \left(\langle H,0| + \langle V,1| \right) + \frac{1 - p_d \eta_c}{2} \mathbb{1}^{(A)} \otimes |\varnothing\rangle_a \langle \varnothing|, \tag{2.58}$$

where $\mathbb{1}^{(A)} = |0\rangle_A \langle 0| + |1\rangle_A \langle 1|$ is the identity operator on the sate of the emitter. At the detection of Alice we might include the possibility of a dark count with probability $p_{dark} \ll 1$. The state shared by Alice and the satellite is then given by,

$$\rho_{\mathrm{II}}^{(a,A)} = \frac{p_d \eta_c}{2} \left(|H,0\rangle + |V,1\rangle \right) \left(\langle H,0| + \langle V,1| \right) + p_{dark} \frac{1 - p_d \eta_c}{2} \mathbb{1}^{(A)} \otimes |\varnothing\rangle_a \langle \varnothing|, \tag{2.59}$$

Furthermore the decay of the qubit stored in the memory in the satellite will be modelled by the depolarising channel

$$\rho_{\mathrm{II}}^{(a,A)} \to \rho_{\mathrm{III}}^{(a,A)} = \eta_a \rho_{\mathrm{II}}^{(a,A)} + (1 - \eta_a) \operatorname{Tr}_A \left[\rho_{\mathrm{II}}^{(a,A)} \right] \otimes \frac{\mathbb{1}^{(A)}}{2}, \tag{2.60}$$

where $\eta_a = \eta' e^{-t/\tau_\eta}$. Thus the state in Alice's half of the system is,

$$\begin{aligned}\rho_{\mathrm{III}}^{(a,A)} = &\frac{\eta_a p_d \eta_c}{2}\left(|H,0\rangle + |V,1\rangle\right)\left(\langle H,0| + \langle V,1|\right) \\ &+ \left(p_{dark}\,|\varnothing\rangle_a\langle\varnothing| + \frac{(1-\eta_a)p_d\eta_c}{2}\mathbb{P}_1^{(a)}\right)\otimes\frac{\mathbb{1}^{(A)}}{2},\end{aligned} \tag{2.61}$$

where we have used $1 - p_d \approx 1$. Similarly Bob's half is described by the same state $\rho_{\mathrm{III}}^{(b,B)}$, where b is the mode at Bob and B is the mode in the satellite. A Bell state measurement will now be performed on A and B thereby entangling a and b. Without loss of generality we assume $|\psi^+\rangle_{A,B}$ to be the outcome of the measurement,

$$\rho_{\mathrm{III}}^{(a,A)} \otimes \rho_{\mathrm{III}}^{(b,B)} \xrightarrow{\mathrm{BSM}} \rho_{\mathrm{IV}}^{(a,b)} = {}_{A,B}\langle\psi^+|\,\rho_{\mathrm{III}}^{(a,A)} \otimes \rho_{\mathrm{III}}^{(b,B)}\,|\psi^+\rangle_{A,B}\,, \tag{2.62}$$

such that,

$$\begin{aligned}\rho_{\mathrm{IV}}^{(a,b)} = &\frac{\eta_a\eta_b p_d^2\eta_c^2}{4}|\phi^+\rangle_{a,b}\langle\phi^+| + \frac{\eta_a p_d\eta_c}{8}\mathbb{P}_1^{(a)}\otimes\left(p_{dark}\,|\varnothing\rangle_b\langle\varnothing| + \frac{(1-\eta_b)p_d\eta_c}{2}\mathbb{P}_1^{(b)}\right) \\ &+ \left(p_{dark}\,|\varnothing\rangle_a\langle\varnothing| + \frac{(1-\eta_a)p_d\eta_c}{2}\mathbb{P}_1^{(a)}\right)\otimes\frac{\eta_b p_d\eta_c}{8}\mathbb{P}_1^{(b)} \\ &+ \frac{1}{4}\left(p_{dark}\,|\varnothing\rangle_a\langle\varnothing| + \frac{(1-\eta_a)p_d\eta_c}{2}\mathbb{P}_1^{(a)}\right)\otimes\left(p_{dark}\,|\varnothing\rangle_b\langle\varnothing| + \frac{(1-\eta_b)p_d\eta_c}{2}\mathbb{P}_1^{(b)}\right).\end{aligned} \tag{2.63}$$

With $|\phi^+\rangle_{a,b}$ being the ideal state, the fidelity as a function of η_a and η_b becomes,

$$f(\eta_a,\eta_b) = \frac{\langle\phi^+|\,\rho_{\mathrm{IV}}^{(a,b)}\,|\phi^+\rangle}{\mathrm{Tr}\left[\rho_{\mathrm{IV}}^{(a,b)}\right]} = \frac{\eta_a\eta_b + \frac{1}{4}(1-\eta_a\eta_b)}{(1+d)^2}, \tag{2.64}$$

where $d = p_{dark}/(p_d\eta_c)$. From the above equation we see that $p_{dark} \ll p_d\eta_c$ is required for a fidelity close to unity. This is quite unsurprising, as it is really just another way of saying, that we require the majority of the detector clicks to stem from photons from the satellite, instead of being dark counts. Furthermore we also see that for $d = 0$ and $\eta_a, \eta_b \to 0$ we get $F \to 1/4$, as is expected since $\eta = 0$ means the complete loss of correlation between the memory and the emitted photon as seen in equation 2.60. As in equation 2.38 we consider the memory efficiencies η_a and η_b as time dependant and take the average to find the fidelity,

$$F = \sum_{\Delta=0}^{N_{max}} p_\Delta f(\eta(\Delta), \eta_{com}), \tag{2.65}$$

where $\eta_{com} = \eta(T_{com}^{S\leftrightarrow G})$ and p_Δ is probability of the Alice's and Bob's parts of the system being ready with Δ attempts between, and is given by equation 2.39. Evaluating the sum yields

$$F = \frac{1}{(1+d)^2}\left(\frac{1}{4} + \frac{3}{4}\eta_{com}^2\frac{p_e}{1-e^{-\frac{1}{\Delta_m}}(1-p_e)}\frac{1+e^{-\frac{1}{\Delta_m}}(1-p_e) - 2e^{-\frac{N_{max}+1}{\Delta_m}}(1-p_e)^{N_{max}+1}}{2-p_e-2(1-p_e)^{N_{max}+1}}\right), \tag{2.66}$$

where $\Delta_m = \tau_\eta r_{rep}$. Defining $\alpha = (N_{max}+1)/\Delta_m$ and assuming $d \ll 1$, we may expand F in the good and bad memory regime to get,

$$F = (1-2d)\left(\frac{1}{4}+\frac{3}{4}\eta_{com}^2\right), \qquad \text{when} \quad \frac{T_{com}^{S\leftrightarrow G}}{\tau_\eta} \ll p_d\eta_c, \tag{2.67}$$

$$F = (1-2d)\left(\frac{1}{4}+\frac{3}{4}\eta_{com}^2 e^{-\alpha/2}\right), \qquad \text{when} \quad \frac{T_{com}^{S\leftrightarrow G}}{\tau_\eta} \gg p_d\eta_c, \tag{2.68}$$

2.4.3 Optimisation

We now return to the question of what value to choose for the maximum storage time N_{max}. If we require the fidelity of the protocol to be fixed F_0, we may solve equation 2.68 for N_{max} in the regime where $F_0 \sim 1$,

$$N_{max} \approx \frac{2\Delta_m}{3}\left(1+3\eta_{com}^2-4F_0-8d\right)-1 \tag{2.69}$$

which is plotted in figure 2.8 along with the exact solution. We also note that even for $\eta_{com}=1$ and $d=0$ we need $\alpha \sim 1-F_0$. This is a striking difference when compared to the previous scheme with ensemble memories, where $\alpha \sim 1$, as seen in figure 2.5. This will then translate into much higher memory time requirements for the emitters than the ensembles. We can understand this difference by looking at the how we have modelled loss in the two situations. For the ensemble memories we modelled loss of the stored mode a, by the beam splitter transformation $a^\dagger \to \sqrt{1-\mu}\, l_a^\dagger + \sqrt{\mu}\, a^\dagger$, followed by a trace over $l_a^\dagger$. This means that lost qubits are in fact lost, such that when unloading the memory nothing will come out. This in turn will often lead to an unsuccessful BSM, that may be post-selected away. For the emitter we modelled the loss by the depolarising channel, this means that the information stored in the qubit is lost, but the qubit itself is not. Therefore decay in the emitter will not show up as an inconclusive BSM, and are thus not able to be post-selected away.

Substituting the expression for N_{max} into equation 2.55 yields,

$$R = \left(\frac{4\Delta_m}{3}\left(1+3\eta_{com}^2-4F_0-8d\right)-1\right)\eta_c^2 p_d^2 \eta_{swap} N_{em} r_{rep}, \quad \text{when} \quad \frac{T_{com}^{S\leftrightarrow G}}{\tau_\eta} \gg p_d\eta_c. \tag{2.70}$$

2.4.4 Performance

For the performance of the emitter and downlink scheme we refer to figure 2.9, wherein the rate per emitter is shown as a function of memory coherence time. We see that in order to beat the benchmark of 1 Hz we require $N_{em} \geq 15$ and $\tau_\eta \geq 60$ s, with $\eta_c = \eta' = \eta_{swap} = 1$. With coherence times of up to 75 s having being demonstrated in NV centres [28], this requirement is within experimental reach.

When compared with the previous memory scheme involving ensembles, this schemes requires much greater coherence times. The first reason being that the limitation on α imposed by the fidelity, as discussed previously. The other reason for the the long coherence time needed, is that we have considered a scheme without multiplexing. If we had considered a setup where the BSM in the satellite is performed by unloading the photons from memory and mixing them on beamsplitters as described in section 2.3.2, it would be possible to multiplex different NV centres. This would therefore decrease the required memory coherence time by $1/N_{mem}$, just like we saw for the

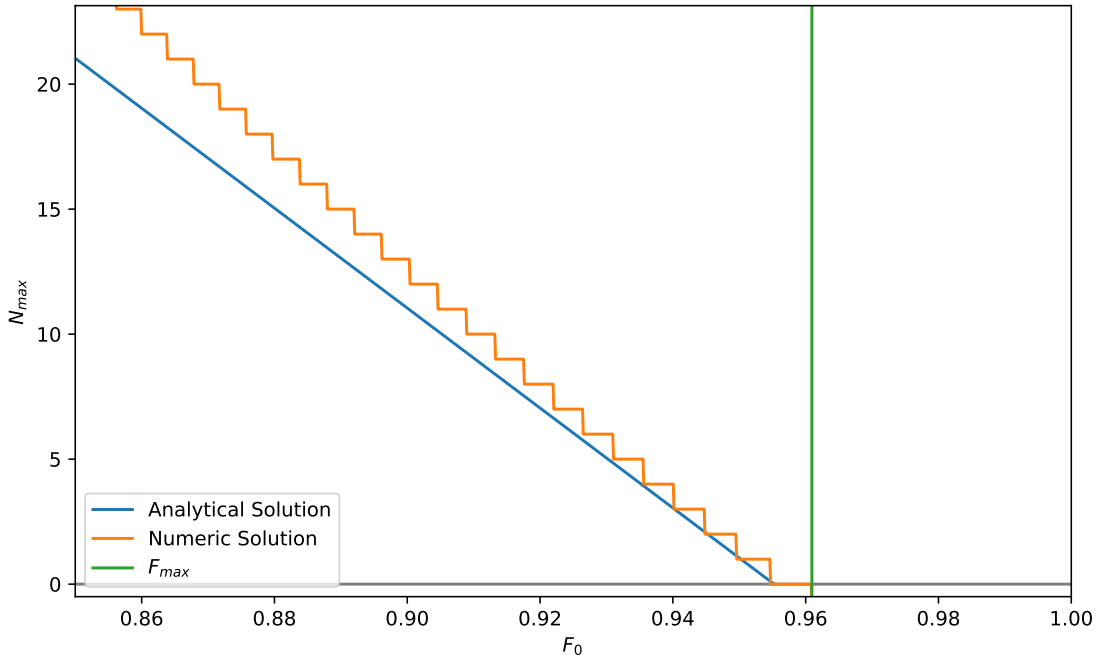


Figure 2.8: Maximum storage time N_{max} needed to achieve a certain fidelity. Analytical model is given by equation 2.69, while the numerical is found by solving equation 2.66. The green line indicate the maximal reachable fidelity $F_{max} = (1 + 3\eta_{com}^2)/(4(1-d)^2)$. Parameters are chosen to be $\eta_c = 0.98$, $p_d = 10^{-3}$, $L = 1000$ km, $d = 0.01$, $\eta' = 1$ and $\tau_\eta = 0.5$ s, to ensure that we are in the bad memory regime.

previous scheme.

Another way of implementing multiplexing, is by utilising NV centres with several nuclear spins coupled to the electronic spin. In [28] the electronic spin of an NV centre is coupled to 9 nuclear spins in the surrounding atoms. Let N_{mem} be the number of addressable memory qubits in a single NV centre,[8] of which we have N_{em} in the satellite. Assume that initially all N_{mem} memory qubits are used to send photons to Alice, and after a photon detection has occurred at Alice, the remaining $N_{mem} - 1$ memory qubits are used to communicate with Bob. This will give the following rate and memory coherence time requirements,

$$R = \frac{N_{mem}(N_{mem}-1)}{2N_{mem}-1} N_{em}\eta_c p_d \eta_{swap} \frac{1}{T_{com}^{s\leftrightarrow g}}, \qquad \text{for} \qquad \tau_\eta \gg \frac{T_{com}^{s\leftrightarrow g}}{(N_{mem}-1)p_d\eta_c} \tag{2.71}$$

Setting $N_{mem} = 2$ in the above equation we recover equation 2.56 as expected and the same memory coherence time requirements. Using this we find that $N_{em} = 5$ NV centres with $N_{mem} = 10$ addressable memory qubits allows us to achieve $R > 1$ Hz with a memory time requirement of $\tau_\eta \geq 6.7$ s, illustrating the advantage of multiplexing memories.

Finally we should address that if NV centres are chosen as the emitter, we run into the problem of the nuclear and electronic spins not being completely independent. For the NV centres used

[8] So one electronic spin coupled to $N_{mem} - 1$ nuclear spins.

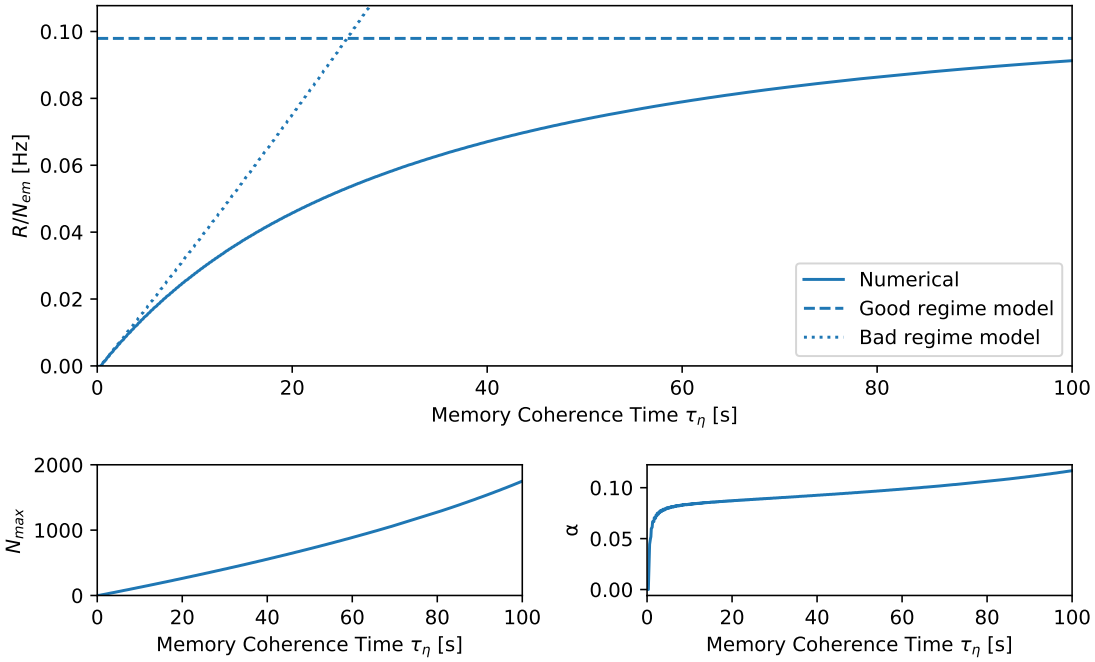


Figure 2.9: (Upper) Rate per emitter in the satellite. Fidelity is fixed at $F_0 = 0.95$, furthermore parameters $\eta_c = 0.98$, $p_d = 10^{-3}$, $\eta_{swap} = 1$, $\eta' = 1$ and $d = 0.01$ are chosen. The dashed and dotted lines are the good and bad regime models as given by equation 2.56 and 2.55 respectively. (Lower left) N_{max} needed in order to ensure $F_0 = 0.95$. (Lower right) α needed in order to ensure $F_0 = 0.95$.

in [26], it is seen that operation of the electronic qubit will cause the memory qubit to dephase. Specifically when storing one of the σ_X or σ_Y eigenstates in the memory qubit, ≈ 270 entangling attempts with the electronic qubit will lead to an e^{-1} decay in the fidelity of the memory qubit. This will severely limit N_{max}, which in turn will make it impossible to enter the good memory regime.

2.5 Ensemble and Uplink

Both of the alternative schemes we have considered so far are limited in their repetition rate by the communication time between the ground and the satellite. This is the case whenever we consider a downlink protocol with memories in the satellite. We can avoid the limitation if we consider uplink protocols, where Alice and Bob sends photons to the satellite, which are loaded onto memories in the satellite. Doing this also only requires two memory qubits in the satellite, one for Alice and one for Bob, as opposed to the downlink schemes considered previously. After the satellite has received a photon from both Alice and Bob, it performs a Bell state measurement on the two qubits and announces the result publicly as before. This scheme is therefore done with the measurement-device-independent quantum key distribution (MDI-QKD) protocol [16]. While the uplink schemes get rid of the harsh limitations on the repetition rate imposed by the communication time, it comes at a cost of lower photon transmission p_u. This is due to the loss stemming from turbulence in the atmosphere, which have a greater impact on uplink schemes compared to downlink schemes,

decreasing the photon transmission by $10 - 20$ dB [29, 30]. Furthermore uplink schemes comes with a new technical challenge, that of quantum nondemolition (QND) detection.

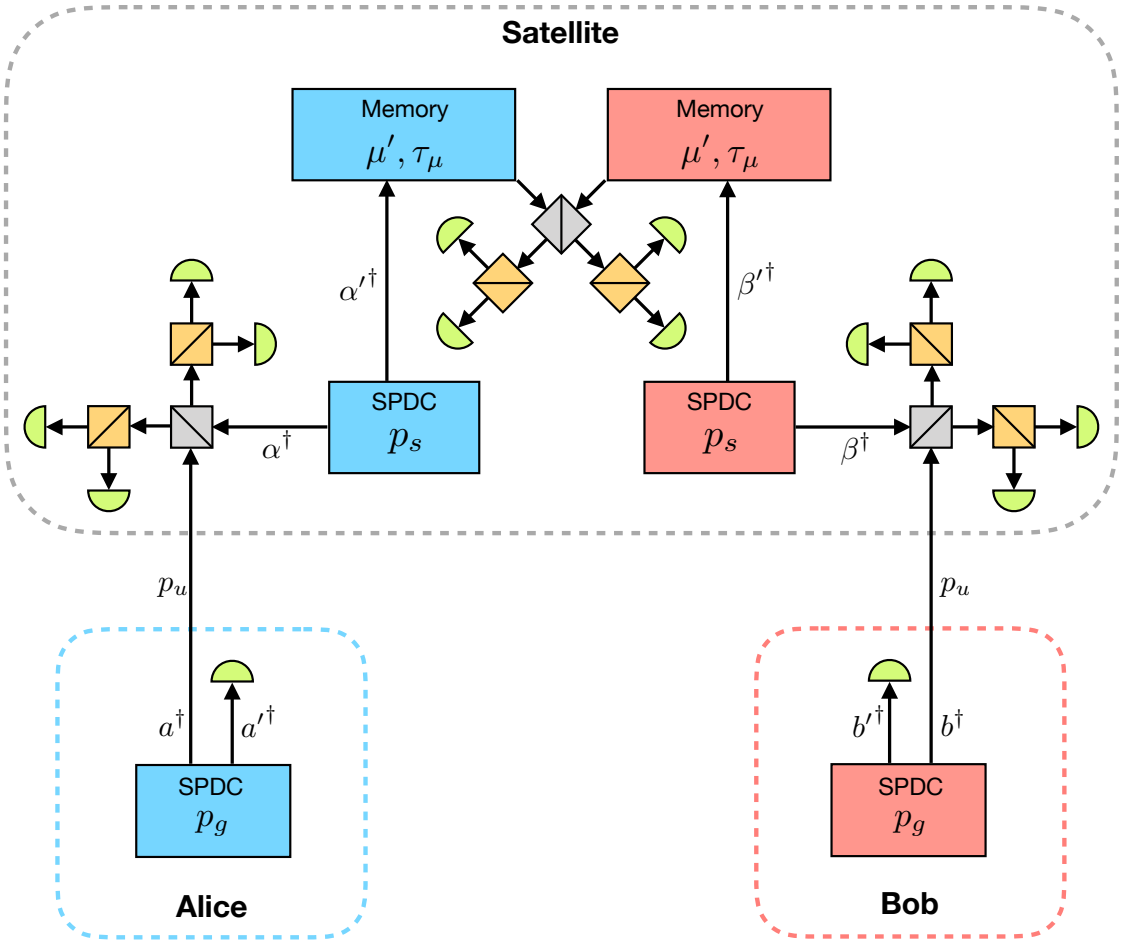


Figure 2.10: Overview of the setup used in the ensemble and uplink QKD scheme.

2.5.1 Photon Teleportation

In order to exploit the advantage of having a memory in the satellite, there needs to be a way of heralding the arrival of a photon, without destroying the information carried by it. A way of doing this is by performing a BSM on the photon coming form the ground, along with one photon from an entangled pair produced in the satellite. This will effectively teleport the information carried by photon from the ground onto the other photon from the entangled pair as seen in figure 2.11.

Let $|\psi\rangle_g = \alpha|0\rangle + \beta|1\rangle$ be the state of the photon arriving from the ground and $|\phi^+\rangle_{b,m} = (|0,0\rangle + |1,1\rangle)/\sqrt{2}$ be the state of two photons produced in the satellite. Measuring the two modes

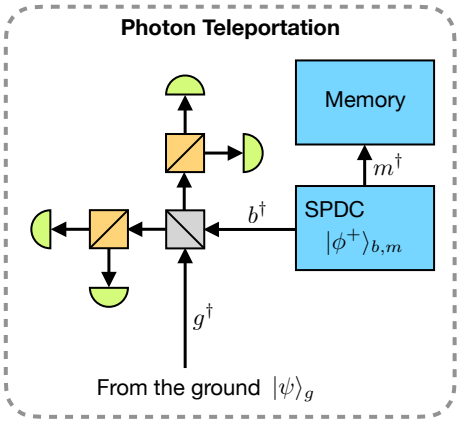


Figure 2.11: Setup considered for employing photon teleportation to load the memory heralded.

g and b in the bell state basis $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$, will project the remaining photon into,

$$\begin{aligned}
|\psi\rangle_g |\phi^+\rangle_{b,m} &\to \alpha |0\rangle_m + \beta |1\rangle_m, \quad \text{for } |\phi^+\rangle_{g,b} \text{ measurement,} \\
|\psi\rangle_g |\phi^+\rangle_{b,m} &\to \alpha |0\rangle_m - \beta |1\rangle_m, \quad \text{for } |\phi^-\rangle_{g,b} \text{ measurement,} \\
|\psi\rangle_g |\phi^+\rangle_{b,m} &\to \beta |0\rangle_m + \alpha |1\rangle_m, \quad \text{for } |\psi^+\rangle_{g,b} \text{ measurement,} \\
|\psi\rangle_g |\phi^+\rangle_{b,m} &\to \beta |0\rangle_m - \alpha |1\rangle_m, \quad \text{for } |\psi^-\rangle_{g,b} \text{ measurement.}
\end{aligned} \tag{2.72}$$

The state is thus transferred, up to a known unitary transformation, to the m mode which is loaded into the memory. As we will see in section 2.5.3 there is severe demands of the photon source used to generate the Bell states in the satellite, which will ultimately lead to this being a inefficient way of heralding photons. In section 2.6 we will consider another and more efficient way to herald the arrival of the photon.

2.5.2 Rate

With an ensemble based memory with time dependant efficiency $\mu(t) = \mu' e^{-t/\tau_\mu}$, we have $\langle n \rangle$ as given by equation 2.27,

$$\langle n \rangle^{-1} = \mu'^2 p_e^2 \frac{e^{\frac{1}{\Delta_m}} \left(1 + (1-p_e) e^{-\frac{1}{\Delta_m}} - 2e^{-\frac{N_{max}+1}{\Delta_m}} (1-p_e)^{N_{max}+1}\right)}{\left(e^{\frac{1}{\Delta_m}} - 1 + p_e\right)\left(3 - 2p_e - 2(1-p_e)^{N_{max}+1}\right)}, \tag{2.73}$$

where the we have used μ' instead of μ_{com}, as this protocol has no reliance on the communication time. We may expand this in the good and bad memory regime,

$$\langle n \rangle^{-1} = \frac{2}{3}\mu'^2 p_e, \qquad \text{when,} \quad \Delta_m \gg \frac{1}{p_e} \gg 1. \tag{2.74}$$

$$\langle n \rangle^{-1} = 2\Delta_m \left(1 - e^{-\alpha}\right) \mu_{com}^2 p_e^2, \qquad \text{when,} \quad p_e \ll \frac{1}{\Delta_m} \ll 1, \tag{2.75}$$

where $\Delta_m = \tau_\mu r_{rep}$ and $\alpha = (N_{max}+1)/\Delta_m$. For the heralding of the photon arrival we will consider using an SPDC producing Bell states with probability p_s, and performing the BSM as

described in section 2.3.2, such that the heralding efficiency becomes $\eta_h = p_s/2$. Finally we will consider SPDCs as photon sources on the ground, producing bell states with probability p_g. The probability of loading a photon into the memory on the satellite is therefore $p_e = p_u p_s p_g/2$. For the central BSM in the satellite we will again load the memory onto beamsplitters, such that $\eta_{swap} = 1/2$. A schematic view of the setup can be seen in figure 2.10. The rate is therefore given by,

$$R = \frac{1}{4}\Delta_m p_s^2 p_g^2 p_u^2 \mu'^2 \left(1 - e^{-\alpha}\right) r_{rep}, \qquad \text{for} \quad p_s p_g p_u \ll \frac{1}{\tau_\mu r_{rep}} \tag{2.76}$$

$$R = \frac{1}{6} p_s p_g p_u \mu'^2 r_{rep}, \qquad \text{for} \quad p_s p_g p_u \gg \frac{1}{\tau_\mu r_{rep}} \tag{2.77}$$

We should note that the repetition rate for the uplink scheme is limited by the memory.

2.5.3 Fidelity

The fidelity of the protocol, as shown in figure 2.10, is a long but otherwise straightforward calculation. Given that the scheme ultimately will turn out to be ineffective, we will not go through the entire calculation in great detail, only to the point where it becomes apparent how and why the stringent demands on the photon sources are there. Starting out with the state as produced on the ground,

$$|\psi\rangle_{a,a'} = \delta_{cond} |\varnothing\rangle + \sqrt{p_1} |\psi^+\rangle - \sqrt{\frac{p_2}{3}} \left(|2H, 2V\rangle + |2V, 2H\rangle + |HV, HV\rangle\right), \tag{2.78}$$

where $\delta_{cond} = 0$ if the state is being conditioned on producing at least two photons and $\delta_{cond} = 1$ if no conditioning occurs. The a' mode is kept at the ground while the a mode is send to the satellite. After loss due to faulty transmission of the a modes, the state is,

$$\begin{aligned}
\rho^{(a,a')} = &\left(\delta_{cond} |\varnothing\rangle + \sqrt{p_1 p_u} |\psi^+\rangle - \sqrt{\frac{p_2 p_u^2}{3}} \left(|2H, 2V\rangle + |2V, 2H\rangle + |HV, HV\rangle\right)\right) \\
&\times \left(\delta_{cond} \langle\varnothing| + \sqrt{p_1 p_u} \langle\psi^+| - \sqrt{\frac{p_2 p_u^2}{3}} \left(\langle 2H, 2V| + \langle 2V, 2H| + \langle HV, HV|\right)\right) \\
&+ \left(\sqrt{\frac{p_1}{2}} |\varnothing, V\rangle - \sqrt{\frac{2p_2 p_u}{3}} |H, 2V\rangle - \sqrt{\frac{p_2 p_u}{3}} |V, HV\rangle\right) \\
&\times \left(\sqrt{\frac{p_1}{2}} \langle\varnothing, V| - \sqrt{\frac{2p_2 p_u}{3}} \langle H, 2V| - \sqrt{\frac{p_2 p_u}{3}} \langle V, HV|\right) \\
&+ \left(\sqrt{\frac{p_1}{2}} |\varnothing, H\rangle - \sqrt{\frac{2p_2 p_u}{3}} |V, 2H\rangle - \sqrt{\frac{p_2 p_u}{3}} |H, HV\rangle\right) \\
&\times \left(\sqrt{\frac{p_1}{2}} \langle\varnothing, H| - \sqrt{\frac{2p_2 p_u}{3}} \langle V, 2H| - \sqrt{\frac{p_2 p_u}{3}} \langle H, HV|\right) \\
&+ p_2 |\varnothing\rangle_a \langle\varnothing| \otimes \frac{\mathbb{P}_2^{(a')}}{3}
\end{aligned} \tag{2.79}$$

	$\|\varnothing\rangle_\alpha$	$\|H\rangle_\alpha$	$\|V\rangle_\alpha$	$\|2H\rangle_\alpha$	$\|2V\rangle_\alpha$	$\|HV\rangle_\alpha$
$\|\varnothing\rangle_a$	No photons	Only one photon	Only one photon	Only one polarisation	Only one polarisation	$p_g p_s^2$ if cond. p_s^2 if no cond.
$\|H\rangle_a$	Only one photon	Only one polarisation	$p_u p_g p_s$	Only one polarisation	$p_u p_g p_s^2$	$p_u p_g p_s^2$
$\|V\rangle_a$	Only one photon	$p_u p_g p_s$	Only one polarisation	$p_u p_g p_s^2$	Only one polarisation	$p_u p_g p_s^2$
$\|2H\rangle_a$	Only one polarisation	Only one polarisation	$p_u^2 p_g^2 p_s$	Only one polarisation	$p_u^2 p_g^2 p_s^2$	$p_u^2 p_g^2 p_s^2$
$\|2V\rangle_a$	Only one polarisation	$p_u^2 p_g^2 p_s$	Only one polarisation	$p_u^2 p_g^2 p_s^2$	Only one polarisation	$p_u^2 p_g^2 p_s^2$
$\|HV\rangle_a$	$p_u^2 p_g^2$	$p_u^2 p_g^2 p_s$	$p_u^2 p_g^2 p_s$	$p_u^2 p_g^2 p_s^2$	$p_u^2 p_g^2 p_s^2$	$p_u^2 p_g^2 p_s^2$

Table 2.2: Overview of the combination of states arriving at the Bell state measurement performed as described in section 2.3.2. Red combinations indicate events that does not lead to the correct detection pattern. Yellow combinations are those which does produce the correct detection pattern, but are unimportant because of their probability of occurring. Green combinations produce the correct detection pattern and occur frequently enough to be important to consider.

where $\mathbb{P}_2 = |2H\rangle\langle 2H| + |2V\rangle\langle 2V| + |HV\rangle\langle HV|$ is the two photon projection operator. The state used for the heralding in the satellite produced by the SPDC is,

$$|\psi\rangle_{\alpha,\alpha'} = |\varnothing\rangle + \sqrt{p_{s1}}\,|\psi^+\rangle - \sqrt{\frac{p_{s2}}{3}}\left(|2H, 2V\rangle + |2V, 2H\rangle + |HV, HV\rangle\right), \tag{2.80}$$

where the α' mode is loaded into the memory. A Bell state measurement is carried out on the a and α modes of the state $\rho^{(a,a')} \otimes |\psi\rangle_{\alpha,\alpha'} \langle\psi|$. Table 2.2 shows the combination of states which will lead to correct detection pattern along with the probability of the term, where we have used $p_g = p_1 = 4p_2/(3p_1)$ and $p_s = p_{s1} = 4p_{s2}/(3p_{s1})$. It should now be apparent why this is a ineffective implementation. In order to achieve fidelity close to unity we need the term $|\psi^+\rangle_{a,a'} |\psi^+\rangle_{\alpha,\alpha'}$ to dominate, which scales like $\sqrt{p_u p_g p_s}$. To suppress the state $|HV\rangle_a |\varnothing\rangle_\alpha$ which is the event where no photons are generated in the satellite, but two photons arrive form the ground, we thus require $p_s \gg p_u p_g$.[9] We also need to suppress the state $|\varnothing\rangle_a |HV\rangle_\alpha$, which stems from the opposite event where no photons arrive form the ground and two are generated in the satellite, we need $p_s \ll p_u$ if conditioning of the sate produced by Alice is happening, and $p_s \ll p_u p_g$ if no conditioning is taking place. Therefore suppressing all events leading to infidelity, is not possible without conditioning. With conditioning we require $1 \gg p_s/p_u \gg p_g$ such that we recover the scaling $R \sim p_u^2$ in the good memory limit, thereby undermining the advantage acquired by having memories in the satellite. We will therefore move on to the next scheme that avoids this downside.

2.6 Emitter and Uplink

So far of the schemes we have examined with memory in the satellite are: Ensemble and Downlink (section 2.3), Emitter and Downlink (section 2.4) and Ensemble and Uplink (section 2.5). In this

[9] It should be noted that even though no photons are loaded into the memory when $|HV\rangle_a |\varnothing\rangle_\alpha$ arrives at the BSM, we do in fact still need to suppress it. If $|HV\rangle_\beta |HV\rangle_{\beta'}$ is made in the other half of the satellite the correct detection pattern is still possible at the central BSM of the setup. Therefore we need to suppress $|HV\rangle_a |\varnothing\rangle_\alpha$ and $|\varnothing\rangle_a |HV\rangle_\alpha$ at the same time.

section we will consider a scheme involving emitters and uplink, specifically a scheme where we will employ emitters as memories in the satellite.

Let us start by considering the heralding of photons at the satellite. One possibility is to let the emitters, which act as a memory, emit a photon entangled with the sate of the emitter,

$$|\psi\rangle_{\alpha,A} = \sqrt{\frac{\eta_c}{2}}\left(|H\rangle_\alpha |0\rangle_A + |V\rangle_\alpha |1\rangle_A\right), \tag{2.81}$$

where $|\cdot\rangle_\alpha$ denotes the emitted photon and $|\cdot\rangle_A$ the state of the emitter. By performing a Bell state measurement on the emitted photon along with the photon coming from the ground, the state will be teleported onto the state of the emitter as described for the previous scheme. This will agian impose stringent demands on the probability $\eta_c^2 p_2$ of emitting and collecting two photons from the emitter. With p_g being the probability of creating a photon at the ground and p_u being the transmission of said photon to the satellite, the requirement becomes $\eta_c p_2 \ll p_g p_u$. Which means that even when using a deterministic photon source at the ground ($p_g \sim 1$) we need $g^{(2)}(0) \ll 10^{-4}$, where $g^{(2)}$ is the second order quantum coherence function of the emitted field. This harsh demand on $g^{(2)}$ leads us to consider an alternative solution for heralding photons.

2.6.1 Mapping Photons by Scattering

Suppose that we have a photonic qubit $|\psi\rangle_\gamma = \alpha|0\rangle + \beta|1\rangle$, which we want to map onto our memory, initially prepared in the state $|+\rangle_M = (|0\rangle + |1\rangle)\sqrt{2}$. Applying a controlled-Z (CZ) gate on the photon and memory entangles the two,

$$|\psi\rangle_\gamma |+\rangle_M \xrightarrow{\text{CZ}} \alpha|0\rangle_\gamma |+\rangle_M + \beta|1\rangle_\gamma |-\rangle_M, \tag{2.82}$$

where $|-\rangle = (|0\rangle - |1\rangle)\sqrt{2}$. We then apply a Hadamard (H) gate to the photon,

$$\xrightarrow{\text{H}} \frac{1}{\sqrt{2}}\Big(|0\rangle_\gamma (\alpha|+\rangle_M + \beta|-\rangle_M) + |1\rangle_\gamma (\alpha|+\rangle_M - \beta|-\rangle_M)\Big). \tag{2.83}$$

Measurement of the photon then projects the state of the memory into,

$$\begin{aligned} |0\rangle_\gamma \text{ detection} &\longrightarrow \alpha|+\rangle_M + \beta|-\rangle_M, \\ |1\rangle_\gamma \text{ detection} &\longrightarrow \alpha|+\rangle_M - \beta|-\rangle_M, \end{aligned} \tag{2.84}$$

meaning we have mapped the qubit from the photon onto the memory, up to a σ_X rotation of the memory qubit. Furthermore, the detection of the photon will serve as heralding of successful photon transmission.

For the physical realisation of the procedure described above, we are going to follow the lead of [31]. The photon is time-bin encoded such that $|0\rangle_\gamma$ is an early photon and $|1\rangle_\gamma$ is a late photon. We place the emitter in a cavity with cavity field $c^\dagger$ as seen in figure 2.12. The emitter has two stable ground state levels $|0\rangle_m$ and $|1\rangle_m$, where the latter is connected to an excited state $|e\rangle_m$. Assuming the cavity field is resonant with the $|1\rangle \leftrightarrow |e\rangle$ transition, the interaction picture Hamiltonian is given by the Jaynes-Cummings model,

$$H = g|e\rangle_m\langle 1| c + g^* |1\rangle_m\langle e| c^\dagger, \tag{2.85}$$

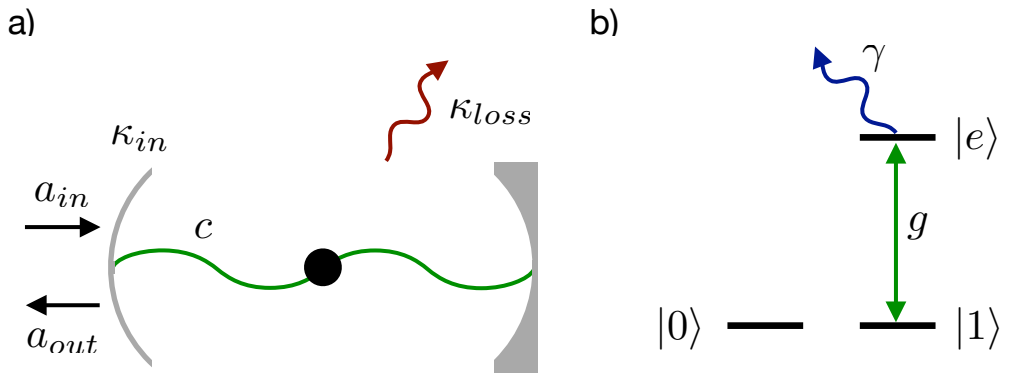


Figure 2.12: a) Overview of the emitter in the cavity. See text for description of the setup. **b)** Level structure of the emitter. The cavity field is resonant with the $|1\rangle \leftrightarrow |e\rangle$ transition. Spontaneous emission out of the cavity with rate γ is considered.

where g is the single photon Rabi frequency and we have set $\hbar = 1$. Furthermore we consider spontaneous emission from the excited level out of the cavity, described by the Lindblad operator $L = \sqrt{\gamma}\,|1\rangle_m\langle e|$. With κ_{in} being the transmission of the input mirror and κ_{loss} the intra-cavity loss rate, we get the total decay rate of the cavity field $\kappa = \kappa_{in} + \kappa_{loss}$. The input-output relations of the the cavity field are

$$\dot{c} = -i\,[c, H] - \frac{\kappa}{2}c + \sqrt{\kappa_{in}}a_{in}, \tag{2.86}$$

$$a_{out} = a_{in} - \sqrt{\kappa_{in}}c, \tag{2.87}$$

where a_{in} corresponds to the input field and a_{out} to the output field. To solve the dynamics of the system, we start by using the Lindblad master equation to find the Fourier transformed equations of motion of the emitter,

$$-i\omega\sigma_z(\omega) = -i2g\int\frac{\mathrm{d}\omega'}{2\pi}\sigma_+(\omega-\omega')c(\omega') + i2g^*\int\frac{\mathrm{d}\omega'}{2\pi}\sigma_-(\omega-\omega')c^\dagger(\omega') - 2\gamma\sigma_{ee}(\omega), \tag{2.88}$$

$$-i\omega\sigma_-(\omega) = ig\int\frac{\mathrm{d}\omega'}{2\pi}\sigma_z(\omega-\omega')c(\omega') - \frac{\gamma}{2}\sigma_-(\omega), \tag{2.89}$$

where $\sigma_z = |e\rangle\langle e| - |1\rangle\langle 1|$, $\sigma_{ee} = |e\rangle\langle e|$ and $\sigma_+ = \sigma_-^\dagger = |e\rangle\langle 1|$. Defining the projection operator $P = |1\rangle\langle 1| + |e\rangle\langle e|$ we may rewrite $\sigma_{ee} = (\sigma_z + P)/2$. By assuming weak cavity field we may neglect terms involving more than one c operator when substituting equation 2.88 into equation 2.89,

$$\sigma_-(\omega) = \frac{-g}{\omega + i\frac{\gamma}{2}}\int\frac{\mathrm{d}\omega'}{2\pi}\frac{-i\gamma P(\omega-\omega')c(\omega')}{\omega-\omega'+i\gamma}. \tag{2.90}$$

By noting that there is no way for the emitter to escape the subspace of $|1\rangle$ and $|e\rangle$, we may write $P(\omega) = 2\pi N_1\delta(\omega)$, where N_1 is the occupation number operator of the state $|1\rangle$ at time $t = 0$ and $\delta(\omega)$ is the Dirac delta function. Using this and substituting equation 2.90 into the Fourier transform of equation 2.86 gives,

$$\sqrt{\kappa_{in}}a_{in}(\omega) = \left(\frac{|g|^2N_1}{\frac{\gamma}{2}-i\omega} + \frac{\kappa}{2} - i\omega\right)c(\omega). \tag{2.91}$$

Evaluating at the cavity frequency $\omega = 0$ and substituting into equation 2.87 yields,

$$a_{out} = S_{N_1} a_{in}, \qquad S_{N_1} = \frac{1 - 2\frac{\kappa_{in}}{\kappa} + 4N_1 C}{1 + 4N_1 C}, \tag{2.92}$$

where the cooperativity of the system $C = |g|^2/\kappa\gamma$ has been defined. Thus for $C \gg 1$ and $\kappa_{loss} \ll \kappa_{in}$ we see that if the emitter starts out in state $|0\rangle_m$ we have $a_{out} \approx -a_{in}$, and if it starts out in $|1\rangle_m$ we get $a_{out} \approx a_{in}$. Therefore depending on the initial state of the emitter the photon picks up a π phase shift.

To implement the the CZ-gate we will exploit the choice of time-bin encoding. The emitter is initially prepared in the state $|0\rangle_M$, such that the early photon picks up the -1 phase when scattering off the cavity. In between the arrival of the early and late photon the emitter is transferred to the $|+\rangle_m$ state, such that the phase of the scattered photon depends on the state of the emitter. We have thus effectively realised the CZ-gate as desired.

Let G be the gate implemented by the scattering of the photon on the cavity. We will now characterise the fidelity of G on the state $|\psi\rangle_\gamma |+\rangle_M$. We may start by writing the action of G as,

$$G = S_0 \left(CZ + \varepsilon \, |1,1\rangle_{\gamma,M} \langle 1,1| \right) \tag{2.93}$$

where $\varepsilon = 1 + \frac{S_1}{S_0}$ and $CZ = |0,0\rangle_{\gamma,M}\langle 0,0| + |0,1\rangle_{\gamma,M}\langle 0,1| + |1,0\rangle_{\gamma,M}\langle 1,0| - |1,1\rangle_{\gamma,M}\langle 1,1|$. Then

$$|\psi(\varepsilon)\rangle = G\,|\psi\rangle_\gamma |+\rangle_M = S_0 \left(\alpha \, |0,+\rangle_{\gamma,M} + \beta \, |1,-\rangle_{\gamma,M} + \frac{\beta\varepsilon}{\sqrt{2}} |1,1\rangle_{\gamma,M} \right). \tag{2.94}$$

For fidelities close to unity we need $|\varepsilon| \ll 1$, which corresponds to the probability of the two paths being almost the same. With $|\psi(0)\rangle$ being the ideal state, we get the fidelity in this regime,

$$F = \frac{|\langle\psi(\varepsilon)|\psi(0)\rangle|^2}{\langle\psi(\varepsilon)|\psi(\varepsilon)\rangle} \approx 1 - \left(1 + |\alpha|^2\right) |\beta|^2 \frac{\varepsilon^2}{4} \tag{2.95}$$

while the probability of succes becomes,

$$\begin{aligned} P_s &= |S_0|^2 \left(|\alpha|^2 + |\beta|^2 \left(1 + \frac{\varepsilon^2}{2} + \varepsilon \right) \right) \\ &\approx 1 - 2\left(1 + |\alpha|^2\right) \frac{\kappa_{loss}}{\kappa_{in}} - |\beta|^2 \frac{1}{2C} \end{aligned} \tag{2.96}$$

where the last expansion has been made for $C \gg 1$ and $\kappa_{loss} \ll \kappa_{in}$. An attractive feature of the fidelity is that $F = 1$ is possible even for $C \sim 1$, all that is required is that $S_1 = -S_0$. Because of this we will moving foreward assume that the mapping of the photon to the emitter is done with unit fidelity but some heralding efficiency $\eta_h \leq 1$.

2.6.2 Rate

The calculation of the rate follows the same procedure as for the scheme with emitter and downlink as presented in section 2.4.1. Inclusion of the heralding efficiency means that $p_e = p_g p_u \eta_h$. With N_{max} being the maximum storage time, r_{rep} the repetition rate and η_{swap} the swapping efficiency we get the following approximate expressions for the rate,

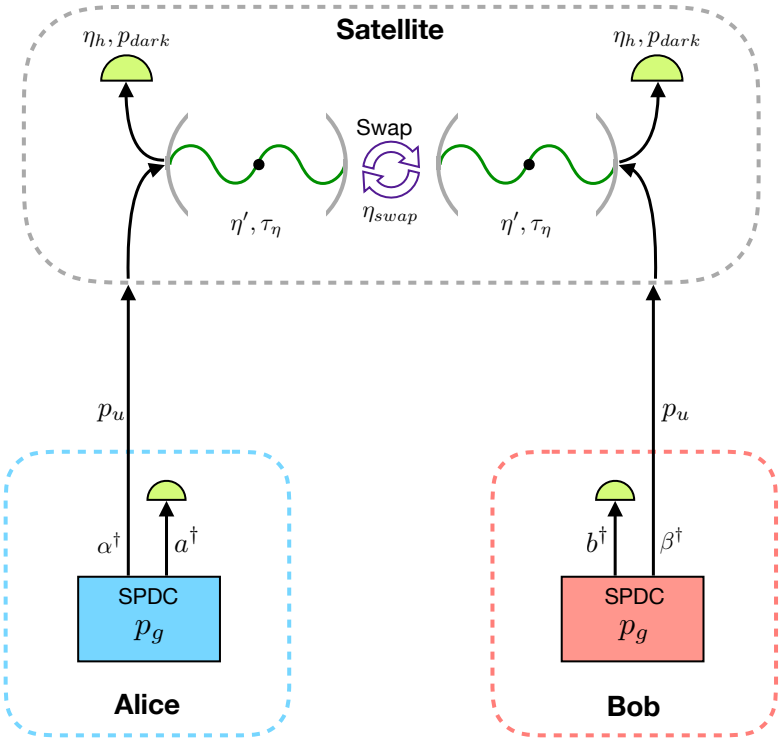


Figure 2.13: Overview of the emitter and uplink scheme.

$$R = \eta_{swap} p_g^2 p_u^2 \eta_h^2 (1 + 2N_{max}) r_{rep} \quad \text{for} \quad \frac{1}{N_{max}} \gg p_u p_g \eta_h \tag{2.97}$$

$$R = \frac{2}{3} \eta_{swap} p_g p_u \eta_h r_{rep} \quad \text{for} \quad \frac{1}{N_{max}} \ll p_u p_g \eta_h \tag{2.98}$$

We note that again r_{rep} is limited by the memory, specifically the temporal width of the photons and the time it takes to perform the unitary rotations of the emitter.

2.6.3 Fidelity

By now the procedure for calculating the fidelity should be familiar. We start out with the state produced by the photon source at the ground,

$$|\psi\rangle_{\alpha,a} = \sqrt{p_0}\,|\varnothing\rangle + \sqrt{p_1}\,|\psi^+\rangle - \sqrt{\frac{p_2}{3}}\left(|2H, 2V\rangle + |2V, 2H\rangle + |HV, HV\rangle\right), \tag{2.99}$$

where $p_0 = 0$ if conditioning of photons is taking place, and $p_0 \approx 1$ if no conditioning is taking place. Guiding the α mode to space towards the satellite, where on the way the photons are lost

with probability $1-p_u$, leaves the state,

$$\begin{aligned}\rho_I^{(\alpha,a)} &= \Big(\sqrt{p_0}\,|\varnothing\rangle + \sqrt{p_1 p_u}\,|\psi^+\rangle\Big)\Big(\sqrt{p_0}\,\langle\varnothing| + \sqrt{p_1 p_u}\,\langle\psi^+|\Big) \\ &+ \left(\sqrt{\frac{p_1}{2}}\,|\varnothing, V\rangle - \sqrt{\frac{2p_2p_u}{3}}\,|H,2V\rangle - \sqrt{\frac{p_2p_u}{3}}\,|V,HV\rangle\right) \\ &\quad\times\left(\sqrt{\frac{p_1}{2}}\,\langle\varnothing, V| - \sqrt{\frac{2p_2p_u}{3}}\,\langle H,2V| - \sqrt{\frac{p_2p_u}{3}}\,\langle V,HV|\right) \\ &+ \left(\sqrt{\frac{p_1}{2}}\,|\varnothing, H\rangle - \sqrt{\frac{2p_2p_u}{3}}\,|V,2H\rangle - \sqrt{\frac{p_2p_u}{3}}\,|H,HV\rangle\right) \\ &\quad\times\left(\sqrt{\frac{p_1}{2}}\,\langle\varnothing, H| - \sqrt{\frac{2p_2p_u}{3}}\,\langle V,2H| - \sqrt{\frac{p_2p_u}{3}}\,\langle H,HV|\right) \\ &+ p_2\,|\varnothing\rangle_\alpha\langle\varnothing|\otimes\frac{\mathbb{P}_2^{(a)}}{3},\end{aligned} \tag{2.100}$$

where we have neglected terms of order p_u^2 as we may safely assume that two photons will not make it to the satellite at the same time. In the satellite the α modes are scattered off the emitter prepared in the state $|+\rangle_A$. After detection of the scattered photon, the qubit is transferred to the emitter as described in the previous section,

$$c_H\,|H\rangle_\alpha + c_V\,|V\rangle_\alpha \to \eta_h\Big(c_H\,|+\rangle_A \pm c_V\,|-\rangle_A\Big), \tag{2.101}$$

where it is $+$ if $|H\rangle_\alpha$ is detected and $-$ if $|V\rangle_\alpha$ is detected. We also account for dark counts in the detector heralding the photons after scattering. This corresponds to the mapping,

$$|\varnothing\rangle_\alpha \to \sqrt{p_{dark}}\,|+\rangle_A\,, \tag{2.102}$$

where p_{dark} is the dark count probability. Therefore we get the sate $\rho_{II}^{(a,A)}$ after scattering,

$$\begin{aligned}\rho_{II}^{(a,A)} &= p_1p_u\eta_h\,|\psi^\pm\rangle_{a,A}\langle\psi^\pm| + p_0p_{dark}\,|\varnothing\rangle_a\langle\varnothing|\otimes|+\rangle_A\langle+| \\ &+ p_1p_{dark}\frac{\mathbb{P}_1^{(a)}}{2}\otimes|+\rangle_A\langle+| + p_2p_{dark}\frac{\mathbb{P}_2^{(a)}}{3}\otimes|+\rangle_A\langle+| \\ &+ \frac{p_2p_u\eta_h}{3}\Big(|HV\rangle_a\,|+\rangle_A \pm \sqrt{2}\,|2H\rangle_a\,|-\rangle_A\Big)\Big(\langle HV|\,\langle+| \pm \sqrt{2}\,\langle 2H|\,\langle-|\Big) \\ &+ \frac{p_2p_u\eta_h}{3}\Big(\sqrt{2}\,|2V\rangle_a\,|+\rangle_A \pm |HV\rangle_a\,|-\rangle_A\Big)\Big(\sqrt{2}\,\langle 2V|\,\langle+| \pm \langle HV|\,\langle-|\Big)\,,\end{aligned} \tag{2.103}$$

where we have introduced the notation $|\psi^\pm\rangle_{a,A} = (|H\rangle_a\,|-\rangle_A \pm |V\rangle_a\,|+\rangle_A)/\sqrt{2}$, with the sign being given by the measurement of the photon. In the emitter the qubit is subject to decay,

$$\rho_{II}^{(a,A)} \to \rho_{III}^{(a,A)} = \eta_A\rho_{II}^{(a,A)} + (1-\eta_A)\,\mathrm{Tr}_A\Big[\rho_{II}^{(a,A)}\Big]\otimes\frac{\mathbb{1}^{(A)}}{2} \tag{2.104}$$

where $\eta_A = \eta(t_a)$, where t_a is the time the qubit spends in the memory. Therefore

$$\begin{aligned}
\rho_{III}^{(a,A)} &= p_1 p_u \eta_h \eta_A \left|\psi^{\pm}\right\rangle \left\langle\psi^{\pm}\right| + \eta_A \rho_{Dark}^{(a)} \otimes \left|+\right\rangle_A \langle +| \\
&+ \frac{p_2 p_u \eta_h \eta_A}{3} \left(\left|HV\right\rangle_a \left|+\right\rangle_A \pm \sqrt{2}\left|2H\right\rangle_a \left|-\right\rangle_A\right) \left(\left\langle HV\right| \left\langle +\right| \pm \sqrt{2}\left\langle 2H\right| \left\langle -\right|\right) \\
&+ \frac{p_2 p_u \eta_h \eta_A}{3} \left(\sqrt{2}\left|2V\right\rangle_a \left|+\right\rangle_A \pm \left|HV\right\rangle_a \left|-\right\rangle_A\right) \left(\sqrt{2}\left\langle 2V\right| \left\langle +\right| \pm \left\langle HV\right| \left\langle -\right|\right) \\
&+ (1-\eta_A)\left(\rho_{Dark}^{(a)} + p_u\left(p_1 \frac{\mathbb{P}_1^{(a)}}{2} + 2p_2 \frac{\mathbb{P}_2^{(a)}}{3}\right)\right) \otimes \frac{\mathbb{1}^{(A)}}{2},
\end{aligned} \tag{2.105}$$

where we have defined $\rho_{Dark} = p_0 p_{dark} \left|\varnothing\right\rangle\!\left\langle\varnothing\right| + p_1 p_{dark} \frac{\mathbb{P}_1}{2} + p_2 p_{dark} \frac{\mathbb{P}_2}{3}$. The last part of the protocol is to perform a Bell state measurement on the two emitters of the state $\rho_{III}^{(a,A)} \otimes \rho_{III}^{(b,B)}$. For a fidelity close to unity we require $p_{dark} \ll p_u \eta_h$, this also allows us to neglect the terms with dark counts in both halves of the system, which in turn cancels the difference in probability of measuring $\left|\psi^{\pm}\right\rangle_{A,B}$ and $\left|\phi^{\pm}\right\rangle_{A,B}$. Thus we may, without loss of generality, assume $\left|\phi^{+}\right\rangle_{A,B}$ to be the outcome of the BSM, thereby projecting the state into,

$$\begin{aligned}
\sigma^{(a,b)} &= \left\langle\phi^{+}\right| \rho_{III}^{(a,A)} \otimes \rho_{III}^{(b,B)} \left|\phi^{+}\right\rangle_{A,B} \\
&= \frac{p_1^2 p_u^2 \eta_h^2 \eta_A \eta_B}{4} \left|\phi^{+}\right\rangle_{a,b} \left\langle\phi^{+}\right| + \frac{p_1 p_u \eta_h}{4} \eta_A \eta_B \left(\rho_{Dark}^{(a)} \otimes \left|V\right\rangle_b \langle V| + \left|V\right\rangle_a \langle V| \otimes \rho_{Dark}^{(b)}\right) \\
&+ \frac{p_1 p_u \eta_h}{4} \eta_A (1-\eta_B) \frac{\mathbb{P}_1^{(a)}}{2} \otimes \left(\rho_{Dark}^{(b)} + p_u \eta_h \left(p_1 \frac{\mathbb{P}_1^{(b)}}{2} + 2p_2 \frac{\mathbb{P}_2^{(b)}}{3}\right)\right) \\
&+ \frac{p_1 p_u \eta_h}{4} (1-\eta_A) \eta_B \left(\rho_{Dark}^{(a)} + p_u \eta_h \left(p_1 \frac{\mathbb{P}_1^{(a)}}{2} + 2p_2 \frac{\mathbb{P}_2^{(a)}}{3}\right)\right) \otimes \frac{\mathbb{P}_1^{(b)}}{2} \\
&+ \frac{p_1 p_2 p_u^2 \eta_h^2 \eta_A \eta_B}{12} \left(\left|H, HV\right\rangle_{a,b} + \sqrt{2}\left|V, 2H\right\rangle_{a,b}\right) \left(\left\langle H, HV\right| + \sqrt{2}\left\langle V, 2H\right|\right) \\
&+ \frac{p_1 p_2 p_u^2 \eta_h^2 \eta_A \eta_B}{12} \left(\left|V, HV\right\rangle_{a,b} + \sqrt{2}\left|H, 2V\right\rangle_{a,b}\right) \left(\left\langle V, HV\right| + \sqrt{2}\left\langle H, 2V\right|\right) \\
&+ \frac{p_1 p_2 p_u^2 \eta_h^2 \eta_A \eta_B}{12} \left(\left|HV, H\right\rangle_{a,b} + \sqrt{2}\left|2H, V\right\rangle_{a,b}\right) \left(\left\langle HV, H\right| + \sqrt{2}\left\langle 2H, V\right|\right) \\
&+ \frac{p_1 p_2 p_u^2 \eta_h^2 \eta_A \eta_B}{12} \left(\left|HV, V\right\rangle_{a,b} + \sqrt{2}\left|2V, H\right\rangle_{a,b}\right) \left(\left\langle HV, V\right| + \sqrt{2}\left\langle 2V, H\right|\right) \\
&+ \frac{p_1 p_u \eta_h \eta_A (1-\eta_B)}{4} \rho_{Dark}^{(a)} \otimes \frac{\mathbb{P}_1^{(b)}}{2} + \frac{p_1 p_u \eta_h (1-\eta_A) \eta_B}{4} \frac{\mathbb{P}_1^{(a)}}{2} \otimes \rho_{Dark}^{(b)} \\
&+ \frac{p_1^2 p_u^2 \eta_h^2 (1-\eta_A)(1-\eta_B)}{4} \frac{\mathbb{P}_1^{(a)}}{2} \otimes \frac{\mathbb{P}_1^{(b)}}{2} \\
&+ \frac{p_1 p_u \eta_h (1-\eta_A)(1-\eta_B)}{4} \left(\frac{\mathbb{P}_1^{(a)}}{2} \otimes \rho_{Dark}^{(b)} + \rho_{Dark}^{(a)} \otimes \frac{\mathbb{P}_1^{(b)}}{2}\right) \\
&+ \frac{p_1 p_2 p_u^2 \eta_h^2 (1-\eta_A)(1-\eta_B)}{2} \left(\frac{\mathbb{P}_1^{(a)}}{2} \otimes \frac{\mathbb{P}_2^{(b)}}{3} + \frac{\mathbb{P}_2^{(a)}}{3} \otimes \frac{\mathbb{P}_1^{(b)}}{2}\right) \\
&+ \frac{p_1 p_2 p_u^2 \eta_h^2}{2} \left((1-\eta_A)\eta_B \frac{\mathbb{P}_1^{(a)}}{2} \otimes \frac{\mathbb{P}_2^{(b)}}{3} + \eta_A (1-\eta_B) \frac{\mathbb{P}_2^{(a)}}{3} \otimes \frac{\mathbb{P}_1^{(b)}}{2}\right).
\end{aligned} \tag{2.106}$$

With $|\phi^+\rangle_{a,b}$ being the ideal state we may find the fidelity,

$$f(\eta_A, \eta_B) = \frac{\frac{1}{4}(1 + 3\eta_A\eta_B + 2d)}{1 + 2\frac{d}{p_1} + 4p_2^*} \approx \frac{1}{4}\left(1 + 3\eta_A\eta_B\left(1 - 2\frac{d}{p_1} - 4p_2^*\right) - 2\frac{d}{p_1}(1 - p_1) - 4p_2^*\right), \tag{2.107}$$

where we have defined $d = p_{dark}/p_u\eta_h$ and $p_2^* = p_2/p_1$. If we assume that Alice and Bob measure on the a and b modes as shown in figure 2.13, conditioning will occur such that effectivily $p_0 = 0$, $p_1 \approx 1$ and $p_2^* = 3p_g/4$. With this we may find the average fidelity by averaging over the storage times. Carrying out an expansion in the good and bad memory regime yields,

$$F = \frac{1}{4}(1 - 3p_g) + \frac{3}{4}\eta'^2 e^{-\alpha/2}(1 - 2d - 3p_g) \qquad \text{for} \quad p_g p_u \eta_h \ll \frac{1}{\tau_\eta r_{rep}} \tag{2.108}$$

$$F = \frac{1}{4}(1 - 3p_g) + \frac{3}{4}\eta'^2 (1 - 2d - 3p_g) \qquad \text{for} \quad p_g p_u \eta_h \gg \frac{1}{\tau_\eta r_{rep}} \tag{2.109}$$

where $\alpha = \frac{N_{max}+1}{\tau_\eta r_{rep}}$.

2.6.4 Optimisation

With $\eta' = 1$, the maximal achievable fidelity of the protocol is given by,

$$F_{max} = \lim_{p_g, \alpha \to 0} F = 1 - \frac{3}{2}d - \frac{1}{2}p_0 d. \tag{2.110}$$

All fidelities $F < F_{max}$ are achievable by suitable choice of p_g and α. Since there is two variables to tune, this leaves an extra degree of freedom in the choice of p_g and α. This extra freedom can be used to maximise the rate of the protocol. In the bad memory limit given by equation 2.108 optimisation over α and p_g given that a certain fidelity F_0 is desired yields,

$$\alpha \approx \frac{8}{9}(F_{max} - F_0), \qquad p_g \approx \frac{2}{9}(F_{max} - F_0) \tag{2.111}$$

valid for $F_{max} - F_0 \ll 1$. Again we see that $\alpha \ll 1$ is needed in the bad memory limit as compared to $\alpha \sim 1$ for the ensemble memory based schemes. Furthermore in the good memory limit and with $\eta' = 1$ we get that $p_g = (F_{max} - F_0)/3$ such that, with perfect memory the rate of the protocol becomes,

$$R = \frac{2}{9}\eta_{swap}(F_{max} - F_0)\, p_u \eta_h r_{rep} \tag{2.112}$$

Finally exact optimisation over α and p_g has been carried out numerically as seen in figure 2.14 along with the analytical expressions shown in the section.

2.6.5 Performance

For the performance of the protocol we consider $p_u = 10^{-4}$, $d = 0.005$, $\eta_{swap} = \eta' = 1$ and a target fidelity of $F_0 = 0.95$. Current experiments with silicon vacancies (SiV) achieves coherence times of $\tau_\eta = 0.2$ ms and heralding efficiencies of $\eta_h = 0.425$ while operating at $R_{rep} = 1.2$ MHz [32], yielding a rate of $R = 3.66 \times 10^{-6}$ Hz. By transferring the stored qubit from the SiV electronic

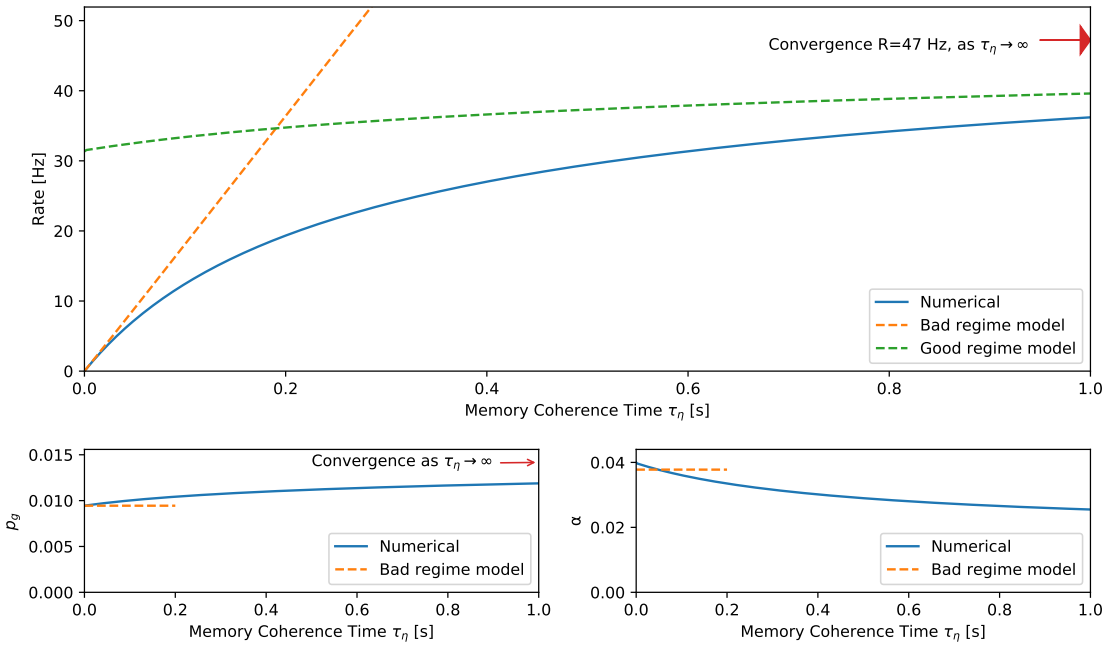


Figure 2.14: (Upper) Optimised rate as a function of memory coherence time with $F_0 = 0.95$, $\eta_{swap} = \eta' = 1$, $\eta_h = 0.5$, $p_u = 10^{-4}$, $r_{rep} = 10^8$ Hz and $d = 0.005$. The solid blue line is numerical optimisation done on the exact expressions while the dashed good and bad memory models are given by equation 2.98 and 2.97 respectively with p_g and α from the numerical optimisation. The red arrow shows the convergence of the rate as $\tau_\eta \to \infty$, which is the rate with perfect memory as given by equation 2.112. (Lower left) The optimised values of p_g along the approximation as $\tau_\mu \to 0$ as given by equation 2.111. The red arrow shows the convergence for $\tau_\eta \to \infty$, as given by $p_g = (F_{max} - F_0)/3$. (Lower right) The optimised values of α along with the bad memory approximation as given by equation 2.111. In the perfect memory limit $\tau_\eta \to \infty$ we expect $N_{max} \to \infty$ but in such a way that $\alpha \to 0$.

spin to the nuclear spin coherence times of $\tau_\eta = 0.2$ s have been demonstrated [33], increasing the rate to $R = 3.65 \times 10^{-3}$ Hz. By employing temporal multiplexing where one fits several early photons in before the $|0\rangle_M \to |+\rangle_M$ rotation of the emitter, one should be able to run the protocol with $r_{rep} = 3 \times 10^7$ Hz, yielding $R = 1.89$ Hz thereby making the benchmark of the direct link satellite well within experimental reach. We should however note that the demands on the dark count rate is higher when compared to all the other schemes presented, primarily due to p_u being smaller than p_d.

2.7 Summary

We will now try to summarise what we have figured out about satellite QKD. Before turning to the direct comparison of the different proposed schemes, we will take a step back and state the main effects having influence on the performance and requirements of satellite QKD:

- *Low repetition rate for downlink schemes.* The need to store the qubits in the memory for the time it takes a photon to reach the ground and the message of success to come back to the satellite means that $r_{rep} \leq \frac{1}{T_{com}^{S \leftrightarrow G}}$. This can be compensated by adding memories capable

of storing several qubits in the satellite.

- *Downlink schemes with probabilistic sources requires high multimode capacity.* In order to suppress the four-photons contributions to the state produced by the photon source, the Bell state generation probability needs to be low ($p_s \ll 1$). This in turn means that the memories most of the times store vacuum. The multimode requirements with a probabilistic source is therefore $N_{mem,prob} = N_{mem,det}/p_s$, where $N_{mem,det}$ is the requirement for deterministic sources.

- *Multiplexing memories leads to lower coherence time requirements.* With the ability to multiplex N_{mem} modes, the required coherence times is lowered by $1/N_{mem}$ compared to schemes without multiplexing.

- *Heralded loss in memories, require smaller coherence times.* The decay process of the ensemble memories allows for $10 - 100$ times longer storage times than the decoherence of the emitter for the same coherence times.

- *Uplink schemes require effective heralding of photons.* While the uplink schemes only requires two memory qubits in the memory, one for Alice and one for Bob, the challenge will be to herald the arrival of the photon without losing the information in the qubit.

2.7.1 Satellite Height

While a full orbital analysis is beyond the scope of this project,[10] there is one orbit parameter which we will briefly mention: satellite height. Throughout this chapter we have used $L = 1000$ km for the distance from Alice and Bob to the satellite. This of course is a bit unrealistic, as satellites needs to move in order to avoid falling down. As the satellite moves across the sky, the distance from Alice and Bob to the satellite will change, and for most orbits of the satellite the distance from Alice and Bob to the satellite will be different. Satellite height is particularly interesting as it allows us to judge what implementations will be relevant as we increase the satellite height from low earth orbit ($L \leq 2000$ km) to geostationary orbit ($L \approx 36000$ km), where the position of the satellite as viewed from earth will be constant. We will assume that as the photons propagate through the vacuum of space the only major contribution to loss will be beam diffraction scaling as L^2. Furthermore any increase in satellite height will increase the communication time as linearly in L. The rightmost column of table 2.3 shows how the rate of the different schemes scales with L under this assumption.

2.7.2 Scheme comparison

When comparing the different proposed schemes as seen in table 2.3, the emitter uplink scheme (2.6) stands out as the most promising implementation. The high repetition rate, only limited by the operation of the memory in the satellite, poses low requirements on the coherence time of the memory while simultaneously providing high rate. Furthermore it only requires the storage of maximum two qubits at a time, and scales best with added height, thereby making it the most promising candidate for a geostationary orbit satellite. Thus it seemingly outperforms all the other schemes, with the only drawback being greater requirements on the dark count rate of the detectors

[10] Some amount of orbital analysis was carried out in [34], if the reader should be interested.

Sec.	Scheme	Rate	τ	Benchmark N_{mem}	Benchmark τ	L Scaling
2.2	Direct Downlink	$p_d^2 p_s r_{rep}$	-	-	-	L^{-4}
2.3	Ensemble Downlink	$\frac{1}{3}\mu_{com}^2 N_{mem} p_s p_d \frac{1}{T_{com}^{S\leftrightarrow G}}$	$\tau_\mu \gg \frac{T_{com}^{S\leftrightarrow G}}{N_{mem} p_s p_d}$	1000	0.5 s	L^{-3}
2.4	Emitter Downlink	$\frac{2}{3}\eta_{swap} N_{em} p_d \eta_c \frac{1}{T_{com}^{S\leftrightarrow G}}$	$\tau_\eta \gg \frac{T_{com}^{S\leftrightarrow G}}{p_d \eta_c}$	15	60 s	L^{-3}
2.5	Ensemble Uplink	$\frac{1}{6}{\mu'}^2 p_g p_s p_u r_{rep}$	$\tau_\mu \gg \frac{1}{p_g p_s p_u r_{rep}}$	*Not possible*		L^{-4}
2.6	Emitter Uplink	$\frac{2}{3}\eta_{swap} p_g p_u \eta_h r_{rep}$	$\tau_\eta \gg \frac{1}{p_g p_u \eta_h r_{rep}}$	1	0.2 s	L^{-2}

Table 2.3: Performance overview for the different QKD schemes at satellite height of $L = 1000$ km. *Rate:* Rate of the protocol in the good memory limit. τ: Requirement on the memory coherence time. *Benchmark:* Requirements of the memory in order to beat the benchmark of $R = 1$ Hz. L *scaling:* Scaling in rate of distance from the ground stations to the satellite L.

in the satellite.

Another encouraging proposal, with possibly the highest performance ceiling, is the ensemble downlink scheme (2.3). With further improvements to the memory efficiency and multimode capabilities, the benchmark is within reach. This scheme is particularly interesting if it can be paired with a deterministic source of entangled photons, thereby increasing the the rate and lowering the coherence time requirements by up to two orders of magnitude.

Finally the emitter uplink scheme (2.4) is also worth a mention. The deterministic nature of its entanglement generation leads to low multimode capacity requirements. The major drawback is the long coherence time, which can partially be overcome if multiplexing is possible.

Chapter 3

Entanglement Distribution

In this chapter we will consider how satellites can be used for entanglement distribution between Alice and Bob. Conceptually entanglement distribution works very similar to QKD, with the only major difference being that instead of Alice and Bob measuring on the qubits they receive they load them into a memory. This is interesting to study because a shared Bell state between Alice and Bob allows them to perform protocols such as super-dense coding [35, p. 97-98], remote state preparation [36] or quantum teleportation [35, p. 26-28]. Furthermore it might even allow for coupling several entanglement distribution setups together to form a quantum repeater to extend the range of communication even further. We will discuss this last point further in chapter 4.

3.1 Direct Downlink

The first scheme that we will consider in this chapter is the based on direct downlink as presented in section 2.2, the structure of this scheme was first proposed in [34]. We consider the scheme where a SPDC produces entangled photon-pairs and sends them to the ground. The SPDC is driven in such a way that with probability p_s the Bell-state $|\psi^-\rangle_{ab} = (|H\rangle_a |V\rangle_b - |H\rangle_a |V\rangle_b)/\sqrt{2}$ is created each repetition. The full state produced by the SPDC each repetition is,

$$|\psi\rangle_{ab} = |\varnothing\rangle + \sqrt{p_s}\,|\psi^-\rangle_{ab} + \frac{p_s}{2}\left(|2H\rangle_a |2V\rangle_b + |2V\rangle_a |2H\rangle_b - |HV\rangle_a |HV\rangle_b\right). \tag{3.1}$$

With the satellite producing $|\psi\rangle_{ab}$ with repetition rate R_{rep}, the rate of Bell state generation is thus given by $R_S = p_s r_{rep}$. On the way to the ground the photons encounter loss such that the probability of a photon completing the journey is p_d. At the ground stations of Alice and Bob the arrival of the photons needs to be heralded, which occurs with probability η_h and stored onto a memory. Collecting everything the rate of the protocol thus becomes,

$$R = \eta_h^2 p_d^2 p_s r_{rep}. \tag{3.2}$$

In figure 3.1 a schematic view of this implementation is shown.

3.1.1 Repetition Rate

Just like with the memory assisted schemes presented in the previous chapter, we need to take the communication time into account when considering the limitation of the repetition rate. For this

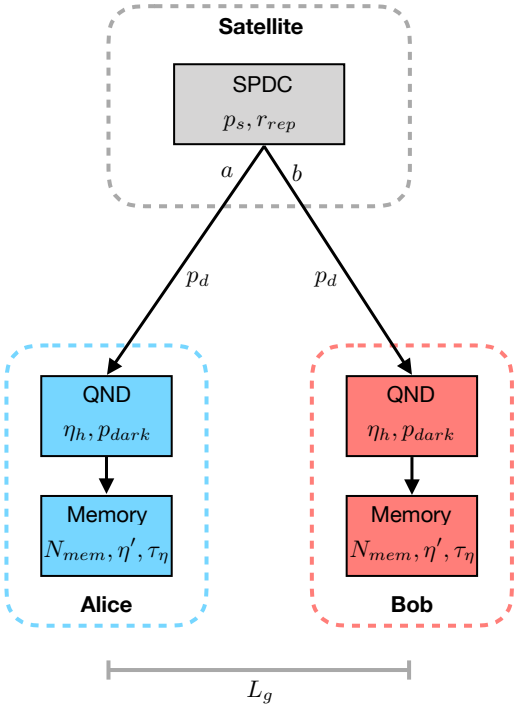


Figure 3.1: The setup used for the direct downlink entanglement distribution scheme. The photons are loaded into memories at the ground stations. Heralding of the photons is represented by QND detectors in this figure, but it should be noted that the heralding can be done after the memory, as seen in the previous chapter.

scheme however the relevant communication time is the time it takes for Alice to send a message to Bob and vice versa,

$$T_{com}^{g\to g} = \frac{L_g}{c}, \tag{3.3}$$

where L_g is the distance between Alice and Bob and c is the speed of light. After Alice has received a photon form the satellite, she will send a message to Bob, informing him of what repetition the photon arrived. At the same time Bob should send a similar message if he received a photon. While Alice waits for the message from Bob she needs to store the qubit in memory, thereby taking up a slot in the memory. If there is no message from Bob at time $T_{com}^{g\to g}$ after Alice received the photon, Alice will know that Bob did not receive the other half of the entangled photon pair, and she may reset her memory and start over. If both Alice and Bob receives photons from the same entangled pair they will thus send out a message to each other, and after $T_{com}^{g\to g}$ get a message from the other person informing them of the protocol being successful.

Let us start by considering how this limits the repetition rate in the case where there is only a single memory qubit $N_{mem} = 1$ available at each ground station. Let $\langle T_\gamma \rangle = 1/p_d p_s \eta_h r_{rep}$ be the average time between photons reaching a ground station, then including the time $T_{com}^{g\to g}$ during which the signal from the satellite is blocked due to the memory being full, we get the effective

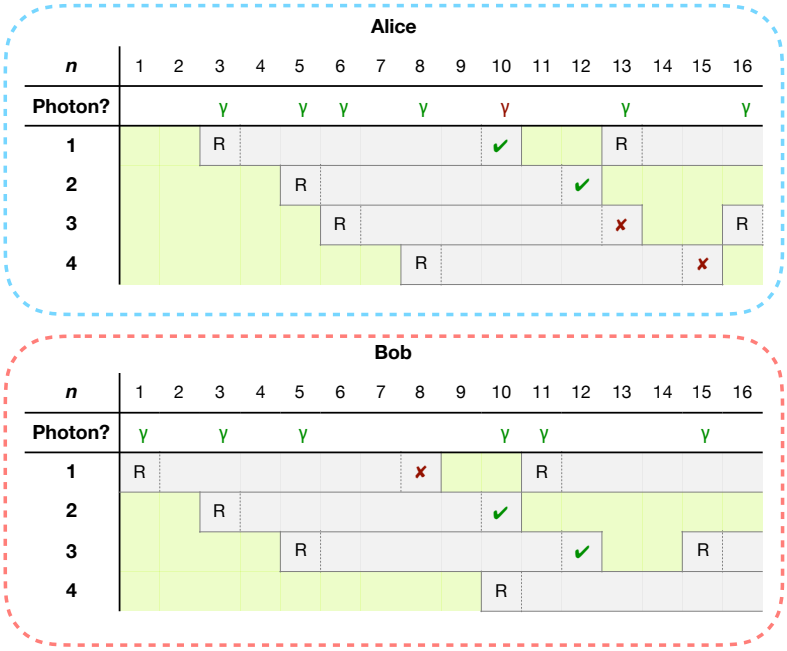


Figure 3.2: Memory usage in the direct downlink protocol with $N_{mem} = 4$ for both Alice and Bob. Green (red) γ indicate arrival of a photon for which there is (no) space in the memory. After a photon is loaded into the memory it needs to be stored until Alice and Bob figures out if the opposing partner received a photon. Checks means that entanglement was effectively distributed, while crosses represents the events where only one photon made it to the ground. Here $T_{com}^{g\to g} r_{rep} = 7$ is used.

time between photons reaching the ground station,

$$\left\langle T_\gamma^{eff} \right\rangle = \langle T_\gamma \rangle + T_{com}^{g\to g}. \tag{3.4}$$

With this we get an effective average rate of the protocol,

$$r_{rep}^{eff} = \frac{\langle n_\gamma \rangle}{\frac{\langle n_\gamma \rangle}{r_{rep}} + T_{com}^{g\to g}} \leq r_{rep}, \tag{3.5}$$

where $\langle n_\gamma \rangle = 1/p_d p_s \eta_h$ is the average number of repetitions between a photon reaching the ground station. For the protocol we consider here $T_{com}^{g\to g} \gg \langle T_\gamma \rangle$[1], meaning that $r_{rep}^{eff} = \langle n_\gamma \rangle / T_{com}^{g\to g}$. Finally we should also consider the probability of the second photon being in the memory. For $T_{com}^{g\to g} \gg \langle T_\gamma \rangle$ the memories at Alice and Bob are essentially always full, meaning that this probability is $\langle T_\gamma \rangle / T_{com}^{g\to g}$, yielding the rate

$$R = \frac{1}{p_s T_{com}^{g\to g\,2} r_{rep}} \tag{3.6}$$

[1]If we assume the Alice, Bob and Satellite setup to be an equilateral triangle with sides $L \sim 1000$ km we get $T_{com}^{g\to g} = L/c \approx 1/300$ s, while $\langle T_\gamma \rangle = 1/1000$ s. For geostationary orbit $p_d \approx 10^{-5}$ such that $\langle T_\gamma \rangle = 1/10$ s, meaning that the communication time no longer is the limiting factor.

We now consider the situation of having multimode memories being able to store N_{mem} qubits. The advantage of multimode memories being that of being able to receive photons from the satellite while waiting for the signal from the ground station from a previous click. We will let p_a be the probability that there is space in the memory for a photon given that it has reached the ground, such that the rate of the protocol becomes,

$$R = \eta_n^2 p_d^2 p_a^2 p_s r_{rep} \tag{3.7}$$

To find p_a we need to consider the probability of the memory having an empty slot,

$$p_a = \sum_{k=0}^{N_{mem}-1} P_{\text{Binom.}}(k, N_w, p_a p_e), \tag{3.8}$$

where $N_w = T_{com}^{g\to g} r_{rep}$ is the amount of time each memory is occupied after being filled, $p_e = p_d \eta_h p_s$ is the entanglement probability and $P_{\text{Binom.}}(k, n, p)$ being the binomial distribution,

$$P_{\text{Binom.}}(k, n, p) = \binom{n}{k} p^k (1-p)^{n-k}. \tag{3.9}$$

Solving equation 3.8 is not possible analytically,[2] but we should still be able to make some statements on the behaviour of p_a. First and foremost as $N_w \gg 1$ and $p_e \ll 1$ we may approximate the binomial distribution as a Poisson distribution with mean $p_a\lambda$, where $\lambda = N_w p_e = T_{com}^{g\to g}/\langle T_\gamma \rangle$,

$$\begin{aligned} p_a &= \sum_{k=0}^{N_{mem}-1} P_{\text{Pois}}(k, p_a\lambda), \qquad P_{\text{Pois}}(k,\lambda) = \frac{\lambda^k e^{-\lambda}}{k!} \\ &= \frac{\Gamma(N_{mem}, p_a\lambda)}{\Gamma(N_{mem})}, \end{aligned} \tag{3.10}$$

where $\Gamma(N_{mem})$ is the gamma function and $\Gamma(N_{mem}, \lambda)$ is the upper incomplete gamma function. Setting $N_{mem} = 1$ yields the equation $p_a = e^{-p_a\lambda}$, which may be solved,

$$p_a = e^{-W_0(\lambda)} \approx \frac{1}{\lambda}, \tag{3.11}$$

where $W_0(z)$ is the principal branch of the Lambert W-fuction and the approximation is valid for $\lambda \gg 1$. Plugging this into equation 3.7 recovers equation 3.6 as desired. In general in the limit $T_{com}^{g\to g} \gg \langle T_\gamma \rangle$ ($\lambda \gg 1$) we expect $N_{mem} = \lambda$ to be sufficient to achieve $p_a = 1$. A plot of p_a for $N_{mem} = \lambda$ can be seen in figure 3.3. This may be understood from the Poissonian distribution, as when $\lambda \gg \infty$, the relative fluctuations of photons arriving during the time N_w will scale as $1/\sqrt{\lambda}$, i.e. the photons that we fail to store, because there is no room for them in the memory, make out a negligible fraction of the total number of photons arriving. Finally we will consider the case of $\lambda = N_{mem} = 1$ by evaluating equation 3.11 giving $p_a = 0.57$, meaning that approximately half of the photons are stored

3.1.2 Photon Heralding

Once again we are presented with the challenge of photon heralding. Figure 3.4 presents an overview of the three methods that we will consider here, with table 3.1 giving an overview of the different implementations.

[2] At least I wasn't able to.

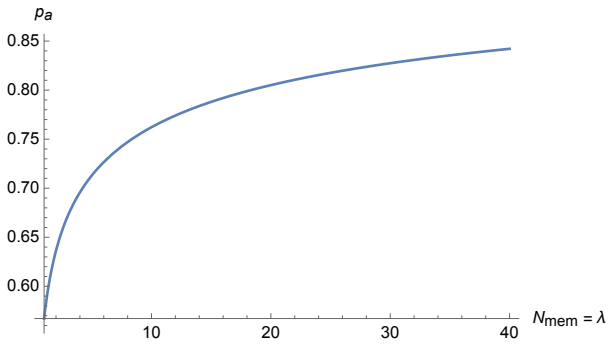


Figure 3.3: Solutions to equation 3.10 for $N_{mem} = \lambda$.

SPDC and Teleportation

The implementation involving SPDC and Teleportation as seen in figure 3.4a, was discussed thoroughly in section 2.5. With p_g being the probability of Bell state generation for the SPDC, the heralding efficiency becomes $\eta_h = p_g/2$, where the factor one half is due to the bell state detection efficiency. Unfortunately errors start to dominate if the probability of generating four photons is bigger than the probability of generating two photons and receiving photons from the satellite. Thus we require $p_g \ll p_d p_s$ which gravely limits the heralding efficiency.

Emitter and Teleportation

The implementation shown in figure 3.4b was discussed briefly at the start of section 2.6. It relies on an emitter sending out a photon entangled with its internal state with probability η_c. A BSM is then done on the emitted photon along with the photon from the satellite, thereby teleporting the state onto the emitter. The efficiency of the heralding is $\eta_h = \eta_c/2$. However like the implementation above, there are extreme demands on the $g^{(2)}(0)$ of the emitter used in order to limit infidelity. This limitation is $\eta_c g^{(2)} \ll p_d p_s$.

Scattering off Emitter

Finally the implementation shown in figure 3.4c was discussed in great detail in section 2.6.1. By scattering the photon from space off an emitter followed by a measurement of the photons, makes it possible to map the qubit from the photon onto the emitter heralded. Current implementations achieve $\eta_h \sim 1/2$. Multimode capabilities can be achieved by having several emitters.

	Implementation	η_h	Limitations
a)	SPDC and Teleportation	$p_s/2$	$p_g \ll p_d p_s$
b)	Emitter and Teleportation	$\eta_c/2$	$\eta_c g^{(2)} \ll p_d p_s$
c)	Scattering off Emitter	$\eta_h \sim 1/2$	

Table 3.1: Overview of three different approaches for heralding the arrival of photons at the ground stations.

Taking the achievable efficiencies and limitations into account we are going to use the scattering

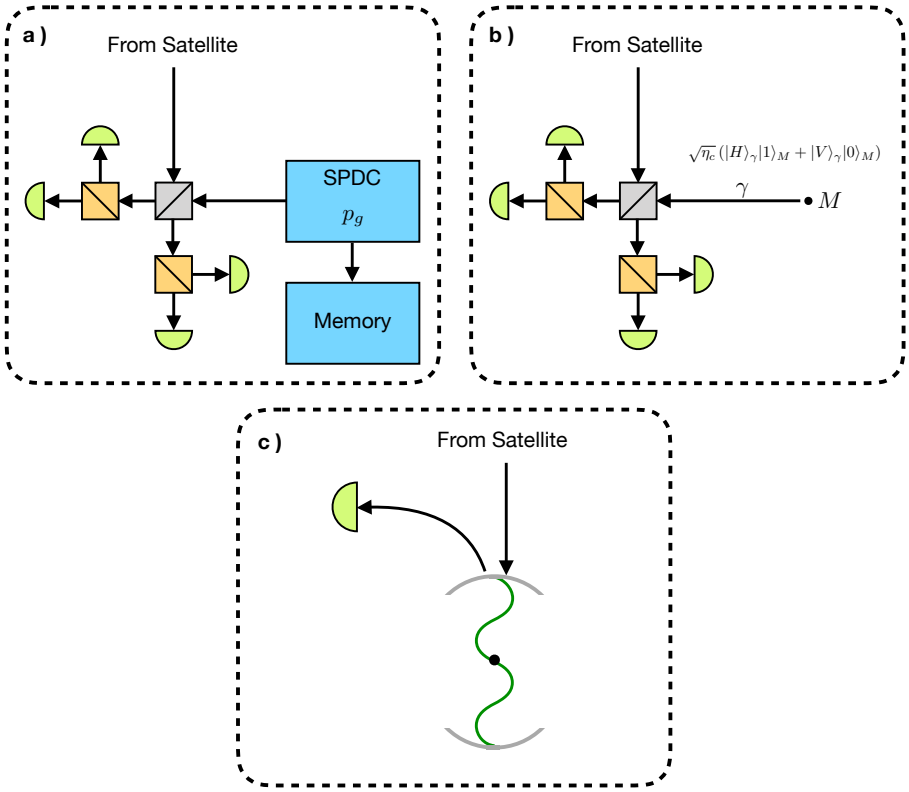


Figure 3.4: The three methods presented for heralding the arrival of a photon from the satellite.

off emitter implementation moving forward. It should be noted however that any of the four could be used.

3.1.3 Rate

As we have already stated above, the rate of the protocol is $R = \eta_h^2 p_d^2 p_a^2 p_s r_{rep}$. For the repetition rate, we are limited by the operation of the photon heralding, as for the emitter uplink QKD scheme (see section 2.6). With the only minor complication being the calculation of p_a, the rate will be given by

$$R = \eta_h^2 p_d^2 p_a^2 p_s r_{rep} \tag{3.12}$$

3.1.4 Fidelity

To calculate the fidelity of the protocol we start with the state arriving at Alice and Bob as given by equation 2.11

$$\begin{aligned}
\rho^{(a,b)} = &\left(|\varnothing,\varnothing\rangle + \sqrt{\frac{p_1 p_d^2}{2}}\Big(|H,V\rangle + |V,H\rangle\Big)\right)\left(\langle\varnothing,\varnothing| + \sqrt{\frac{p_1 p_d^2}{2}}\Big(\langle H,V| + \langle V,H|\Big)\right)\\
&+ \left(\frac{p_1 p_d}{2} + p_2 p_d\right)\Big(|H,\varnothing\rangle\langle H,\varnothing| + |V,\varnothing\rangle\langle V,\varnothing| + |\varnothing,H\rangle\langle\varnothing,H| + |\varnothing,V\rangle\langle\varnothing,V|\Big)\\
&+ \left(\sqrt{\frac{p_1}{2}}|\varnothing,\varnothing\rangle - \sqrt{\frac{4p_2p_d^2}{3}}|H,V\rangle - \sqrt{\frac{p_2p_d^2}{3}}|V,H\rangle\right)\left(\sqrt{\frac{p_1}{2}}\langle\varnothing,\varnothing| - \sqrt{\frac{4p_2p_d^2}{3}}\langle H,V| - \sqrt{\frac{p_2p_d^2}{3}}\langle V,H|\right)\\
&+ \left(\sqrt{\frac{p_1}{2}}|\varnothing,\varnothing\rangle - \sqrt{\frac{4p_2p_d^2}{3}}|V,H\rangle - \sqrt{\frac{p_2p_d^2}{3}}|H,V\rangle\right)\left(\sqrt{\frac{p_1}{2}}\langle\varnothing,\varnothing| - \sqrt{\frac{4p_2p_d^2}{3}}\langle V,H| - \sqrt{\frac{p_2p_d^2}{3}}\langle H,V|\right)\\
&+ \frac{p_2p_d^2}{3}\Big(|2H,\varnothing\rangle\langle 2H,\varnothing| + |2V,\varnothing\rangle\langle 2V,\varnothing| + |\varnothing,2H\rangle\langle\varnothing,2H| + |\varnothing,2V\rangle\langle\varnothing,2V| + |HV,\varnothing\rangle\langle HV,\varnothing|\\
&+ |\varnothing,HV\rangle\langle\varnothing,HV| + |H,H\rangle\langle H,H| + |V,V\rangle\langle V,V|\Big) + p_2|\varnothing\rangle\langle\varnothing|\,.
\end{aligned} \tag{3.13}$$

The mapping of the photonic qubit onto the memory is modelled by $c_\varnothing|\varnothing\rangle_\gamma + c_H|H\rangle_\gamma + c_V|V\rangle_\gamma \to \eta_h\left(c_H|+\rangle_M \pm c_V|-\rangle_M\right)$, where the sign is dependent on the photon measurement outcome. We will also consider dark counts at the detectors performing the measurements on the photons after scattering, which with probability p_{dark} will map vacuum terms into $|+\rangle_M$. Recall that $p_s p_d^2 \eta_h^2$ is the probability of the desired process where both of the photons of an entangled pair gets mapped onto the memories. We are interested in suppressing all events involving dark counts, but we only need to consider the most probable. The process where one photon makes it to the ground and a dark count occur at the other ground station happens with probability $p_s p_d \eta_h p_{dark}$, meaning that we require $p_{dark} \ll p_d\eta_h$. On the other hand the process with dark counts in both ground stations occur with probability p_{dark}^2, meaning that we require $p_{dark} \ll \sqrt{p_s}p_d\eta_h$. Therefore to the leading order, dark counts only enter the state in form of the latter process. We thus get the following state after loading onto memory,

$$\rho_{\text{mem}}^{(A,B)} = \left(p_1 p_d^2\eta_h^2 + \frac{8}{3}p_2p_d^2\eta_h^2\right)|\psi_X^\pm\rangle\langle\psi_X^\pm| + \frac{p_2p_d^2\eta_h^2}{3}\mathbb{1}_1^{(A)}\otimes\mathbb{1}_1^{(B)} + p_{dark}^2|+\rangle\langle+|\otimes|+\rangle\langle+|\,, \tag{3.14}$$

where $|\psi_X^\pm\rangle = (|+-\rangle \pm |-+\rangle)/\sqrt{2}$, and the sign of $\pm$ is given by the product of the signs of the individual photon measurements. Finally we need to take the decay of the emitters during the communication time into account. We do this by applying the depolarising channel to both qubits,

$$\begin{aligned}
\rho_{\text{mem}}^{(A,B)} \to \rho_f^{(A,B)} = &\,\eta_a\eta_b\rho_{\text{mem}}^{(A,B)} + \eta_a(1-\eta_b)\,\text{Tr}_B\left[\rho_{\text{mem}}^{(A,B)}\right]\otimes\frac{\mathbb{1}_1^{(B)}}{2}\\
&+ (1-\eta_a)\eta_b\frac{\mathbb{1}_1^{(A)}}{2}\otimes\text{Tr}_A\left[\rho_{\text{mem}}^{(A,B)}\right] + (1-\eta_a)(1-\eta_b)\frac{\mathbb{1}_1^{(A)}}{2}\otimes\frac{\mathbb{1}_1^{(B)}}{2},
\end{aligned} \tag{3.15}$$

with η_a and η_b being the memory efficiency at Alice and Bob respectively. Therefore the final state shared by Alice and Bob becomes,

$$\begin{aligned}\rho_f^{(A,B)} &= \eta_a\eta_b\left(p_1p_d^2\eta_h^2+\frac{8}{3}p_2p_d^2\eta_h^2\right)\left|\psi_X^{\pm}\right\rangle\!\left\langle\psi_X^{\pm}\right| + \eta_a\eta_b p_{dark}^2\left|+\right\rangle\!\left\langle+\right|\otimes\left|+\right\rangle\!\left\langle+\right| \\ &+\left[(1-\eta_a\eta_b)\left(p_1p_d^2\eta_h^2+\frac{8}{3}p_2p_d^2\eta_h^2\right)+\frac{4p_2p_d^2\eta_h^2}{3}+(1-\eta_a)(1-\eta_b)p_{dark}^2\right]\frac{\mathbb{1}_1^{(A)}}{2}\otimes\frac{\mathbb{1}_1^{(B)}}{2} \\ &+(1-\eta_a)\eta_b p_{dark}^2\frac{\mathbb{1}_1^{(A)}}{2}\otimes\left|+\right\rangle\!\left\langle+\right| + \eta_a(1-\eta_b)p_{dark}^2\left|+\right\rangle\!\left\langle+\right|\otimes\frac{\mathbb{1}_1^{(B)}}{2}.\end{aligned} \tag{3.16}$$

As the memories of Alice and Bob are assumed identical, we set $\eta_a = \eta_b = \eta_{gcom}$, where we have introduced $\eta_{gcom} = \eta\left(T_{com}^{g\to g}\right)$. With $\left|\psi_X^{\pm}\right\rangle$ being the ideal state, we may now calculate the fidelity,

$$F = \frac{1+3\eta_{gcom}^2+\frac{d^2}{p_1}\left(1-\eta_{gcom}^2\right)+4p_2^*(1+2\eta_{gcom}^2)}{4\left(1+4p_2^*+\frac{d^2}{p_1}\right)} \approx \frac{1}{4}+\eta_{gcom}^2\left(\frac{3}{4}-p_2^*-\frac{d^2}{p_1}\right), \tag{3.17}$$

where we again have defined $p_2^* = p_2/p_1$ and $d = p_{dark}/p_d\eta_h$, and the expansion being valid for fidelities close to unity. Using $p_2 = 3p_s/4$ and $p_1 = p_s$ we get,

$$F = \frac{1}{4}+\eta_{gcom}^2\left(\frac{3}{4}-\frac{3}{4}p_s-\frac{d^2}{p_s}\right) \tag{3.18}$$

3.1.5 Optimisation

The maximum fidelity of the protocol is being given by,

$$F_{max} = \frac{1}{4}+\eta_{gcom}^2\left(\frac{3}{4}-\sqrt{3}d\right), \quad \text{for} \quad p_s = \frac{2d}{\sqrt{3}}. \tag{3.19}$$

For any desired fidelity $F_0 \leq F_{max}$, the optimisation is done by solving equation 3.18 and picking the largest of the two solutions. Therefore

$$p_s = \frac{1-4F_0+3\eta_{gcom}^2+\sqrt{-48d^2\eta_{gcom}^2+(1-4F_0+3\eta_{gcom}^2)^2}}{6\eta_{gcom}^2}. \tag{3.20}$$

3.1.6 Performance

We will now find the rate of the direct downlink scheme in order to get a benchmark of performance. Employing silicon-vacancy centres as the choice of memories at the ground, we use the following parameters $r_{rep} = 3\times10^7$ Hz and $\eta_h = 0.5$. Furthermore we will use a ground distance of $L_g = 1000$ km, $p_d = 10^{-3}$, $d = 0.01$ and a desired fidelity of $F_0 = 0.95$. With these parameters equation 3.19 gives $\eta_{gcom} \geq 0.98$, which for $\eta' = 1$ translate into the memory requirement $\tau_\eta \geq 0.14$ s. Figure 3.5 shows the rate as a function of coherence time for different number of memories. At $\tau_\eta = 1$ s, we get $\lambda \approx 3$, meaning that on average approximately 3 photons reach the ground station per communication time (see figure 3.6). We therefore need $N_{mem} \gtrsim 7$ to saturate the need of memories and get $p_a \sim 1$. As a benchmark for the following schemes we will therefore use $N_{mem} = 7$ and $\tau_\eta = 1$ s, yielding $R = 0.41$ Hz. This is also fairly close to the maximum rate $R = 0.48$ Hz, given by $N_{mem}, \tau_\eta \to \infty$.

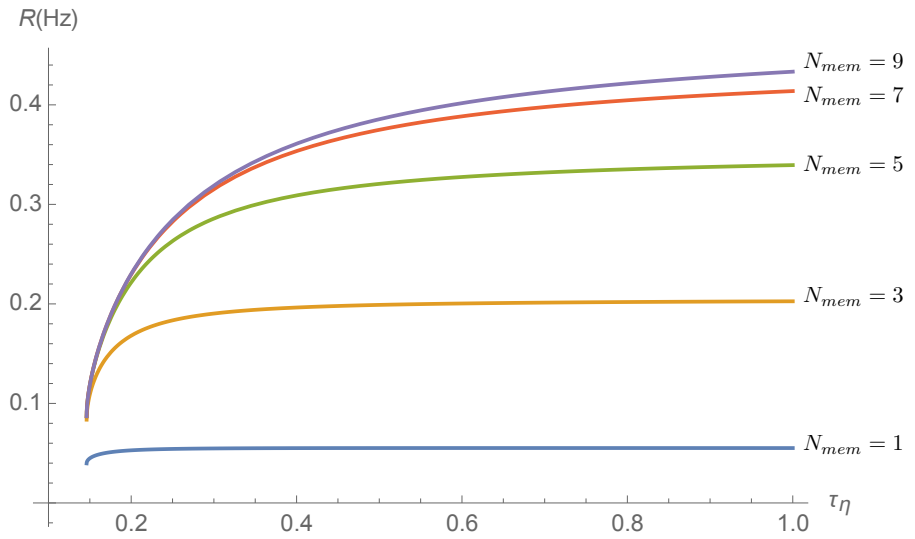


Figure 3.5: Rate of the direct downlink scheme as a function of memory coherence times for different number of memories. Parameters $r_{rep} = 3 \times 10^7$ Hz, $\eta_h = 0.5$, $\eta' = 1$, $L_g = 1000$ km, $p_d = 10^{-3}$, $d = 0.01$ and $F_0 = 0.95$. As $N_{mem}, \tau_\eta \to \infty$, we get $R \to 0.48$ Hz. See figure 3.6 for plots of p_s, λ and p_a for the same parameters.

3.2 Memory Assisted - General Structure

Inspired by the things we learned in the QKD chapter, we will now consider the general structure of an memory assisted protocol for entanglement distribution. For the memory assisted entanglement distribution protocols, we need to have memories both at the ground and at the satellite. The requirements for the memories will however be very different depending on wether they are next to the photon source or at the opposite station.[3] For the memory next to the photon source a great multimode capacity is required, this is because the repetition rate of the photon source is limited by the communication time $T_{com}^{s \leftrightarrow g}$, like the downlink schemes discussed in the previous chapter. We should note that this limitation is in place for both uplink and downlink schemes. For this reason we are going to consider ensemble memories next to the photon source. For the memories at the station where the photons are received, only a single qubit is needed for storage[4], however the receiving station needs to herald the arrival of the photon, thereby imposing completely different requirements for the two memories. For the memory at the receiving station we thus consider an emitter as discussed in section 2.6.1.

The difference between the uplink and the downlink memory assisted schemes is therefore rather minor, but they do exist. First and foremost there is a difference in the transmission of the photon, as discussed previously. Secondly there is a difference in the entanglement swap as it is done differently for emitters and ensemble based memories. Finally for the uplink protocol the heralding of the photons is done at the satellite, meaning that we also need to take into account that the memories at the ground might have decayed before the swap is done. This last part will

[3] Recall that for a downlink scheme the photon source is placed in the satellite and for a downlink scheme the photon source is placed at the ground.

[4] If the consider the goal of the protocol to be to create one entangled pair of qubits at a time. If Alice and Bob desires N entangled qubits they of course need at least N memories.

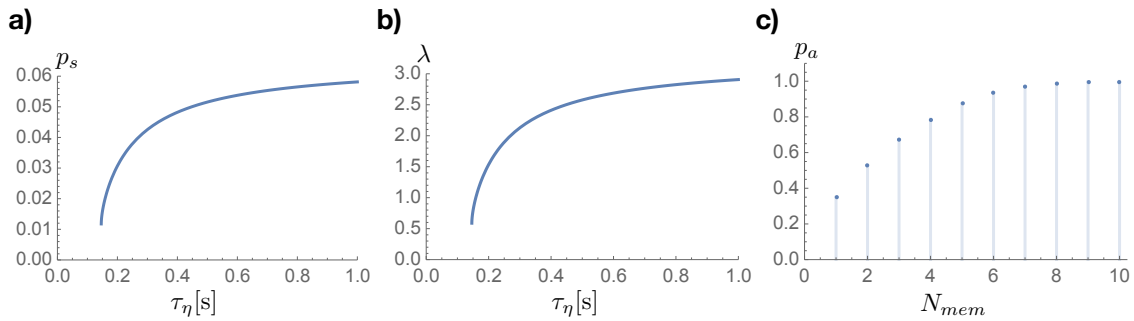


Figure 3.6: a) The bell state generation p_s as a function of memory coherence time as given by equation 3.20. Parameters used are $F_0 = 0.95$, $L_g = 1000$ km, $d = 0.01$ and $\eta' = 1$. **b)** The average number of photons λ arriving at a ground station per communication time $T_{com}^{g\to g}$. The parameters used are $L_g = 1000$ km, $p_d = 10^{-3}$, η_h and p_s given by subplot a. **c)** The probability of there being a memory qubit available for a photon reaching the ground stations as a function of number of memory qubits N_{mem}. $\lambda = 3$ was chosen, corresponding to the value when the memory coherence time requirement is saturated in subplot b.

be discussed in greater detail in section 3.3.2.

3.2.1 Rate

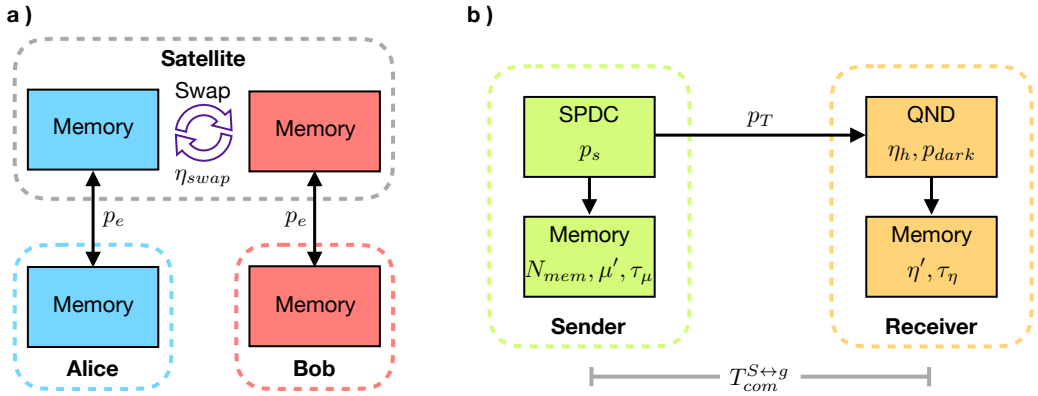


Figure 3.7: a) The basic setup for memory assisted entanglement distribution, consisting of two pairs of memories. The probability of entangling a pair of memories is p_e per repetition, and after both pairs are entangled an entanglement swap is performed with efficiency η_{swap}. **b)** A pair of memories consisting of a sender and a receiver setup. The SPDC produces entangled pair of photons where one is sent to the memory next to it, while the other is sent to the receiver station. At the receiver station the photon is loaded into the memory heralded.

We will now calculate the rate of the memory assisted schemes. Figure 3.7 shows a schematic view of the scheme. We assume that a pair of entangled photons are produced with probability p_s from the photon source. Let p_T be the probability of transmission and η_h be the heralding efficiency at the receiver. Then with the memory at the photon source able to store N_{mem} qubits, the probability of entangling the two memories in one arm of the system per communication time

is,

$$\begin{aligned} p_e &= 1-(1-p_s p_T \eta_h)^{N_{mem}} \\ &\approx N_{mem} p_s p_T \eta_h, \end{aligned} \tag{3.21}$$

where the expansion is valid for $N_{mem} p_s p_T \eta_h \ll 1$. With lossy memories next to the photon source having the coherence time τ_μ and efficiency $\mu(t) = \mu' e^{-t/\tau_\mu}$, we may calculate the rate with the same methods as presented in section 2.3.3. Therefore

$$\langle n \rangle^{-1} = \mu_{com}^2 p_e^2 \frac{e^{\frac{1}{\Delta_{\mu m}}} \left(1 + (1-p_e)\, e^{-\frac{1}{\Delta_{\mu m}}} - 2e^{-\frac{N_{max}+1}{\Delta_{\mu m}}} (1-p_e)^{N_{max}+1}\right)}{\left(e^{\frac{1}{\Delta_{\mu m}}} - 1 + p_e\right)\left(3 - 2p_e - 2(1-p_e)^{N_{max}+1}\right)} \tag{3.22}$$

where $\mu_{com} = \mu(T_{com}^{s\leftrightarrow g})$, $\Delta_{\mu m} = \tau_\mu r_{rep}$ and N_{max} is the maximal storage time after the first entanglement is made until the second entanglement is made. With the inclusion of the swapping efficiency η_{swap} and expanding $\langle n \rangle^{-1}$ in the limit $p_e \ll 1$ gives the rate,

$$R = 2\eta_{swap} \Delta_{\mu m} \mu_{com}^2 N_{mem}^2 p_s^2 p_T^2 \eta_h^2 (1 - e^{-\alpha_\mu}) r_{rep} \quad \text{for} \quad N_{mem} p_s p_T \eta_h \ll \frac{T_{com}^{s\leftrightarrow g}}{\tau_\mu} \tag{3.23}$$

$$R = \frac{2}{3} \eta_{swap} \mu_{com}^2 N_{mem} p_s p_T \eta_h r_{rep}, \quad \text{for} \quad N_{mem} p_s p_T \eta_h \gg \frac{T_{com}^{s\leftrightarrow g}}{\tau_\mu} \tag{3.24}$$

where $r_{rep} = \frac{1}{T_{com}^{s\leftrightarrow g}}$ and $\alpha_\mu = \frac{N_{max}+1}{\Delta_{\mu m}}$.

3.3 Memory Assisted - Uplink

Let us now take a closer look at the memory assisted uplink scheme, as seen in figure 3.8. The rate of the protocol is given by equation 3.23 and 3.24, but with $p_T = p_u$ and $p_s = p_g$.

3.3.1 Fidelity

For the calculation of the fidelity, we may start out with the final state $\sigma^{(a,b)}$ of the emitter and uplink scheme as given by equation 2.106. To find the final state we need to apply the loss of the modes a and b when stored in the memories on the ground, which we will describe by the transformation

$$c_\sigma^\dagger \to \sqrt{1-\mu_c}\, l_{c_\sigma}^\dagger + \sqrt{\mu_c}\, c_\sigma^\dagger, \qquad c \in \{a, b\} \tag{3.25}$$

where σ is the polarisation and $\mu_c = \mu(t_c)$ where t_c is the time mode c has spend in memory. We now define the quantum channel $\Lambda'_\mu(\rho)$ which performs the transformation of equation 3.25 followed by a partial trace over the loss operators $l_{c_\sigma}^\dagger$. We should note that Λ'_μ is trace preserving meaning that $\mathrm{Tr}\left[\Lambda'_\mu(\rho)\right] = \mathrm{Tr}[\rho]$, such that the time dependent fidelity is given by,

$$f(t_a, t_b) = \frac{\langle \psi_{ideal} |\, \Lambda'_\mu(\sigma^{(a,b)})\, | \psi_{ideal} \rangle}{\mathrm{Tr}\left[\sigma^{(a,b)}\right]}. \tag{3.26}$$

Furthermore we define the post selection mapping $\Lambda_\mu(\rho)$ which projects $\Lambda'_\mu(\rho)$ into the subspace where theres at least one photon in each memory, by

$$\Lambda_\mu(\rho^{(a,b)}) = \left(\mathbb{P}_{1+2}^{(a)} \otimes \mathbb{P}_{1+2}^{(b)}\right) \Lambda'_\mu(\rho^{(a,b)}) \left(\mathbb{P}_{1+2}^{(a)} \otimes \mathbb{P}_{1+2}^{(b)}\right), \tag{3.27}$$

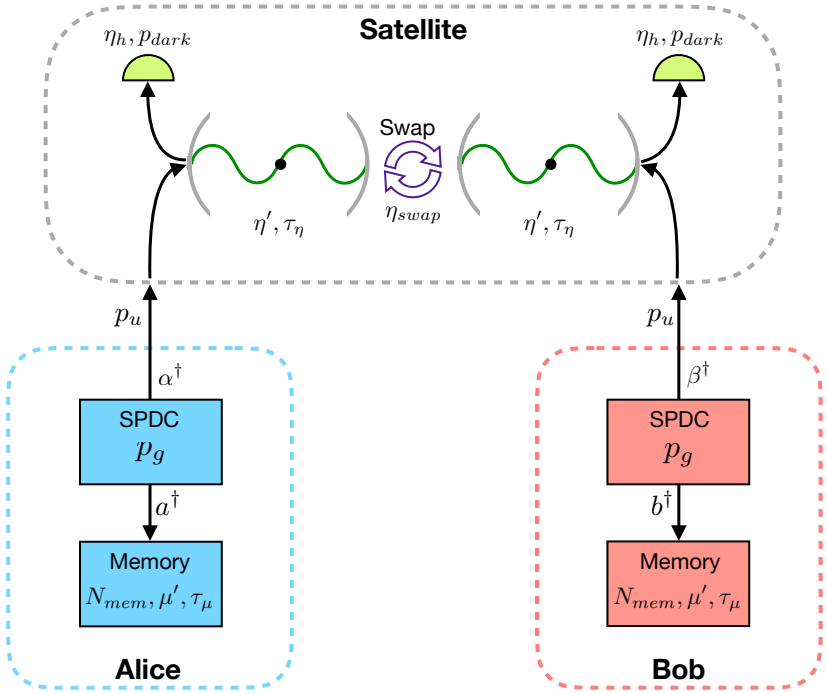


Figure 3.8: Setup considered for the memory assisted uplink scheme.

where $\mathbb{P}^{(c)}_{1+2} = \mathbb{P}^{(c)}_1 + \mathbb{P}^{(c)}_2$. Thus

$$f(t_a, t_b) = \frac{\langle \psi_{ideal} | \, \Lambda_\mu(\sigma^{(a,b)}) \, | \psi_{ideal} \rangle}{\mathrm{Tr}\left[\sigma^{(a,b)}\right]}. \tag{3.28}$$

We may also calculate the fidelity conditioned on having at least one photon stored in each memory by,

$$f_{PS}(t_a, t_b) = \frac{\langle \psi_{ideal} | \, \Lambda_\mu(\sigma^{(a,b)}) \, | \psi_{ideal} \rangle}{\mathrm{Tr}\left[\Lambda_\mu(\sigma^{(a,b)})\right]}. \tag{3.29}$$

Applying Λ_μ to $\sigma^{(a,b)}$ as given by equation 2.106, yields

$$\begin{aligned}
\Lambda_\mu(\sigma^{(a,b)}) = &\frac{\eta_h^2 p_1^2 p_u^2 \eta_a\eta_b\mu_a\mu_b}{4}\left|\phi^+\right\rangle\!\left\langle\phi^+\right| + \frac{\eta_h p_1^2 p_u p_{dark}}{4}\eta_a\eta_b\mu_a\mu_b\left(\frac{\mathbb{P}_1}{2}\otimes|V\rangle\langle V| + |V\rangle\langle V|\otimes\frac{\mathbb{P}_1}{2}\right)\\
&+\frac{\eta_h p_1^2 p_u p_{dark}}{8}\mu_a\mu_b(1-\eta_a\eta_b)\left(\mathbb{P}_1\otimes\mathbb{P}_1\right) + \frac{\eta_h^2 p_1^2 p_u^2}{16}\mu_a\mu_b(1-\eta_a\eta_b)\left(\mathbb{P}_1\otimes\mathbb{P}_1\right)\\
&+\frac{\eta_h^2 p_1 p_2 p_u^2}{12}(1-\eta_a\eta_b)\left(\mu_a^2\mu_b\mathbb{P}_2\otimes\mathbb{P}_1 + \mu_a\mu_b^2\mathbb{P}_1\otimes\mathbb{P}_2\right)\\
&+\frac{\eta_h^2 p_1 p_2 p_u^2}{4}(1-\eta_a\eta_b)\mu_a\mu_b(2-\mu_a-\mu_b)\mathbb{P}_1\otimes\mathbb{P}_1\\
&+\frac{\eta_h^2 p_1 p_2 p_u^2}{12}\eta_a\eta_b\mu_a\mu_b^2\left(|H,HV\rangle+\sqrt{2}\,|V,2H\rangle\right)\left(\langle H,HV|+\sqrt{2}\,\langle V,2H|\right)\\
&+\frac{\eta_h^2 p_1 p_2 p_u^2}{12}\eta_a\eta_b\mu_a\mu_b^2\left(|V,HV\rangle+\sqrt{2}\,|H,2V\rangle\right)\left(\langle V,HV|+\sqrt{2}\,\langle H,2V|\right)\\
&+\frac{\eta_h^2 p_1 p_2 p_u^2}{12}\eta_a\eta_b\mu_a^2\mu_b\left(|HV,H\rangle+\sqrt{2}\,|2H,V\rangle\right)\left(\langle HV,H|+\sqrt{2}\,\langle 2H,V|\right)\\
&+\frac{\eta_h^2 p_1 p_2 p_u^2}{12}\eta_a\eta_b\mu_a^2\mu_b\left(|HV,V\rangle+\sqrt{2}\,|2V,H\rangle\right)\left(\langle HV,V|+\sqrt{2}\,\langle 2V,H|\right)\\
&+\frac{\eta_h^2 p_1 p_2 p_u^2}{12}\eta_a\eta_b\mu_a\mu_b(2-\mu_a-\mu_b)\mathbb{P}_1\otimes\mathbb{P}_1 + \frac{2}{3}\eta_h^2 p_1 p_2 p_u^2\eta_a\eta_b(2-\mu_a-\mu_b)\left|\psi^+\right\rangle\!\left\langle\psi^+\right|.
\end{aligned} \tag{3.30}$$

With $|\phi^+\rangle$ being the ideal state we get,

$$\begin{aligned}
f_{PS}(t_a,t_b) &= \frac{\frac{1}{4}+\frac{3}{4}\eta_a\eta_b+\frac{1}{2}d+\frac{1}{3}p_2^*}{1+2d+2p_2^*(4-\mu_a-\mu_b)}\\
&= \frac{1}{4}-\frac{1}{2}p_2^*(\mu_a+\mu_b)+\eta_a\eta_b\left(\frac{3}{4}-\frac{3}{2}d-\frac{22}{3}p_2^*\right)+\frac{13}{6}p_2^*\eta_a\eta_b(\mu_a+\mu_b)
\end{aligned} \tag{3.31}$$

where we have used $d = p_{dark}/\eta_h p_u$ and $p_2^* = p_2/p_1$ as usual and expanded in the high fidelity regime $d, p_2^* \ll 1$ in the second line. Finding the post selected fidelity is then done by averaging the memory efficiencies μ and η, as has been done previously. We should however note that since the heralding is done at the satellite the minimal waiting time before the swap is 0 for the emitters and $T_{com}^{s\leftrightarrow g}$ for the memories at the ground. Using $p_2^* = \frac{3}{4}p_g$ and

$$F_{PS} = \sum_{\Delta=0}^{N_{max}} p_\Delta f_{PS}(\Delta,0), \tag{3.32}$$

with p_Δ given by equation 2.39, we state the post selected fidelity in terms of the average memory efficiencies,

$$F_{PS} = \frac{1}{4}-\frac{3}{8}p_g\left\langle\mu_a+\mu_b\right\rangle_\Delta + \left\langle\eta_a\eta_b\right\rangle_\Delta\left(\frac{3}{4}-\frac{3}{2}d-\frac{11}{2}p_g\right)+\frac{13}{8}p_g\left\langle\eta_a\eta_b(\mu_a+\mu_b)\right\rangle_\Delta, \tag{3.33}$$

where $\langle g\rangle_\Delta = \sum_{\Delta=0}^{N_{max}} p_\Delta g(\Delta)$

The average memory efficiencies may be evaluated by setting $\mu_a = \mu_{com}e^{-\Delta/\Delta_{\mu m}}$, $\mu_b = \mu_{com}$, $\eta_a = \eta' e^{-\Delta/\Delta_{\eta m}}$ and $\eta_b = \eta'$, where we have defined $\Delta_{\eta m} = \tau_\eta r_{rep}$. We may also calculate the

fidelity without conditioning on having at least one photon in each memory by using $f(t_a, t_b)$ as given by equation 3.28 instead of $f_{PS}(t_a, t_b)$,

$$F = \langle \mu_a \mu_b \rangle_\Delta \left(\frac{1}{4} - \frac{d}{2p_g}(1-p_g) + \frac{3}{4}p_g \right) + \langle \mu_a \mu_b \eta_a \eta_b \rangle_\Delta \left(\frac{3}{4} - \frac{13}{4}p_g - \frac{3d}{2p_g} \right) + \langle \mu_a \mu_b (\mu_a + \mu_b) \rangle_\Delta \frac{3}{4}p_g + \langle \mu_a \mu_b \eta_a \eta_b (\mu_a + \mu_b) \rangle_\Delta \frac{1}{2}p_g \tag{3.34}$$

We see that that the fidelity without post selection requires $p_{dark} \ll p_g p_u \eta_h$, this is significantly harsher requirements on the dark count probability than for the other schemes we have seen in this thesis. As we will see now, we also require $p_{dark} \ll p_g p_u \eta_h$ when using the post selected fidelity.

3.3.2 A deterministic source of entanglement?

For the uplink protocol the heralding occurs in the satellite, this introduces the risk of decay of the photons stored in the memory on the ground. A way of taking this into account is through the fidelity F as calculated in the previous section. However depending on what the entanglement will be used for it might be more beneficial to address the F_{PS} conditioned on extracting photons from both memories and probability extracting the entangled photons independently of each other.

Let M_a (M_b) be the event of having at least one photon in the memory of Alice (Bob), furthermore let H_a (H_b) be the event where a photon gets heralded at the satellite from Alice (Bob). With this the $P(M_a M_b | H_a H_b)$ will be the probability of having at least two non decayed photons in the memories at Alice and Bob given the satellite performed the swap. In order for the protocol to produce entangled photons quasi-deterministically we will impose a lower bound on the conditional probability,

$$\langle P(M_a M_b | H_a H_b) \rangle_\Delta \geq P_0 \tag{3.35}$$

for some predetermined P_0. Since the two branches of the setup operate independently of each other we may factor the probabilities,

$$P(M_a M_b | H_a H_b) = P(M_a | H_a) P(M_b | H_b). \tag{3.36}$$

From the definition of a conditional probability we then get,[5]

$$P(M_a | H_a) = \frac{P(M_a H_a)}{P(H_a)} \tag{3.37}$$

With $P(H_a) = p_1 p_u \eta_h (1 + 2p_2^* + \frac{d}{p_1})$ and $P(M_a H_a) = p_1 p_u \eta_h \mu_a (1 + 2p_2^*(\mu_a + 2(1-\mu_a)))$, we expand $P(M_a|H_a)$ in the regime $p_2^*, \frac{d}{p_1} \ll 1$ to get,

$$P(M_a | H_a) = \mu_a \left(1 + 2p_2^*(1-\mu_a) - \frac{d}{p_1} \right), \tag{3.38}$$

and

$$P(M_a M_b | H_a H_b) = \mu_a \mu_b \left(1 + 2p_2^*(2 - \mu_a - \mu_b) - 2\frac{d}{p_1} \right). \tag{3.39}$$

[5]Notice the similarity with $F = \langle \psi | \rho | \psi \rangle / \mathrm{Tr}[\rho]$. Just like $\mathrm{Tr}[\rho]$ ensures the normalisation of $\rho/\mathrm{Tr}[\rho]$, $P(H_a)$ ensures the normalisation of $P(M_a|H_a)$.

Such that the condition becomes,

$$\langle \mu_a \mu_b \rangle_\Delta \left(1 + 3p_g - 2\frac{d}{p_g}\right) - \langle \mu_a \mu_b (\mu_a + \mu_b) \rangle_\Delta \frac{3}{2} p_g \geq P_0 \tag{3.40}$$

Again we note the comparably harsher requirements on the detector dark count probability. The value of P_0 chosen for this condition will depend on what the entanglement created will be used for afterwards. If Alice and Bob would like to violate Bells inequality by performing measurements of the extracted qubits P_0 close to unity is needed in order to close the detection loophole. On the other hand, if the scheme presented here is part of a repeater chain $P_0 \approx 0.33\mu_{com}^2$ is optimal for a two satellite link repeater as we will see in section 4.3.

3.3.3 Optimisation and Performance

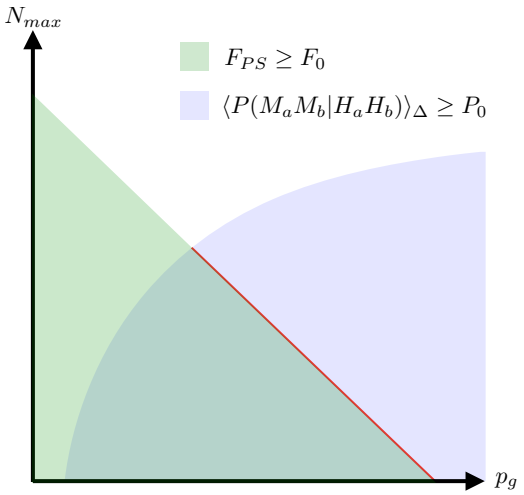


Figure 3.9: Conditions on N_{max} and p_g imposed by $F_{PS} \geq F_0$ and $\langle P(M_a M_b | H_a H_b) \rangle_\Delta \geq P_0$. The red line represents the accepted values of N_{max} and p_g where $F_{PS} = F_0$.

We will now look at the optimisation of the protocol with post selection. Under the conditions of $F_{PS} \geq F_0$ and $\langle P(M_a M_b | H_a H_b) \rangle_\Delta \geq P_0$, we will maximise the rate by over the parameters p_g and N_{max}. For a fixed N_{max} the condition of $\langle P(M_a M_b | H_a H_b) \rangle_\Delta \geq P_0$ as given by equation 3.40 will impose a lower bound on p_g, while $F_{PS} \geq F_0$ will impose an upper bound. Making the observation of $\partial_{p_g} R > 0$, we may thus conclude that it is sufficient to do the optimisation over the subspace of p_g and N_{max} where $F_{PS} = F_0$ and $\langle P(M_a M_b | H_a H_b) \rangle_\Delta \geq P_0$ as indicated by the red line in figure 3.9. With this simplification made optimisation is then done numerically.

Figure 3.10 shows the results of optimising the rate over different values for τ_μ and τ_η. The first thing to note from the figure is that for the same coherence of the emitter (τ_η) and the ensemble (τ_μ), the emitter will be the limiting factor. The same effect was seen in the QKD chapter where the schemes involving emitters needed $\alpha = (N_{max} + 1)/\tau_\eta r_{rep} \sim 0.01$ in order to achieve $F = 0.95$, while for the schemes with ensemble memories $\alpha = (N_{max} + 1)/\tau_\mu r_{rep} \sim 1$ for the same fidelity.

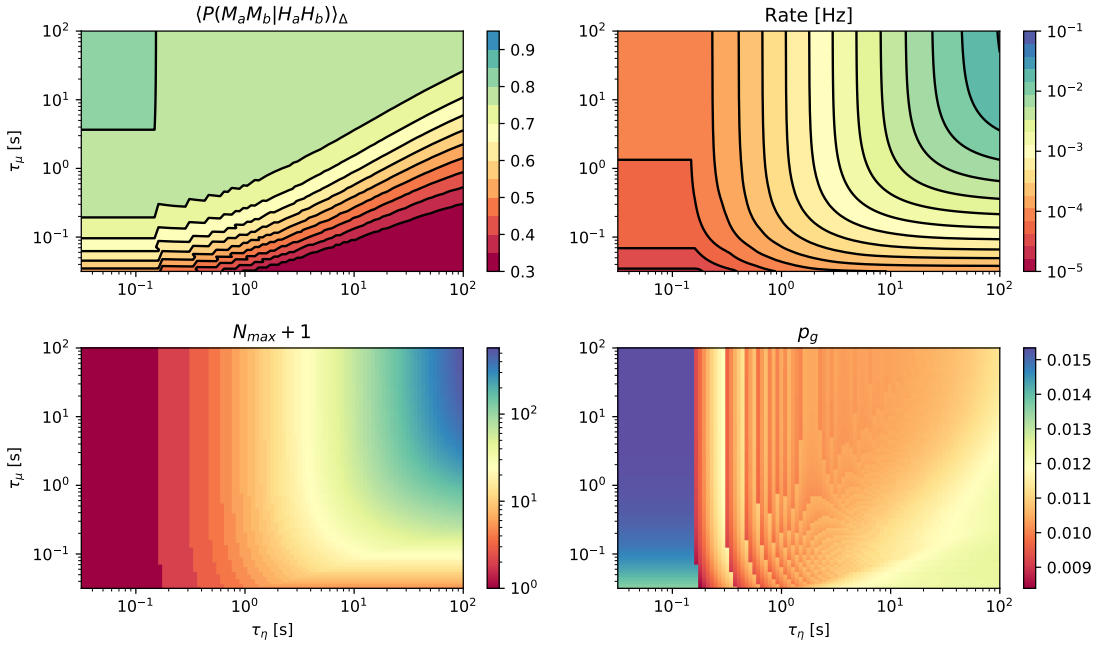


Figure 3.10: Optimisation of the rate under the conditions $P_0 = 0.33$ and $F_0 = 0.95$ for various values of τ_μ and τ_η. Parameters $p_u = 10^{-4}$, $\eta_h = 0.5$, $N_{mem} = 1000$, $\mu' = 0.9$, $\eta' = 1$, $L = 1000$ km, $\eta_{swap} = 1$ and $d = 0.0001$ are used. (Upper left) Contour plot showing $\langle P(M_aM_b|H_aH_b)\rangle_\Delta$. It is seen by the dark red triangular region that the demand of $\langle P(M_aM_b|H_aH_b)\rangle_\Delta \geq P_0$ is relevant for $\tau_\eta \gg \tau_\mu$. (Upper right) Contour plot of the optimised rate. (Lower left) Contour plot of the parameter N_{max} which was used for optimisation. In the region of $\tau_\eta \lesssim 0.2$ s $N_{max} = 0$, meaning that the coherence time of the emitters in the satellite is too small to allow for storage for even one repetition. (Lower right) Contour plot of the parameter p_g which was used for optimisation.

Furthermore we see that the condition $\langle P(M_aM_b|H_aH_b)\rangle_\Delta \geq P_0$ as imposed by equation 3.40 is saturated for $\tau_\mu \ll \tau_\eta$. This is also what one would expect as the post selected fidelity is more robust against loss in the memories on the ground than in the satellite, because a loss on the ground most of the times will lead to no photons coming out of the memory, which can be post selected away. Finally we observe that for $\tau_\eta \sim T_{com}^{s\leftrightarrow g}$ we get $N_{max} = 0$. When this is the case we need a photon to arrive from Alice and Bob in the same repetition, thereby severely limiting the rate.[6]

An overview of the rate of the protocol as a function of N_{mem} and τ_μ with $\tau_\eta = \tau_\mu$, $\tau_\eta = 10\tau_\mu$, $\tau_\eta = 100\tau_\mu$ and $\tau_\eta = 1000\tau_\mu$ can be seen in figure 3.11. To beat the benchmark of $R = 0.41$ Hz as set by the direct downlink protocol we require $N_{mem} \approx 10000$, $\tau_\mu \approx 5$ s and $\tau_\eta \approx 50$ s. Which is quite a bit more than what is currently possible.

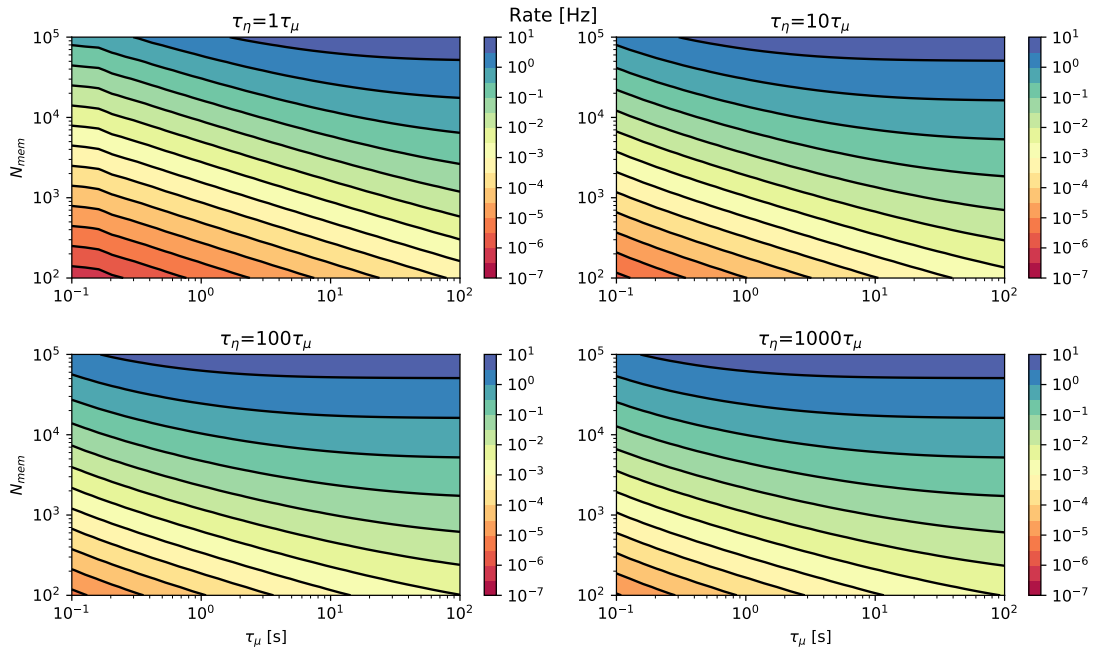


Figure 3.11: Performance of the memory assisted uplink scheme under the conditions $P_0 = 0.33$ and $F_0 = 0.95$ for various values of τ_μ, τ_η and N_{mem}. Parameters $p_u = 10^{-4}$, $\eta_h = 0.5$, $\mu' = 0.9$, $\eta' = 1$, $L = 1000$ km, $\eta_{swap} = 1$ and $d = 0.0001$ are used.

3.4 Memory Assisted - Downlink

Finally let us consider the downlink memory assisted scheme as seen in figure 3.12. The rate of the protocol is given by equation 3.23 and 3.24, with $p_T = p_d$, $p_S = p_s$ and $\eta_{swap} = \frac{1}{2}$ as the BSM in the satellite is done by loading the memories onto beam splitters as described in section 2.3.2.

3.4.1 Fidelity

The starting point for calculating the fidelity will be the density matrix $\sigma^{(a,A)}$ of equation 2.105 describing the state in one branch of the system after heralding and decoherence at the memory on the ground, but before loss in the memory in the satellite is considered. We thus have

$$\begin{aligned}\sigma^{(a,A)} = \eta_a \Big[& p_1 p_d \eta_h \left|\psi^{S_a}\right\rangle\!\left\langle\psi^{S_a}\right| + \rho^{(a)}_{dark} \otimes |+\rangle\langle+| \\ & + \frac{p_2 p_d \eta_h}{3} \left(|HV\rangle|+\rangle + S_a\sqrt{2}\,|2H\rangle|-\rangle\right)\left(\langle HV|\langle+| + S_a\sqrt{2}\,\langle 2H|\langle-|\right) \\ & + \frac{p_2 p_d \eta_h}{3} \left(|HV\rangle|-\rangle + S_a\sqrt{2}\,|2V\rangle|+\rangle\right)\left(\langle HV|\langle-| + S_a\sqrt{2}\,\langle 2V|\langle+|\right) \Big] \\ & + (1-\eta_a)\left[\left(\rho^{(a)}_{dark} + p_d\eta_h\left(p_1\frac{\mathbb{P}^{(a)}_1}{2} + 2p_2\frac{\mathbb{P}^{(a)}_2}{3}\right)\right) \otimes \frac{\mathbb{1}^{(A)}}{2}\right],\end{aligned} \tag{3.41}$$

where $\left|\psi^{S_a}\right\rangle = \left(|H\rangle_a|-\rangle_A + S_a|V\rangle_a|-\rangle_A\right)/\sqrt{2}$ and $S_a \in \{+,-\}$ depending on the outcome of the photon measurement at the ground station. Applying the loss in the memory in the satellite and

[6] Recall that a single repetition is a train of N_{mem} photons.

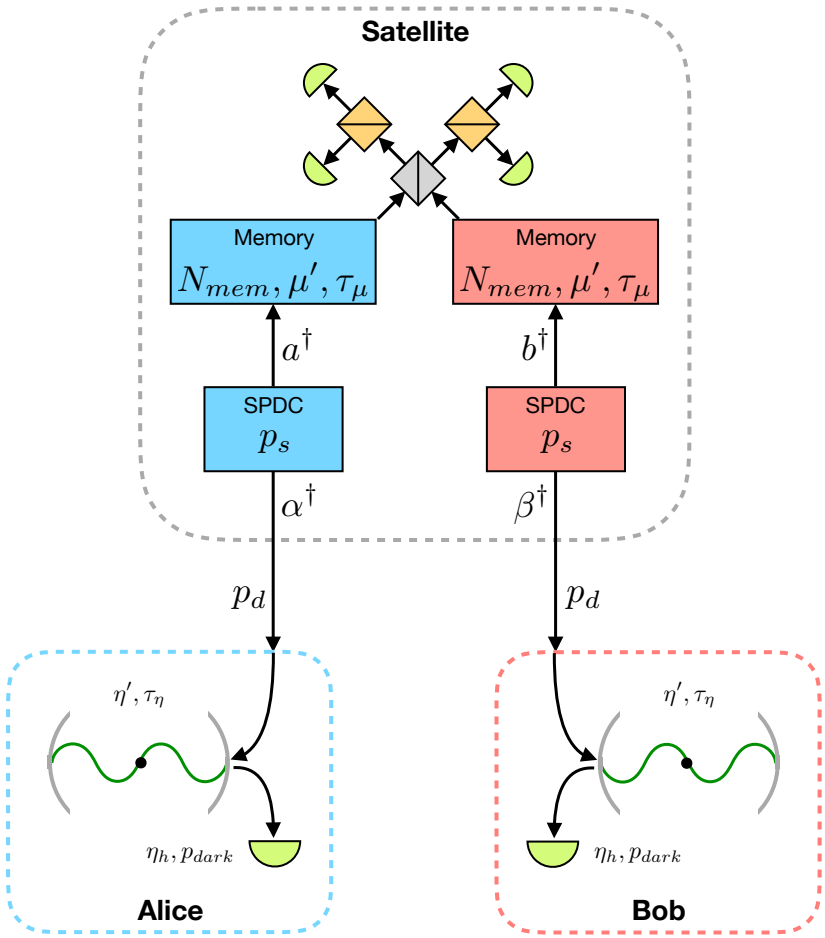


Figure 3.12: Setup considered for the memory assisted downlink scheme.

keeping only the relevant terms and using $p_0 \approx 1$ gives,

$$\begin{aligned}
\sigma_{\text{II}}^{(a,A)} = {} & \eta_a \mu_a p_d \eta_h \left(p_1 + \frac{8}{3}(1-\mu_a)p_2 \right) |\psi^{S_a}\rangle\langle\psi^{S_a}| \\
& + \left((1-\mu_a)p_1 p_d \eta_h + (1-\eta_a)p_{dark}\right) |\varnothing\rangle\langle\varnothing| \otimes \frac{\mathbb{1}^{(A)}}{2} \\
& + \eta_a p_{dark} |\varnothing\rangle\langle\varnothing| \otimes |+\rangle\langle+| + \eta_a \mu_a p_{dark} p_1 \frac{\mathbb{P}_1^{(a)}}{2} \otimes |+\rangle\langle+| \\
& + \frac{1}{3}\eta_a \mu_a^2 p_2 p_d \eta_h \Big[\left(|HV\rangle |+\rangle + S_a\sqrt{2}\,|2H\rangle |-\rangle \right) \left(\langle HV| \langle+| + S_a\sqrt{2}\,\langle 2H| \langle-| \right) \\
& \qquad + \left(|HV\rangle |-\rangle + S_a\sqrt{2}\,|2V\rangle |+\rangle \right) \left(\langle HV| \langle-| + S_a\sqrt{2}\,\langle 2V| \langle+| \right) \Big] \\
& + \left[(1-\eta_a)\mu_a p_1 p_d \eta_h + 4\left(1 - \frac{2}{3}\eta_a\right)\mu_a(1-\mu_a)p_2 p_d \eta_h + (1-\eta_a)\mu_a p_{dark} p_1 \right] \frac{\mathbb{P}_1^{(a)}}{2} \otimes \frac{\mathbb{1}^{(A)}}{2} \\
& + 2(1-\eta_a)\mu_a^2 p_2 p_d \eta_h \frac{\mathbb{P}_2^{(a)}}{3} \otimes \frac{\mathbb{1}^{(A)}}{2}.
\end{aligned} \tag{3.42}$$

Without loss of generality we assume detector clicks corresponding to a $|\psi^+\rangle_{a,b}$ measurement to be the outcome of the BSM on the a and b mode of $\sigma_{\mathrm{II}}^{(a,A)} \otimes \sigma_{\mathrm{II}}^{(b,B)}$. Furthermore we assume $S_a = S_b = +$, such that the state after swap becomes,

$$\begin{aligned}
\rho^{(A,B)} = &\frac{1}{8}\eta_a\eta_b\mu_a\mu_b\left(1+\frac{8}{3}p_2^*(2-\mu_a-\mu_b)\right)|\psi_X^+\rangle\langle\psi_X^+| \\
&+\left[\frac{\mu_a\mu_b(1-\eta_a\eta_b)}{8}+d\frac{\mu_a\mu_b(2-\eta_a-\eta_b)}{8}+p_2^*\frac{d}{p_1}\frac{\mu_a^2(1-\eta_b)+\mu_b^2(1-\eta_a)}{6}\right. \\
&\quad+p_2^*\left(\frac{\mu_a^2+\mu_b^2}{6}+\mu_a\mu_b\left(1-\frac{2}{3}\eta_a\eta_b-\frac{2}{3}(\mu_a+\mu_b)\right)+\frac{1}{12}(\eta_a+\eta_b)\mu_a\mu_b(\mu_a+\mu_b)\right. \\
&\qquad\left.\left.+\frac{1}{6}\eta_a\eta_b\mu_a\mu_b(\mu_a+\mu_b)\right)\right]\frac{\mathbb{1}^{(A)}}{2}\otimes\frac{\mathbb{1}^{(B)}}{2} \\
&+\frac{1}{24}p_2^*\eta_a\eta_b\mu_a\mu_b(\mu_a+\mu_b)\Big[\left(|-,-\rangle+|+,-\rangle+|-,+\rangle\right)\left(\langle-,-|+\langle+,-|+\langle-,+|\right) \\
&\qquad+\left(|+,+\rangle+|+,-\rangle+|-,+\rangle\right)\left(\langle+,+|+\langle+,-|+\langle-,+|\right)\Big] \\
&+\eta_b\mu_a\left(\frac{1}{6}p_2^*\frac{d}{p_1}\mu_a+\frac{1}{8}d\mu_b\right)\frac{\mathbb{1}^{(A)}}{2}\otimes|+\rangle\langle+|+\eta_a\mu_b\left(\frac{1}{6}p_2^*\frac{d}{p_1}\mu_b+\frac{1}{8}d\mu_a\right)|+\rangle\langle+|\otimes\frac{\mathbb{1}^{(B)}}{2} \\
&+\frac{1}{6}p_2^*\mu_a\mu_b(\mu_a+\mu_b)\left[\eta_a(1-\eta_b)\,|0\rangle\langle0|\otimes\frac{\mathbb{1}^{(B)}}{2}+(1-\eta_a)\eta_b\frac{\mathbb{1}^{(A)}}{2}\otimes|0\rangle\langle0|\right]
\end{aligned} \tag{3.43}$$

where we have divided through with $p_1^2p_d^2\eta_h^2$, defined $d=\frac{p_{dark}}{p_d\eta_h}$ and $p_2^*=p_2/p_1$ and expanded in the regime $d, p_2^* \ll 1$. With $\left|\psi_X^+\right\rangle$ being the ideal state we get,

$$\begin{aligned}
f(t_a,t_b) = &\frac{1}{4}+\frac{3}{4}\eta_a\eta_b(1-2d)-\frac{3}{4}d\eta_a\eta_b\frac{\mu_a^2+\mu_b^2}{\mu_a\mu_b} \\
&+\frac{1}{8}p_s\frac{\eta_a\eta_b(\mu_a+\mu_b)}{\mu_a\mu_b}\left(17\mu_a\mu_b+9(\eta_a\eta_b-\eta_a-\eta_b)\mu_a\mu_b-6(\mu_a+\mu_b)\right)
\end{aligned} \tag{3.44}$$

where we have expanded for $f\sim 1$ and used $p_2^*=3p_s/4$. To find the average fidelity of the protocol we should note that the minimum storage time for all memories is $T_{com}^{s\leftrightarrow g}$ for the downlink protocols. Thus setting $\mu_a=\mu_{com}e^{-\Delta/\Delta_{\mu m}}$, $\mu_b=\mu_{com}$, $\eta_a=\eta_{com}e^{-\Delta/\Delta_{\eta m}}$ and $\eta_b=\eta_{com}$ the fidelity may be found by averaging over Δ, such that

$$\begin{aligned}
F = &\frac{1}{4}+\frac{3}{4}\left\langle\eta_a\eta_b\right\rangle_\Delta(1-2d)-\frac{3}{4}d\left\langle\eta_a\eta_b\frac{\mu_a^2+\mu_b^2}{\mu_a\mu_b}\right\rangle_\Delta+\frac{1}{8}p_s\Bigg[17\left\langle\eta_a\eta_b(\mu_a+\mu_b)\right\rangle_\Delta \\
&+9\left\langle\eta_a^2\eta_b^2(\mu_a+\mu_b)\right\rangle_\Delta-9\left\langle\eta_a\eta_b(\eta_a+\eta_b)(\mu_a+\mu_b)\right\rangle_\Delta-6\left\langle\eta_a\eta_b\frac{(\mu_a+\mu_b)^2}{\mu_a\mu_b}\right\rangle_\Delta\Bigg],
\end{aligned} \tag{3.45}$$

where $\langle g\rangle_\Delta=\sum_{\Delta=0}^{N_{max}}p_\Delta g(\Delta)$ with p_Δ as given by equation 2.39.

From the fidelity expression we see that a major limitation on the operation of the protocol will be η_{com}, the efficiencies of the emitters after one communication time. To estimate the minimum required η_{com} needed for operation of the protocol with some given fidelity $F=F_0$, we let $N_{max}=0$

and $p_s \to 0$ in equation 3.45. This produces the following constraint on the memory efficiencies of the emitter,

$$\eta_{com} \geq \sqrt{\frac{4F_0 - 1}{3(1 - 4d)}}. \tag{3.46}$$

The constraint may also be formulated as,

$$\frac{\tau_\eta}{T_{com}^{s\leftrightarrow g}} \geq -\frac{2}{\ln\left(\frac{4F_0-1}{3(1-4d)\eta'^2}\right)}. \tag{3.47}$$

3.4.2 Optimisation and Performance

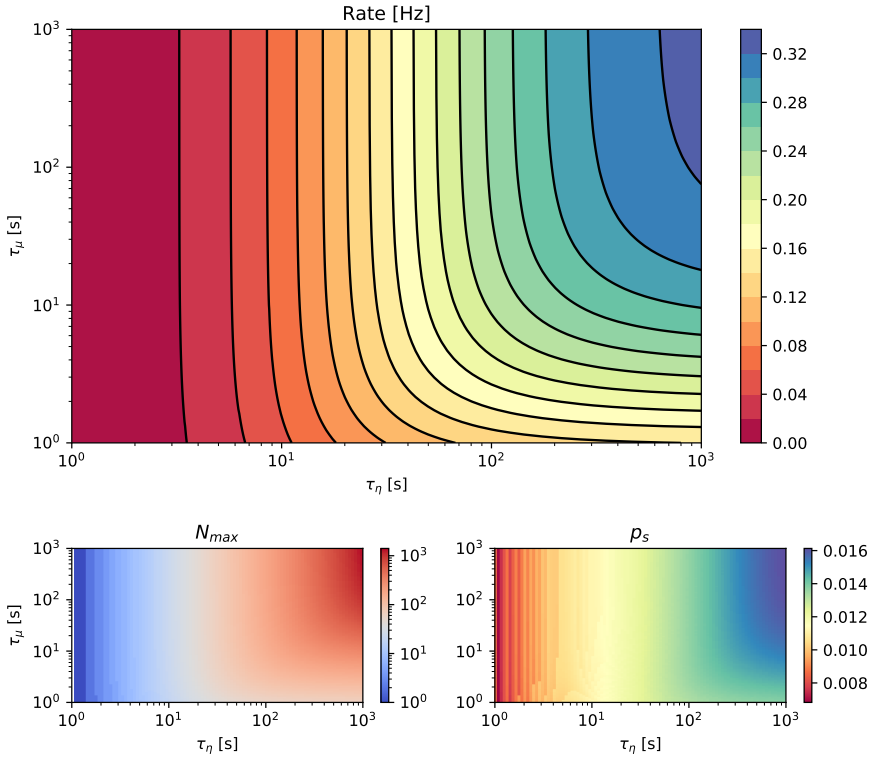


Figure 3.13: (Upper) Contour plot of the optimised rate of the downlink memory assisted scheme such that $F = 0.95$. Parameters are chosen to be $p_d = 10^{-3}$, $\eta_h = 0.5$, $N_{mem} = 1000$, $L = 1000$ km, $\mu' = 0.9$, $\eta' = 1$ and $p_{dark}/p_d\eta_h = 0.01$. (Lower left) The maximum storage time N_{max} found by the optimisation. (Lower right) The Bell state probability of the photon source as found by the optimisation.

The optimisation of the protocol is straightforwardly done numerically, by demanding a certain fidelity $F = F_0$ and optimising over N_{max} and p_s. A contour plot showing the optimised rate, along with the parameters N_{max} and p_s, over the memory coherence times τ_μ and τ_η can be found in figure 3.13.

For the performance of the scheme we refer to figure 3.14, where the rate is shown as a function of N_{mem} and τ_μ with $\tau_\eta = \tau_\mu$, $\tau_\eta = 10\tau_\mu$, $\tau_\eta = 100\tau_\mu$ and $\tau_\eta = 1000\tau_\mu$. We see that in order to beat the benchmark of $R = 0.41$ Hz as given by the direct downlink protocol, we need $N_{mem} \approx 2000$, $\tau_\mu \approx 4$ s and $\tau_\eta \approx 40$ s.

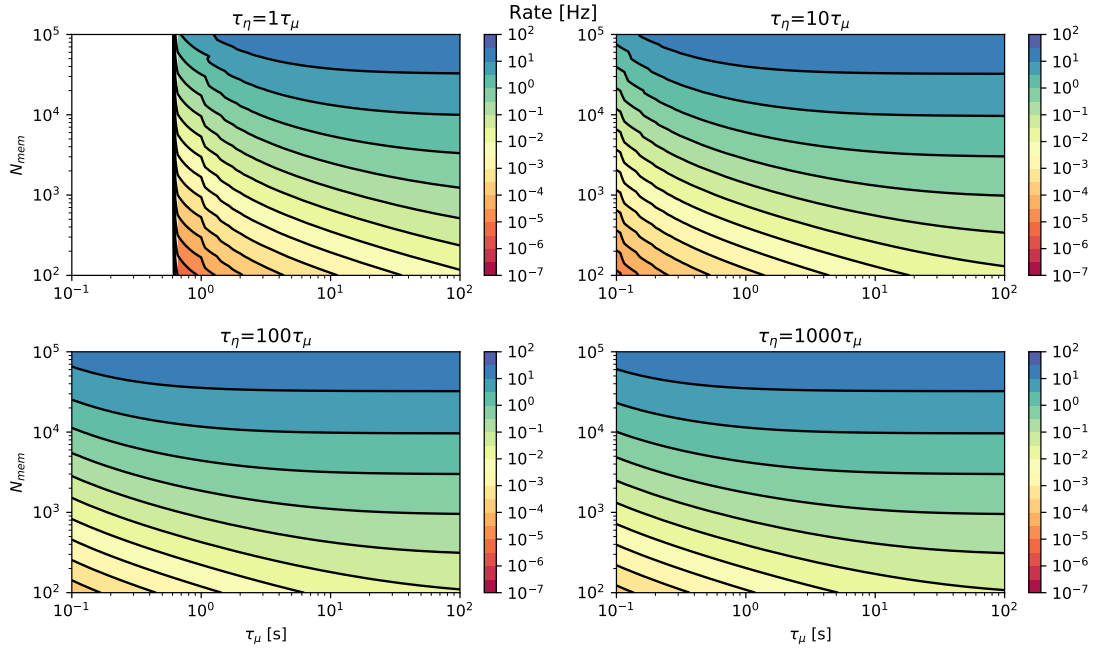


Figure 3.14: Performance of the memory assisted downlink scheme under the condition $F_0 = 0.95$ for various values of τ_μ, τ_η and N_{mem}. The parameters used are $p_d = 10^{-3}$, $\eta_h = 0.5$, $\mu' = 0.9$, $\eta' = 1$, $L = 1000$ km and $d = 0.01$. In the white region in the plot with $\tau_\mu = \tau_\eta$ operation of the scheme is not possible with the required fidelity due to η_{com} being too small.

3.5 Summary

Before the final comparison of the schemes we will again try to summarise the main points of this chapter:

- *Low memory requirements of direct downlink.* With the average time between a photon reaching the ground, being $\langle T_\gamma \rangle = 1/p_d p_s \eta_h r_{rep}$ the memory only requires storing of $N_{mem} = T_{com}^{g\to g}$ modes in order to store most photons coming from the satellite. Furthermore these low requirements on memory coherence time are given by that any single mode only needs to be stored for $T_{com}^{g\to g}$.

- *Very few dark counts required for uplink.* The only measurements of photons in the uplink schemes occur in the satellite, and therefore we require $p_{dark} \ll p_g p_u \eta_h$. This is opposed to the downlink protocol, where the BSM is done by measuring on the photons from the two halves of the system, thereby lowering the requirement to $p_{dark} \ll p_d \eta_h$.

Sec.	Scheme	Rate	τ	Benchmark		
				N_{mem}	τ_η	τ_μ
3.1	Direct Downlink	$\eta_h^2 p_d^2 p_a^2 p_s r_{rep}$	$\tau_\eta \gg T_{com}^{g\to g}$	7	1 s	-
3.3	M.A. Uplink	$\frac{2}{3} N_{mem} \eta_{swap} \mu_{com}^2 p_g p_u \eta_h \frac{1}{T_{com}^{s\leftrightarrow g}}$	$\tau_\mu, \tau_\eta \gg \frac{T_{com}^{s\leftrightarrow g}}{p_g p_u \eta_h N_{mem}}$	10000	50 s	5 s
3.4	M.A. Downlink	$\frac{1}{3} N_{mem} \mu_{com}^2 p_s p_d \eta_h \frac{1}{T_{com}^{s\leftrightarrow g}}$	$\tau_\mu, \tau_\eta \gg \frac{T_{com}^{s\leftrightarrow g}}{p_s p_d \eta_h N_{mem}}$	2000	40 s	4 s
3.5.1	M.A. Emitter Uplink	$\frac{2}{3} N_{mem} \eta_{swap} \mu_{com}^2 \eta_c p_u \eta_h \frac{1}{T_{com}^{s\leftrightarrow g}}$	$\tau_\mu, \tau_\eta \gg \frac{T_{com}^{s\leftrightarrow g}}{\eta_c p_u \eta_h N_{mem}}$	100	50 s	5 s
3.5.1	M.A. Emitter Downlink	$\frac{1}{3} N_{mem} \mu_{com}^2 \eta_c p_d \eta_h \frac{1}{T_{com}^{s\leftrightarrow g}}$	$\tau_\mu, \tau_\eta \gg \frac{T_{com}^{s\leftrightarrow g}}{\eta_c p_d \eta_h N_{mem}}$	20	40 s	4 s

Table 3.2: Performance overview for the different entanglement distribution schemes. *Rate:* Entanglement distribution rate in the good memory regime. τ : Memory coherence time requirements in order to be in the good memory regime. *Benchmark:* Proposed memory parameters in order to achieve the rate $R = 0.41$ Hz, as set by the direct downlink scheme.

- *The uplink scheme is quasi-deterministic.* For the uplink scheme the heralding of the photons occurs in the satellite. This introduces the possibility of loosing the photons stored in the memory on the ground. Instead of only considering the fidelity it is therefore beneficial to also consider the probability of Alice and Bob being able to retrieve entangled photons.
- *Very high memory requirements for memory assisted schemes.* Compared to the direct downlink scheme the requirements of the multimode capacity and the coherence times is significant. This unfortunately makes these proposals quite unfeasible.

3.5.1 Deterministic sources

Throughout this chapter we have considered using SPDC to generate the entangled photons, which is a probabilistic entanglement source. We are now briefly going to consider employing a deterministic source of entangled photons instead. For the direct downlink scheme (section 3.1) the repetition rate is limited by the memories at the ground station. Using the value of p_s from figure 3.6, we estimate that switching to a deterministic source would therefore make the rate ≈ 20 times greater, provided the ground stations have sufficient memory capabilities.

For the memory assisted schemes the effect of switching to a deterministic source of entangled photons would be even greater. As seen in figure 3.10 and 3.13, the Bell state probability is on the order of 1%. A switch to deterministic sources would therefore make the coherence time and multimode capacity requirements ≈ 100 times lower, to achieve the same rate as when employing the SPDC as a photon source.

3.5.2 Comparison of schemes

Table 3.2 shows a compact overview of the schemes discussed in detail in this chapter along with the ad hoc schemes with deterministic entanglement sources. The benchmark parameters are suggested parameters in order to achieve $R = 0.41$ Hz.

The most promising implementation of satellite entanglement distribution seems to be the direct downlink proposal (3.1), which on top of being the simplest, also is the one with lowest requirements. With no need of storing qubits in the satellite and with low requirements of the multimode capacity combined with the acheivable requirements on the coherence time, makes for

modest demands of the memories compared to the memory assisted schemes.

The other scheme worth considering is the memory assisted downlink scheme (3.4). Although the performance is not exactly encouraging when utilising a probabilistic source of entanglement, the story is different when considering a deterministic source of entanglement. With such a source and memories capable of storing 10^3 modes, the coherence time requirements will be saturated for $\tau_\mu \approx 1$ s and $\tau_\eta \approx 10$ s, where the rate becomes $R \approx 25$ Hz, illustrating the high performance ceiling of this scheme.

Finally we have the memory assisted uplink scheme (3.3), which does not seem worthy of further consideration. The performance suffers from the lower photon transmission connected to uplink schemes, while the advantages of being able to perform the swap immediately after the second entanglement is made, becomes irrelevant when considering the overall waiting times in the scheme.

Chapter 4

Repeater

In this chapter, we are going to explore a simple quantum repeater made by linking up two neighbouring entanglement distribution setups. The chapter is motivated by trying to find a suitable value of P_0 for the condition $\langle P(M_a M_b|H_a H_b)\rangle_\Delta \geq P_0$ as specified in section 3.3.2.

4.1 A Quantum Repeater

As mentioned in the introduction of this thesis, there is another way of overcoming the exponential decrease in transmission of photons through fibres, which is the implementation of quantum repeaters. We have, in a sense, already studied quantum repeaters in the earlier chapters, when we studied the memory assisted schemes. The idea behind quantum repeaters is the splitting of the distance between Alice and Bob into several smaller segments. A segment will consist of a memory in both ends with some way to entangle the memories. At the nodes connecting the segments, repeater stations will be build, containing two memories and a method to perform a entanglement swap on the memories. The quantum repeater therefore works by creating entanglement in the individual segments, followed by entanglement swaps in neighbouring segments, thereby extending the distance of entanglement. The memory assisted satellites we have considered in the previous chapters, are therefore a two segment quantum repeater with the satellite serving as the repeater station.

We will now take the hybridisation of satellite links and quantum repeaters even further by initiating the study of linking several of the proposed satellite schemes up to become a repeater. This idea was originally studied in [34], where the performance of several direct downlink connections of section 3.1, was analysed. But first, we will consider two general cases of a quantum repeater.

4.1.1 Deterministic Swapping

We will now consider a repeater with N identical segments. At each of the $N-1$ repeater stations, we will assume perfect memories with unit swapping efficiency. With deterministic swapping, the time it takes for Alice and Bob to be entangled is the same as the time it takes for all N segments to be entangled $\langle T_N\rangle$.[1] To find this time, we are going to partition the chain of of N segments into a block containing $N-1$ segments and a block of a single segment. As all the links are identical,

[1] We assume that the time it takes to perform the swaps is negligible compared to $\langle T_N\rangle$.

the probability of entanglement being created in all $N-1$ links of the great block before the single segment block is $1/N$. In this case the time it takes for the repeater to finish is $\langle T_{N-1}\rangle + \langle T_1\rangle$. On the other hand if the probability of entanglement being made in the single segment before all $N-1$ links of the other block is $(N-1)/N$. In this case the time is $\langle T_{N-1}\rangle$. By taking the weighted average of the two situations we arrive at,

$$\langle T_N\rangle = \frac{1}{N}\left(\langle T_{N-1}\rangle + \langle T_1\rangle\right) + \frac{N-1}{N}\langle T_{N-1}\rangle\,. \tag{4.1}$$

This recursive relation has the solution,

$$\langle T_N\rangle = \langle T_1\rangle \sum_{n=1}^{N} \frac{1}{n}. \tag{4.2}$$

We see that for $N = 2$ we get $\langle T_2\rangle = \frac{3}{2}\langle T_1\rangle$, which is where the the factor 2/3 in all the rate expression stems from. Another value of interest is that of a four segment repeater, which is $\langle T_4\rangle = \frac{25}{12}\langle T_1\rangle$. Finally the value of the sum $\sum_{n=1}^{N}\frac{1}{n}$ is called the N-th harmonic number and is denoted H_N. For large N an asymptotic expansion of H_N yields,

$$\langle T_N\rangle = \langle T_1\rangle \ln N. \tag{4.3}$$

With each segment being of a certain length, the logarithmic scaling in number of segments is also a logarithmic scaling in the distance between Alice and Bob. We therefore see that by building repeater stations, we have effectively overcome the exponential scaling of photon transmission through fibres.

4.1.2 Non-Deterministic Swapping

Another interesting regime is that of a non-deterministic swapping efficiency η_{swap}. We now consider a repeater with $N = 2^n$ segments, where n is called the nesting level. The idea is to perform the swaps with the neighbouring segment, in n levels as seen in 4.1. With this we minimise the impact of an unsuccessful swapping attempt. A common approach to finding $\langle T_{2^n}\rangle$, is then to apply the two level approximation from above to each nesting level of the repeater [37]. With the inclusion of the swapping efficiency at each level the approximation becomes,

$$\langle T_{2^n}\rangle = \left(\frac{3}{2\eta_{swap}}\right)^n \langle T_1\rangle\,. \tag{4.4}$$

This approximation is especially good for $\eta_{swap} \ll 1$, because it implicitly assumes that segments at any level entanglement either is there or not there, which is a good approximation if the hardest part of the repeater is the swap. Figure 4.2 shows the approximation of equation 4.4, along with simulated completion times for $\eta_{swap} = 0.5$. We see that for nesting level $n = 8$ (i.e. $N = 256$ repeater segments[2]), the relative error is 44%, meaning that the model is good at estimating the rate to the nearest order of magnitude.

4.2 Good Memory Regime

We will now consider the performance of a repeater involving two satellites in the limit of no decay in the memories as seen in figure 4.3. We will consider the general situation where the swapping

[2]Which is way more segments than ever needed for a global quantum repeater.

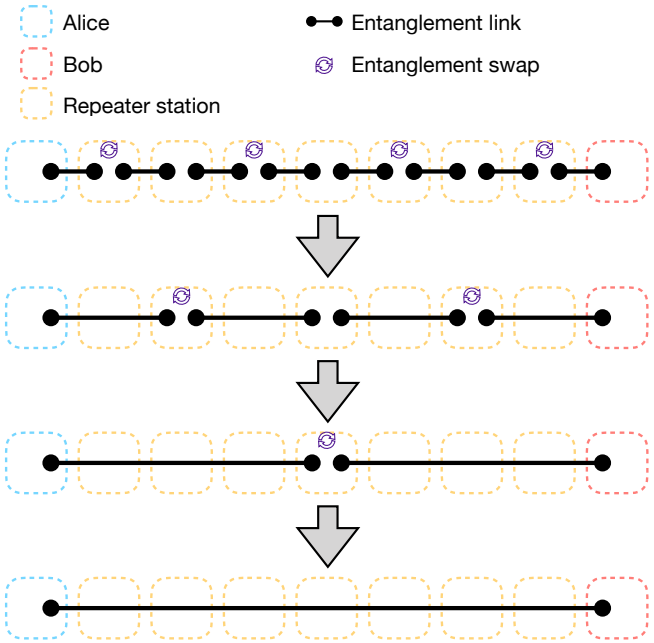


Figure 4.1: The swapping order of a nested repeater with $N = 2^3$.

efficiencies is different at the different nesting levels. Specifically we will η_1 be the swapping efficiency in the satellite and η_2 be the swapping efficiency at the repeater station. At each repetition the probability of successfully entangling a single segment of the repeater is p_e.

To calculate $\langle n \rangle$ the average number of attempts needed to distribute entanglement across the repeater, we are going to employ the Markov chain approach developed in [38]. We start out by introducing the notation where we use a bit string $n_1 n_2 n_3 n_4$, $n_i \in \{0, 1\}$ to represent the state of the repeater, such that $n_i = 1$ if there is entanglement in the i'th link and $n_i = 0$ if there is no entanglement. Furthermore we denote a successful swap between to neighbouring links by a bar. The final state of the repeater where Alice and Bob share an entangled pair of qubits is given by the state $\overline{\overline{11}\,\overline{11}}$. We may also exploit the symmetry of the repeater to lump together different states. All possible states of the repeater are,

$$\begin{aligned}
S_1 &= 0000 = \{0000\} \\
S_2 &= 0001 = \{0001, 0010, 0100, 1000\} \\
S_3 &= 0101 = \{0101, 0110, 1001, 1010\} \\
S_4 &= 00\overline{11} = \{00\overline{11}, \overline{11}00\} \\
S_5 &= 01\overline{11} = \{01\overline{11}, 10\overline{11}, \overline{11}01, \overline{11}10\} \\
S_6 &= \overline{\overline{11}\,\overline{11}} = \{\overline{\overline{11}\,\overline{11}}\},
\end{aligned} \tag{4.5}$$

where the sets represents the states that are equivalent and thus are lumped together. If we assume the swapping procedure to be instantaneous, we may consider the probabilities of transferring from one state to another. As $p_e \ll 1$, we are going to neglect all processes $\mathcal{O}(p_e^2)$. A diagram of all such possible transfers from one state to another may be found in figure 4.4. We should note that

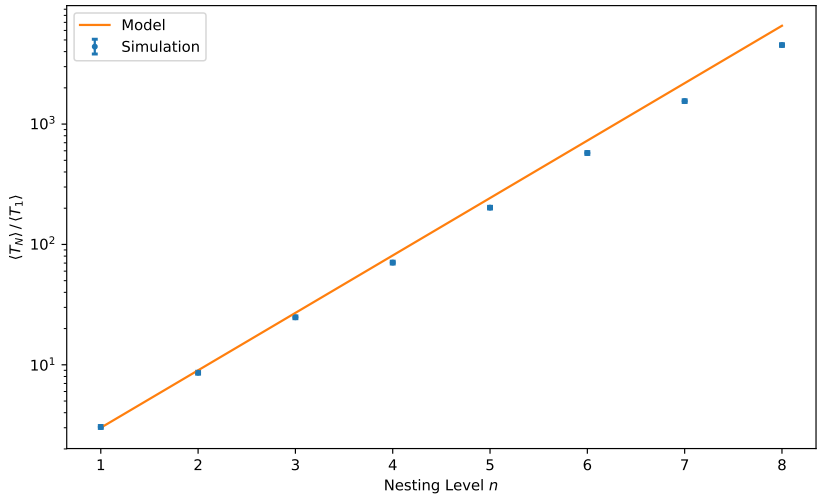


Figure 4.2: Model of entanglement time for a quantum repeater as given by 4.4, along with simulated entanglement times for different nesting levels. The swapping efficiency $\eta_{swap} = 0.5$ was used.

the state $\overline{\overline{11}\,\overline{11}}$ is an absorbing state because, once the repeater enters this state there is no way to escape from it again. The average number of time steps $\langle n \rangle$ it takes for the repeater to end up in state is called the absorption time.

To find the absorption time we are going to construct the transition probability matrix $P_{ij} = Prob(S_i \to S_j)$,

$$P = \begin{pmatrix} 1-4p_e & 4p_e & 0 & 0 & 0 & 0 \\ (1-\eta_1)p_e & 1-3p_e & 2p_e & \eta_1 p_e & 0 & 0 \\ 0 & 2(1-\eta_1) & 1-2p_e & 0 & 2\eta_1 p_e & 0 \\ 0 & 0 & 0 & 1-2p_e & 2p_e & 0 \\ \eta_1(1-\eta_2)p_e & 0 & 0 & (1-\eta_1)p_e & 1-p_e & \eta_1\eta_2 p_e \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} Q & \mathbf{u} \\ \mathbf{0}^T & 1 \end{pmatrix} \tag{4.6}$$

where Q is the 5×5 transition probability matrix of the non-absorbing states, $\mathbf{u}$ is the vector with the transition probabilities to the absorbing state and $\mathbf{0}$ being the 0-vector. In [38] it is shown that the absorbtion times $\langle n_{i\to 6} \rangle$ starting out in state S_i is given by,

$$\begin{pmatrix} \langle n_{1\to 6} \rangle \\ \langle n_{2\to 6} \rangle \\ \langle n_{3\to 6} \rangle \\ \langle n_{4\to 6} \rangle \\ \langle n_{5\to 6} \rangle \end{pmatrix} = (\mathbb{1} - Q)^{-1} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}. \tag{4.7}$$

As the repeater starts out in state $S_1 = 0000$, the quantity we are interested in is $\langle n_{1\to 6} \rangle = \langle n \rangle$. Evaluating the matrix product gives,

$$\langle n \rangle = \frac{27 - 2\eta_1}{12\eta_1\eta_2 p_e}. \tag{4.8}$$

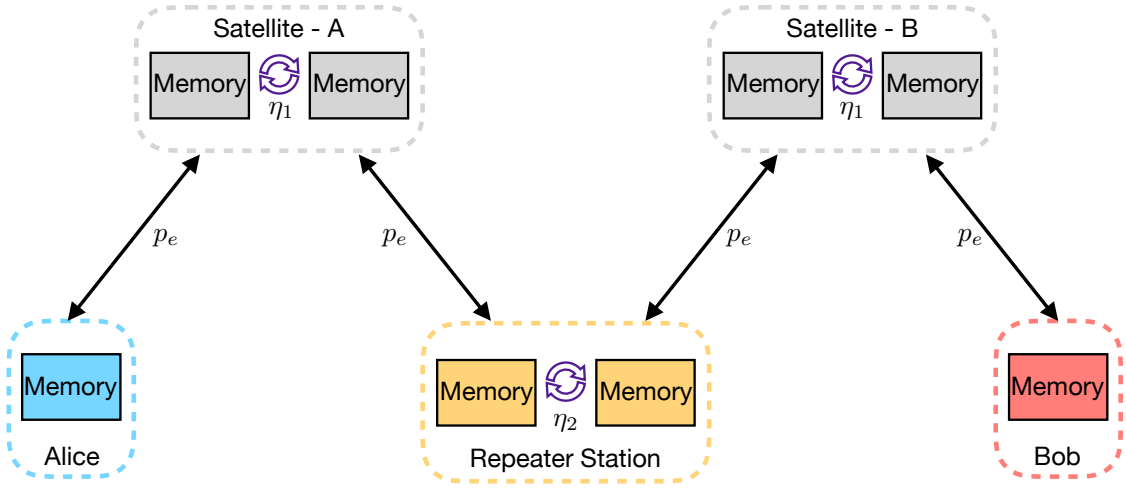


Figure 4.3: A four segment repeater involving two satellites. The probability of entangling a single segment of the repeater per attempts is p_e. The swapping efficiency in the satellites is η_1 and η_2 at the repeater station on the ground.

We see that for deterministic swapping $\eta_1 = \eta_2 = 1$ we recover $\langle n \rangle = 25/12 p_e$ as expected. In the opposing limit of $\eta_1 \to 1$ we recover $\langle n \rangle = 9/4 \eta_1 \eta_2 p_e$ which is expected as well. With the inclusion of the memory efficiency μ' of the memories at Alice and Bob the rate of the repeater becomes,

$$R = \mu'^2 \frac{12\eta_1}{27 - 2\eta_1} \eta_2 p_e r_{rep}. \tag{4.9}$$

Where we again see linear scaling in p_e, compared to the quartic scaling without memories. We should also note that the method provided here also works for bigger repeater chains, but that the number of states S_i needed scales like $\mathcal{O}(1.34^n)$ with nesting level n [38].

4.2.1 Example: Memory Assisted - Uplink

We will now consider the specific implementation of the four segment repeater as two memory assisted uplink schemes of section 3.3. η_1 is the swapping efficiency in the satellite, which now is the swapping efficiency between the two emitters which we have previously called η_{swap}. For η_2 we are considering the swapping efficiency at the ground station, which is done by unloading the photons from the memories onto beam splitters as described in section 2.3.2. With D_{BSM} being the event of the correct detection pattern at the BSM we have,

$$\eta_2 = P(D_{BSM} | H_{SAR} H_{SBL}), \tag{4.10}$$

where H_{SAR} (H_{SBL}) is the heralding event in the right (left) emitter of satellite-A (satellite-B). The calculation made to find $P(D_{BSM}|H_{SAR}H_{SBL})$ is completely analogous to the fidelity calculations involving ensemble memories, and involves conditioning the state in the memory on the ground on the heralding at the satellite followed by a consideration of which combination of states will produce the correct combination clicks. Doing this simple calculation yields,

$$\eta_2 = \frac{1}{2}\mu^2 \left(1 + 5p_g(1-\mu) - 2\frac{d}{p_g}\right). \tag{4.11}$$

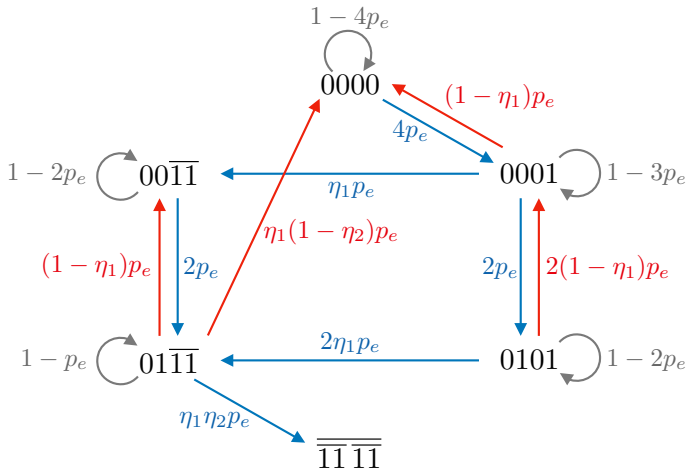


Figure 4.4: Markov chain diagram for the four segment repeater shown in figure 4.3.

With this the rate of the repeater becomes,

$$R = \frac{12\eta_{swap}}{54-4\eta_{swap}}\mu^4\left(1+5p_g(1-\mu)-2\frac{d}{pg}\right)\eta_h p_g p_u r_{rep}. \tag{4.12}$$

We see that while the scaling in p_u is linear, the scaling in memory efficiency is quartic. For $\mu \ll 1$ it might therefore not be favourable to increase the number of segments, but instead have fewer longer segments.

4.3 Good Emitter and Bad Ensemble

We are now going to turn our attention to the situation where the coherence time of the ensemble memory is poor and the emitter good, this being the regime where the condition $\langle P(M_aM_b|H_aH_b)\rangle_\Delta \geq P_0$ is relevant. With an imperfect memory, the Markov chain approach is no longer an effective weapon as it relies on the assumption that an entangled link is not destroyed unless an unsuccessful swapping attempt is made.

We assume that the memories in the satellite are perfect memories, meaning that they have unit efficiency for all storage times and unit swapping efficiency. We are going treat the attempts as continuously occurring such that the probability density function of a link being entangled is,

$$p(\tilde{t}) = e^{-\tilde{t}}, \tag{4.13}$$

where $\tilde{t} = t/\langle T_e\rangle$ is the time in terms of the average time for a single link being entangled $\langle T_e\rangle = 1/(p_e r_{rep})$. Quickly dropping the tilde from the time variable, we are going to introduce a cutoff time T_{cut} from the first link is entangled until we require all four links to be entangled.[3] The

[3]This is the simplest form of cutoff time which is relevant for the scheme. For optimised running of the repeater one might have several cutoff times for when to require the different number of links to be entangled. Furthermore one might update these cutoff times depending on what times the previous links where entangled. However due to the cutoff time imposed by the deadline of handing in this thesis, this will have to be a story for another time.

probability of the remaining three links being entangled before the cutoff time is then,

$$\eta_{cut} = \int_0^{T_{cut}} \mathrm{d}t_1 \mathrm{d}t_2 \mathrm{d}t_3 \, p(t_1)p(t_2)p(t_3). \tag{4.14}$$

We will also consider the time average time it takes the three links to be entangled given that it happens within the cutoff time,

$$\langle T_{3c} \rangle = 3 \int_0^{T_{cut}} \mathrm{d}t_1 \, p(t_1) t_1 \int_0^{t_1} \mathrm{d}t_2 \mathrm{d}t_3 \, p(t_2)p(t_3). \tag{4.15}$$

Finally we are going to need the average memory efficiency,

$$\langle \mu \rangle = 3\mu_{com} \int_0^{T_{cut}} \mathrm{d}t_1 \, p(t_1)\mu(t_1) \int_0^{t_1} \mathrm{d}t_2 \mathrm{d}t_3 \, p(t_2)p(t_3)\mu(t_1 - t_2)\mu(t_1 - t_3) \tag{4.16}$$

where $\mu(t) = \mu_{com} e^{-t/\tau}$ with τ being the coherence time of the memory in terms of $\langle T_e \rangle$. Employing equation 2.23 we may now find the average expected time to create entanglement in all four segments,

$$\langle T_4 \rangle = \frac{\langle T_{3c} \rangle + \frac{1}{4} + (1 - \eta_{cut}) T_{cut}}{\langle \mu \rangle}, \tag{4.17}$$

where we have used that the expected time of the first entanglement is 1/4.

We will now consider the bad memory limit $\tau \ll 1$. From all the previous schemes involving a cutoff time we have seen $T_{cut} \lesssim \tau$, such that we expect the greatest rate for $T_{cut} \ll 1$. When this is the case $\eta_{cut} \ll 1$ meaning that most attempts will be terminated because of the cutoff. Therefore $\langle T_{3c} \rangle \ll T_{cut}$, such that

$$\langle T_4 \rangle = \frac{\frac{1}{4} + T_{cut}}{\langle \mu \rangle} \tag{4.18}$$

Additionally we calculate $\langle \mu \rangle$ in the limit $\tau \ll 1$ to get,

$$\langle \mu \rangle = \mu_{com}^4 \tau^3 e^{-T_{cut}/\tau} (e^{T_{cut}/\tau} - 1)^3. \tag{4.19}$$

Plugging this result into equation 4.18 and solving the equation $\frac{\mathrm{d}}{\mathrm{d}T_{cut}} \langle T_4 \rangle = 0$, for T_{cut} to maximise the rate yields,

$$T_{cut} = \frac{1}{12}(3 + 4\tau + 12\tau W_{-1}(-\frac{1}{3} e^{-\frac{1}{3} - \frac{1}{4\tau}})), \tag{4.20}$$

where $W_{-1}(z)$ is the Lambert W function. A rough estimation of the cutoff time turns out to be $T_{cut} \approx 3\tau$. Employing this restriction on equation 3.40 gives,

$$\langle P(M_a M_b | H_a H_b) \rangle_\Delta \approx \frac{1}{3} \mu_{com}^2 \tag{4.21}$$

which is where the choice of which is the value we used in section 3.3.2. We have hereby illustrated how one might approach the problem of finding a suitable value for P_0, here done for the specific purpose of using the uplink memory assisted entanglement distribution scheme as a part of a repeater.

We will conclude this chapter by noting that this is by no means an exhaustive investigation into the field of satellite quantum repeaters.

Chapter 5

Conclusion

In this thesis we have studied quantum communication with satellite links. We have examined how the addition of quantum memories to the satellite affects the rate and fidelity of the communication, and compared it against the direct downlink satellite architectures without memories.

For quantum key distribution we found a significant potential for improvement when considering satellites with memories. Using the Micius satellite as the benchmark [2], we found the uplink schemes where the photon heralding is done scattering of the emitter acting as a memory, as the most promising implementation, with the benchmark requirement for the coherence time of 0.2 s, having already been demonstrated experimentally in silicon-vacancy centres [33]. The memory assisted downlink proposals, both with emitters and ensembles, are also promising candidates for future quantum communication satellites.

When considering satellite links for entanglement distribution, the direct downlink implementation is the most promising implementation, requiring the lowest amount of memory qubits and the shortest coherence time. The memory assisted schemes, are only realistically going to improve upon the direct downlink proposal with the introduction of deterministic sources of entangled photons. However, deterministic sources would also be beneficial for the direct downlink proposal, albeit to a lesser extent.

Finally we took the initial steps of a study into satellite quantum repeaters. We saw how to use Markov chain diagrams to calculate the rate of repeater chains with perfect memories and non-deterministic swapping. Furthermore we calculated the maximum waiting time of a repeater consisting of two uplink memory assisted setups, with ensemble memories with finite coherence times.

5.1 Outlook

As a concluding remark we will look at how to proceed with the studies initialised in this thesis. Broadly speaking we may split the avenues of further research into two categories: adding detail or branching out. By adding detail we mean considering the proposed setups in the thesis closer. A way to do this would be to consider how errors that we have not considered in this thesis, such as non-unit detector efficiencies or not completely distinguishable photons, affect the protocols

considered. One might also go more into depth with the orbital motion of the satellite. This could include a more detailed analysis of photon transmission through the atmosphere accompanied by new models for rate and fidelity introducing different photon transmission probabilities for Alice and Bob. Another interesting aspect of the orbital motion of satellites, is considering how different orbits influences the average rates, when taking into account that satellites are visible only part of the time. Finally it would also be interesting to consider the implementation deterministic sources of entanglement further, as this could lead to significant performance increases.

Moreover it might be interesting to expand some of the ideas proposed. Specifically carrying out further analysis on the satellite quantum repeaters, would be a worthwhile endeavour. Analysis on how many satellite links for a given distance between Alice and Bob could be interesting. Furthermore the performance of quantum repeaters with imperfect memories and imperfect swaps remains an open question. Finally we will mention the avenue of entanglement distillation as a source of greater rates for entanglement distribution. The idea being that lowering the requirement on the fidelity F_0 would lead to more entangled pairs of photons being distributed to Alice and Bob, who could then perform entanglement distillation protocols to create entanglement with higher fidelity.

Bibliography

[1] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.*, 117:190501, Nov 2016.

[2] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[3] Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Yuan Cao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Shuang-Lin Li, Rong Shu, Yong-Mei Huang, Lei Deng, Li Li, Qiang Zhang, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Xiang-Bin Wang, Feihu Xu, Jian-Yu Wang, Cheng-Zhi Peng, Artur K. Ekert, and Jian-Wei Pan. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*, 582(7813):501–505, 2020.

[4] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C. Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando G. S. L. Brandao, David A. Buell, Brian Burkett, Yu Chen, Zijun Chen, Ben Chiaro, Roberto Collins, William Courtney, Andrew Dunsworth, Edward Farhi, Brooks Foxen, Austin Fowler, Craig Gidney, Marissa Giustina, Rob Graff, Keith Guerin, Steve Habegger, Matthew P. Harrigan, Michael J. Hartmann, Alan Ho, Markus Hoffmann, Trent Huang, Travis S. Humble, Sergei V. Isakov, Evan Jeffrey, Zhang Jiang, Dvir Kafri, Kostyantyn Kechedzhi, Julian Kelly, Paul V. Klimov, Sergey Knysh, Alexander Korotkov, Fedor Kostritsa, David Landhuis, Mike Lindmark, Erik Lucero, Dmitry Lyakh, Salvatore Mandrà, Jarrod R. McClean, Matthew McEwen, Anthony Megrant, Xiao Mi, Kristel Michielsen, Masoud Mohseni, Josh Mutus, Ofer Naaman, Matthew Neeley, Charles Neill, Murphy Yuezhen Niu, Eric Ostby, Andre Petukhov, John C. Platt, Chris Quintana, Eleanor G. Rieffel, Pedram Roushan, Nicholas C. Rubin, Daniel Sank, Kevin J. Satzinger, Vadim Smelyanskiy, Kevin J. Sung, Matthew D. Trevithick, Amit Vainsencher, Benjamin Villalonga, Theodore White, Z. Jamie Yao, Ping Yeh, Adam Zalcman, Hartmut Neven, and John M. Martinis. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019.

[5] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[6] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[7] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7 – 11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[8] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[9] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[10] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[11] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[12] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992.

[13] Dominic Mayers and Andrew Yao. Self testing quantum apparatus, 2003.

[14] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, Jun 2005.

[15] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, apr 2009.

[16] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[17] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, Aug 2003.

[18] Christopher C. Gerry and Peter L. Knight. *Introductory Quantum Optics*. Cambridge University Press, 2008.

[19] Heonoh Kim, Osung Kwon, and Han Seb Moon. Pulsed sagnac source of polarization-entangled photon pairs in telecommunication band. *Scientific reports*, 9(1):5031–5031, 03 2019.

[20] Mikael Afzelius, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin. Multimode quantum memory based on atomic frequency combs. *Phys. Rev. A*, 79:052329, May 2009.

[21] Adrian Holzäpfel, Jean Etesse, Krzysztof T Kaczmarek, Alexey Tiranov, Nicolas Gisin, and Mikael Afzelius. Optical storage for 0.53 s in a solid-state atomic frequency comb memory using dynamical decoupling. *New Journal of Physics*, 22(6):063009, jun 2020.

[22] Pierre Jobez, Cyril Laplane, Nuala Timoney, Nicolas Gisin, Alban Ferrier, Philippe Goldner, and Mikael Afzelius. Coherent spin control at the quantum level in an ensemble-based optical memory. *Phys. Rev. Lett.*, 114:230502, Jun 2015.

[23] Pierre Jobez, Nuala Timoney, Cyril Laplane, Jean Etesse, Alban Ferrier, Philippe Goldner, Nicolas Gisin, and Mikael Afzelius. Towards highly multimode optical quantum memory for quantum repeaters. *Phys. Rev. A*, 93:032327, Mar 2016.

[24] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59:2044–2046, Nov 1987.

[25] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[26] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. W. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson. Entanglement distillation between solid-state quantum network nodes. *Science*, 356(6341):928–932, 2017.

[27] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy. Multiplexed memory-insensitive quantum repeaters. *Phys. Rev. Lett.*, 98:060502, Feb 2007.

[28] C. E. Bradley, J. Randall, M. H. Abobeih, R. C. Berrevoets, M. J. Degen, M. A. Bakker, M. Markham, D. J. Twitchen, and T. H. Taminiau. A ten-qubit solid-state spin register with quantum memory up to one minute. *Phys. Rev. X*, 9:031045, Sep 2019.

[29] J. Bourgoin, Evan Meyer-Scott, B. Higgins, B. Helou, Chris Erven, Hannes Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and Thomas Jennewein. A comprehensive design and performance analysis of leo satellite quantum communication. *New Journal of Physics*, 15, 11 2012.

[30] Mustafa Gündoğan, Jasminder S. Sidhu, Victoria Henderson, Luca Mazzarella, Janik Wolters, Daniel K. L. Oi, and Markus Krutzik. Space-borne quantum memories for global quantum communication, 2020.

[31] Johannes Borregaard, Hannes Pichler, Tim Schröder, Mikhail D. Lukin, Peter Lodahl, and Anders S. Sørensen. One-way quantum repeater based on near-deterministic photon-emitter interfaces. *Phys. Rev. X*, 10:021071, Jun 2020.

[32] Mihir K. Bhaskar, Ralf Riedinger, Bartholomeus Machielse, David S. Levonian, Christian T. Nguyen, Erik N. Knall, Hongkun Park, Dirk Englund, Marko Lončar, Denis D. Sukachev, and Mikhail D. Lukin. Experimental demonstration of memory-enhanced quantum communication. 2019.

[33] C. T. Nguyen, D. D. Sukachev, M. K. Bhaskar, B. Machielse, D. S. Levonian, E. N. Knall, P. Stroganov, R. Riedinger, H. Park, M. Lončar, and M. D. Lukin. Quantum network nodes based on diamond qubits with an efficient nanophotonic interface. *Phys. Rev. Lett.*, 123:183602, Oct 2019.

[34] K. Boone, J.-P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon. Entanglement over global distances via quantum repeaters with satellite links. *Phys. Rev. A*, 91:052325, May 2015.

[35] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 10th anniversary edition edition, 2010.

[36] Charles H. Bennett, David P. DiVincenzo, Peter W. Shor, John A. Smolin, Barbara M. Terhal, and William K. Wootters. Remote state preparation. *Phys. Rev. Lett.*, 87:077902, Jul 2001.

[37] Nicolas Sangouard, Christoph Simon, Hugues de Riedmatten, and Nicolas Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83:33–80, Mar 2011.

[38] E. Shchukin, F. Schmidt, and P. van Loock. Waiting time in quantum repeaters with probabilistic entanglement swapping. *Phys. Rev. A*, 100:032322, Sep 2019.