Building blocks of quantum repeater networks

Rozpedek, Filip

DOI
10.4233/uuid:ed0af513-7621-4007-9a34-1a3e17370952

Publication date
2019

Document Version
Final published version

Citation (APA)
Rozpedek, F. (2019). *Building blocks of quantum repeater networks*. [Dissertation (TU Delft), Delft University of Technology]. https://doi.org/10.4233/uuid:ed0af513-7621-4007-9a34-1a3e17370952

BUILDING BLOCKS OF QUANTUM REPEATER NETWORKS

BUILDING BLOCKS OF QUANTUM REPEATER NETWORKS

Proefschrift

ter verkrijging van de graad van doctor
aan de Technische Universiteit Delft,
op gezag van de Rector Magnificus prof. dr. ir. T.H.J.J. van der Hagen,
voorzitter van het College voor Promoties,
in het openbaar te verdedigen op woensdag 19 juni 2019 om 10:00 uur

door

Filip Damian ROZPĘDEK

Master in Physics with Honours in Mathematics and Theoretical Physics,
University of St Andrews, Schotland, Verenigd Koninkrijk
geboren te Warschau, Polen.

Dit proefschrift is goedgekeurd door de promotoren.

Samenstelling promotiecommissie:

Rector Magnificus,	voorzitter
Prof. dr. S.D.C. Wehner,	Technische Universiteit Delft, promotor
Prof. dr. ir. R. Hanson,	Technische Universiteit Delft, promotor
Onafhankelijke leden:	
Prof. dr. H. de Riedmatten,	Institut de Ciències Fotòniques
Prof. dr. A. Sørensen,	Københavns Universitet
Prof. dr. B.M. Terhal,	Technische Universiteit Delft
Prof. dr. W. Tittel,	Technische Universiteit Delft

Printed by: Gildeprint

Cover: Design by Dmytro Vasylyev

ISBN 978-94-6384-043-9

An electronic version of this dissertation is available at
`http://repository.tudelft.nl/`.

Nobody expects the Spanish Inquisition!

Michael Palin

CONTENTS

SUMMARY

Future quantum networks will enable the realisation of a large family of quantum protocols, hence allowing for implementation of various tasks ranging from quantum cryptography through quantum computing to quantum metrology.

In this thesis we analyse and develop the building blocks of quantum repeater networks. These networks consist of quantum repeater nodes, which are equipped with quantum memories enabling storage of quantum information. The repeater nodes are connected using optical fibres that enable for the transmission of photonic quantum signals between the repeater nodes.

We specifically focus on the two building blocks: remote entanglement generation and entanglement distillation. We then investigate various proof of principle quantum repeater schemes used for generating shared secret key between distant parties. The repeater schemes that we consider utilise one to three memory nodes capable of generating memory-photon entanglement. Finally, we introduce a novel framework for investigating a foundational aspect in the use of quantum communication related to the uncertainty principle.

Efficient remote entanglement generation is an indispensable building block of most near-term quantum repeater networks. In this thesis we consider various remote entanglement generation schemes that permit multiplexing, which aims at increasing the throughput of this procedure. We find that for the specific schemes that are suitable for platforms with a single communication qubit and multiple memory qubits, the performance of the multiplexing approach is strongly dependent on the time it takes to perform local operations within the memory nodes.

Entanglement distillation enables for filtering out the noise from imperfect entangled states using only local operations and classical communication. Using a general framework for optimising such schemes, which we have developed, we have proven optimality of specific generic and experimentally relevant distillation schemes. We have developed a general framework for optimising such schemes, which we have used to prove optimality of various generic and experimentally relevant distillation schemes.

In designing proof of principle quantum repeater schemes we assume an information-theoretic approach, which enables us to assess their performance in a hardware-agnostic way. We find that all the schemes that we consider can prove useful in specific parameter regimes for the nitrogen-vacancy centre platform. Moreover, we find that one scheme which has already been realised experimentally in the context of remote entanglement generation, is expected to significantly outperform every possible system based on direct communication without repeaters. However, our analysis shows that encapsulating the nitrogen-vacancy centres in optical cavities for the enhancement of the emission rates is a necessary requirement for such a successful demonstration of the first proof-of-principle quantum repeater.

Finally, we investigate the quantum uncertainty principle which is a fundamental feature of quantum mechanics, allowing for security in many quantum cryptographic protocols. We find that in a particular scenario, relevant from the perspective of quantum key distribution, a significant part of the observed uncertainty is in fact due to lack of information rather than intrinsic. If the eavesdropper could access that information, she would be able to much better, or in some cases even with certainty, guess the value of the raw bit of the generated key.

SAMENVATTING

Toekomstige kwantumnetwerken zullen het mogelijk maken om een groot aantal protocollen in de kwantumcryptografie, kwantumcomputatie en kwantummetrologie te realiseren.

In deze thesis analyseren en ontwikkelen wij de bouwblokken voor netwerken die op kwantum repeaters gebaseerd zijn. Zulk soort netwerken bestaan uit kwantumknooppunten, die kwantumgeheugens bezitten die kwantuminformatie kunnen bewaren. Verschillende knooppunten kunnen met elkaar verbonden zijn met optische fibers, die gebruikt kunnen worden om fotonen door te sturen.

Hier zijn we specifiek geïnteresseerd in twee van de bouwblokken, namelijk de generatie van kwantum verstrengeling over lange afstanden en de distillatie van deze verstrengeling. We onderzoeken experimenteel toegankelijke kwantum repeater protocollen die het mogelijk maken om cryptografische sleutels tussen twee personen te generen. Deze repeater protocollen gebruiken één tot drie knooppunten, waarvan elk in staat is om verstrengeling te generen tussen het geheugen en een foton. We concluderen met een nieuw perspectief op fundamentele aspecten van de kwantumcommunicatie gerelateerd aan het onzekerheidsprincipe.

De effectieve generatie van verstrengeling is essentieel voor bijna alle kwantum repeater netwerken. In deze thesis onderzoeken wij verschillende protocollen voor de generatie van verstrengeling, die geparallelliseerd kunnen worden, wat de generatie van verstrengeling versnelt.

De distillatie van verstrengeling is een protocol om de fouten in verstrengeling te verminderen, waarbij enkel gebruik wordt gemaakt van lokale operaties en klassieke communicatie. Wij ontwikkelen een nieuwe procedure voor de optimalisatie van verstrengeling distillatie protocollen. We gebruiken deze procedure om de optimaliteit van bepaalde algemene en experimentele relevante distillatie protocollen aan te tonen.

Wij gebruiken een informatie-theoretisch perspectief om verschillende repeater protocollen tegen elkaar af te wegen. Dit maakt het mogelijk om de protocollen op een hardware-onafhankelijke manier te beoordelen. We bevinden dat elk van de overwogen protocollen gebaseerd op stikstof-gatcentra voor bepaalde parameters nuttig kunnen zijn voor de generatie van verstrengeling op lange afstand. In het bijzonder bevinden we dat één bepaald protocol – dat al experimenteel geïmplementeerd is – veelbelovend is, en de capaciteit heeft om effectiever cryptografische sleutels te genereren dan theoretisch mogelijk is met directe communicatie. Echter, dit vereist wel dat het stikstofgatcentrum wordt ingesloten in een optische trilholte, wat de emissie van fotonen effectiever maakt.

Ten slotte onderzoeken wij kwantum onzekerheidsrelaties – één van de fundamentele kenmerken van de kwantum mechanica. Kwantum onzekerheidsrelaties worden toegepast in het aantonen van de veiligheid van vele kwantumcryptografie protocollen. Wij onderzoeken een relevante situatie voor het genereren van cryptografische sleutels,

waar een groot deel van de onzekerheid niet intrinsiek is, maar zijn oorsprong vindt in het ontbreken van informatie. Mocht een mogelijke afluisteraar die informatie achterhalen, dan is het mogelijk om de cryptografische sleutel effectiever – en soms zelfs met complete zekerheid – te raden.

1

INTRODUCTION

1

Quantum information, or more specifically, quantum communication and quantum cryptography rely on the most fundamental features of quantum physics. In the twentieth century those features could in general only be observed in individual proof of principle experiments. Hence, in the early days of quantum information, it was a scientific field mostly inhabited by theorists who, working in an abstract Hilbert space where quantum states can be easily generated, stored, manipulated and transmitted, devised lot of fascinating practical applications based on quantum mechanical phenomena. However, due to the recent experimental progress in control of various quantum systems, multiple of those application protocols or their parts no longer take place exclusively in the Hilbert space, but can also be realised in a lab. Finally, the field of quantum engineering has recently emerged in response to the recent experimental progress in the development of various quantum technologies.

The subfields of quantum communication and quantum cryptography rely on two fundamental corner-stones of the quantum theory: the uncertainty principle and quantum correlations. The first one, originally formalised by Heisenberg [1], Kennard [2] and Robertson [3] in the context of standard deviations, has over the years been subjected to a new, information-theoretic approach. This has led to the development of the entropic formulation of the uncertainty principle [4] which has become a fundamental tool in analysing and proving security of various quantum cryptographic protocols. Quantum correlations on the other hand have first led to a strong turmoil in the quantum physics community after the release of the famous EPR paper [5]. The later developed mathematical framework of Bell's inequalities [6], enabling rigorous and practical quantification of these correlations, has become another fundamental tool within the field of quantum cryptography.

The first cryptographic applications of quantum theory can be linked to Wiesner's proposal for quantum money [7]. This has been followed by the BB84 prepare-and-measure quantum key distribution protocol [8] and the protocol based on quantum correlations for which the security is quantified using Bell's Theorem [9]. Since then, a large number of quantum cryptographic protocols have been proposed. The common feature of most of them, together with certain protocols from the fields of quantum computing and quantum metrology, is the requirement for being able to either generate remote entanglement between distant parties, or be able to reliably transmit between them at least certain specific quantum states.

Recent experimental developments in the ability to prepare, transmit and measure individual photons and weak laser pulses have opened the way for the real-life demonstrations of many of those proposed quantum communication protocols. Nevertheless, the ability to transfer quantum states over arbitrarily long distances is still a technological challenge. In this thesis, guided by the recent experimental milestones in the development of quantum communication technologies, we propose, optimise and assess various practical schemes and protocols for demonstrating different building blocks of the quantum repeater network.

In Chapter 2 we introduce the mathematical tools that we use throughout the thesis. In particular we introduce the quantum channel formalism that we use to model quantum operations and noise processes. We then introduce various relevant ways for quantifying entanglement and the framework of semidefinite programming which will

prove useful in dealing with multiple optimisation problems. In Chapter 3 we provide a basic introduction to different types of quantum repeaters and their building blocks. We also discuss different ways of assessing the performance of such quantum repeater networks. In Chapter 4 we analyse remote entanglement generation between two memory nodes, each equipped with one communication qubit with an optical interface, and possibly multiple additional memory qubits, enabling multiplexing. We assess different remote entanglement generation schemes for this setup aiming at maximising the throughput. We then apply our model to the nitrogen-vacancy (NV) centre platform. In Chapter 5 we develop a framework for assessing optimality of existing, realistic entanglement distillation schemes and for finding new schemes starting from the existing ones. We then apply this framework to multiple generic and experimentally relevant scenarios. In Chapter 6 we assess the performance of a simple proof of principle repeater scheme utilising one memory node. We again perform a specific numerical analysis for the NV-centre setup. This time we use a different metric than throughput, which allows us to make information-theoretic statements about the candidate repeater scheme. In Chapter 7 we extend this analysis to three additional NV-centre based schemes utilising two or three memory nodes. In Chapter 8 we revisit the fundamental feature of the quantum theory - the uncertainty principle. We consider a particular guessing game scenario, which provides a natural extension to the well-known framework from the literature used for developing novel entropic uncertainty relations. Moreover, this scenario directly reflects certain attacks of the eavesdropper in quantum key distribution and therefore our investigation provides new insights into security of specific cryptographic protocols. Finally, in Chapter 9 we summarise the results of this thesis, briefly discuss the prospects of applying our models to other physical platforms, and provide an outlook for the future research.

REFERENCES

[1] W. Heisenberg, *Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik,* Zeitschrift für Physik **43**, 172 (1927).

[2] E. H. Kennard, *Zur Quantenmechanik einfacher Bewegungstypen,* Zeitschrift fur Physik **44**, 326 (1927).

[3] H. P. Robertson, *The uncertainty principle,* Physical Review **34**, 163 (1929).

[4] I. Białynicki-Birula and J. Mycielski, *Uncertainty relations for information entropy in wave mechanics,* Communications in Mathematical Physics **44**, 129 (1975).

[5] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?* Physical Review **47**, 777 (1935).

[6] J. S. Bell, *On the Einstein Podolsky Rosen paradox,* Physics **1**, 195 (1964).

[7] S. Wiesner, *Conjugate coding,* ACM Sigact News **15**, 78 (1983).

[8] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* in *International Conference on Computer System and Signal Processing, IEEE, 1984* (1984) pp. 175–179.

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

2

MATHEMATICAL PRELIMINARIES

In this chapter we introduce certain mathematical concepts and tools that we will frequently use throughout the thesis. Firstly we will introduce the general framework for quantum channels and quantum operations. We will also provide specific examples of channels that we will later use to model the noise or loss in our quantum repeater schemes. Secondly, we will introduce a few ways of quantifying the quality of entanglement which we will use in assessing the performance of quantum repeater schemes and their individual building blocks. Finally we will introduce the convex optimisation method of semidefinite programming that is widely used in quantum information theory and which we extensively use in Chapters 5 and 8.

2.1. QUANTUM CHANNELS AND OPERATIONS

Transformations between different quantum states are at a core of quantum information theory. In general we can consider two types of transformations. Firstly, we want to be able to manipulate quantum states in a controlled manner in order to be able to perform desired quantum operations. Secondly, various noise processes will necessarily also transform a quantum state and these are the transformations that ideally we would like to suppress. In fact all such transformations describing valid physical processes can be treated together within the framework of quantum channels. Quantum channels are described by Completely Positive Trace Preserving (CPTP) linear maps [1] which we define below together with the linear operators on which they act.

Definition 2.1.1. *A linear operator B acting on a Hilbert space $\mathcal{H}$, is a linear map from $\mathcal{H}$ onto itself, $B : \mathcal{H} \to \mathcal{H}$. The set of all linear operators acting on a Hilbert space $\mathcal{H}$ is denoted as $\mathcal{B}(\mathcal{H})$.*

Definition 2.1.2. *A Completely Positive Trace Preserving (CPTP) linear map $\Lambda_{A\to\hat{A}}$ is a linear map transforming linear operators $\mathcal{B}(\mathcal{H}_A)$ acting on a Hilbert space $\mathcal{H}_A$ into linear operators $\mathcal{B}\left(\mathcal{H}_{\hat{A}}\right)$ acting on a Hilbert space $\mathcal{H}_{\hat{A}}$:*

$$\Lambda_{A\to\hat{A}} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}\left(\mathcal{H}_{\hat{A}}\right), \tag{2.1}$$

such that:

- *It is trace-preserving, that is:*

$$\forall \rho \in \mathcal{B}(\mathcal{H}_A) : \ \mathrm{tr}[\Lambda_{A\to\hat{A}}(\rho)] = \mathrm{tr}[\rho] \tag{2.2}$$

- *It is completely positive, that is:*

$$\forall \rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B), \text{ such that } \rho \geq 0 : \ (\Lambda_{A\to\hat{A}} \otimes \mathbb{1}_{B\to\hat{B}})\rho \geq 0. \tag{2.3}$$

A useful way of describing the action of a channel is by using its Kraus operators.

Theorem 2.1.3. *To every CPTP map $\Lambda_{A\to\hat{A}} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}\left(\mathcal{H}_{\hat{A}}\right)$ we can associate the set of Kraus operators $\{E_i\}$, such that the action of the channel can be represented as:*

$$\forall \rho \in \mathcal{B}(\mathcal{H}_A) : \ \Lambda_{A\to\hat{A}}(\rho) = \sum_i E_i \rho E_i^\dagger \tag{2.4}$$

The trace-preserving property of the channel requires the Kraus operators to satisfy the condition $\sum_i E_i^\dagger E_i = \mathbb{I}$.

In this thesis we will be mostly concerned with the action of quantum channels on density matrices, hence we will study the action of CPTP maps on the elements of the set $\mathcal{D}(\mathcal{H}) \subset \mathcal{B}(\mathcal{H})$ such that: $\mathcal{D}(\mathcal{H}) = \{\rho \in \mathcal{B}(\mathcal{H}) : \rho \geq 0 \wedge \mathrm{tr}[\rho] = 1\}$. Moreover, from now on, we will use ρ to denote density matrices, i.e. the elements of the set $\mathcal{D}(\mathcal{H})$.

We will now provide a few examples of well-known qubit channels [1] that we will often use throughout the thesis to describe various noise and loss processes.

2.1.1. DEPOLARISING CHANNEL

A depolarising channel with parameter λ performs the mapping:

$$\Lambda^{\lambda}(\rho) = \lambda\rho + (1-\lambda)\frac{\mathbb{I}}{2}. \tag{2.5}$$

This channel can also be described in terms of its Kraus operators:

$$E_0 = \frac{\sqrt{1+3\lambda}}{2}\mathbb{I},\ E_1 = \frac{\sqrt{1-\lambda}}{2}X,\ E_2 = \frac{\sqrt{1-\lambda}}{2}Y,\ E_3 = \frac{\sqrt{1-\lambda}}{2}Z. \tag{2.6}$$

We see that this channel with probability $1-\lambda$ erases all the information about the state. Hence we can often think of a depolarising channel as a worst case scenario model of a particular noise process. We will often use this channel to model the noise due to imperfect gates performed within the quantum nodes and to model certain decoherence noise processes within NV (Nitrogen-Vacancy) centre memory nodes (the NV platform is discussed in more detail in Chapters 4, 6 and 7).

2.1.2. DEPHASING CHANNEL

The dephasing channel is defined with respect to a given basis. A dephasing in the basis $P \in \{X, Y, Z\}$ with parameter λ performs the mapping:

$$\Lambda^{\lambda}(\rho) = \lambda\rho + (1-\lambda)P\rho P. \tag{2.7}$$

This channel can also be described in terms of its Kraus operators:

$$E_0 = \sqrt{\lambda}\mathbb{I},\ E_1 = \sqrt{1-\lambda}P. \tag{2.8}$$

The dephasing channel will be used as a common noise model for the dominant decoherence noise processes within NV centre memory nodes as well as for loss of information about the optical phase of the photonic qubit.

2.1.3. AMPLITUDE DAMPING CHANNEL

An amplitude damping channel is best described using its Kraus operators. Specifically, the amplitude damping channel with damping parameter γ has Kraus operators:

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{pmatrix},\ E_1 = \begin{pmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{pmatrix}. \tag{2.9}$$

This channel will be used to describe the effect of photon loss when the qubit is encoded in the presence/absence of a photon.

2.1.4. ERASURE CHANNEL

An erasure channel is a channel which probabilistically erases the qubit. Such a channel with an erasure probability γ can be described by a mapping:

$$\Lambda(\rho) = \gamma\rho + (1-\gamma)|\perp\rangle\langle\perp|. \tag{2.10}$$

Here, $|\perp\rangle$ is a flag carrying the information that the qubit ρ has been erased. This flag is orthogonal to all the input states. An erasure channel will be used to describe effect of photon loss when the dual rail encoding of the photonic qubit is used e.g. time-bin encoding.

2.2. QUANTIFYING ENTANGLEMENT

Bipartite quantum states can be divided into two classes of states: entangled states and separable states [2]. Let us first define these two terms:

Definition 2.2.1. *A bipartite quantum state ρ_{AB} is a separable state if there exists a convex decomposition:*

$$\rho = \sum_i p_i \sigma_A^i \otimes \tau_B^i \tag{2.11}$$

for some $\{p_i\}$ such that $\forall i, p_i \geq 0$ and $\sum_i p_i = 1$ and for some ensembles of quantum states $\{\sigma^i\}$ and $\{\tau^i\}$. We will label the set of all such separable states as SEP.

Definition 2.2.2. *A bipartite quantum state ρ_{AB} is an entangled state if it does not admit a decomposition of the form given in Eq.* (2.11)*. In other words ρ_{AB} is entangled if and only if $\rho \notin SEP$.*

In general it is an NP-hard problem to determine whether a given ρ is in SEP or not [3, 4]. To help us characterise entangled states we will now introduce two ways of quantifying entanglement that we will use in this thesis. Firstly, let us introduce the notion of an entanglement monotone and an entanglement measure. We note that throughout the literature there have been many different definitions of these two notions. In particular, some definitions impose on these notions large number of necessary properties such as, e.g. additivity or convexity while others do not, see e.g. [2, 5, 6]. Here we introduce minimalistic definitions that are sufficient for our purposes.

Definition 2.2.3. *An entanglement monotone g is a function that maps a quantum state to a non-negative real number:*

$$g : \mathscr{D}(\mathscr{H}) \to \mathbb{R}_{\geq 0} \tag{2.12}$$

such that:

- *the function g does not increase under local operations and classical communication (LOCC).*

Definition 2.2.4. *An entanglement measure G is a function that maps a quantum state to a non-negative real number:*

$$G : \mathscr{D}(\mathscr{H}) \to \mathbb{R}_{\geq 0} \tag{2.13}$$

such that:

- *the function G is an entanglement monotone,*
- $\forall \rho \in SEP, G(\rho) = 0$

Clearly the second condition implies that if $G(\rho) > 0$, then ρ must be entangled. A widely used entanglement measure which has a clear operational meaning is the distillable entanglement [5, 6].

Definition 2.2.5. *Let $|\Phi_D^+\rangle = \frac{1}{\sqrt{D}} \sum_{i=0}^{D-1} |ii\rangle$ denote an EPR pair of local dimension D and let $\Phi_D^+ = |\Phi_D^+\rangle\langle\Phi_D^+|$. Then the distillable entanglement of a state ρ is defined as:*

$$E_D(\rho) = \sup\left\{ r : \lim_{n\to\infty} \left(\inf_{\Lambda \in LOCC} \left\| \Lambda\left(\rho^{\otimes n}\right) - \Phi_{2^{rn}}^+ \right\|_1 \right) = 0 \right\}. \tag{2.14}$$

Here $\|.\|_1$ denotes the trace norm. As this rigorous definition might not be very intuitive, let us try to paraphrase it in an informal and non-rigorous way.

Let $N(\rho)$ denote the number of available copies of the state ρ. Let $M_\Lambda(N(\rho))$ denote the number of close to perfect EPR pairs of local dimension $D = 2$ that can be distilled from those N copies of the state ρ with the LOCC distillation protocol Λ such that for large N these output states approach perfect EPR pairs [6]. Then the distillable entanglement of the state ρ can be interpreted as:

$$E_D(\rho) = \lim_{N\to\infty} \sup_{\Lambda\in LOCC} \frac{M_\Lambda(N(\rho))}{N(\rho)} \tag{2.15}$$

In other words distillable entanglement of the state ρ is an optimal rate of distilling perfect Bell pairs in the limit of infinitely many copies of the input state ρ and after optimising over all LOCC protocols.

Let us now list some useful properties of distillable entanglement. Let $\rho \in \mathscr{D}(\mathscr{H}_A \otimes \mathscr{H}_B)$ be a bipartite state acting on the Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$, where $\dim(\mathscr{H}_A) = \dim(\mathscr{H}_B) = D$. Then:

- $0 \leq E_D(\rho) \leq \log D$
- $E_D(\rho) = \log D$ if and only if there exists a local unitary U such that $(\mathbb{I}\otimes U)\rho(\mathbb{I}\otimes U^\dagger) = \Phi_D^+$. That is the value of $\log D$ is reached only by maximally entangled states of local dimension D.

Unfortunately distillable entanglement is in general very hard to compute. Therefore here we will often use a different way of assessing the amount of entanglement using fidelity to the closest maximally entangled state referred to also as the singlet fraction. Let us first define fidelity between two quantum states [1].

Definition 2.2.6. *Let $\rho_1 \in \mathscr{D}(\mathscr{H})$ and $\rho_2 \in \mathscr{D}(\mathscr{H})$ denote two quantum states acting on the Hilbert space $\mathscr{H}$, such that* $\dim(\mathscr{H}) = D$. *Then the fidelity of ρ_1 to ρ_2 is defined as:*

$$f(\rho_1,\rho_2) = \left(\mathrm{tr}\left[\sqrt{\sqrt{\rho_2}\rho_1\sqrt{\rho_2}}\right]\right)^2 \tag{2.16}$$

Remark 2.2.7. *We note that if $\rho_2 = |\psi\rangle\langle\psi|$ is a pure state, then fidelity reduces to $f(\rho,|\psi\rangle) = \langle\psi|\rho|\psi\rangle$.*

Now let us define the singlet fraction, which is just the fidelity to the closest maximally entangled state [7].

Definition 2.2.8. *Let U denote a local unitary of dimension D. The singlet fraction of the bipartite quantum state $\rho \in \mathscr{D}(\mathscr{H}_A \otimes \mathscr{H}_B)$ acting on the Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$, where* $\dim(\mathscr{H}_A) = \dim(\mathscr{H}_B) = D$, *is then given by:*

$$F(\rho) = \max_U f(\rho, (\mathbb{I}\otimes U)\Phi_D^+(\mathbb{I}\otimes U^\dagger)) \tag{2.17}$$

We note that in most cases it is very obvious what the closest maximally entangled state is or we want to measure fidelity to a fixed maximally entangled state such as $|\Phi_D^+\rangle$. Hence in this thesis we will often use just the term fidelity to describe both fidelity to a specific maximally entangled state and the singlet fraction, as in most cases they will be the same.

Such a singlet fraction has certain very useful properties which allow us to make various claims about the entanglement of the state:

Lemma 2.2.9. *Let $\rho \in \mathscr{D}(\mathscr{H}_A \otimes \mathscr{H}_B)$ be a bipartite state acting on the Hilbert space $\mathscr{H}_A \otimes \mathscr{H}_B$, where $\dim(\mathscr{H}_A) = \dim(\mathscr{H}_B) = D$. Then:*

- *$F(\rho) = 1$ if and only if there exists a local unitary U such that $(\mathbb{I} \otimes U)\rho(\mathbb{I} \otimes U^\dagger) = \Phi_D^+$. That is the value of one is reached only by maximally entangled states of local dimension D.*
- *$\forall \rho \in SEP, F(\rho) \leq \frac{1}{D}$ [8].*
- *If $F(\rho) > \frac{1}{D}$ then $E_D(\rho) > 0$ [8].*

An important comment to be made here is that while fidelity is easy to compute, it is not an entanglement measure. Not only does it not vanish for separable states but it can also increase under LOCC. In particular there exists a class of entangled two-qubit states with $1/3 \leq F < 2/3$ for which it is possible to increase the singlet fraction using LOCC. This is quite obvious in the regime $F < 0.5$ where one can just replace the state with a product state for which $F = 0.5$ (possibly destroying all the entanglement), but it is interesting to note that even for some entangled states for which $F > 0.5$ it is still possible to increase the singlet fraction via LOCC. For two-qubit states, for high fidelities the singlet fraction becomes close to certain entanglement monotones and therefore can no longer increase via LOCC [9]. Hence, although throughout this thesis we will often aim at maximising fidelity of remote entangled states it must be noted that it is only the high fidelity regime, where fidelity can be treated as a reliable indicator of the amount of entanglement in the state. This is also the regime in which we are interested, as highly entangled states are needed for most practical applications of quantum networks.

In this section we have already been explicitly referring to specific maximally entangled states. Throughout this thesis we will most often be interested in two-qubit maximally entangled states. We will then frequently use the four maximally entangled states defining the so called Bell basis: $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$, where:

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \tag{2.18}$$

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right). \tag{2.19}$$

Moreover we will often use the notation ψ to denote the density matrix corresponding to the pure state $|\psi\rangle$.

2.3. SEMIDEFINITE PROGRAMMING

The last section of this chapter will discuss the tool of semidefinite programming which is a widely used tool from convex optimisation that has many applications in quantum information.

Let us first define the concept of a convex optimisation problem. For that we will need to define the notions of a convex set and convex function.

Definition 2.3.1. *A given set S is a convex set if for every $a, b \in S$ and for every $p \in [0,1]$, it holds that $pa + (1-p)b \in S$.*

Definition 2.3.2. *A given real valued function f defined on a convex set S:*

$$f : S \to \mathbb{R} \tag{2.20}$$

is a convex function if for all $a, b \in S$ and for every $p \in [0,1]$, it holds that $f(pa+(1-p)b) \leq pf(a) + (1-p)f(b)$.

Analogously we can also define a concave function:

Definition 2.3.3. *A given real valued function f defined on a convex set S:*

$$f : S \to \mathbb{R} \tag{2.21}$$

is a concave function if for all $a, b \in S$ and for every $p \in [0,1]$, it holds that $f(pa+(1-p)b) \geq pf(a) + (1-p)f(b)$.

Now we define the general form of a convex optimisation problem:

Definition 2.3.4. *A convex optimisation problem is an optimisation problem that can be written in the form:*

$$\begin{array}{ll} \textit{minimize} & f(x) \\ \textit{subject to} & x \in S \ . \end{array}$$

Optimisation Program 1.

where S is a convex set and f is a convex function on the set S.

Note that every problem that can be written in this form can also be written in the form of a maximisation problem (e.g. by just redefining the objective function $f(x) \to g(x) = -f(x)$):

$$\begin{array}{ll} \text{maximize} & g(x) \\ \text{subject to} & x \in S \ . \end{array}$$

Optimisation Program 2.

where S is a convex set and g is a concave function on the set S.

Hence for convex optimisation we require the objective function to be convex for minimisation problems and concave for maximisation ones. The crucial property of the convex optimisation problems is that any local optimum of such a problem is guaranteed to be a global one. This property makes it possible to solve such problems efficiently.

Semidefinite programs (SDP) form a specific family of convex optimisation problems. In a semidefinite program the set S is defined via linear and semidefinite constraints. Such a set is a convex set and the objective function f is linear. We remark that an appealing feature of semidefinite programs is the duality [10] of the SDP. For every SDP that we will call a *primal program* and where we perform optimisation over the variable X so that we can denote the objective function as $p(X)$, there exists a *dual program* which depends on variables Y_1, Y_2 and whose objective function we will denote as $d(Y_1, Y_2)$. If we choose the convention that the primal problem is the maximisation problem, then its dual is then a minimisation problem. It is an appealing feature of SDP duality - known as *weak duality* - that

$$d(Y_1, Y_2) - p(X) \geq 0. \tag{2.22}$$

Finding values for Y_1, Y_2, that satisfy the constraints of the dual SDP thus always results in upper bounds $d(Y_1, Y_2) \geq p^*$, where p^* denotes the optimal solution of the primal program. Furthermore, if such variables satisfy $d(Y_1, Y_2) = p(X)$, then we know that the optimal solution has been found.

We remark that it is this feature that makes SDPs highly appealing as a numerical method, since a numerical SDP solver will find primal and dual variables which form a certificate for optimality, or - if due to finite precision in numerical calculations optimality is reached only approximately - a certificate for approximate optimality in which the difference between the dual and primal $(d - p)$ is sufficiently small [10]. In addition, however, SDPs can thus also be used to prove optimality analytically, if one can make an educated guess for the primal and dual variables.

Let us now be more specific and specify exactly the forms of the two problems. There are various ways of presenting a general semidefinite program. It is most convenient for our purposes to use the following form, given in [11], for an SDP and its dual:

- Primal:

$$\begin{array}{ll} \text{maximise} & \text{tr}[AX] \\ \text{subject to} & \Phi_1(X) = B_1 \ , \\ & \Phi_2(X) \leq B_2 \ , \\ & X \geq 0 \ . \end{array}$$

Optimisation Program 3.

- Dual:

$$\begin{array}{ll} \text{minimize} & \text{tr}[B_1 Y_1] + \text{tr}[B_2 Y_2] \\ \text{subject to} & \Phi_1^\dagger(Y_1) + \Phi_2^\dagger(Y_2) \geq A \ , \\ & Y_1 = Y_1^\dagger \ , \\ & Y_2 \geq 0 \ . \end{array}$$

Optimisation Program 4.

Here A, B_1, B_2 are Hermitian matrices, Φ_1 and Φ_2 are Hermiticity preserving linear maps and $\Phi^\dagger$ is a Hermiticity preserving linear map uniquely defined in terms of Φ through the following relation: $\text{tr}[\Phi(X)Y] = \text{tr}\left[X\Phi^\dagger(Y)\right]$ for all Hermitian matrices X and Y. Notice that the map $\Phi^\dagger$ reverses the order of the spaces as compared to the original map Φ.

The variables of the primal SDP are the matrix elements of the Hermitian matrix X and any X that satisfies the constraints is termed a *feasible* X. Likewise the variables of the dual SDP are the Hermitian matrices Y_1 and Y_2, and such matrices are termed feasible if they satisfy the constraints of the dual SDP. It is a very straightforward observation that feasible points of the dual SDP can be used to provide bounds on the primal optimum and vice versa. To show this consider feasible variables X, Y_1, Y_2; then we have

$$\begin{aligned} d(Y_1, Y_2) - p(X) &= \text{tr}[B_1 Y_1] + \text{tr}[B_2 Y_2] - \text{tr}[AX] \\ &= \text{tr}[\Phi_1(X) Y_1] + \text{tr}[\Phi_2(X) Y_2] \\ &\quad + \text{tr}[(B_2 - \Phi_2(X)) Y_2] - \text{tr}[AX] \\ &= \text{tr}\left[X(\Phi_1^\dagger(Y_1) + \Phi_2^\dagger(Y_2) - A)\right] + \text{tr}[(B_2 - \Phi_2(X)) Y_2] \geq 0. \end{aligned} \tag{2.23}$$

The first equality just comes from implementing the equality constraints of the primal SDP. The second equality is just an application of the definition of $\Phi^\dagger$, and the final inequality arises from the inequality constraints of the SDP and the fact that $\text{tr}[XY] \geq 0$ if $X \geq 0$ and $Y \geq 0$. This weak duality is the key tool that we will use in Chapters 5 and 8.

REFERENCES

[1] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information* (Cambridge University Press, 2010).

[2] D. Bruß, *Characterizing entanglement,* Journal of Mathematical Physics **43**, 4237 (2002).

[3] L. Gurvits, *Classical deterministic complexity of edmonds' problem and quantum entanglement,* in *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing* (ACM, 2003) pp. 10–19.

[4] S. Gharibian, *Strong np-hardness of the quantum separability problem,* Quantum Info. Comput. **10**, 343 (2010).

[5] M. B. Plenio and S. Virmani, *An introduction to entanglement measures,* Quantum Info. Comput. **7**, 1 (2007).

[6] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Quantum entanglement,* Reviews of Modern Physics **81**, 865 (2009).

[7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed-state entanglement and quantum error correction,* Physical Review A **54**, 3824 (1996).

[8] M. Horodecki and P. Horodecki, *Reduction criterion of separability and limits for a class of distillation protocols,* Physical Review A **59**, 4206 (1999).

[9] F. Verstraete and H. Verschelde, *Fidelity of mixed states of two qubits,* Physical Review A **66**, 022307 (2002).

[10] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, 2004).

[11] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).

3

QUANTUM REPEATER BASED QUANTUM NETWORKS

This chapter introduces the concept of a quantum repeater network and discusses the three conceptually different techniques of distributing long distance entanglement, the so called three generations of quantum repeaters. These three generations offer a trade-off between the efficiency of the network and required experimental resources. For the first generation, which will be the focus of this thesis, we then in detail introduce the three main building blocks of such a network: remote entanglement generation, entanglement distillation and entanglement swapping. Finally we introduce different measures of assessing and quantifying the performance of both the total repeater network as well as its individual building blocks for different quantum information processing tasks. We also discuss in detail the advantages and disadvantages of each of these assessment methods.

3.1. QUANTUM REPEATERS

Quantum communication enables the implementation of tasks with qualitative advantages with respect to classical communication, including secret key distribution [1, 2], various two-party cryptographic tasks [3–7], clock synchronization [8, 9], extending baseline of telescopes [10], anonymous state transfer [11] and secure quantum cloud computation [12, 13]. Unfortunately, the transmission of both classical and quantum information over optical fibres decreases exponentially with the distance. While the problem of losses applies both to classical and quantum communication, classical information can be amplified at intermediate nodes, preventing the signal from dying out and thus increasing the rate of transmitted information. At the same time, the existence of a quantum analogue of a classical amplifier is prohibited by the no-cloning theorem [14]. Fortunately, in principle it is possible to construct a *quantum repeater* to increase the rate of transmission without having to amplify the signal [15, 16]. Hence, the construction of a quantum repeater would represent a fundamental milestone towards long-distance quantum communications.

The basic idea of a quantum repeater protocol has undergone many changes since its original proposal [15]. The authors of this scheme showed that by dividing the entire communication distance into smaller segments, generating entanglement over those short links and performing an entanglement swapping operation at each of the intermediate nodes in a nested way, one can establish long-distance entanglement. It was also shown that by including the procedure of entanglement distillation, one can furthermore overcome the problem of noise. Effectively, the authors proposed a scheme that enables one to generate a high-quality long-distance entangled link with an overhead in resources that scales polynomially with distance. Unfortunately, this model does not go into detail of how the physical imperfections of realistic devices, such as decoherence of the quantum memories with time or possibly the probabilistic nature of entanglement swapping, affect the performance. These observations have led to the development of significantly more detailed and accurate, but at the same time significantly more complex, repeater schemes [17–21]. Many quantum repeater proposals require significant resources and are thus not within experimental reach. However, the recent experimental progress in the development of quantum memories [22–24] has brought the realisation of a quantum repeater closer than ever.

Before we start discussing specific repeater proposals, it is important to note that such quantum repeater networks could be used for different tasks. In fact different stages of a future quantum internet have been proposed [25] where each higher stage introduces new capabilities. It is clear that designing a repeater scheme that only enables long distance quantum key distribution (QKD) is experimentally easier than designing a scheme for distribution of long distance entanglement that can later be stored for some time and possibly operated on in some way. In particular, even entanglement-based QKD does not require an individual moment in time in which Alice and Bob directly hold entangled particles. This can significantly reduce the required quantum storage time with respect to entanglement distribution networks. However, it must be emphasised that whenever we refer here to QKD networks we still require the intermediate quantum repeaters to be *untrusted*. This means that in none of the intermediate nodes is it allowed for the encoded bit value to be decoded into classical information and subse-

quently encoded again in the new quantum signal. Such trusted repeater networks for QKD already exist and require one to trust the intermediate decoding/encoding nodes.

3.2. GENERATIONS OF QUANTUM REPEATERS

Over the years a large number of repeater schemes have been proposed. The main bottle-neck is related to the classical communication within the network. Not only does a large amount of classical communication make the network slow, but more importantly, it places high requirement on the storage capabilities of quantum memories. Such long required storage time might become unachievable for any realistic quantum memories which provides a strong motivation for developing repeater schemes with reduced storage demand. As we will see, there is a trade-off between the required capabilities of the quantum operations that we can perform and the required storage time.

3.2.1. FIRST GENERATION

The first generation of quantum repeaters requires the ability to perform relatively simple quantum operations but if it is applied over large distances, it requires quantum memories with very long coherence times. A primary example of a quantum repeater from within this generation is the original repeater scheme [15]. This scheme consists of the following building blocks:

- Remote entanglement generation of the elementary links,
- Entanglement distillation,
- Entanglement swapping.

The general idea behind the first generation repeaters is also depicted in Fig. 3.1.

We will later go into more detail with regard to each of these building blocks. For the moment let us assume that we have a way of generating entanglement between neighbouring nodes in a network which are sufficiently close to each other such that with dominant probability an entangled link can be generated within a fixed time. Many experimental platforms allow for various multiplexing techniques which can help us achieve this goal, see e.g. [26–31] and Chapter 4.

Entanglement distillation is a technique for overcoming noise. In particular, it enables us to concentrate entanglement from a number of weakly entangled copies into a smaller number of more strongly entangled ones. Such entanglement distillation techniques are normally probabilistic, yet heralded. Most of the studied practical entanglement distillation schemes operate on two copies and aim at distilling a single more strongly entangled copy. We will go into more detail with regard to entanglement distillation later. For now let us also assume that we can perform single- and two-qubit operations and that the noise introduced by those operations is sufficiently small such that it indeed pays off to perform entanglement distillation.

Finally, the generated and distilled high quality entangled links are then connected at the intermediate memory nodes using entanglement swapping, which is effectively a Bell state measurement that enables us to perform the transformation: $|\Phi\rangle_{AB_1}|\Phi\rangle_{B_2C} \rightarrow |\Phi\rangle_{AC}|\Phi\rangle_{B_1B_2}$. Here A and C are the end-nodes with a single intermediate node storing

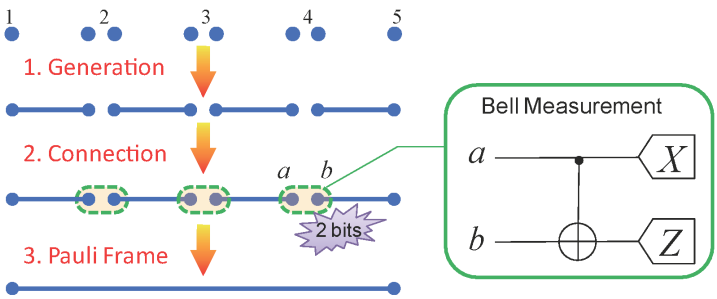

Figure 3.1: The general framework of a first generation quantum repeater scheme. For simplicity distillation is excluded from this figure. In the step "1. Generation", Bell-pairs are generated between physical qubits located at neighbouring repeater nodes. In the step "2. Connection", Bell measurements are performed at the repeater stations. Depending on the specific repeater scheme, the order in which different repeaters perform entanglement swapping can vary, with possible inclusion of entanglement distillation in between the swaps. Entanglement swapping can be either probabilistic or deterministic depending on the specific physical platform. In this thesis we will focus mostly on deterministic swapping implemented inside NV-centre based memory nodes. For those systems the Bell measurement can be performed using a single two-qubit gate followed by two single-qubit measurements as shown in the green-framed window. Such a Bell measurement gives a two-bit outcome carrying information about which effective Bell state projector was implemented. Finally, in the step "3. Pauli Frame", this information about the Bell measurement outcomes from all the repeater stations is forwarded to the end nodes. This determines the Pauli frame for those end-node qubits, or equivalently, it determines the local correction that the end nodes need to implement in order to obtain a desired long-distance Bell state. Figure taken from [18], courtesy of Liang Jiang.

two qubits B_1B_2 on which the Bell state measurement is performed and $|\Phi\rangle$ denotes a maximally entangled state. As was discussed in [15, 26, 32] thanks to the possibility of independent entanglement generation of each of the elementary links, even with probabilistic entanglement distillation, the time of generating the effective states increases only polynomially with the total distance between Alice and Bob. The number of needed qubits per node increases also either polynomially or logarithmically depending on the way entanglement distillation is performed [15]. We note that some memories enable the implementation of deterministic entanglement swapping [33, 34] while the so called read-and-write memories require us to perform this operation optically which is inherently probabilistic, even in the limit of no intrinsic losses [26]. Fortunately, it has been shown that even if the entanglement swapping is probabilistic, one can still maintain polynomial scaling of the generation time [26]. Let us now for a moment assume that we have access to memories allowing for deterministic swapping. We have hence envisioned a highly optimistic scenario: memories enabling deterministic swapping with high quality gates enabling efficient entanglement distillation.

However, although we have already mentioned that we want to include entanglement distillation in order to increase the quality of the generated quantum states, we have not discussed yet what would be the effective quality of the resulting state. This issue is very strongly linked to the coherence time of the quantum memories that we use. Within our repeater protocol there are many processes that require us to be able to store quantum states while other operations are being performed.

First of all, unfortunately being able to connect all entangled links requires us to firstly generate all of them. While we effectively can start performing entanglement swapping between the neighbouring nodes before all the elementary links are there, we will inevitably need to store some of the states while waiting for the generation of certain other links. The corresponding decoherence can significantly decrease the quality of entangled links, even if they were generated absolutely perfect, if we do not have access to quantum memories with sufficiently long coherence times.

Secondly, there are certain storage requirements related to entanglement distillation itself. It has been proposed that one should interleave entanglement swapping with multiple rounds of entanglement distillation to preserve the effective quality of the state [15]. Unfortunately scaling up such a procedure is a significant challenge, since, as we will discuss later, entanglement distillation requires two-way communication and hence effectively the required waiting time would scale with the total distance between Alice and Bob. While for first short network demonstrations this might not be a problem, for larger networks such a scheme could possibly be rendered unscalable by the fact that storage time corresponding to multiple rounds of communication over very long distances might not be achievable.

This naturally brings us to a question whether this entanglement distillation at every nested level is actually necessary. Unfortunately even small imperfections in the operations can significantly decrease quality of entanglement during multiple entanglement swappings. Finally, even perfect entanglement swapping will significantly decrease the quality of the resulting states if the Bell pairs to be swapped are imperfect. Let us con-

sider a scenario, where just before swapping the copies are in an isotropic state:

$$\rho = p|\Phi\rangle\langle\Phi| + (1-p)\frac{\mathbb{I}}{4}. \tag{3.1}$$

Then performing entanglement swapping on such two copies would effectively result in a state:

$$\rho = p^2|\Phi\rangle\langle\Phi| + (1-p^2)\frac{\mathbb{I}}{4}. \tag{3.2}$$

These considerations make it clear that it is indeed necessary to continuously keep compensating for the loss of fidelity during swapping by performing repeated entanglement distillation, which as we mentioned, places high demands on the quantum memories. This procedure would not be necessary only if all the elementary links at the time of entanglement swapping and the local operations are close to perfect.

Of course systems with probabilistic entanglement swapping make this even more challenging. They will either require us to be able to store certain links for longer while we try to restore certain neighbouring links which failed during swapping or it can exponentially decrease the success rate of the total link in case all the swapping operations were performed at the same time. The second option could also only be taken into consideration if the noise coming from other sources than memory decoherence was negligible, as discussed in the previous paragraph. Finally, independently which option we choose, if the goal of the repeater scheme is to generate end to end entanglement rather than only generate shared secret key, then probabilistic swapping will in general also require the end nodes to store quantum information while awaiting failure/success information from all the swapping stations, again requiring quantum storage scaling linearly with the length of the network.

We see that the main challenge of the first generation quantum repeaters relates to the requirement on quantum storage. However, since for many physical systems achieving coherence times of the order of at least seconds has already been demonstrated [22, 35–39], in principle it should be possible to face this challenge. Another advantage of such repeater schemes is that they only require the ability to perform a limited number of simple single- and two-qubit operations hence placing very limited demands on the processing power of the individual nodes. For these reasons we will focus in this thesis on developing reliable building blocks of certain repeater schemes belonging to this category.

Nevertheless, there have been many proposals for repeater architectures that significantly reduce the storage requirement of the memories and allow for much faster remote entanglement generation. However, as we will now see, they require the ability to perform much more involved local operations and therefore it is not expected that the first proof of principle repeaters will be of this kind. These higher generations are introduced in the next sections.

3.2.2. SECOND GENERATION

To overcome the necessity of communication time scaling linearly with the total distance between the end nodes, one needs to replace the corresponding problematic components which impose these limitations. These are entanglement distillation and proba-

bilistic entanglement swapping. As we have already discussed, probabilistic entanglement swapping can be overcome just by using specific platforms that allow for performing deterministic Bell measurements between matter qubits.

The problem of two way communication needed for heralding success of distillation is more tricky. To overcome this problem it was proposed to replace such heralded distillation with either distillation based on one-way quantum error correction [32, 40–42] or with classical error correction combined with entanglement swapping performed on the encoded level [18]. In the first method we effectively perform a deterministic entanglement distillation. In the second method we can also obtain protection against imperfect entanglement swapping. Specifically, we convert the physical elementary links into large encoded Bell pairs where the encoding guarantees protection against operational errors. Then all the entanglement swapping operations can be reliably performed on this encoded level such that no distillation is now necessary, see Figure 3.2. In this way the required storage time scales linearly only with the distance corresponding to the initial elementary links. Moreover, it has been also found that for such a scheme the average time of generating long distance entanglement will grow only poly-logarithmically with distance.

Hence, we see that the second generation of quantum repeaters significantly reduces the requirement on the memory storage time and improves the scaling of the rate of generating these pairs. However in order to be able to realise such a repeater scheme, a much larger number of possibly more complicated operations needs to be performed, hence requiring the ability to perform much better gates than for the first generation repeaters.

3.2.3. THIRD GENERATION

In the second generation repeaters error correction has been used to overcome only the operational errors and noise. It has also been suggested that loss tolerant codes could as well be used to overcome the problem of losses. In this way heralded remote entanglement generation will no longer be required, eliminating the need to maintain coherence during the communication time over the elementary links. These proposals form the basis of third generation repeaters [20, 43]. In those schemes, logical qubits become encoded in large number of photons using such loss tolerant codes. These photons are then transmitted to the next neighbouring node where the encoded state is transferred to the memories. The loss errors are then corrected and the logical qubit is again transferred to photonic qubits and then forwarded to the next node. We depict such a third generation repeater in Fig. 3.3. Now the only requirement on the memories is to be able to reliably store the state during the process of error correction, making it completely independent of the communication time between nodes. Of course, using error correcting codes to overcome both the operational errors and losses requires more advanced operations than in the second generation repeaters. This in turn requires even higher gate fidelities. Finally it must be noted that such one-way loss tolerant codes can only tolerate losses up to 50% [44]. Intuitively this can be explained by noting that for losses of more than 50%, effectively, Eve could receive more signal from Alice than Bob. This means that the repeater stations are now required to be placed much more densely.

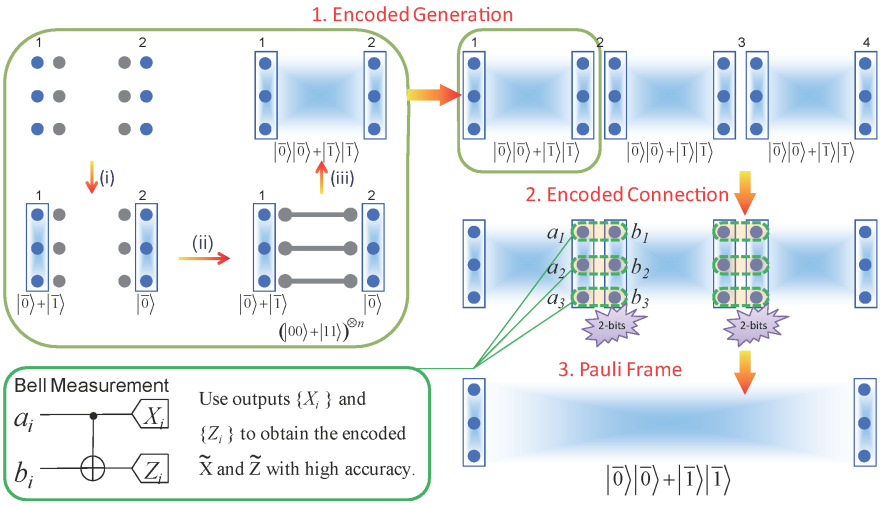

Figure 3.2: Schematic overview of the second generation repeater scheme proposed in [18]. In phase "1. Encoded Generation", encoded Bell states are generated between neighbouring repeater nodes. This can be achieved by i) encoding local qubits in neighbouring nodes, ii) using additional physical qubits in those nodes to generate physical Bell pairs, iii) using the physical Bell pairs to transform the tensor product of the encoded qubits in the two nodes into an encoded Bell pair. In phase "2. Encoded Connection", a logical noise-tolerant entanglement swapping is performed on the encoded Bell pairs at the repeater nodes. Each node generates two bits of classical information carrying information about the outcome of the Bell measurement on the encoded level. In phase "3. Pauli Frame" these classical bits are sent to the end nodes, carrying information about the Pauli frame of the logical end-qubits and effectively allowing for establishment of a target logical long-distance Bell-pair. Figure taken from [18], courtesy of Liang Jiang.

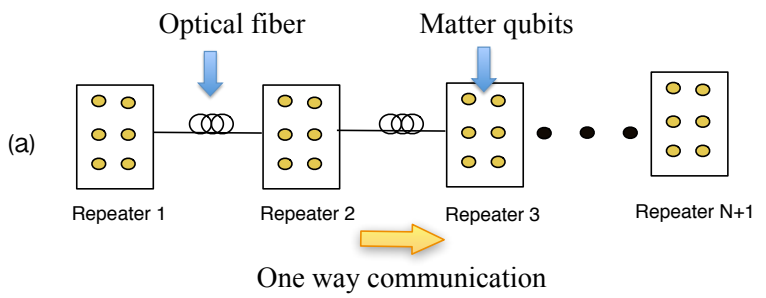

Figure 3.3: Schematic overview of a third generation repeater scheme. Each repeater node contains a large number of memory qubits and the optical fibre enables simultaneous transmission of a large number of single photonic qubits. The quantum state is then encoded in those photonic qubits using some loss-tolerant code. Photons are then sent to the next repeater station where the state is transferred to the memory qubits. Error correction on this logical state is performed in the repeater node followed by again encoding the state in photons and sending them to the next repeater. Such procedure is subsequently performed at all the repeater nodes until the state becomes successfully transmitted from Alice to Bob. Figure taken from [43], courtesy of Liang Jiang.

3.3. BUILDING BLOCKS OF THE FIRST GENERATION REPEATERS

Having provided a background with regard to different repeater frameworks that have been considered, we will now zoom into the first generation repeater architectures. Although the slowest, these repeater architectures have very moderate hardware requirement compared to the second and third generation repeaters, making them promising candidates for the first demonstration of a quantum internet. We also note that the initial networks are expected to cover moderate distances which means that the memory storage time requirement due to the two-way communication needed for entanglement distillation does not need to be a significant constraint. Hence, in this thesis we will focus on specific implementations of such first generation repeaters, or more specifically of the corresponding building blocks that we have already mentioned. Let us now go through all these building blocks in detail.

3.3.1. REMOTE ENTANGLEMENT GENERATION OF THE ELEMENTARY LINKS

The first step in the original repeater protocol [15] (also known as the BDCZ protocol) is the generation of the elementary entangled links between the individual repeater stations. From the theorist's perspective a natural way of doing so would be to locally generate an EPR pair in one of the nodes and then send one-half of it to the neighbouring node. However, deterministic or even heralded state transfer of a qubit state from a photon to a memory is still a very significant challenge and is not expected to be realised with high fidelity on a significant number of physical platforms in the near future. In systems that utilise cavities this task can be performed, provided that one can realise a low-loss overcoupled cavity with high cooperativity. While such a scenario has been demonstrated experimentally in trapped atoms by achieving the strong coupling regime [45], demonstrating high cooperativity is very challenging in general.

Due to this experimental reason, many physical platforms use the help of a middle heralding station to facilitate such a remote entanglement generation procedure. This middle heralding station effectively implements an optical Bell state measurement similar to entanglement swapping. Effectively the two nodes generate memory-photon entanglement and transmit the two photonic qubits to a heralding station. This station then entangles the two memories by performing a Bell state measurement on the two photonic qubits. The remote entanglement generation and quantum repeater schemes that make use of such a heralding station are analysed in Chapters 4 and 7. A comparison of specific repeater schemes that make use of either a heralded state transfer from a photonic qubit to a quantum memory or of the heralding stations are described in Section 6.9.3 in Chapter 6.

Here we will consider two ways of encoding a qubit into a photonic state. These two types of photonic encodings are qualitatively different from each other and we describe them in more detail below.

PHOTON NUMBER ENCODING AND THE SINGLE-PHOTON ENTANGLEMENT GENERATION SCHEME

The first encoding is the *photon-number* or the so-called *single-rail* encoding. In this encoding the two logical states correspond to the presence and absence of the photon respectively. The main limitation of this encoding is that photon loss maintains the qubit in the logical subspace thus resulting in noise. This can already be seen intuitively by

noting that a loss of a photon cannot be distinguished from the logical zero. Let us show it in a more mathematical way. We start by preparing a qubit:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle\,, \tag{3.3}$$

where $|0\rangle$ ($|1\rangle$) denote the absence (presence) of the photon. Now the so-called pure loss channel which we will subsequently use to model the loss processes during photon transmission can be represented by a simple beam-splitter with the signal entering at one port and vacuum entering at the other one. As a result only a fraction of the signal becomes transmitted and the remaining part gets lost to the environment [46, 47]. Hence, a pure-loss channel of transmissivity η can be represented in Heisenberg picture using the following transformation of the optical modes:

$$\hat{a}_{\text{in}} \rightarrow \hat{a}_{\text{out}} = \sqrt{\eta}\hat{a}_{\text{in}} + \sqrt{1-\eta}\hat{a}_{\text{env}} \tag{3.4}$$

One can show that for such a photon number encoding, this channel effectively acts as an amplitude damping channel with the damping parameter given by one minus the transmissivity [46]. Hence, under the action of the pure-loss channel, the state $|\psi\rangle$ will become transformed into:

$$\rho = \left(|\alpha|^2 + \left|\beta\right|^2\eta\right)|\phi\rangle\langle\phi| + \left|\beta\right|^2(1-\eta)|0\rangle\langle 0|\,, \tag{3.5}$$

where

$$|\phi\rangle = \frac{1}{\sqrt{|\alpha|^2 + \left|\beta\right|^2\eta)}}\left(\alpha|0\rangle + \beta\sqrt{\eta}|1\rangle\right)\,. \tag{3.6}$$

Let us now also denote the two states of the memory qubit as $|\uparrow\rangle$ and $|\downarrow\rangle$. We will refer to the first of these states as a bright state since applying a specific optical pulse to it will result in a photon emission and the second one we will call a dark state as it will not emit a photon in that case. Hence, preparing the memory in the state:

$$|\psi\rangle = \sin\theta|\downarrow\rangle + \cos\theta|\uparrow\rangle \tag{3.7}$$

and applying the optical pulse, results in a spin-photon entangled state:

$$|\psi^+\rangle = \sin(\theta)|\downarrow\rangle|0\rangle + \cos(\theta)|\uparrow\rangle|1\rangle\,. \tag{3.8}$$

Let us now consider the scenario where this operation is performed at two distant nodes to which we will refer here as Alice and Bob. Both Alice and Bob perform locally such a memory-photon entanglement generation protocol and transmit the photonic qubits to a heralding station located halfway between them so that the transmissivity of the channel between Alice or Bob and the heralding station is η. Hence, the memory-photon state after the photon has arrived in the heralding station will be:

$$\rho = \left(\sin^2(\theta) + \eta\cos^2(\theta)\right)|\psi_\eta^+\rangle\langle\psi_\eta^+| + (1-\eta)\cos^2(\theta)|\uparrow\rangle\langle\uparrow||0\rangle\langle 0|\,, \tag{3.9}$$

where:

$$|\psi_\eta^+\rangle = \frac{1}{\sqrt{\sin^2(\theta) + \eta\cos^2(\theta)}}(\sin(\theta)|\downarrow\rangle|0\rangle + \sqrt{\eta}\cos(\theta)|\uparrow\rangle|1\rangle)\,. \tag{3.10}$$

The heralding station is effectively just a beamsplitter with two detectors. Here we consider the scenario with non photon-number resolving detectors. Assuming for the moment the scenario without dark counts, we have at most two photons in the system. Therefore we can consider three possible outcomes of our optical measurement: left detector clicked, right detector clicked, none of the detectors clicked. The measurement operators can be easily derived by noting that in our scenario without dark counts, each of the detectors can be triggered either by one or two photons and no cross-clicks between detectors are possible due to the photon-bunching effect. Then we can apply the reverse of the beam splitter mode transformations to the projectors on the events with one or two photons in each of the detectors to obtain these projectors in terms of the input modes. Finally we truncate the resulting projectors to the qubit space since in our scenario it is not possible for more than one photon to be present in each of the input modes of the beam splitter. In this way we obtain the following measurement operators:

$$\begin{aligned} A_0 &= |\Psi^+\rangle\langle\Psi^+| + \frac{1}{\sqrt{2}}|11\rangle\langle 11|\,, \\ A_1 &= |\Psi^-\rangle\langle\Psi^-| + \frac{1}{\sqrt{2}}|11\rangle\langle 11|\,, \\ A_2 &= |00\rangle\langle 00|\,. \end{aligned} \tag{3.11}$$

Here $|\Psi^{\pm}\rangle$ corresponds to the two Bell states that are orthogonal to the product state $|11\rangle$. Specifically the first two outcomes correspond to the click in the left/right detector while the third outcome A_2 corresponds to the no-click event. Applying this measurement to the two photonic qubits of the state $\rho^{\otimes 2}$ and post-selecting on the outcomes A_1 or A_2, projects the two memories into an entangled state. In particular in the limit of high losses $\eta \to 0$ the resulting state of the two memories can be brought to the form:

$$\rho_{AB} = \sin^2\theta|\Psi^+\rangle\langle\Psi^+| + \cos^2\theta|\uparrow\uparrow\rangle\langle\uparrow\uparrow| \tag{3.12}$$

with probability of success $p_{\text{succ}} = 2\eta\cos^2\theta$. We indeed see that although we have assumed perfect operations, the resulting state is not a perfect maximally entangled state since losses affect the quality of the resulting state. Fortunately the experimentally tuneable parameter θ allows for a trade-off between the probability of success and the fidelity of the resulting state. The important feature of this scheme is that the probability of success scales linearly with η while the total transmissivity between Alice and Bob is η^2. As we will later see this makes the single-photon entanglement generation scheme [48] a promising candidate for a proof of principle quantum repeater in itself.

The main experimental challenge with this scheme is that high optical stability of the setup is required. In particular, the photonic qubits acquire optical phase both from the lasers at the emission time and while being transmitted through the optical fibre. If the difference in phase between these two photonic qubits is not known, an unknown local phase will become imprinted on the state in Eq. (3.12), see [49]. If this phase is completely unknown all entanglement becomes lost. Hence, optical phase stabilisation is one of the key requirements of this single-photon scheme.

We discuss in more detail the experimental demonstrations of this scheme and the repeater proposals based on such single-photon interference in Chapter 7.

DUAL-RAIL ENCODING AND TWO-PHOTON ENTANGLEMENT GENERATION SCHEME

The second photon encoding that we will consider here is the so called *dual-rail* encoding, where the logical qubit is encoded in some additional degree of freedom of the photon, e.g. polarisation or time-bin. Using the relation in Eq. (3.4) one can show that on this encoding the pure loss channel acts as an erasure channel with the erasure probability given by one minus the corresponding transmissivity η,

$$D(\rho) = \eta\rho + (1-\eta)|\perp\rangle\langle\perp| \,. \tag{3.13}$$

Here $|\perp\rangle$ is the loss flag, corresponding to the non-detection of a photon. Now it is possible to post-select the successful transmission events by declaring success only when a photon detection event occurred.

Let us now consider the remote entanglement generation for this encoding. Here we will consider specifically the time-bin encoding, but an analogous procedure exists for polarisation. This remote entanglement generation scheme using time-bin encoding of photons has been devised by Barrett and Kok [50] and can effectively be seen as running the single-photon entanglement generation scheme twice with a bit flip applied to the two memories between the two runs. That is, we start with a locally generated spin photon state given in Eq. (3.8). After applying the bit flip to the memory followed by the second optical pulse, we obtain a state:

$$|\psi^+\rangle = \sin(\theta)|\uparrow\rangle|l\rangle + \cos(\theta)|\downarrow\rangle|e\rangle \,, \tag{3.14}$$

where now $|e\rangle = |1\rangle_e|0\rangle_l$ and $|l\rangle = |0\rangle_e|1\rangle_l$ refer to the early and late photon respectively. These photonic qubits from Alice and Bob are then sent to the heralding station, each through a pure loss channel of transmissivity η. Hence just before the heralding station the spin-photon state reads:

$$\rho = \eta|\psi^+\rangle\langle\psi^+| + (1-\eta)\left(\sin^2(\theta)|\uparrow\rangle\langle\uparrow| + \cos^2(\theta)|\downarrow\rangle\langle\downarrow|\right) \otimes |00\rangle\langle 00|_{e,l} \,. \tag{3.15}$$

Then at the heralding station the two photons from Alice and Bob interfere on the beamsplitter followed by photon detection over the two time-windows. One can show that depending on the specific detection event configuration, detecting a photon in each of the two time windows implements one of the two projectors $|\Psi^\pm\rangle\langle\Psi^\pm|$, where

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|el\rangle \pm |le\rangle\right) \,. \tag{3.16}$$

These corresponding outcomes herald success, while all the configurations in which there is no photon detection in at least one of the two time-windows are treated as failure. One can then show that successful events projects the memories into one of the two perfect Bell states $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle)$ where the total probability of success is given by $p_{\text{succ}} = 2\eta^2\sin^2(\theta)\cos^2(\theta)$ which achieves its maximum value for $\theta = \pi/4$ giving $p_{\text{succ}}^{\max} = \eta^2/2$. We now see that while the Barrett-Kok scheme enables for the generation of perfect EPR pairs, it achieves it at a rate that is quadratically worse than for the single-photon scheme.

An additional advantage of the Barrett-Kok scheme is that it does not require phase stabilisation, we only require this phase to be stable over the two consecutive time-windows. This can be easily seen by noting that in equation Eq. (3.14), if we apply a

phase $e^{i\phi}$ to both the early and late photon states, this phase factorises and becomes an irrelevant global phase.

OTHER REMOTE ENTANGLEMENT GENERATION SCHEMES

There also exists a third remote entanglement generation scheme utilising the heralding station, that is able to extract the benefits from both previous schemes: in the ideal case the rate of generating the EPR pairs should scale linearly with η and achieve a fidelity of one. This scheme generates two copies of the state in Eq. (3.12) and distils a perfect EPR pair from them [51, 52]. Moreover, it also does not require high optical phase stability. However, entanglement distillation involves more complex operations and longer quantum storage than needed for the previous two entanglement generation schemes. We discuss the details of the corresponding distillation procedure in Section 3.3.2 and in Chapter 5.

Finally we will also consider an entanglement generation scheme that utilises a source of entangled photons placed in the middle between Alice and Bob. This scheme together with the Barrett-Kok and the scheme based on entanglement distillation are analysed in the context of multiplexing in Chapter 4.

3.3.2. ENTANGLEMENT DISTILLATION

The second crucial component of first generation quantum repeaters is entanglement distillation which is used to compensate for all the operational errors. Entanglement distillation is a procedure by which large dimensional entanglement can be concentrated into smaller dimensional systems, thus effectively increasing "the density of entanglement". While in quantum information theory one often considers optimal distillation procedures that can be performed on asymptotically many copies and using a large number of ancilla systems, here we will focus on practical distillation schemes which operate only on few copies. In most cases we will focus on the scenario where two weakly entangled copies are distilled to a single copy. In this few copy regime, most entanglement distillation protocols are probabilistic yet heralded, which means that the distilling parties know whether the distillation procedure succeeded or not. If it did, they are guaranteed that the entanglement has been successfully condensed into the, in general, smaller dimensional output state. We note here that certain subtleties need to be considered. Specifically, here we will use fidelity to the closest maximally entangled state as a quantifier of the amount of entanglement in the state and we will aim at establishing distillation protocols that maximise this fidelity. However, as discussed in Section 2.2 in Chapter 2 fidelity is not an entanglement measure and loses its meaning as a quantifier of entanglement for its lower values.

Due to a limited lifetime of local quantum memories, practical distillation schemes are not expected to employ multi-round operations in the near future. Instead, practically employed schemes consist of applying a local operation and measurement on Alice's and Bob's side, followed by a single exchange of measurement outcomes using classical communication in order to decide success or failure. Here, we will refer to this subset of Local Operations and Classical Communication (LOCC) as measure and exchange (MX) operations due to their reduced technical demands. The general framework of distillation using MX operations is depicted in Figure 3.4.

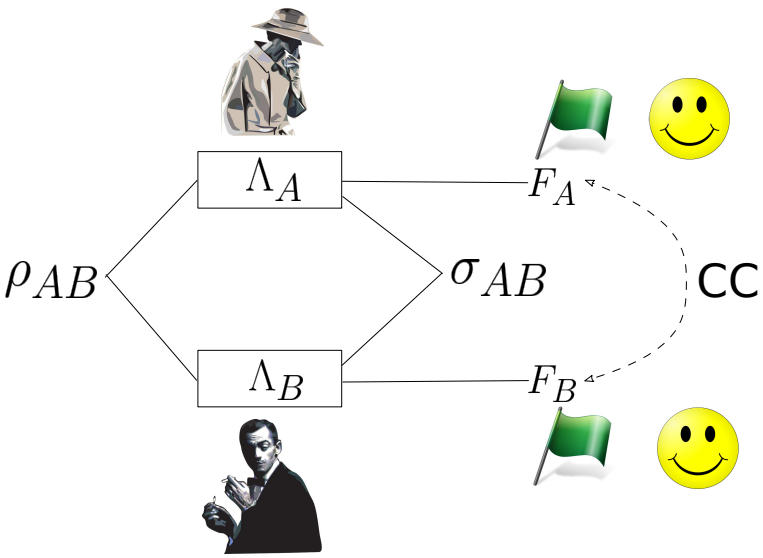

Figure 3.4: The general framework of realistic entanglement distillation using the measure and exchange (MX) operations. Alice and Bob share a state ρ_{AB}. Each of them applies their local operation denoted by Λ. Alice and Bob output then a state σ_{AB}, which, in general, will be smaller dimensional than the input state ρ_{AB}. Additionally, they output classical flags which carry the information regarding success or failure of the protocol. These flags are then exchanged over the classical channel to determine whether the distillation succeeded or not.

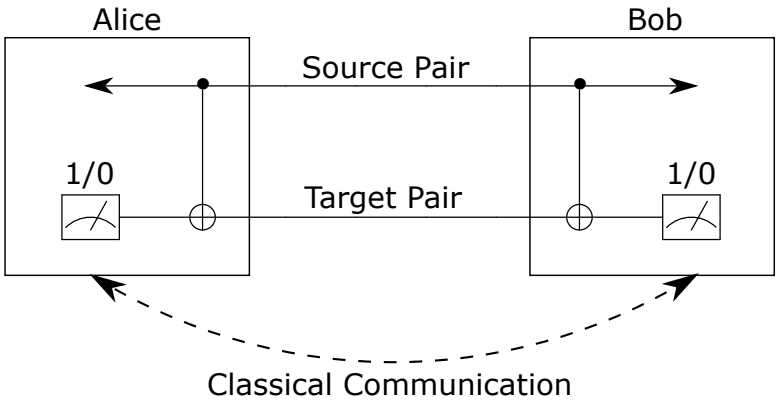

Figure 3.5: Distillation circuit of a specific class of $2 \rightarrow 1$ distillation protocols. In this circuit firstly Alice and Bob apply bilocal CNOT gates followed by a measurement of the target copy in the standard basis. They then exchange the outcomes of that measurement. Depending on the protocol, different outcome configurations determine success or failure. Another difference between the protocols from this class is that before applying this circuit Alice and Bob need to apply specific local rotations to their individual qubits which also depend on the specific protocol.

From the experimental perspective performing operations on three input copies can be already very challenging. Hence, here we will mostly consider distillation protocols that distil from two to one copies. A large family of such protocols involves firstly applying specific single qubit rotations to each qubit followed by the implementation of the circuit depicted in Figure 3.5.

We will consider here three distillation protocols from this class. In general, the more information we have about the states we are distilling, the better we can tailor the distillation protocol to that state. Having little information about the state requires us to apply a very generic distillation protocol whose efficiency is in general low. We will start here with the most generic distillation protocol from this class which requires us only to know the specific maximally entangled state to which the fidelity is the highest. Moreover, we require this fidelity to satisfy $F > 0.5$ in order for this protocol to be able to increase it. In this protocol Alice and Bob firstly twirl the state over the group $\{U \otimes U^*\}$ to bring the state to the isotropic form given in Eq. (3.1) without affecting the fidelity. Here, twirling over the group means applying uniformly at random operations corresponding to the elements of that group. This so-called BBPSSW [53] protocol is described in Algorithm 1.

If we possess more information about the two two-qubit states, in particular if additionally to the dominant Bell state we also know the ordering in terms of magnitude of the other three Bell diagonal coefficients, then we can apply a more efficient protocol. This protocol uses this information by twirling only over the smaller group of correlated Pauli operators: $\{\mathbb{I} \otimes \mathbb{I}, X \otimes X, Y \otimes Y, Z \otimes Z\}$. Applying these operations at random transforms the state into the Bell diagonal state which contains more information than the isotropic state used in BBPSSW. Here, we consider a version of DEJMPS protocol [54] in which the Bell coefficients are first permuted in a way which maximises output fidelity [55]. Again, this protocol is applicable to states whose fidelity with some maximally en-

Algorithm 1 BBPSSW protocol

1: Depolarise the two available copies of the state to the isotropic state form:

$$\tau = p|\Phi^+\rangle\langle\Phi^+| + (1-p)\frac{\mathbb{I}}{4},$$

with fidelity $F = (3p+1)/4$.
2: Apply bi-local CNOT gates between the two copies.
3: Measure the target qubits and communicate the results.
4: **if** The measured flags are 00 or 11 (this occurs with probability $p_{\text{succ}} = F^2 + 2F(1-F)/3 + 5[(1-F)/3]^2$) **then**
5: The source (first) copy becomes more entangled than before (fidelity to $|\Phi^+\rangle$ increases). We obtain a Bell diagonal state with fidelity F' such that

$$F' = \frac{F^2 + [(1-F)/3]^2}{p_{\text{succ}}}.$$

6: **return**

tangled state satisfies $F > 0.5$. The DEJMPS protocol is described in Algorithm 2

Finally let us come back to the remote entanglement generation through distillation. As we have seen, the main source of errors for the single-photon entanglement generation scheme comes from the photon loss. However, this noise in the state in Eq. (3.12) is of a very specific form. Hence, it is reasonable to think that since the form of the state is known, there could exist a specific distillation scheme that targets these states and therefore is more efficient than the BBPSSW and DEJMPS protocols for these states. In fact such a protocol is known and was proposed in [56], see Algorithm 3 for its description. Since this distillation protocol is utilized within the Extreme Photon Loss (EPL) entanglement generation scheme [51, 52] (see below), we refer to it here as EPL-D.

When applied to two copies of the state in Eq. (3.12), arising in the remote entanglement generation scheme that uses a single photon detection scheme, the EPL-D protocol extracts a perfect maximally entangled state with probability of success given by $p_{\text{succ}} = \sin^4\theta/2$. Hence, EPL-D will be a very natural element of such a remote entanglement generation scheme. The scheme for remote entanglement generation using a single photon detection scheme and a distillation operation under the condition of extreme photon loss has been proposed in [51]. Here we will consider an adaptation of this entanglement generation scheme as proposed in [52], which performs distillation on a modified version of the state given in Eq. (3.12) that includes also the noise arising from the lack of knowledge about the internal phase of the generated entangled state due to low optical stability of the setup. The intuition why this protocol works is as follows. Firstly, as established in [56], the success condition of measuring the flags to be 11 can only be satisfied if both of the states were actually in the $|\Psi^+\rangle$ part of the mixture in Eq. (3.12). Now let us have a look at the case if that term in both states has acquired a fixed phase $e^{i\phi}$. Then the action of the CNOT for this successful case with the phase

Algorithm 2 DEJMPS protocol

1: Twirl the two available copies of the state to the Bell diagonal state
2: Perform local rotations on both Alice's and Bob's qubits so that the two copies are in the form

$$\tau = p_1|\Phi^+\rangle\langle\Phi^+| + p_2|\Psi^+\rangle\langle\Psi^+| + p_3|\Phi^-\rangle\langle\Phi^-| + p_4|\Psi^-\rangle\langle\Psi^-|,$$

with $p_1 > 0.5$, $p_1 > p_2 \geq p_3 \geq p_4$ and $p_1 + p_2 + p_3 + p_4 = 1$. This ordering of the Bell coefficients allows to achieve the highest fidelity [55].
3: Perform additional rotations: rotate both qubits on Alice's side by $\pi/2$ around X-axis and by $-\pi/2$ on Bob's side.
4: Apply bi-local CNOT gates between the two copies.
5: Measure the target qubits and communicate the results.
6: **if** The measured flags are 00 or 11 (this occurs with probability $p_{\text{succ}} = (p_1 + p_4)^2 + (p_2 + p_3)^2$) **then**
7: The source (first) copy becomes more entangled than before (fidelity to $|\Phi^+\rangle$ increases). We obtain a state:

$$\eta = p_1'|\Phi^+\rangle\langle\Phi^+| + p_2'|\Psi^+\rangle\langle\Psi^+| + p_3'|\Psi^-\rangle\langle\Psi^-| + p_4'|\Phi^-\rangle\langle\Phi^-|,$$

with $p_1' = (p_1^2 + p_4^2)/p_{\text{succ}}$, $p_2' = (p_2^2 + p_3^2)/p_{\text{succ}}$, $p_3' = 2p_2p_3/p_{\text{succ}}$, $p_4' = 2p_1p_4/p_{\text{succ}}$.
8: **return**

Algorithm 3 EPL-D protocol

1: Apply bi-local CNOT gates between the two copies.
2: Measure the target qubits and communicate the results.
3: **if** The measured flags are 11 **then**
4: Output the source (first) copy.
5: **return**

included is (forgetting the normalisation):

$$\begin{aligned}&(|01\rangle_{A_1B_1} + e^{i\phi}|10\rangle_{A_1B_1})(|01\rangle_{A_2B_2} + e^{i\phi}|10\rangle_{A_2B_2}) \rightarrow \text{bilocal CNOTs} \rightarrow \\ &(|01\rangle_{A_1B_1} + e^{2i\phi}|10\rangle_{A_1B_1})|00\rangle_{A_2B_2} + e^{i\phi}(|01\rangle_{A_1B_1} + |10\rangle_{A_1B_1})|11\rangle_{A_2B_2}\,.\end{aligned} \tag{3.17}$$

Hence, indeed we see that the phase becomes the global irrelevant phase for the successful scenario where the target qubits are measured in 11. Note however, that while it is now not required to know what that phase is, it is still necessary for this phase to be stable over the generation of these two copies so that the acquired phase $e^{i\phi}$ is the same for both copies. The scheme presented in [52], which we will refer to here as the Extreme Photon Loss (EPL) scheme utilizes EPL-D to eliminate both the effect of photon loss and lack of knowledge about the internal phase of the generated states. Let us first define the state:

$$|\Psi^+(\phi)\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + e^{i\phi}|10\rangle\right) \tag{3.18}$$

We then describe the EPL entanglement generation scheme in Algorithm 4.

Algorithm 4 EPL entanglement generation scheme

1: Generate node-photon entanglement at both remote nodes, where the photonic qubit is encoded in the presence-absence of a photon.
2: Send the photonic qubit towards a beam-splitter station in the middle.
3: Conditioned on the detection of a single photon, store the resulting state in quantum memories.
4: Repeat the above procedure to generate the second copy.
5: Assuming stability of the experimental apparatus over the time of generating those two copies, Alice and Bob share then an effective state:

$$\rho_{AB}(p) = \frac{1}{2\pi}\int d\phi \tau_{A1B1}(\phi, p) \otimes \tau_{A2B2}(\phi, p),$$

where

$$\tau_{AB}(\phi, p) = p|\Psi^+(\phi)\rangle\langle\Psi^+(\phi)| + (1-p)|11\rangle\langle 11|.$$

6: Apply EPL-D distillation scheme.
7: **if** EPL-D succeeds (this occurs with probability $p_{\text{succ}} = p^2/2$) **then**
8: We obtain a perfect Bell state:

$$\eta_{\hat{A}\hat{B}} = |\Psi^+(\phi = 0)\rangle\langle\Psi^+(\phi = 0)|.$$

9: **return**

In Chapter 5 we consider a more realistic noise model for the EPL scheme, where we also include a dephasing noise.

Finally we will now also introduce the concept of filtering. It is clear that it is not possible to increase the amount of entanglement using LOCC. However, it is possible to do that probabilistically in a post-selected fashion. This shows that it is in fact possible

to perform distillation on a single copy of a two-qubit state using POVM measurements. A well-known filtering protocol [57] is detailed below.

Algorithm 5 Filtering protocol

1: Perform local measurements given by the POVMs: $\{M_A^0, M_A^1\}$ and $\{M_B^0, M_B^1\}$ with $M_A^1 = (A_A^1)^\dagger A_A^1$, where $A_A^1 = \sqrt{\epsilon}|0\rangle\langle 0| + |1\rangle\langle 1|$ and $M_A^0 = (A_A^0)^\dagger A_A^0 = \mathbb{I} - M_A^1$ and with $M_B^1 = (A_B^1)^\dagger A_B^1$, where $A_B^1 = \sqrt{\epsilon}|1\rangle\langle 1| + |0\rangle\langle 0|$ and $M_B^0 = (A_B^0)^\dagger A_B^0 = \mathbb{I} - M_B^1$ for some parameter $\epsilon \in [0,1]$.
2: Communicate the results.
3: **if** The measurement outcomes corresponding to M_A^1 and M_B^1 are obtained **then**
4: Output the post-measurement state.
5: **return**

This protocol is designed to perform well for the state $\rho_{AB} = p|\Phi^+\rangle\langle\Phi^+| + (1-p)|01\rangle\langle 01|$ [which is the state defined in Eq. (3.12) up to a local bit flip]. For this state, conditioned on success the post-measurement state is: $\eta_{\hat{A}\hat{B}} = \frac{p\epsilon}{p_{\text{succ}}}|\Phi^+\rangle\langle\Phi^+| + \frac{(1-p)\epsilon^2}{p_{\text{succ}}}|01\rangle\langle 01|$ with fidelity $F = \frac{p\epsilon}{p_{\text{succ}}}$ and with the probability of success of the filtering procedure given by $p_{\text{succ}} = p\epsilon + (1-p)\epsilon^2$. At the end of Appendix 5.6.2.2 in Chapter 5 we describe the modification of this filtering scheme that allows us to achieve higher fidelities for the above defined states ρ_{AB} with smaller values of p in the case of larger desired probability of success.

3.3.3. ENTANGLEMENT SWAPPING

The final building block of a first generation quantum repeater scheme is entanglement swapping performed within the quantum memories. In this thesis we will consider the implementation of NV-center based quantum memories which allow for performing deterministic entanglement swapping by effectively performing a CNOT gate between the two memories followed by single-qubit measurements, see Chapters 6 and 7 for more details. However, there are many other platforms such as atomic ensembles, for which entanglement swapping needs to be performed optically in an inherently probabilistic manner. For those systems there in principle exist various strategies that could overcome this problem. We briefly discuss such methods in Section 9.2.1 in Chapter 9.

3.4. ASSESSING THE PERFORMANCE OF QUANTUM REPEATERS

3.4.1. SECRET-KEY RATE AND E-BIT RATE

We have already established two crucial metrics of performance of remote entanglement generation and repeater schemes in general. These are the probability of success or more generally the rate of generating the long distance entanglement and the quality of the resulting state (which we often measure by the fidelity to the closest maximally entangled state). It would now be useful to have some way of combining these two metrics into a single figure of merit.

Fortunately quantum key distribution, which seems experimentally to be the easiest application of quantum networks, provides us with such a figure of merit. This figure of

merit is effectively the rate of generating shared secret key. This rate can be seen as a product of the amount of key that can be extracted from a single copy of a state, called a secret-key fraction, and the yield of generating those states, with some possible prefactors depending on the specific QKD protocol that we implement. The secret-key fraction, which we will denote as r, quantifies the quality of the state. It is a function of the so-called quantum bit error rate (QBER) which effectively tells us what is the probability that if both Alice and Bob use the same basis, they will obtain uncorrelated results. Clearly if Alice and Bob share a perfect EPR pair and measure in the same basis, for each of those bases they will always obtain correlated results and so the QBER is in that case equal to zero for all the bases (we note that depending on the shared maximally entangled state, the perfect correlation might manifest itself as anti-correlated bits; QBER effectively quantifies the deviation from the measurement outcomes that would occur for a perfect maximally entangled state).

We also note that for simplicity we will consider here the secret-key fraction in the asymptotic regime, that is in the limit when Alice and Bob generate infinitely many raw bits from infinitely many copies of the shared quantum states. Clearly that assumes a huge amount of classical post-processing, which however, due to its classical nature, should not be challenging from the technological perspective. Another independent motivation for assessing the repeater with respect to the task of generating secret keys is related to the fact that quantum key distribution is, at the moment, the most mature quantum technology [58]. Finally, we note that estimating QBER can be also useful for assessing other tasks than secret key generation. In particular, with the QBER at hand, one can also estimate an optimal rate of sending qubits over the corresponding noisy quantum channel [59].

One could also consider a similar figure of merit for the rate of generating remote entanglement. In this case a natural counterpart to the asymptotic secret-key fraction would be the distillable entanglement of the generated state. However, there are two problems with this concept. Firstly, distillable entanglement assumes that we are able to perform an effectively infinite amount of quantum processing, acting on infinitely many qubits at once and without introducing any noise. Of course this is practically infeasible to implement. Secondly, distillable entanglement is very difficult to calculate in most cases and we can only calculate certain upper and lower bounds for it. Hence, we will not pursue this direction here.

Moreover, it is worth noting that in practical large quantum networks there might be some links which will need to be used very often and for which the yield would need to be high. Certain other links reaching to specific end users might not need to be used so often and hence for them one could sacrifice some of the yield in order to improve the quality of the generated state. Hence, it many cases it might be useful to keep the yield and the fidelity (or some other way of quantifying the quality of generated entanglement) as two separate independent metrics.

3.4.2. CHANNEL USES PICTURE VERSUS THROUGHPUT PICTURE

We have discussed here the rate of generating secret-key or EPR pairs. However, we have not yet specified in what units we will be evaluating this rate. Here there are two distinct perspectives that we need to discuss. It is clear that on the practical level we would like to

quantify how fast we can generate the remote entangled states or the secret key. Hence it is natural for the yield to be evaluated with respect to time and the corresponding rate of secret-key bits or e-bits per second we will refer to here as throughput. It is natural then to aim at designing a repeater scheme that achieves as high a throughput as possible.

This brings us to a very fundamental question, regarding what actually is a quantum repeater. Let us imagine that we are able to experimentally implement the BDCZ repeater scheme as proposed by the authors. That is we implement remote entanglement generation of the elementary links, entanglement distillation and entanglement swapping. However, because of all the noise in the system and intrinsic losses we find that the achieved throughput is much lower that in a similar experiment where we just use a direct transmission channel. Can we then claim that we have implemented a quantum repeater? Clearly this is highly debatable.

One way of defining a quantum repeater that has been originally proposed is by the argument based on the scaling of resources [15, 32]. Let us apply this argument to the task of remote entanglement generation. As we mentioned earlier we can now consider two quantities, the time (or rate) of generating the remote entanglement and the fidelity of the generated state. Let us now fix the target fidelity. Now, if we find that using the specific proposed scheme, both the time needed to generate these long-distance links of the target fidelity and the number of required quantum systems per each network node scale polynomially or better with distance, then our scheme is indeed an implementation of a quantum repeater.

It is unfortunately very unlikely, that this criterion could be applied to the first proof of principle repeaters. The first experimental realizations of various proposed schemes will certainly be demonstrated over limited distance with very small number of repeater stations, possibly not even more than one or two. In such a scenario based on such a short distance it is indeed very hard to talk about any scaling arguments. This suggests that different methods should be applied for benchmarking such proof of principle quantum repeaters.

One of the ways to solve this problem is to consider the information-theoretic framework. In quantum channel theory one of the vital questions that one considers is how to find optimal quantum encoding and decoding procedures for reliably performing different tasks over a specific quantum channel [60]. The communication performance through such a channel is quantified with respect to the number of times that we make use of this channel. Effectively making use of the channel corresponds to inputing a specific state into the channel. This concept of a channel use has practical motivation as of course every time we input a quantum state into the channel we effectively need to mark this channel as occupied and at that time cannot make use of it for any other task. Of course such mathematical channels can have certain dimensional restrictions, e.g. if a channel is a qubit channel, then in each channel use we cannot input a state that is higher dimensional than a qubit.

One of the fundamental questions of quantum communication theory then is to find the optimal rate with respect to the number of such channel uses of performing different quantum information processing tasks over different quantum channels. This optimal rate is called a capacity of a channel [60]. For the reason mentioned in the previous subsection, we will focus here on the rate of generating secret key and therefore we will

consider the so called private capacity, which is the number of secret bits per channel use that can be generated over the channel in the limit of infinite number of channel uses. The specific channel that is of primary importance to us is a pure-loss channel as it provides a reliable model of the loss processes in the optical fibre. Hence we will then say that if a given repeater scheme allows us to demonstrate a secret-key rate, defined with respect to the number of channel uses, that is larger than the private capacity of such a pure loss channel between the end parties, then we can indeed claim the experiment to be a demonstration of such a proof of principle quantum repeater [61].

We also note that the secret-key rate is more universal in the sense that it can be easily converted into the throughput using the repetition rate of the scheme (number of attempts we can perform in a unit time). The converse, that is converting capacity into the optimal throughput achievable with direct transmission is also possible. However, that requires making an assumption about the use of a particular source with a fixed repetition rate. Therefore comparison of the achieved throughput with such an optimal throughput of the direct transmission channel cannot be formulated without a reference to a specific direct transmission setup, hence losing the universal aspect of the channel uses picture.

Nevertheless, one must be aware of the limitations of the secret-key rate metric. In particular, it does not take into account the waiting time related to transmission latency or, in general, the repetition time of the protocol. This means that a hypothetical platform with perfect memories and operations and high efficiencies but with a constraint that each attempt to generate memory-photon entanglement can be performed only once per day, could easily overcome the secret-key capacity. These differences between secret-key rate and the throughput for specific repeater proposals are discussed in more detail in Chapter 7.

REFERENCES

[1] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* in *International Conference on Computer System and Signal Processing, IEEE, 1984* (1984) pp. 175–179.

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

[3] A. Chailloux and I. Kerenidis, *Optimal bounds for quantum bit commitment,* in *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on* (IEEE, 2011) pp. 354–362.

[4] D. Aharonov, A. Ta-Shma, U. V. Vazirani, and A. C. Yao, *Quantum bit escrow,* in *Proc. STOC* (ACM, 2000) pp. 705–714.

[5] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, *Cryptography in the bounded-quantum-storage model,* SIAM Journal on Computing **37**, 1865 (2008).

[6] S. Wehner, C. Schaffner, and B. M. Terhal, *Cryptography from noisy storage,* Physical Review Letters **100**, 220502 (2008).

[7] J. Ribeiro and F. Grosshans, *A tight lower bound for the bb84-states quantum-position-verification protocol,* arXiv preprint arXiv:1504.07171 (2015).

[8] V. Giovannetti, S. Lloyd, and L. Maccone, *Quantum-enhanced positioning and clock synchronization,* Nature **412**, 417 (2001).

[9] P. Komar, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin, *A quantum network of clocks,* Nature Physics **10**, 582 (2014).

[10] D. Gottesman, T. Jennewein, and S. Croke, *Longer-baseline telescopes using quantum repeaters,* Physical review letters **109**, 070503 (2012).

[11] M. Christandl and S. Wehner, *Quantum anonymous transmissions,* in *International Conference on the Theory and Application of Cryptology and Information Security* (Springer, 2005) pp. 217–235.

[12] A. Broadbent, J. Fitzsimons, and E. Kashefi, *Universal Blind Quantum Computation,* in *Prpc. IEEE Symposium on Foundations of Computer Science* (IEEE, 2009) pp. 517–526, arXiv:0807.4154 .

[13] J. F. Fitzsimons and E. Kashefi, *Unconditionally verifiable blind quantum computation,* Physical Review A **96**, 012303 (2017).

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

[15] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum repeaters: The role of imperfect local operations in quantum communication,* Physical Review Letters **81**, 5932 (1998).

[16] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *Inside quantum repeaters,* Selected Topics in Quantum Electronics, IEEE Journal of **21**, 1 (2015).

[17] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, *Long-distance quantum communication with atomic ensembles and linear optics,* Nature **414**, 413 (2001).

[18] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, *Quantum repeater with encoding,* Physical Review A **79**, 032325 (2009).

[19] W. Munro, K. Harrison, A. Stephens, S. Devitt, and K. Nemoto, *From quantum multiplexing to high-performance quantum networking,* Nature Photonics **4**, 792 (2010).

[20] W. Munro, A. Stephens, S. Devitt, K. Harrison, and K. Nemoto, *Quantum communication without the necessity of quantum memories,* Nature Photonics **6**, 777 (2012).

[21] K. Azuma, K. Tamaki, and H.-K. Lo, *All-photonic quantum repeaters,* Nature Communications **6**, 6787 (2015).

[22] A. Reiserer, N. Kalb, M. S. Blok, K. J. van Bemmelen, T. H. Taminiau, R. Hanson, D. J. Twitchen, and M. Markham, *Robust quantum-network memory using decoherence-protected subspaces of nuclear spins,* Physical Review X **6**, 021040 (2016).

[23] A. I. Lvovsky, B. C. Sanders, and W. Tittel, *Optical quantum memory,* Nature Photonics **3**, 706 (2009).

[24] H. P. Specht, C. Nölleke, A. Reiserer, M. Uphoff, E. Figueroa, S. Ritter, and G. Rempe, *A single-atom quantum memory,* Nature **473**, 190 (2011).

[25] S. Wehner, D. Elkouss, and R. Hanson, *Quantum internet: A vision for the road ahead,* Science **362**, eaam9288 (2018).

[26] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, *Quantum repeaters based on atomic ensembles and linear optics,* Reviews of Modern Physics **83**, 33 (2011).

[27] M. Afzelius, C. Simon, H. De Riedmatten, and N. Gisin, *Multimode quantum memory based on atomic frequency combs,* Physical Review A **79**, 052329 (2009).

[28] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken, M. P. Hedges, D. Oblak, C. Simon, W. Sohler, *et al.*, *Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control,* Physical Review Letters **113**, 053603 (2014).

[29] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, *Rate-loss analysis of an efficient quantum repeater architecture,* Physical Review A **92**, 022357 (2015).

[30] H. Krovi, S. Guha, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, *Practical quantum repeaters with parametric down-conversion sources,* Applied Physics B **122**, 52 (2016).

[31] C. Jones, D. Kim, M. T. Rakher, P. G. Kwiat, and T. D. Ladd, *Design and analysis of communication protocols for quantum repeater networks,* New Journal of Physics **18**, 083015 (2016).

[32] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *Inside quantum repeaters,* IEEE Journal of Selected Topics in Quantum Electronics **21**, 78 (2015).

[33] W. Pfaff, B. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, *et al.*, *Unconditional quantum teleportation between distant solid-state quantum bits,* Science **345**, 532 (2014).

[34] M. Riebe, T. Monz, K. Kim, A. Villar, P. Schindler, M. Chwalla, M. Hennrich, and R. Blatt, *Deterministic entanglement swapping with an ion-trap quantum computer,* Nature Physics **4**, 839 (2008).

[35] M. Rančić, M. P. Hedges, R. L. Ahlefeldt, and M. J. Sellars, *Coherence time of over a second in a telecom-compatible quantum memory storage material,* Nature Physics **14**, 50 (2018).

[36] M. Zhong, M. P. Hedges, R. L. Ahlefeldt, J. G. Bartholomew, S. E. Beavan, S. M. Wittig, J. J. Longdell, and M. J. Sellars, *Optically addressable nuclear spins in a solid with a six-hour coherence time,* Nature **517**, 177 (2015).

[37] Y. Wang, M. Um, J. Zhang, S. An, M. Lyu, J.-N. Zhang, L.-M. Duan, D. Yum, and K. Kim, *Single-qubit quantum memory exceeding ten-minute coherence time,* Nature Photonics **11**, 646 (2017).

[38] N. Kalb, P. Humphreys, J. Slim, and R. Hanson, *Dephasing mechanisms of diamond-based nuclear-spin memories for quantum networks,* Physical Review A **97**, 062330 (2018).

[39] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham, *et al.*, *Room-temperature quantum bit memory exceeding one second,* Science **336**, 1283 (2012).

[40] H. Aschauer, *Quantum communication in noisy environments*, Ph.D. thesis, LMU Munich (2005).

[41] A. M. Stephens, J. Huang, K. Nemoto, and W. J. Munro, *Hybrid-system approach to fault-tolerant quantum communication,* Physical Review A **87**, 052333 (2013).

[42] W. Dür and H. J. Briegel, *Entanglement purification and quantum error correction,* Reports on Progress in Physics **70**, 1381 (2007).

[43] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Ultrafast and fault-tolerant quantum communication across long distances,* Physical Review Letters **112**, 250501 (2014).

[44] M. M. Wolf, D. Pérez-García, and G. Giedke, *Quantum capacities of bosonic channels,* Physical Review Letters **98**, 130501 (2007).

[45] N. Kalb, A. Reiserer, S. Ritter, and G. Rempe, *Heralded storage of a photonic quantum bit in a single atom,* Physical Review Letters **114**, 220501 (2015).

[46] I. L. Chuang, D. W. Leung, and Y. Yamamoto, *Bosonic quantum codes for amplitude damping,* Physical Review A **56**, 1114 (1997).

[47] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian quantum information,* Reviews of Modern Physics **84**, 621 (2012).

[48] C. Cabrillo, J. Cirac, P. Garcia-Fernandez, and P. Zoller, *Creation of entangled states of distant atoms by interference,* Physical Review A **59**, 1025 (1999).

[49] P. C. Humphreys, N. Kalb, J. P. Morits, R. N. Schouten, R. F. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, *Deterministic delivery of remote entanglement on a quantum network,* Nature **558**, 268 (2018).

[50] S. D. Barrett and P. Kok, *Efficient high-fidelity quantum computation using matter qubits and linear optics,* Physical Review A **71**, 060310 (2005).

[51] E. T. Campbell and S. C. Benjamin, *Measurement-based entanglement under conditions of extreme photon loss,* Physical Review Letters **101**, 130502 (2008).

[52] N. H. Nickerson, J. F. Fitzsimons, and S. C. Benjamin, *Freely scalable quantum technologies using cells of 5-to-50 qubits with very lossy and noisy photonic links,* Physical Review X **4**, 041041 (2014).

[53] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Purification of noisy entanglement and faithful teleportation via noisy channels,* Physical Review Letters **76**, 722 (1996).

[54] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Quantum privacy amplification and the security of quantum cryptography over noisy channels,* Physical Review Letters **77**, 2818 (1996).

[55] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, *Local permutations of products of Bell states and entanglement distillation,* Physical Review A **67**, 022310 (2003).

[56] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed-state entanglement and quantum error correction,* Physical Review A **54**, 3824 (1996).

[57] N. Gisin, *Hidden quantum nonlocality revealed by local filters,* Physics Letters A **210**, 151 (1996).

[58] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution,* Reviews of Modern Physics **81**, 1301 (2009).

[59] C. Pfister, M. A. Rol, A. Mantri, M. Tomamichel, and S. Wehner, *Capacity estimation and verification of quantum channels with arbitrarily correlated errors,* Nature Communications **9**, 27 (2018).

[60] M. M. Wilde, *Quantum information theory* (Cambridge University Press, 2013).

[61] M. Takeoka, S. Guha, and M. M. Wilde, *Fundamental rate-loss tradeoff for optical quantum key distribution,* Nature Communications **5**, 5235 (2014).

4

MULTIPLEXED ENTANGLEMENT GENERATION OVER QUANTUM NETWORKS USING MULTI-QUBIT NODES

Suzanne B. van Dam [*], Peter C. Humphreys [*], Filip Rozpędek [*], Stephanie Wehner, Ronald Hanson

Quantum networks distributed over distances greater than a few kilometers will be limited by the time required for information to propagate between nodes. We analyze protocols that are able to circumvent this bottleneck by employing multi-qubit nodes and multiplexing. For each protocol, we investigate the key network parameters that determine its performance. We model achievable entangling rates based on the anticipated near-term performance of nitrogen-vacancy centres and other promising network platforms. This analysis allows us to compare the potential of the proposed multiplexed protocols in different regimes. Moreover, by identifying the gains that may be achieved by improving particular network parameters, our analysis suggests the most promising avenues for research and development of prototype quantum networks.

The results of this chapter have been published in Quantum Sci. Technol. 2, 034002 (2017).
[*]These authors contributed equally.

Recent progress in the generation, manipulation, and storage of distant entangled quantum states has opened up an avenue to the construction of a quantum network over metropolitan-scale distances in the near future [1, 2]. One of the key challenges in realizing such quantum networks will be to overcome the communications bottleneck induced by the long distances separating nodes. This occurs because probabilistic protocols require two-way communication and, for such distances, the entanglement generation rate becomes limited by the time required for quantum and classical signals to propagate.

It is unlikely that quantum networks will attain sufficient levels of complexity in the near future to support the transmission of complex multi-photon entangled states necessary to overcome this bottleneck through error correction [3, 4]. This motivates the development of alternative methods to circumventing this limited communication rate, of which the most promising near-term approach is through multiplexing entanglement generation [5–10].

Previous proposals have developed multiplexed entanglement-generation protocols for networks based on atomic-ensemble quantum memories and linear optics [6, 9, 11] and for networks in which each node consists of many optically accessible qubits that can be temporally, spectrally or spatially multiplexed [5, 7, 8, 10]. However, these proposals are not effective for promising multi-qubit hybrid network node architectures [12], in which one (or a few) optically accessible communication qubits in each node provide a communication bus to interface with multiple local memory qubits. Several platforms have demonstrated the key elements of such a system, including nitrogen-vacancy (NV) centres in diamond [13, 14], trapped ions [2], and quantum dots[14, 15].

Here we focus on the scenario of efficiently generating heralded remote entanglement between two hybrid multi-qubit nodes separated by tens of kilometers in a quantum network (Fig. 4.1). We propose two strategies for multiplexing entanglement generation using multi-qubit architectures, identifying the scaling of the entangling rates with the distance between nodes. We compare these strategies to an alternative protocol based on the distribution of entangled photon-pairs [16], modelling all three protocols analytically and with Monte Carlo simulations. This allows us to identify optimal protocols for different regimes of distance and node performance.

In order to be able to effectively assess the potential of these network protocols, it is vital to incorporate the known and anticipated limitations of potential platforms from the start. In this paper we therefore use network parameters representing the expected near-term performance of NV centre nodes. These centres are promising nodes for such a network, combining a robust and long-lived ^{13}C nuclear-spin quantum register [17, 18] with a photonic interface (Fig. 4.1). Our conclusions are nonetheless broadly applicable to other platforms with comparable system performances, particularly including trapped ions [2].

4.1. QUANTUM NETWORK PROTOCOLS

We begin by briefly introducing the three candidate protocols that we consider for a metropolitan-scale quantum network. For each network, we identify the scaling of the entanglement generation rate with the system transmission efficiency and the distance between nodes.

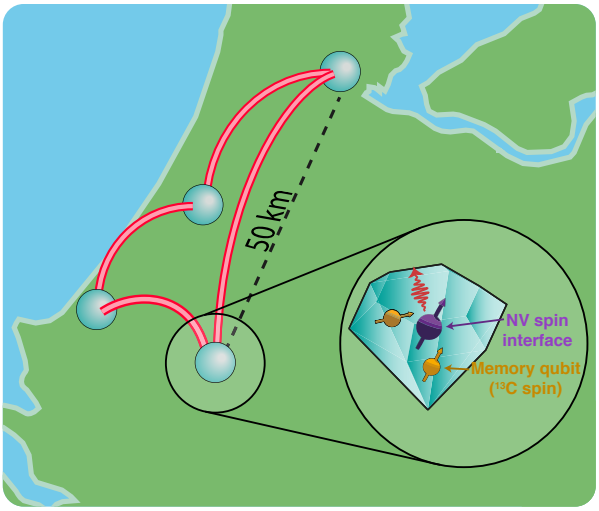

Figure 4.1: Quantum networks have the potential to reach metropolitan scales in the near term, opening up new challenges due to the time required to signal successful entanglement generation between nodes separated by many kilometers. Nitrogen-vacancy centres in diamond are promising candidates for the nodes of such a network, combining an electronic spin communication qubit interface for entanglement generation and local processing with long lived ^{13}C nuclear-spin memory qubits.

4.1.1. MULTIPLEXED BARRETT-KOK PROTOCOL

The first scheme is a multiplexed version of the Barrett-Kok (BK) protocol. In this scheme, entanglement is generated at both nodes locally between the spin state of the communication qubit and the modal occupation of a single photon (typically the photonic state is time-bin encoded for NVs). This procedure constitutes a single attempt to generate remote entanglement. The two photons are then transmitted to a remote beam splitter, where a probabilistic joint Bell state measurement (BSM) on the photons projects the two distant communication qubits into an entangled state upon measurement of the appropriate outcomes [19].

In this protocol each photon needs to be transmitted over a distance $d/2$ from the nodes to the central BSM station. This is followed by the transmission of classical information over the same $d/2$ distance heralding to the nodes the success or failure of the entangling attempt. Hence in the standard BK protocol, the entanglement attempt rate r_{BK} is limited by the combined quantum and classical communication time ($t_c = d/c$) required to establish whether the protocol succeeded: $r_{BK} \sim t_c^{-1}$. Even for modest distances, this time delay is sizable; e.g. for $d = 50$ km the delay is $t_c = 250\,\mu$s, limiting the attempt rate to 4 kHz.

This rate limitation can be mitigated by using a multiplexed version of the BK protocol (Fig. 4.2), in which the spin state of the communication qubit is swapped to a memory qubit directly after spin-photon entanglement generation, freeing up the communication qubit for additional entanglement generation attempts. For the NV system, naturally occuring nearby ^{13}C nuclear spins provide robust memory qubits [18, 20]. The state is stored in this memory qubit until information about the success of the attempt arrives. In the meantime, spin-photon entanglement generation and subsequent state swapping to other memories can continue until all of the memories are occupied. The multiplexed protocol allows N qubits per node to be utilised, where N includes both the communication qubit and the memory qubits.

The maximum number of qubits per node that can be usefully employed in this protocol is given by $N_{\max} = \lceil t_c/t_{sg} \rceil$ * where t_{sg} is the duration of the swap gate (typically much longer than the duration of entanglement generation attempts t_{eg}). The attempt rate of the multiplexed Barrett-Kok (mBK) protocol is therefore a factor N larger than for the standard BK scheme: $r_{\mathrm{mBK}} \sim N/t_c$ for $N \leq N_{\max}$. This rate is upper bounded by $r_{\mathrm{mBK}} \leq 1/t_{sg}$.

The success of each attempt of the BK scheme is conditioned on the detection of both the photons emitted by the communication qubits in the BSM. As a result, the system transmission efficiency η appears quadratically in the entanglement success rate R_{mBK}. Hence for $N \leq N_{\max}$:

$$R_{\mathrm{mBK}} \sim r_{\mathrm{mBK}} \frac{\eta^2}{2} = \frac{1}{2} N \eta^2 / t_c. \tag{4.1}$$

The factor of half corresponds to the probability of a successful BSM at the beam splitter.

4.1.2. MULTIPLEXED EXTREME-PHOTON-LOSS PROTOCOL

In the case of high levels of photon loss ($\eta \ll 1$), a protocol based on entanglement distillation can be more effective than the BK protocol. In this protocol, instead of directly

* $\lceil x \rceil$ denotes ceil(x)

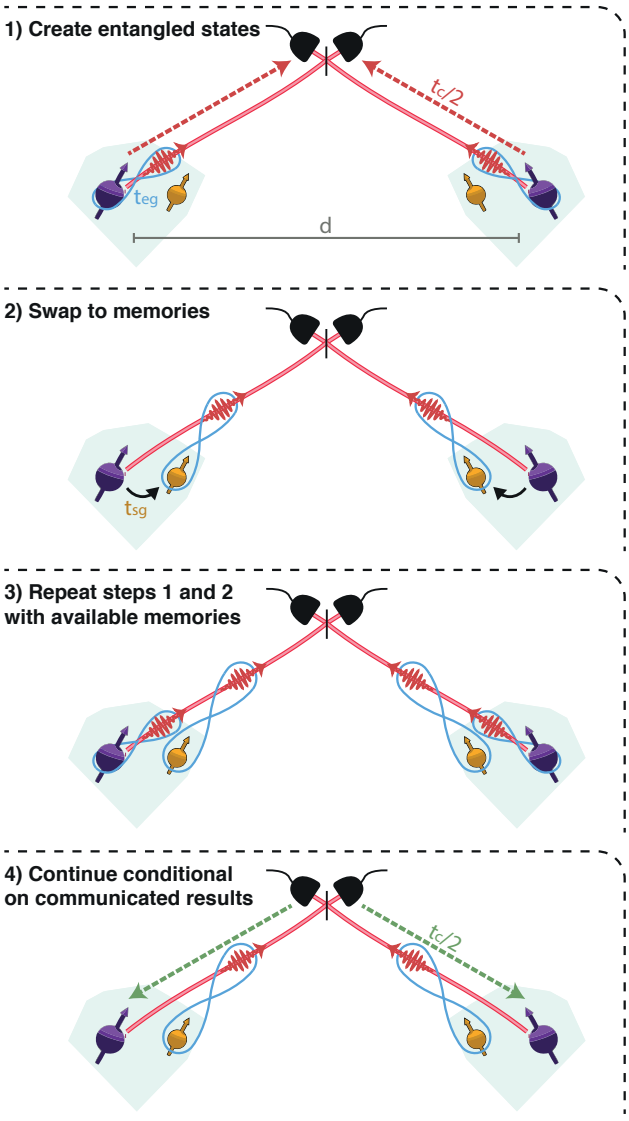

Figure 4.2: Multiplexing concept. The protocol starts with a creation of local entanglement between the communication qubits and single photons at both nodes (step 1). The state of the communication qubits is then immediately transferred to the memory qubits (step 2), which allows for a second entanglement attempt before the result of the first one is known (step 3). Once the signal heralding success or failure of the attempt is received at the nodes, the occupied memories can be reused for new attempts (step 4).

trying to generate a maximally entangled state $|\Psi\rangle = (1/\sqrt{2})(|01\rangle + |10\rangle)$, two weakly entangled states of the form $\rho \approx \frac{1}{2}|\Psi\rangle\langle\Psi| + \frac{1}{2}|00\rangle\langle 00|$ are efficiently generated conditional on the detection of only a single photon at the beam splitter station [12, 21]. Here $|0\rangle$ ($|1\rangle$) denotes the state of the communication qubit from which a photon is (is not) emitted. These weakly entangled states contain a contribution $|00\rangle\langle 00|$ from the case in which both communication qubits emitted a photon, but only one was detected. After the two states are successfully generated, an entanglement distillation procedure is performed using local operations and classical communication. This distillation produces a pure entangled state with a 1/8 probability. Since two raw states are consumed to generate a final entangled state, this extreme-photon-loss (EPL) protocol requires at least two qubits per node, as the first state has to be stored in a memory qubit until the second entangled state is generated.

The advantage of this scheme over the BK protocol is that it does not require the detection of coincident photons, instead allowing for multiple attempts to generate the second state. This results in a success probability that is proportional to η rather than η^2 and thus an entangling rate $R_{\mathrm{EPL}} \sim \eta/(16t_c)$, where a factor 1/8 corresponds to the probability that the distillation operation succeeds, and a factor 1/2 reflects the need to generate two entangled states.

Analogously to the BK protocol, a multiplexed version of the scheme can be envisioned in which multiple entanglement generation attempts are performed within one communication cycle. Since, in the second stage of the protocol one memory is continuously occupied by the first entangled state, the maximum number of qubits that can be effectively utilised is one more than in the BK protocol: $N_{\max} = \lceil t_c/t_{sg} \rceil + 1$. The resulting entanglement success rate R_{mEPL} for the multiplexed extreme-photon-loss protocol for $N \leq N_{\max}$ is proportional to the inverse of the sum of the time spent in the first stage ($t_c/(\eta N)$) and second stage ($t_c/(\eta(N-1))$) of the protocol:

$$R_{\mathrm{mEPL}} \sim \frac{N(N-1)}{2N-1}\frac{\eta}{8t_c}. \tag{4.2}$$

The entangled state fidelity in this protocol is sensitive to decoherence of the memories during entanglement attempts. In order to ensure a minimum fidelity, stored entangled states can be discarded after a set number of subsequent entanglement attempts, at the expense of decreasing the entanglement rate. Entanglement generated from a single photon detection event is expected to succeed within at most a few hundred attempts (~100 attempts at 50 km, ~1000 attempts at 100 km) for the range of parameters considered here. For nitrogen-vacancy centre nodes, recent results indicate that ^{13}C nuclear-spin memories may effectively preserve quantum states over this number of attempts [18], and so this effect is not expected to significantly impact our conclusions.

4.1.3. MIDPOINT-SOURCE PROTOCOL

The final configuration that we consider is the midpoint-source (MPS) protocol following Ref. [16]. In addition to the two nodes, this protocol requires an entangled-photon source (which emits pairs of photons with probability p_{em}) positioned midway between the nodes (Fig. 4.3). In this protocol, pairs of entangled photons generated by the photon source are split and one is sent to each of the two nodes. At each of the nodes, a

BSM is performed between this photon and a photon generated by the local communication qubit. Entanglement swapping succeeds only if both BSMs succeed (requiring the detection of four photons in total).

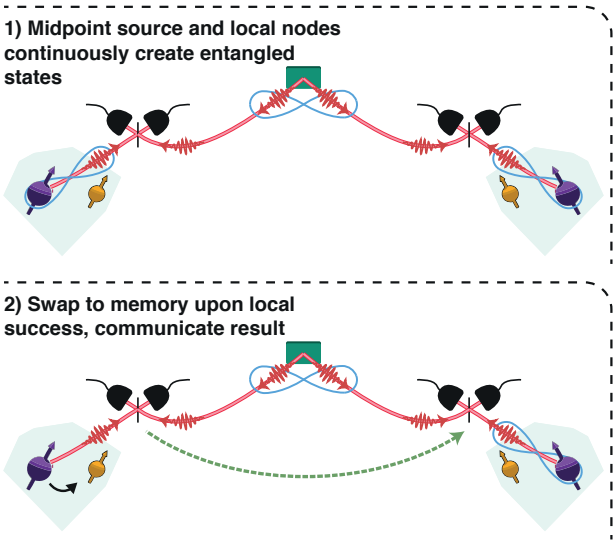

Figure 4.3: Midpoint-source (MPS) protocol. The photon source in the middle continuously generates pairs of entangled photons with probability p_{em} and transmits them to the two nodes (step 1). At the same time both nodes synchronously generate local entanglement between the communication qubit and emitted photons. Local beam splitter stations at each node perform BSM measurements between photons emitted from the source and the the photons emitted from the local node. This gives the local node immediate knowledge of the local success or failure of each attempt. This information is also communicated to the other node, arriving d/c later.

Since the successes of the BSMs can be reported to their local nodes immediately, in the case of local failure the nodes can quickly proceed to a new entanglement generation attempt. In this way the entanglement attempt rate can be significantly increased. The attempt rate is upper bounded by $r_{\text{MPS}} \leq t_{eg}^{-1}$, where t_{eg} is the duration of the spin-photon entanglement generation.

This upper bound is saturated if the number of successful local BSMs per communication time t_c, $n = p_{\text{BSM}}\, t_c/t_{eg} \approx (1/2) p_{em}\eta\, t_c/t_{eg}$, satisfies $n \ll 1$. In this limit the protocol can be effectively run with a single qubit per node, and the rate is therefore insensitive to the swap gate time t_{sg}. When operating the MPS protocol in this low n regime, the entanglement success rate is given by

$$R_{\text{MPS}} \sim p_{\text{em}}\eta^2/(4t_{eg}), \tag{4.3}$$

where the factor of 1/4 arises because both BSMs must succeed in the same round, and η includes the system losses for both the photon from the entangled photon source and the locally generated photon.

This scaling is different to that identified in Ref. 16 since, for the system parameters that we consider, t_{eg} is not small enough to ensure that the expected number of successes n per communication time t_c approaches unity. As shown in Fig 4.5, for a shorter t_{eg}, the network could leave this low-success-probability regime. If the attempt rate is high enough to ensure that at least one attempt succeeds locally per t_c, the overall entanglement success rate will only primarily depend on whether there was a simultaneous success at the other node; the scaling is thus effectively proportional to η, which is the scaling described in Ref. 16. However, achieving this limit clearly requires a shorter t_{eg} as the loss (1-η) increases.

For $n \sim 1$, the inclusion of additional memory qubits becomes beneficial to prevent idle time. In this case, after a local success, the communication qubit state is swapped to a memory qubit. This swapping operation therefore prevents the node from performing further entanglement generation attempts during a time t_{sg}, limiting the overall attempt rate.

4.2. MODELLING

We model each of the protocols described in the previous section with an approximate analytical approach as well as with Monte Carlo simulations. We use system parameters that are expected to be achievable for NVs and trapped ions in the near term (Tab. 4.1). The outcoupling efficiency of the NV centre is assumed to benefit from coupling to an optical cavity (with outcoupling efficiency $p_{\text{out}} = 0.3$), and emitted photons are assumed to be frequency-converted to telecom-wavelength photons with efficiency $p_{\text{fc}} = 0.3$. Fiber losses are therefore limited to standard telecom values of $\alpha = 0.2$ dB/km. Hence the overall system transmission efficiency is given by $\eta = p_{\text{out}}\, p_{\text{fc}}\, 10^{-\alpha d/20}$ where the last term corresponds to the fiber losses over a distance of $d/2$.

It is as yet unclear how much progress will be made in the near term in overcoming the technical challenges necessary to demonstrate an entangled-photon-source with a high brightness and with spectral properties that are well-matched to the node emission. We therefore consider two possible values for p_{em} (0.1 and 0.01), taking 0.01 to be more technically feasible [22, 23].

Table 4.1: Anticipated near-term parameters for a quantum network based on NV centers [13, 17, 24, 25]. These parameters are also anticipated to be achievable using trapped ions [2].

Variable	Description	Value
N	Total number of qubits at each node	2
p_{fc}	Frequency-conversion efficiency	0.3
p_{out}	NV-outcoupling efficiency	0.3
t_{eg}	Spin-photon entanglement generation time	1 μs
t_{sg}	NV-carbon swap gate time	200 μs
p_{em}	Midpoint-source photon-pair emission probability	0.01, 0.1

4.2.1. SCALING WITH DISTANCE

The modelled dependency of the entangling rate on the node separation is shown in Fig. 4.4. As expected from Section 7.2, the scaling with distance is most favorable for the mEPL protocol ($R_{\text{mEPL}} \sim 10^{-\alpha d/20}\, d^{-1}$), whereas the BK protocol scales worst ($R_{\text{mBK}} \sim 10^{-\alpha d/10}\, d^{-1}$). Even for an MPS protocol with an extremely efficient source ($p_{em} = 0.1$), the mEPL protocol outperforms it for distances greater than ~ 100 km since R_{MPS} scales less favourably with distance as $R_{\text{MPS}} \sim 10^{-\alpha d/10}$.

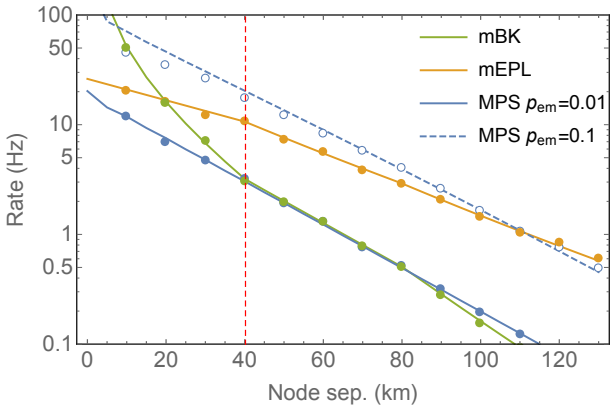

Figure 4.4: Modelled entanglement generation rates as a function of distance for the system parameters listed in Table 4.1. Plotted lines give the results of our analytical model while the circles give equivalent Monte Carlo simulation data. Although two qubits are available to the system, the MPS protocol is always found to be in the low success probability regime ($n < 1$), in which only one qubit is required. For distances to the left of the red vertical dashed line the memory storage time t_{sg} is larger than the communication time t_c. In this regime it is optimal to use only one qubit for the mBK scheme. As the mEPL-scheme requires one memory qubit to store the first generated state in the second part of the protocol, for all distances both qubits are actively employed. The error bars associated with the Monte Carlo simulations are smaller than the plotted circles.

In Fig. 4.5 we justify our claim that the MPS protocol will not benefit from more than a single qubit per node. We plot the expected number of successful BSMs n during the communication time as a function of distance, and observe that for our network parameters this stays well below one even for the case of a very efficient source ($p_{em} = 0.1$).

4.2.2. SCALING WITH NUMBER OF MEMORIES

Notably, for these near-term parameters, scaling up to a large number of qubits per node does not speed up the entanglement rate. As previously noted, the MPS protocol always operates in the low success probability regime in which only the communication qubit is actively used. For the mBK and mEPL protocols, the duration of the swap gate significantly limits the number of qubits per node that can be used over relevant node separations. We investigate the rate dependency of the mEPL protocol on the number of

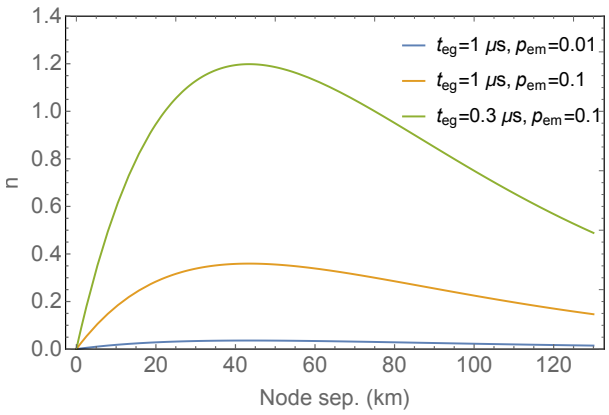

Figure 4.5: Expected number of successful local BSMs n at each node per communication time t_c for the MPS protocol as a function of node separation. We see that for both values of p_{em} and for all distances $n < 1$, and hence a single qubit per node is sufficient.

memory qubits in Fig. 4.6 for a fixed node separation of $d = 50$ km and a varying swap gate duration t_{sg}. For $t_{\text{sg}} \ll t_c$ the rate scales linearly with the number of qubits. However, as explained in Section 7.2, once $N t_{\text{sg}} \approx t_c$ is reached, adding more memory qubits does not boost the entangling rate.

4.3. CONCLUSIONS

Our analysis highlights the potential of multiplexed distillation-based schemes to provide high rates of remote entanglement generation and the most favourable scaling with respect to losses. For such schemes, we have identified the swap gate time t_{sg} between the communication and the memory qubits as the key parameter in constraining the achievable entanglement generation rate, as this limits the number of quantum memories that can be used. This highlights the importance of developing methods to increase this storage rate while ensuring that memories remain robust to decoherence. One promising approach for nitrogen-vacancy centre nodes may be to use pairs of strongly coupled carbons to encode quantum memories in decoherence protected subspaces that combine rapid gates (due to their strong coupling) with long memory lifetimes [18].

We find that the midpoint-source protocol has a different dependence on the system parameters, with its performance only weakly constrained by the memory storage time. However, its increased sensitivity to losses hinders its performance over long distances. In addition, there is considerable uncertainty in the projected performance of entangled-pair sources in the near-term, particularly with regard to the source brightness. Until brightnesses on the order of 0.1 per attempt can be achieved, our analysis suggests that these schemes will not perform as effectively as the multiplexed distillation-based protocols.

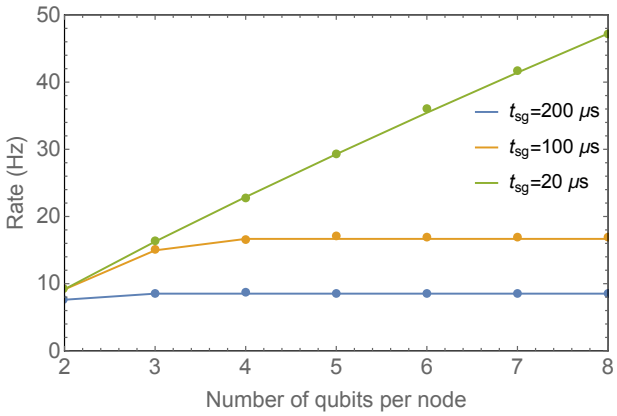

Figure 4.6: Modelled entanglement-generation rate for the mEPL scheme as a function of the number of qubits per node at $d = 50$ km. The three curves correspond to different values of the swap-gate time t_{sg}. An initial linear scaling of the rate with the total number of qubits is observed, as predicted by Equation (4.2). The rate increases only up to $N_{max} = \lceil t_c / t_{sg} \rceil + 1$, beyond which there is no further benefit. This rate saturation occurs over the addition of two qubits. This is because, while generating the second entangled state in the mEPL protocol, one memory qubit is always occupied by the first generated state. The addition of a further memory qubit beyond $N = \lceil t_c / t_{sg} \rceil$ therefore ensures that there are $\lceil t_c / t_{sg} \rceil$ qubits available for entanglement generation during both phases. However, this memory qubit is only used for the second state generation and so does not contribute as much as previous qubits. Error bars associated with the Monte Carlo simulations are smaller than the plotted circles.

REFERENCES

[1] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, *et al.*, *Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres,* Nature **526**, 682 (2015).

[2] D. Hucul, I. Inlek, G. Vittorini, C. Crocker, S. Debnath, S. Clark, and C. Monroe, *Modular entanglement of atomic qubits using photons and phonons,* Nature Physics **11**, 37 (2015).

[3] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *Inside quantum repeaters,* IEEE Journal of Selected Topics in Quantum Electronics **21**, 78 (2015).

[4] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Optimal architectures for long distance quantum communication,* Scientific Reports **6** (2016).

[5] O. A. Collins, S. D. Jenkins, A. Kuzmich, and T. A. B. Kennedy, *Multiplexed Memory-Insensitive Quantum Repeaters,* Physical Review Letters **98**, 060502 (2007).

[6] C. Simon, H. De Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, *Quantum repeaters with photon pair sources and multimode memories,* Physical Review Letters **98**, 190503 (2007), 0701239 .

[7] N. Sangouard, R. Dubessy, and C. Simon, *Quantum repeaters based on single trapped ions,* Physical Review A **79**, 042340 (2009).

[8] W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto, *From quantum multiplexing to high-performance quantum networking,* Nature Photonics **4**, 792 (2010), 0401076 .

[9] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken, M. P. Hedges, D. Oblak, C. Simon, W. Sohler, *et al.*, *Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control,* Physical Review Letters **113**, 053603 (2014).

[10] S. E. Vinay and P. Kok, *Practical repeaters for ultralong-distance quantum communication,* Physical Review A **95**, 052336 (2017).

[11] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, *Quantum repeaters based on atomic ensembles and linear optics,* Reviews of Modern Physics **83**, 33 (2011).

[12] N. H. Nickerson, Y. Li, and S. C. Benjamin, *Topological quantum computing with a very noisy network and local error rates approaching one percent,* Nature Communications **4**, 1756 (2013).

[13] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. S. Blok, L. Robledo, T. H. Taminiau, M. Markham, D. J. Twitchen, L. Childress, and R. Hanson, *Heralded entanglement between solid-state qubits separated by three metres.* Nature **497**, 86 (2013).

[14] W. B. Gao, A. Imamoglu, H. Bernien, and R. Hanson, *Coherent manipulation, measurement and entanglement of individual solid-state spins using optical fields,* Nature Photonics **9**, 363 (2015).

[15] A. Delteil, Z. Sun, W. B. Gao, E. Togan, and S. Faelt, *Generation of heralded entanglement between distant hole spins,* Nature Physics **12**, 218 (2016).

[16] C. Jones, D. Kim, M. T. Rakher, P. G. Kwiat, and T. D. Ladd, *Design and analysis of communication protocols for quantum repeater networks,* New Journal of Physics **18**, 083015 (2016).

[17] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau, *Repeated quantum error correction on a continuously encoded qubit by real-time feedback,* Nature Communications **7**, 11526 (2016).

[18] A. Reiserer, N. Kalb, M. S. Blok, K. J. M. van Bemmelen, T. H. Taminiau, R. Hanson, D. J. Twitchen, and M. Markham, *Robust quantum-network memory using decoherence-protected subspaces of nuclear spins,* Physical Review X **6**, 021040 (2016).

[19] S. D. Barrett and P. Kok, *Efficient high-fidelity quantum computation using matter qubits and linear optics,* Physical Review A **71**, 060310 (2005).

[20] M. Blok, N. Kalb, A. Reiserer, T. Taminiau, and R. Hanson, *Towards quantum networks of single spins: analysis of a quantum memory with an optical interface in diamond,* Faraday Discussions **184**, 173 (2015).

[21] E. T. Campbell and S. C. Benjamin, *Measurement-based entanglement under conditions of extreme photon loss,* Physical Review Letters **101**, 130502 (2008).

[22] C. Clausen, F. Bussieres, A. Tiranov, H. Herrmann, C. Silberhorn, W. Sohler, M. Afzelius, and N. Gisin, *A source of polarization-entangled photon pairs interfacing quantum memories with telecom photons,* New Journal of Physics **16**, 093058 (2014).

[23] J. C. Loredo, N. A. Zakaria, N. Somaschi, C. Anton, L. de Santis, V. Giesz, T. Grange, M. A. Broome, O. Gazzano, G. Coppola, I. Sagnes, A. Lemaitre, A. Auffeves, P. Senellart, M. P. Almeida, and A. G. White, *Scalable performance in solid-state single-photon sources,* Optica **3**, 433 (2016).

[24] S. Bogdanović, S. B. van Dam, C. Bonato, L. C. Coenen, A.-M. J. Zwerver, B. Hensen, M. S. Liddy, T. Fink, A. Reiserer, M. Lončar, *et al., Design and low-temperature characterization of a tunable microcavity for diamond-based quantum networks,* Applied Physics Letters **110**, 171103 (2017).

[25] S. Zaske, A. Lenhard, C. A. Keßler, J. Kettler, C. Hepp, C. Arend, R. Albrecht, W. M. Schulz, M. Jetter, P. Michler, and C. Becher, *Visible-to-telecom quantum frequency conversion of light from a single quantum emitter,* Physical Review Letters **109**, 147404 (2012).

5

OPTIMIZING PRACTICAL ENTANGLEMENT DISTILLATION

Filip Rozpędek *, Thomas Schiet *, Le Phuc Thinh, David Elkouss, Andrew Doherty and Stephanie Wehner

The goal of entanglement distillation is to turn a large number of weakly entangled states into a smaller number of highly entangled ones. Practical entanglement distillation schemes offer a tradeoff between the fidelity to the target state, and the probability of successful distillation. Exploiting such tradeoffs is of interest in the design of quantum repeater protocols. Here, we present a number of methods to assess and optimize entanglement distillation schemes. We start by giving a numerical method to compute upper bounds on the maximum achievable fidelity for a desired probability of success. We show that this method performs well for many known examples by comparing it to well-known distillation protocols. This allows us to show optimality for many well-known distillation protocols for specific states of interest. As an example, we analytically prove optimality of the distillation protocol utilized within the Extreme Photon Loss (EPL) entanglement generation scheme, even in the asymptotic limit. We proceed to present a numerical method that can improve an existing distillation scheme for a given input state, and we present an example for which this method finds an optimal distillation protocol. An implementation of our numerical methods is available as a Julia package.

The results of this chapter have been published in Phys. Rev. A 97, 062333 (2018).
*These authors contributed equally.

5.1. INTRODUCTION

Entanglement distillation forms an important element of many proposals for quantum repeaters [1–5], as well as networked quantum computers [6, 7]. It has seen widespread study across several areas ranging from practical entanglement distillation schemes [7–13] and their experimental implementations [14–18], to a general understanding of some of its possibilities and limitations in quantum information theory [19]. The general goal of bipartite entanglement distillation is to convert a state ρ_{AB} into a state $\eta_{\hat{A}\hat{B}}$ that is close to a maximally entangled state $\Phi_{\hat{A}\hat{B}}$ using only local operations and classical communication (LOCC) between the network node holding A (Alice) and the one holding B (Bob). Here by A and B we denote the input registers and by $\hat{A}$ and $\hat{B}$ the output ones. Closeness is measured in terms of the fidelity

$$F = \langle \Phi_D | \eta_{\hat{A}\hat{B}} | \Phi_D \rangle \geq 1 - \epsilon \,, \tag{5.1}$$

to the target state

$$|\Phi_D\rangle = \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} |j\rangle_{\hat{A}} |j\rangle_{\hat{B}} \,, \tag{5.2}$$

which is maximally entangled across $\hat{A}$ and $\hat{B}$.

There is a slight difference between the meaning of *entanglement distillation* in the quantum information theory literature and in practical schemes. In quantum information theory, one typically considers the case where $\rho_{AB} \approx (\tau_{ab})^{\otimes n}$ consist of n copies of a state τ_{ab}. If we want to distil states that are arbitrarily close to the perfect maximally entangled state, then the distillable entanglement $E_D(\tau_{ab})$ of τ_{ab} answers the question of how large this output state can be. Specifically, it tells us what would be the dimension $|\hat{A}\hat{B}|$ relative to the input dimension $|AB|$, under distillation using LOCC as $n \to \infty$ [20]. As such, the dimension of the output state $|\hat{A}\hat{B}|$ is generally smaller than the dimension $|AB|$ of the input state, unless the input is already maximally entangled. While E_D is difficult to compute in general, several computable bounds have been proposed [21–24]. Recent years have seen one-shot variants of distillable entanglement in which n can be finite, or indeed ρ_{AB} may have an arbitrary structureless form [25–27]. Bounds on the one-shot distillable entanglement may be computed numerically [28]. Crucially, the task of entanglement distillation as it is considered in quantum information theory always produces an output state $\eta_{\hat{A}\hat{B}}$, and considers no failure. The possibility of failure is allowed implicitly by assuming that if the entanglement distillation procedure fails, then Alice and Bob output an arbitrary state leading to a reduced fidelity of the output state to the target state.

In contrast, practical schemes for entanglement distillation explicitly allow for the possibility of failure [7–13]. The fidelity F to the target state is in that case of interest only in the event of success. Not surprisingly, there exist interesting tradeoffs between this fidelity F, and the probability of success p_{succ} of the distillation procedure. A simple example of such a tradeoff is the possibility of *filtering* in which the dimensions $|\hat{A}|$ and $|\hat{B}|$ of the output systems $\hat{A}$ and $\hat{B}$ are equal to the input dimensions $|A|$ and $|B|$, that is, $|\hat{A}| = |A|$ and $|\hat{B}| = |B|$. Yet, it is possible to probabilistically increase the fidelity to the target state by LOCC, where a higher fidelity F leads to a lower success probability p_{succ}.

More generally, trading off the fidelity F against p_{succ} is relevant to the construction of quantum networks: here, the initial generation of entanglement is typically already probabilistic such as when using a heralded scheme to produce the initial (imperfect) entanglement [29, 30]. Most significantly, however, the local quantum memory used to store entanglement is itself imperfect. This means that both the initial as well as the resulting entanglement cannot be preserved for an arbitrary amount of time. Clearly, the success probability p_{succ} dictates the rate at which we can hope to produce high-fidelity entanglement between different nodes in the network. This rate imposes requirements on the coherence times of the memory if multiple entangled pairs are generated such that they should undergo further processing, for example, to generate more complex entangled states in a multi-node network. In such a scenario, one may thus wish to obtain a higher probability of success at the expense of a lower fidelity (or vice versa) in relation to the local storage capabilities of the nodes.

We have already discussed in Section 3.3.2 in Chapter 3 that due to hardware limitations, practical distillation protocols can be restricted to a class involving only one round of local operations followed by one round of classical communication. We have referred to these operations as the *measure and exchange (MX) operations* (see Section 5.3.1 for a precise definition). Here we will be specifically interested in this class of protocols.

5.2. OVERVIEW

In this paper, we develop *a set of tools* for optimising and assessing existing practical distillation schemes. Specifically, our tools allow for a detailed investigation of the tradeoff between the possible output fidelity and probability of success of distillation schemes.

- In Section 5.3.1, we first formally define the set of measure and exchange (MX) operations, and illustrate it with an example of an existing filtering protocol.
- In Section 5.3.3, we state a semidefinite programming (SDP) method to compute upper bounds on the achievable fidelity (or success probability) of a distillation scheme for a given success probability (or fidelity). These methods adapt the ideas of Rains [21] as well as the later methods of Bose symmetric extensions [31, 32] to the case of MX operations, where immediate measurements are performed to decide success or failure. We implement these methods in a numerical package that is freely available on GitHub [33].
- In Section 5.3.4, we present a numerical seesaw method based on semidefinite programming that takes a specific distillation scheme and entangled state as input, and iteratively searches for a better distillation scheme adapted to the state of interest. This method is also included in our numerical package.
- In Section 5.4, we illustrate our method with a variety of examples, considering different entangled states of interest. We compare upper bounds attained with existing distillation schemes (and interpolations between existing distillation schemes) to determine their performance. We observe optimality for a number of schemes for specific states of interest, including modifications of such schemes and certain new schemes obtained from existing ones using our tools. Specifically, we present

an instance in which the seesaw method will find an optimal distillation scheme from an existing one that is suboptimal for the given state.

- In the appendix (summary in Section 5.4) we employ our semidefinite programming methods to analytically prove optimality of the DEJMPS protocol [9] for distilling Bell diagonal states of rank up to three. Furthermore we show optimality of the distillation procedure used within the Extreme Photon Loss (EPL) remote entanglement generation scheme as described in [7, 13], even in the limit of asymptotically many copies.

5.3. OPTIMISATION METHODS

Let us now first define MX operations, and specify the problem of interest in terms of such operations. Throughout, we will use the convention $\sigma_X = \mathrm{tr}_Y(\sigma_{XY})$ to denote the marginal σ_X of a larger state σ_{XY}. Moreover, for the purpose of the compactness of notation, we will often omit writing explicitly the identity matrix or the identity channel. That is, for $(\mathbb{I}_A \otimes M_B)\rho_{AB}$ we will often use the shorthand $M_B\rho_{AB}$ and for $(\mathbb{1}_A \otimes \Lambda_{B\to\hat{B}})(\rho_{AB})$ we will use $\Lambda_{B\to\hat{B}}(\rho_{AB})$.

5.3.1. MEASURE AND EXCHANGE (MX) OPERATIONS

All MX operations can be modelled as completely positive trace-preserving (CPTP) maps, e.g for Alice

$$\Lambda_{A\to\hat{A}F_A} : \mathscr{D}(\mathscr{H}_A) \to \mathscr{D}\left(\mathscr{H}_{\hat{A}F_A}\right), \tag{5.3}$$

where $\mathscr{H}_A$ and $\mathscr{H}_{\hat{A}F_A} := \mathscr{H}_{\hat{A}} \otimes \mathscr{H}_{F_A}$ denote the input and output spaces respectively and $\mathscr{D}$ denotes the set of density operators living on the space. The registers F_A and F_B denote classical flag registers, which Alice and Bob will compare in order to decide success or failure. Applying these maps locally yields the state

$$\sigma_{\hat{A}F_A\hat{B}F_B} = \Lambda_{A\to\hat{A}F_A} \otimes \Lambda_{B\to\hat{B}F_B}\left(\rho_{AB}\right). \tag{5.4}$$

Since Alice and Bob use classical communication to compare the flags, we may without loss of generality assume that the state after a measurement on F_A and F_B is of the form

$$\sigma_{\hat{A}\hat{B}F_AF_B} = \sum_{f_A,f_B} \sigma_{\hat{A}\hat{B}}^{f_A,f_B} \otimes |f_A\rangle\langle f_A|_{F_A} \otimes |f_B\rangle\langle f_B|_{F_B}, \tag{5.5}$$

where the sum is taken over strings f_A and f_B, and $0 \le \mathrm{tr}(\sigma_{\hat{A}\hat{B}}^{f_A,f_B}) \le 1$. Comparing the flags to decide success or failure can be understood as subsequently projecting the state using a projector

$$P_{\checkmark} = \sum_{(f_A,f_B)\in\mathscr{S}} |f_A\rangle\langle f_A|_{F_A} \otimes |f_B\rangle\langle f_B|_{F_B}, \tag{5.6}$$

where $\mathscr{S} = \{(f_A, f_B) \mid \text{Alice and Bob declare success}\}$. The success probability can thus be expressed as

$$p_{\text{succ}} = \mathrm{tr}\left(P_{\checkmark}\sigma_{F_AF_B}\right). \tag{5.7}$$

The global state conditioned on success can in turn be written as

$$\eta_{\hat{A}\hat{B}F_AF_B} = \frac{(\mathbb{I}_{\hat{A}\hat{B}} \otimes P_{\checkmark})\sigma_{\hat{A}\hat{B}F_AF_B}(\mathbb{I}_{\hat{A}\hat{B}} \otimes P_{\checkmark})}{p_{\text{succ}}}, \tag{5.8}$$

which has a fidelity to the ideal maximally entangled state

$$F = \langle \Phi_D | \eta_{\hat{A}\hat{B}} | \Phi_D \rangle . \tag{5.9}$$

Our formalism captures all practical schemes by appropriate definition of $P_{\checkmark}$.

As an example let us consider the filtering protocol [34]. This protocol is adapted to perform well for an input state with $|A| = |B| = 2$ of the form

$$\rho_{AB} = p|\Phi_2\rangle\langle\Phi_2| + (1-p)|01\rangle\langle 01| . \tag{5.10}$$

In this procedure, Alice performs a measurement given by the POVM: $\{M_A^0, M_A^1\}$ with $M_A^1 = (A_A^1)^\dagger A_A^1$, where $A_A^1 = \sqrt{\epsilon}|0\rangle\langle 0| + |1\rangle\langle 1|$ and $M_A^0 = (A_A^0)^\dagger A_A^0 = \mathbb{I} - M_A^1$ for some parameter ϵ determining the tradeoff between F and p_{succ}. In terms of the map this measurement can be expressed as

$$\Lambda_{A\to\hat{A},F_A}(\rho) = \sum_{f_A\in\{0,1\}} A_A^{f_A} \rho \left(A_A^{f_A}\right)^\dagger \otimes |f_A\rangle\langle f_A|_{F_A} . \tag{5.11}$$

Similarly, Bob performs a measurement given by the POVM: $\{M_B^0, M_B^1\}$ with $M_B^1 = (A_B^1)^\dagger A_B^1$, where $A_B^1 = \sqrt{\epsilon}|1\rangle\langle 1| + |0\rangle\langle 0|$ and $M_B^0 = (A_B^0)^\dagger A_B^0 = \mathbb{I} - M_B^1$, giving the map

$$\Lambda_{B\to\hat{B},F_B}(\rho) = \sum_{f_B\in\{0,1\}} A_B^{f_B} \rho \left(A_B^{f_B}\right)^\dagger \otimes |f_B\rangle\langle f_B|_{F_B} . \tag{5.12}$$

Alice and Bob declare success if $f_A = f_B = 1$, corresponding to a choice of $P_{\checkmark} = |11\rangle\langle 11|_{F_AF_B}$.

When optimising over measure and exchange operations, it is sometimes convenient to consider a slightly more general class of operations which we call *measure and exchange operations with shared randomness (MXS operations)*. As the name suggests, Alice and Bob have additional access to classical shared randomness, which is easy to distribute ahead of time. Specifically, if Alice and Bob have a classical symbol r chosen with probability p_r, then they can perform MX operations that depend on r. This means the output state is of the form

$$\sigma_{\hat{A}\hat{B}F_AF_B} = \sum_r p_r \Lambda_{r,A\to\hat{A}F_A} \otimes \Lambda_{r,B\to\hat{B}F_B}\left(\rho_{AB}\right) . \tag{5.13}$$

Note the set of MXS operations is a convex set unlike the set of MX operations.

5.3.2. OPTIMISING OVER MX OPERATIONS

GENERAL FORM

We are now going to consider various optimisations related to the distillation problem. As we have seen, we would like to optimize one of the three parameters D, p_{succ}, ϵ, where D is the local output dimension, p_{succ} is the success probability and the fidelity is $1-\epsilon$. We will typically fix the output dimension D and for now we will consider optimising the fidelity for fixed success probability $p_{\text{succ}} = \delta$. It is straightforward to adapt the techniques below to optimize p_{succ} instead. Ideally, we thus wish to solve the following (quadratic) optimisation problem over maps $\Lambda_{A\to\hat{A}F_A}$ and $\Lambda_{B\to\hat{B}F_B}$

$$\begin{aligned} &\text{maximise} && \tfrac{1}{\delta}\,\mathrm{tr}\left(|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}} \otimes P_{\checkmark}\,\sigma_{\hat{A}\hat{B}F_AF_B}\right) \\ &\text{subject to} && \mathrm{tr}\left(P_{\checkmark}\sigma_{F_AF_B}\right) = \delta \\ & && \sigma_{\hat{A}\hat{B}F_AF_B} = \Lambda_{A\to\hat{A}F_A} \otimes \Lambda_{B\to\hat{B}F_B}\left(\rho_{AB}\right). \end{aligned}$$

Optimisation Program 5.

SIMPLIFYING THE OPTIMISATION PROBLEM

How do we optimize over quantum operations? The key is to employ the Choi isomorphism which gives a one-to-one correspondence between quantum channels and quantum states with certain properties. Specifically, for any quantum channel $\Gamma_{S\to R}$ from a system S to system R, there corresponds a unique Choi state

$$C_{RS'} = \Gamma_{S\to R} \otimes \mathbb{1}_{S'}\left(\Phi_{SS'}\right), \tag{5.14}$$

satisfying

$$C_{RS'} \geq 0\,, C_{S'} = \frac{\mathbb{I}_{S'}}{|S|}, \tag{5.15}$$

where $\Phi_{SS'}$ is the density matrix of the normalised maximally entangled state from Eq. (5.2) of dimension $D = |S|$. The Choi state carries all information of the original channel, in the sense that

$$\mathrm{tr}\left[M_R\Gamma_{S\to R}(\rho_S)\right] = |S|\,\mathrm{tr}[M_R \otimes \rho_{S'}^T(C_{RS'})] \tag{5.16}$$

for all matrices M_R on R.

For the case of MX operations the Choi states take a product form. This is because a maximally entangled state of a larger system whose dimension D is a composite number is formed by taking the tensor product of maximally entangled states:

$$\begin{aligned} C_{\hat{A}F_A\hat{B}F_B,A'B'} &= \Lambda_{A\to\hat{A}F_A} \otimes \Lambda_{B\to\hat{B}F_B}\left(\Phi_{AA'} \otimes \Phi_{BB'}\right) \\ &= C_{\hat{A}F_AA'} \otimes C_{\hat{B}F_BB'}\,. \end{aligned} \tag{5.17}$$

This translates the optimisation to the space of product of two Choi states. Similarly, for MXS operations we obtain the optimisation over the subset of separable Choi states that can be decomposed as follows (we denote this set here as SEP-C):

$$C_{\hat{A}F_A\hat{B}F_B,A'B'} = \sum_r p_r C_{r,\hat{A}F_AA'} \otimes C_{r,\hat{B}F_BB'}\,. \tag{5.18}$$

Note that SEP-C is a strict subset of the set SEP of separable states, since we require that the individual components satisfy the Choi condition Eq. (5.15).

Before delving into the various approaches to optimize our function below, let us first simplify the problem slightly. Our goal will be to remove the registers F_A and F_B from the expressions above. In particular, let us imagine that $C^*_{\hat{A}F_A,A'}$ and $C^*_{\hat{B}F_B,B'}$ are optimal solutions to the optimisation problem above. We then claim that

$$\tilde{C}_{\hat{A}F_A,A'} = \sum_{f_A\in\{0,1\}} |f_A\rangle\langle f_A|_{F_A} C^*_{\hat{A}F_AA'} |f_A\rangle\langle f_A|_{F_A}\,, \tag{5.19}$$

$$\tilde{C}_{\hat{B}F_B,B'} = \sum_{f_B\in\{0,1\}} |f_B\rangle\langle f_B|_{F_B} C^*_{\hat{B}F_BB'} |f_B\rangle\langle f_B|_{F_B}\,, \tag{5.20}$$

are also optimal. This is an immediate consequence of the fact that in our optimisation problem, we always measure the registers F_A and F_B. We can thus without loss of generality assume that both states are cq-states

$$\tilde{C}_{\hat{A}F_AA'} = \sum_{f_A\in\{0,1\}} \hat{C}_{f_A,\hat{A}A'} \otimes |f_A\rangle\langle f_A|_{F_A} \,, \tag{5.21}$$

$$\tilde{C}_{\hat{B}F_BB'} = \sum_{f_B\in\{0,1\}} \hat{C}_{f_B,\hat{B}B'} \otimes |f_B\rangle\langle f_B|_{F_B} \,, \tag{5.22}$$

that is the flags are always classical registers.

Observing that our optimisation problem is only concerned with the case that Alice and Bob succeed, we can now express the problem in terms of the Choi states. We can now consider two cases:

1. Some protocols have local success flags, e.g. the protocol succeeds if Alice and Bob both measure "1", which is the case in the filtering protocol described in Section 5.3.1 or the distillation protocol used within the EPL scheme (both are also described in Section 3.3.2 in Chapter 3). The meaning of "local" refers to the fact that here Alice and Bob can individually already declare failure if they observe a "0" (success evidently requires a comparison). For this example we arrive at the optimisation problem

$$\begin{array}{ll} \text{maximise} & \frac{|A||B|}{\delta}\operatorname{tr}\left(|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}} \otimes \rho^T_{A'B'}\left(\hat{C}_{1,\hat{A}A'}\otimes\hat{C}_{1,\hat{B}B'}\right)\right) \\ \text{subject to} & |A||B|\operatorname{tr}\left[\rho^T_{A'B'}\left(\hat{C}_{1,A'}\otimes\hat{C}_{1,B'}\right)\right] = \delta \,, \\ & \hat{C}_{1,\hat{A}A'} \geq 0, \hat{C}_{1,\hat{B}B'} \geq 0 \,, \\ & \hat{C}_{1,A'} \leq \frac{\mathbb{I}_{A'}}{|A|}, \hat{C}_{1,B'} \leq \frac{\mathbb{I}_{B'}}{|B|} \,. \end{array}$$

Optimisation Program 6.

Here the last condition follows from the Choi condition Eq. (5.15) because we have eliminated the states $\hat{C}_{0,\hat{A}A'}$ and $\hat{C}_{0,\hat{B}B'}$ from explicit consideration.

2. The other case is the one of the non-local success flags, e.g. Alice and Bob succeed if $f_A = f_B$. This is the case for example for the BBPSSW [8] or DEJMPS [9] protocols (again see also Section 3.3.2 in Chapter 3). In this case we obtain

$$\begin{array}{ll} \text{maximise} & \frac{|A||B|}{\delta}\operatorname{tr}\left(|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}} \otimes \rho^T_{A'B'}\left(\hat{C}_{1,\hat{A}A'}\otimes\hat{C}_{1,\hat{B}B'} + \hat{C}_{0,\hat{A}A'}\otimes\hat{C}_{0,\hat{B}B'}\right)\right) \\ \text{subject to} & |A||B|\operatorname{tr}\left[\rho^T_{A'B'}\left(\hat{C}_{1,A'}\otimes\hat{C}_{1,B'} + \hat{C}_{0,A'}\otimes\hat{C}_{0,B'}\right)\right] = \delta \,, \\ & \hat{C}_{1,\hat{A}A'} \geq 0, \hat{C}_{1,\hat{B}B'} \geq 0, \hat{C}_{0,\hat{A}A'} \geq 0, \hat{C}_{0,\hat{B}B'} \geq 0 \,, \\ & \hat{C}_{1,A'} + \hat{C}_{0,A'} = \frac{\mathbb{I}_{A'}}{|A|}, \hat{C}_{1,B'} + \hat{C}_{0,A'} = \frac{\mathbb{I}_{B'}}{|B|} \,. \end{array}$$

Optimisation Program 7.

5.3.3. RELIABLE UPPER BOUNDS USING SDP RELAXATIONS

The Choi isomorphism only transfers the optimisation from channel space to state space, but it does not deal with the (quadratic) non-convex nature of the program. In this section we perform a set of convex relaxations on the domain of optimisation. First, in Section 5.3.3.1 we consider optimisation over positive partial transpose (PPT) operations and in Section 5.3.3.2 we add an additional constraint related to the extendibility of separable states. We will call the resulting bounds reliable, since these numerical methods are guaranteed to produce an upper bound on our objective function. In contrast, later in Section 5.3.4 we discuss a heuristic method which does not have this property.

PPT RELAXATIONS

The first method to obtain an upper bound on the objective is a direct extension of Rains [21]. Here, we relax the set of SEP-C states to the set of PPT Choi states— Choi states which are positive under partial transpose. We perform an easy adaption of this method to the case of MX operations including classical flags, resulting in Optimisation Program 8. This method is implemented in our numerical software package available at [33].

Enforcing the PPT condition is an SDP constraint, whereas membership of SEP is more difficult to characterise and optimisation over the set of separable states is in general hard. Applying the PPT constraint to our problem means that we construct a single Choi state variable on all the registers, such that it obeys the PPT condition, i.e.,

$$C^{\Gamma}_{\hat{A}F_A A'\hat{B}F_B B'} \geq 0, \tag{5.23}$$

where Γ denotes the transpose on all the registers of Bob.

To introduce some helpful notation, we can split this Choi of the distillation channel into the success and failure parts

$$C_{\hat{A}F_A A'\hat{B}F_B B'} = \hat{C}_{\checkmark,\hat{A}F_A A'\hat{B}F_B B'} + \hat{C}_{\times,\hat{A}F_A A'\hat{B}F_B B'} \tag{5.24}$$

obeying the condition

$$\hat{C}_{\checkmark,A'B'} + \hat{C}_{\times,A'B'} = \frac{\mathbb{I}_{A'B'}}{|A||B|}. \tag{5.25}$$

For a protocol with local flags we have

$$\hat{C}_{\checkmark,\hat{A}F_A A'\hat{B}F_B B'} = \hat{C}_{1,\hat{A}A'} \otimes \hat{C}_{1,\hat{B}B'} \otimes |11\rangle\langle 11|_{F_A F_B}, \tag{5.26}$$

whereas for a protocol with non-local flags

$$\begin{aligned}\hat{C}_{\checkmark,\hat{A}F_A A'\hat{B}F_B B'} = \hat{C}_{1,\hat{A}A'} \otimes \hat{C}_{1,\hat{B}B'} \otimes |11\rangle\langle 11|_{F_A F_B} \\ + \hat{C}_{0,\hat{A}A'} \otimes \hat{C}_{0,\hat{B}B'} \otimes |00\rangle\langle 00|_{F_A F_B}.\end{aligned} \tag{5.27}$$

Clearly $\hat{C}_{\checkmark,\hat{A}F_A A'\hat{B}F_B B'}$ and $\hat{C}_{\times,\hat{A}F_A A'\hat{B}F_B B'}$ are orthogonal on the flag registers. As a result imposing the PPT constraint on $C_{\hat{A}F_A A'\hat{B}F_B B'}$ is equivalent to imposing it on both $\hat{C}_{\checkmark,\hat{A}F_A A'\hat{B}F_B B'}$ and $\hat{C}_{\times,\hat{A}F_A A'\hat{B}F_B B'}$. Finally, $\hat{C}_{\times,\hat{A}F_A A'\hat{B}F_B B'}$ does not appear explicitly in our

optimisation problem, but because of the relation in Eq. (5.25), it translates directly to the following condition on the marginal of $\hat{C}_{\checkmark,\hat{A}F_AA'\hat{B}F_BB'}$:

$$\hat{C}^{\Gamma}_{\checkmark,A'B'} \leq \frac{\mathbb{I}_{A'B'}}{|A||B|}, \tag{5.28}$$

where Γ again denotes the partial transpose on all registers of B. Of course Eq. (5.25) also implies that

$$\hat{C}_{\checkmark,A'B'} \leq \frac{\mathbb{I}_{A'B'}}{|A||B|}\,. \tag{5.29}$$

Since in our program we have already eliminated the flags, our SDP variable is $\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}$. *We note that both the case with local and non local flags as well as any other flag configuration reduce to exactly the same relaxed PPT program.* All other constraints in terms of the reduced state of $\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}$ remain the same so that now we will obtain the following program:

$$\begin{aligned}
\text{maximise}\quad & \tfrac{|A||B|}{\delta}\operatorname{tr}\left[\left(|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}}\otimes\rho^T_{A'B'}\right)\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}\right]\\
\text{subject to}\quad & |A||B|\operatorname{tr}\left[\left(\mathbb{I}_{\hat{A}\hat{B}}\otimes\rho^T_{A'B'}\right)\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}\right]=\delta\,,\\
& \hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}\geq 0\,,\\
& \hat{C}^{\Gamma}_{\checkmark,\hat{A}A'\hat{B}B'}\geq 0\,,\\
& \hat{C}_{\checkmark,A'B'}\leq\tfrac{\mathbb{I}_{A'B'}}{|A||B|}\,,\\
& \hat{C}^{\Gamma}_{\checkmark,A'B'}\leq\tfrac{\mathbb{I}_{A'B'}}{|A||B|}\,.
\end{aligned}$$

Optimisation Program 8.

We give a side remark regarding terminologies. Such a PPT Choi state $C_{\hat{A}F_AA'\hat{B}F_BB'}$ corresponds to an operation that Rains defines as a PPT operation [21, 35, 36]. These PPT operations include all LOCC operations as a strict subset. Hence our relaxed program provides upper bounds on the achievable fidelity not only over MX and MXS operations but also over all LOCC operations. See Appendix 5.6.1 for a short discussion of these PPT channels.

The Optimisation Program 8 is a semidefinite program with very high symmetry. This allows considerable further simplifications (see Appendix 5.6.3). We finally obtain the semidefinite program corresponding to the Rains style bound on the fidelity of distillation with fixed success probability δ

$$\begin{aligned}
\text{maximise}\quad & p(M_{A'B'},E_{A'B'})=\tfrac{|A||B|}{\delta}\operatorname{tr}\left[\rho^T_{A'B'}M_{A'B'}\right]\\
\text{subject to}\quad & M_{A'B'}\geq 0,\,E_{A'B'}\geq 0\,,\\
& M_{A'B'}+E_{A'B'}\leq\tfrac{\mathbb{I}_{A'B'}}{|A||B|}\,,\\
& M^{\Gamma}_{A'B'}+E^{\Gamma}_{A'B'}\leq\tfrac{\mathbb{I}_{A'B'}}{|A||B|}\,,\\
& |A||B|\operatorname{tr}\left[\rho^T_{A'B'}(M_{A'B'}+E_{A'B'})\right]=\delta\,,\\
& M^{\Gamma}_{A'B'}+\tfrac{1}{D+1}E^{\Gamma}_{A'B'}\geq 0\,,\\
& -M^{\Gamma}_{A'B'}+\tfrac{1}{D-1}E^{\Gamma}_{A'B'}\geq 0\,.
\end{aligned}$$

Optimisation Program 9.

Recall that $\rho_{A'B'}$ is the initial input state that Alice and Bob are attempting to distil and in

most examples considered here, it will consist of two copies of some two-qubit state. In what follows and on all the plots shown in Section 5.4 we will refer to the bound obtained using this program as the *PPT bound*.

We note here that by following an analogous procedure, one can construct a similar program which aims at maximising probability of success subject to a constraint of fixed output fidelity. This program can also be relaxed to a PPT program which is also an SDP. Effectively it results in a similar program to the one above just with the objective function and constraint on probability of success interchanged:

$$\begin{aligned}
\text{maximise} \quad & |A||B|\,\mathrm{tr}\left[\rho^T_{A'B'}(M_{A'B'}+E_{A'B'})\right] \\
\text{subject to} \quad & M_{A'B'}\geq 0,\, E_{A'B'}\geq 0\,, \\
& M_{A'B'}+E_{A'B'}\leq \tfrac{\mathbb{I}_{A'B'}}{|A||B|}\,, \\
& M^\Gamma_{A'B'}+E^\Gamma_{A'B'}\leq \tfrac{\mathbb{I}_{A'B'}}{|A||B|}\,, \\
& \mathrm{tr}\left[\rho^T_{A'B'}[(1-F)M_{A'B'}-FE_{A'B'}]\right]=0\,, \\
& M^\Gamma_{A'B'}+\tfrac{1}{D+1}E^\Gamma_{A'B'}\geq 0\,, \\
& -M^\Gamma_{A'B'}+\tfrac{1}{D-1}E^\Gamma_{A'B'}\geq 0\,.
\end{aligned}$$

Optimisation Program 10.

Now F is a constant fidelity and so the fidelity constraint is just:

$$\frac{\mathrm{tr}[\rho^T_{A'B'}M_{A'B'}]}{\mathrm{tr}[\rho^T_{A'B'}(M_{A'B'}+E_{A'B'})]}=F. \tag{5.30}$$

Hereafter, we will drop the subscripts on ρ, E and M to simplify the notation.

BOSE SYMMETRIC EXTENSIONS

The goodness of the relaxation above depends on how well the set of PPT Choi states approximates the set SEP-C. A sharper approximation could evidently be obtained by approximating the set of separable states SEP itself by more stringent conditions. A standard technique for doing so is by the method of extensions [31, 32] which is closely related to the sums-of-squares relaxations for polynomial optimisation problems.

In the case at hand, in addition to the PPT constraint in Eq. (5.23) we will add the constraint that the state is k-Bose-symmetric-extendible (k-BSE) [37]. By definition, a (Choi) state $\hat{C}_{(\hat{A}A')\hat{B}B'}$ is k-BSE iff there exists $\hat{C}_{(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})\hat{B}B'}$ satisfying

1. $\hat{C}_{(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})\hat{B}B'}\geq 0$,
2. $\mathrm{tr}_{(\hat{A}_2A'_2)\ldots(\hat{A}_{k+1}A'_{k+1})}\left(\hat{C}_{(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})\hat{B}B'}\right)=\hat{C}_{(\hat{A}A')\hat{B}B'}$,
3. $\left(P_{\mathrm{Sym}}\otimes\mathbb{I}_{\hat{B}B'}\right)\left(\hat{C}_{(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})\hat{B}B'}\right)=\hat{C}_{(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})\hat{B}B'}$, where P_{Sym} is the projector onto the symmetric subspace of $(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})$.

It is clear that adding this constraint to the PPT constraint constitutes a sharper approximation of SEP-C because any separable state is k-BSE for all $k\in\mathbb{N}$. To see this, it is

sufficient to note that $\sum_i p_i |u_i\rangle\langle u_i|^{\otimes k+1} \otimes |v_i\rangle\langle v_i|$ is a k Bose symmetric extension of the separable state $\sum_i p_i |u_i\rangle\langle u_i| \otimes |v_i\rangle\langle v_i|$.

In this way, we obtain a sharper and sharper approximation of SEP-C by choosing larger values of k — the accuracy scales not worse than $O(|\hat{A}A'|^2/(k+1)^2)$ [38]. The only drawback is the size of the resulting SDP. Although it increases only polynomially with k, for practically interesting problems we were only able to introduce $k = 1$ Bose symmetric extensions. We refer to Appendix 5.6.5 for the detailed calculations and the exact form of the resulting SDP. Whenever we refer to the *1-BSE bound*, we mean the bound arising from this optimisation over Choi matrices that are both PPT and 1-BSE.

5.3.4. OPTIMISING EXISTING SCHEMES

While the previous methods are concerned with deriving upper bounds on the fidelity, we can as well start from an existing distillation protocol and try to find a better protocol. In the following we discuss one such a scheme that we dub the seesaw method. Looking at the original Optimisation Programs 6 and 7, we see that there is no need for any PPT style relaxation if one of the distillation maps for either Alice or Bob is fixed: for a fixed value of one of the maps, the optimisation problem is already an SDP. If we thus fix the operation of Alice (or Bob), then we may use an SDP solver to optimize over the possible distillation schemes in terms of the Choi state of Bob (or Alice). Once solved, we may iterate the procedure in a seesaw fashion. We now fix the operation of Bob (Alice) with the outcome of the previous step and we optimize over the operation of Alice (Bob). The optimisation problem is again an SDP. These steps can then be repeated, as often as desired optimising iteratively over either Alice or Bob. While not guaranteed to find the optimal solution, the seesaw method often performs rather well in practice and is implemented in our numerical package [33]. In fact, in the next section we provide an example where this method finds an optimal filtering scheme, as the numerical results show that it achieves fidelities corresponding to the PPT bound. We remark that given the new Choi states, one may find the corresponding isometry (or unitary) that implements the map using an ancilla (see, e.g., lecture notes [39]) and then compile it into a quantum circuit for the specific architecture in question.

5.4. STATES AND DISTILLATION SCHEMES

Let us now illustrate our methods with a number of states commonly studied in the entanglement distillation literature, or arising in experiments. We thereby demonstrate the use of our methods as a numerical tool to compute the trade-offs between the fidelity F and probability of success p_{succ}, as well as their use as an analytical tool to formally prove optimality of certain entanglement distillation schemes. We also provide a simple example illustrating the use of the seesaw method to improve an existing distillation scheme for a specific state.

Here we will use the term "a copy of a state" to denote a two-qubit state shared between Alice and Bob. In these examples, we will for simplicity only consider distillation to a single copy i.e. when the output of the procedure is a two-qubit state. More examples can easily be explored using the freely available numerical package [33].

5.4.1. ISOTROPIC STATES

As a warm-up, let us consider distilling isotropic states. These states are often considered in the quantum information theory literature due to their beautiful symmetries. Moreover, they are the states that arise when a maximally entangled state undergoes depolarising noise, which is often used as a simplified pessimistic model for the noise caused by the imperfect operations in physical implementations of quantum memories. Specifically, an isotropic state is of the form

$$\tau_{AB} = p|\Phi_D\rangle\langle\Phi_D| + (1-p)\frac{\mathbb{I}}{D^2}, \tag{5.31}$$

where $|\Phi_D\rangle$ is the maximally entangled state defined in Eq. (5.2). The isotropic state is invariant under $U \otimes U^*$ on A and B for all U.

NUMERICAL EXAMPLES

FIG. 5.1 illustrates the upper bounds obtained by PPT and the 1-BSE relaxation, in comparison to the BBPSSW and DEJMPS protocols when distilling 2 copies of the isotropic state $\rho_{AB} = \tau_{ab}^{\otimes 2}$ to a single two-qubit state (see Section 3.3.2 in Chapter 3 for the description of these well-known protocols). We remark that when performing a single round of distillation, the two protocols coincide for the case of the isotropic state. The continuous red line corresponds to an achievable scheme based on the interpolation or extrapolation of those existing schemes. The details of how this is performed are included in Appendix 5.6.2.2 and for simplicity on the plots we always label this curve arising from both extrapolation and interpolation as "Interpolation". Similarly in FIG. 5.2 we depict the corresponding results for distilling 3 copies of the isotropic state $\rho_{AB} = \tau_{ab}^{\otimes 3}$ to a two-qubit state.

In FIG. 5.1 and FIG. 5.2 we see that both the PPT and 1-BSE bounds are non trivial and the 1-BSE bound is tighter than the PPT bound for smaller values of the probability of success. In particular we observe that deterministic distillation (with $p_{\text{succ}} = 1$) when operating on 2 copies of the isotropic state is not possible. For 3 copies it is possible to deterministically increase the fidelity, and this can be achieved, e.g., using the protocol DEJMPS A (see caption of FIG. 5.2 for details of this protocol).

5.4.2. BELL DIAGONAL STATES

More generally, we now consider states τ_{AB} that are diagonal in the Bell basis given by

$$|\Phi^+\rangle = |\Phi_2\rangle, \tag{5.32}$$
$$|\Phi^-\rangle = (\mathbb{I}\otimes Z)|\Phi_2\rangle, \tag{5.33}$$
$$|\Psi^+\rangle = (\mathbb{I}\otimes X)|\Phi_2\rangle, \tag{5.34}$$
$$|\Psi^-\rangle = (\mathbb{I}\otimes XZ)|\Phi_2\rangle. \tag{5.35}$$

These are interesting states to consider since indeed any two-qubit state ρ_{AB} can be brought into this form by twirling it over the group of correlated Pauli operators: $\{X\otimes X, Y\otimes Y, Z\otimes Z, \mathbb{I}\otimes\mathbb{I}\}$. This can be achieved if Alice and Bob have access to some

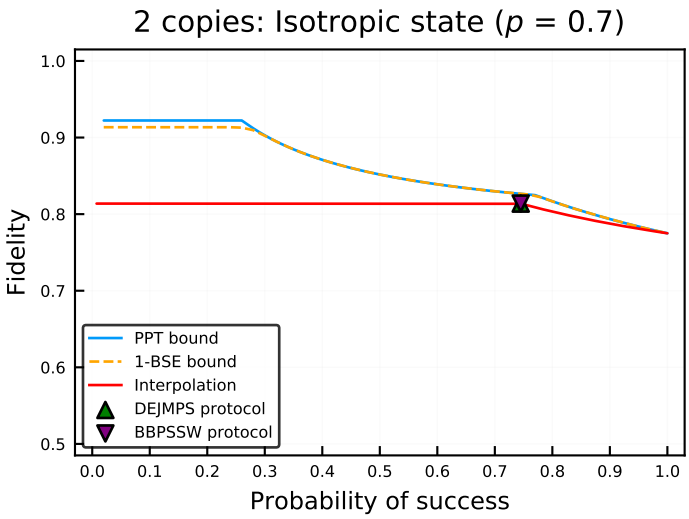

Figure 5.1: Distilling the isotropic states $\tau_{ab}^{\otimes 2}$ with $D = 2$ and $p = 0.7$ in Eq. (5.31) to a two-qubit state. The fidelity of each input copy is $F_{\text{in}} = 0.775$ and we observe that deterministic distillation (with $p_{\text{succ}} = 1$) is not possible for two copies of the isotropic state. We also find that the method of 1-BSE provides tighter bounds than the PPT method alone.

shared randomness. We can thus consider entangled states

$$\begin{aligned}\tau_{AB} = p_1|\Phi^+\rangle\langle\Phi^+| + p_2|\Psi^+\rangle\langle\Psi^+| + p_3|\Phi^-\rangle\langle\Phi^-| \\ + (1-p_1-p_2-p_3)|\Psi^-\rangle\langle\Psi^-|\,,\end{aligned} \tag{5.36}$$

where $p_1 > 0.5$ and $p_1 > p_2 \geq p_3 \geq 1-p_1-p_2-p_3$. Any Bell diagonal state for which one of the Bell coefficients is larger than 0.5 can be rotated into this form using only local Clifford operations performed by Alice and Bob.

The distillation of such states has been studied in the literature, and we will focus here on the action of the DEJMPS protocol on these states since it is known for achieving higher fidelities than the BBPSSW protocol. Specifically, Alice and Bob share two copies of a Bell diagonal state τ_{AB}, that is, $\rho_{AB} = \tau_{ab}^{\otimes 2}$. The decreasing order of the Bell coefficients in τ_{AB} is important as this specific ordering allows us to achieve the highest fidelity over all the orderings [40].

We note that it has been recently shown that the DEJMPS protocol achieves the highest possible fidelity over LOCC operations when distilling a two-qubit state from two copies of a Bell diagonal state of rank two [41]. Moreover, in [40] protocols that permute Bell states in the mixture were analyzed and it was claimed that for two copies of all Bell diagonal states, DEJMPS protocol achieves the highest achievable fidelity when distilling a two-qubit state, but only among all such permuting protocols. Here our results indicate that we can make a much wider range of optimality statements about DEJMPS in relation to Bell diagonal states than has been known before.

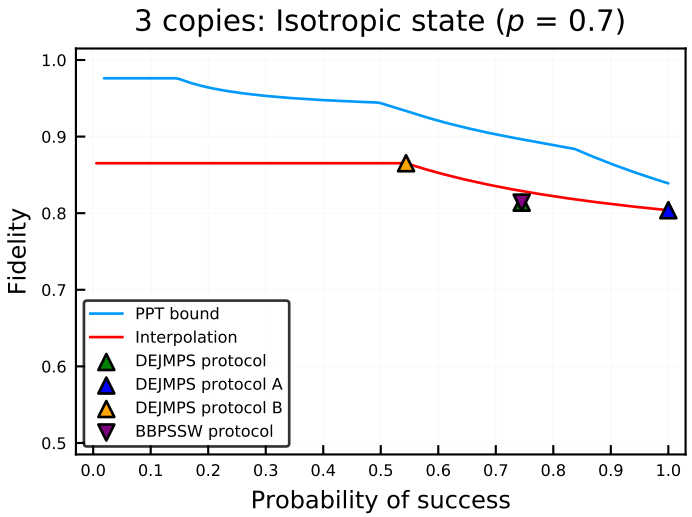

Figure 5.2: Distilling the isotropic states $\tau_{ab}^{\otimes 3}$ with $D = 2$ and $p = 0.7$ in Eq. (5.31) to a two-qubit state. The fidelity of each input copy is $F_{\text{in}} = 0.775$. The protocol DEJMPS A corresponds to applying DEJMPS to the first two copies and outputting the resulting state in case of success and outputting the remaining third copy in case of failure. This protocol allows for deterministic increase of fidelity. The protocol DEJMPS B corresponds to applying DEJMPS to the first two copies and then conditioned on success, applying it to the remaining two copies. Failure at any stage results in outputting the failure flag. The 1-BSE bound was already computationally too expensive for this 3-copy scenario.

NUMERICAL EXAMPLES

We first investigate a number of examples using our numerical procedure. We present the results in FIG. 5.3 and in FIG. 5.4. We again emphasize that for simplicity we only consider distilling a two-qubit state from two copies of a Bell diagonal state and we note that all these optimality statements apply when optimising over all LOCC protocols.

First, we observe that for all Bell diagonal states of rank up to three DEJMPS achieves the highest possible output fidelity and achieves it with the highest possible probability of success, as can be seen in a specific example in FIG. 5.3. This statement we also prove analytically as described in the next subsection. Moreover, as we also illustrate in FIG. 5.3, we numerically observe that for Bell diagonal states of rank up to three, extrapolating from DEJMPS allows us to achieve the highest possible output fidelity for each extrapolation protocol's probability of success.

Finally, we also numerically observe that for Bell diagonal states of rank four, apart from a certain set of states including and around the isotropic state, DEJMPS achieves the highest possible fidelity for this protocol's probability of success when applied to these states. In FIG. 5.5 we fix p_1 and p_2 and plot the gap between our numerical upper bound and the output fidelity of DEJMPS, both evaluated at the probability of success of DEJMPS, versus the parameter p_3. We see that in this space of Bell coefficients the gap vanishes when one moves far enough from the isotropic state. In this space, we observe a similar gap in any other direction away from the isotropic state. However, only by moving exactly along the axis of one of those coefficients do we obtain a gap that is symmetric around the isotropic state as in FIG. 5.5. The reason for this fact is that on those axes the two states that are located symmetrically on two sides of the peak at the isotropic state are the same up to the permutation of the Bell coefficients.

OPTIMAL FIDELITY AND SUCCESS PROBABILITY

Semidefinite programming duality now allows us to prove analytically that DEJMPS is an optimal protocol for distilling from two copies of all Bell diagonal states of rank up to three, which was not known before.

Theorem 5.4.1. *(Informal) Given two copies of a Bell diagonal state of rank at most three and distillation towards the target maximally entangled state with $D = 2$, there is no protocol that achieves a larger fidelity than DEJMPS and there is no protocol that achieves this fidelity with a larger success probability than DEJMPS.*

In the following we sketch the proof of Theorem 5.4.1. We leave the full details including a precise definition of optimality to Appendix 5.6.7.

The entangled Bell diagonal states of rank up to three can be written as

$$\tau_{AB} = p_1|\Phi^+\rangle\langle\Phi^+| + p_2|\Psi^+\rangle\langle\Psi^+| + (1-p_1-p_2)|\Phi^-\rangle\langle\Phi^-|, \tag{5.37}$$

with $p_1 > 0.5$ and $p_1 > p_2 \geq 1 - p_1 - p_2$. First, we note that the DEJMPS protocol applied to two copies of the state in Eq. (5.37) conditioned on success results in a state

$$\rho_{\hat{A}\hat{B}} = p_1'|\Phi^+\rangle\langle\Phi^+| + p_2'|\Psi^+\rangle\langle\Psi^+| + (1-p_1'-p_2')|\Psi^-\rangle\langle\Psi^-|, \tag{5.38}$$

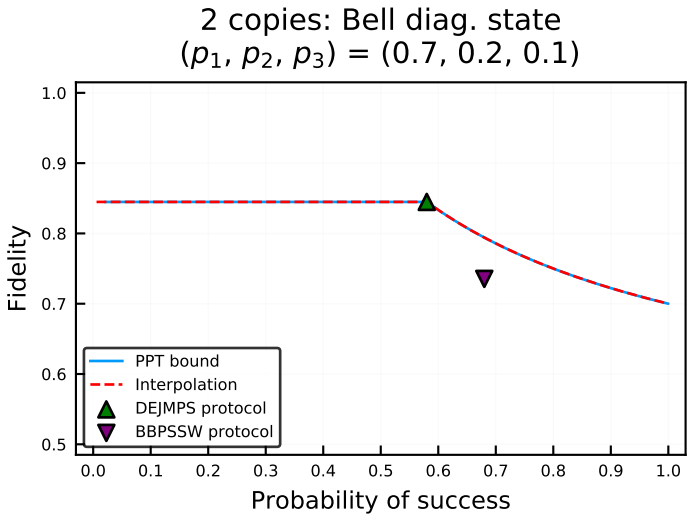

Figure 5.3: Distilling the Bell diagonal states of rank-three $\tau_{ab}^{\otimes 2}$ with $D = 2$ and $p_1 = 0.7, p_2 = 0.2, p_3 = 0.1$ in Eq. (5.36) to a two-qubit state. The fidelity of each input copy is $F_{\text{in}} = 0.7$ and we observe that deterministic distillation (with $p_{\text{succ}} = 1$) is not possible for two copies of this state. We see that DEJMPS is optimal for a mixture of three Bell states. Moreover, extrapolating from DEJMPS to higher probability of success as described in Appendix 5.6.2.2, we see that the extrapolation curve overlaps with the PPT bound for all values of the probability of success. This means that this extrapolation also results in optimal schemes achieving the highest possible output fidelity for the specific fixed probability of success. The 1-BSE bound is not included because it overlaps with the PPT bound.

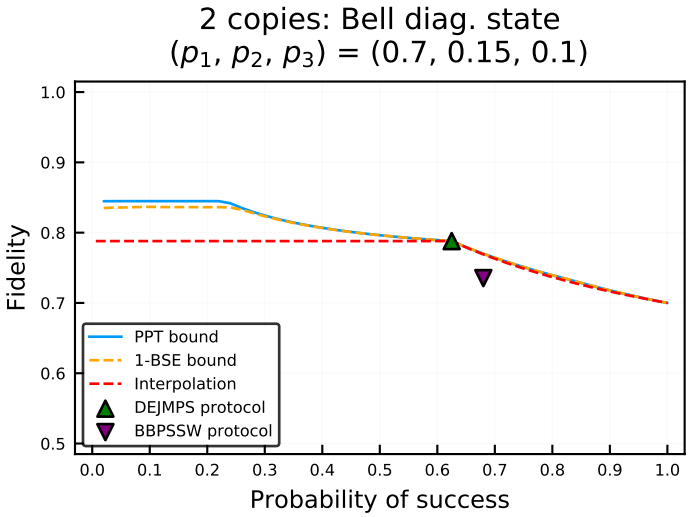

Figure 5.4: Distilling the Bell diagonal states of rank-four $\tau_{ab}^{\otimes 2}$ with $D = 2$ and $p_1 = 0.7, p_2 = 0.15, p_3 = 0.1$ in Eq. (5.36) to a two-qubit state. The fidelity of each input copy is $F_{\text{in}} = 0.7$ and we observe that deterministic distillation (with $p_{\text{succ}} = 1$) is not possible for two copies of this state. We also find that the 1-BSE bound is tighter than the PPT bound for smaller values of the probability of success. Finally, we observe that DEJMPS achieves the highest possible output fidelity for this protocol's probability of success for a mixture of four Bell states which are far enough from the isotropic state.

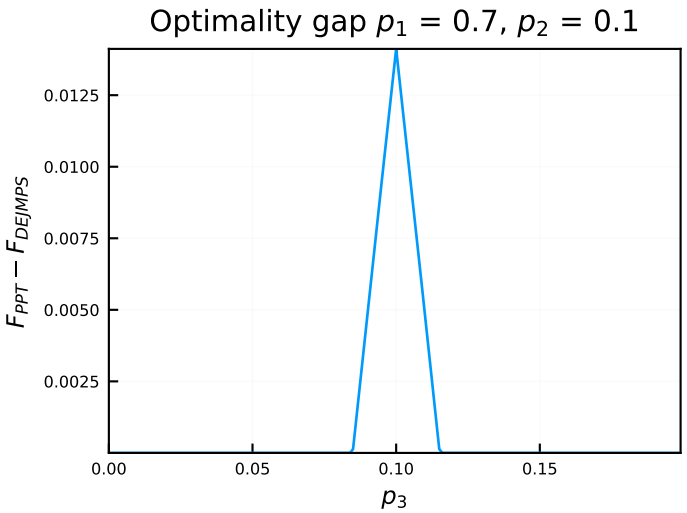

Figure 5.5: Distilling the Bell diagonal states of rank-four $\tau_{ab}^{\otimes 2}$ with $D = 2$ and $p_1 = 0.7, p_2 = 0.1$ in Eq. (5.36) to a two-qubit state. The fidelity of each input copy is $F_{\text{in}} = 0.7$. The plot shows the difference between the PPT bound and the fidelity achievable through DEJMPS as a function of p_3 for the probability of success of DEJMPS. We see that DEJMPS achieves the highest possible output fidelity for this protocol's probability of success for a mixture of four Bell states which are far enough from the isotropic state (the middle of the peak). Clearly the states considered on this plot for which $p_3 \neq 0.1$ do not satisfy the condition $p_1 > p_2 \geq p_3 \geq 1 - p_1 - p_2 - p_3$, therefore when applying the DEJMPS protocol to such a state we first permute the Bell coefficients to this order. The 1-BSE bound is not included because it overlaps with the PPT bound.

where

$$p_1' = \frac{p_1^2}{N}, \tag{5.39}$$

$$p_2' = \frac{p_2^2 + (1-p_1-p_2)^2}{N}, \tag{5.40}$$

and $N = p_1^2 + (1-p_1)^2$ is the probability that the protocol succeeds. Note that $p_1' > p_2' \geq 1 - p_1' - p_2'$. Moreover the fidelity increases, that is, $p_1' > p_1$.

The strategy to show optimal fidelity relies on the dual formulation of the SDP in Optimisation Program 9. In particular, we prove that there exists a feasible solution of the dual program with the objective function value corresponding to p_1' for all $\delta \in (0,1]$. Hence p_1' is an upper bound on the achievable fidelity for all δ and there cannot exist an LOCC protocol that takes two copies of the state in Eq. (5.37) and outputs a state with fidelity larger than p_1'.

The proof of N being the optimal success probability for all protocols that output fidelity equal to p_1' also follows from SDP duality. That is, we show that there exists a feasible solution of the dual program for optimising the probability of success with the objective function taking the value N for the output fidelity $F = p_1'$.

5.4.3. R STATES

Another interesting class of states are quantum states that form a mixture between a maximally entangled state and a product state. In particular let us first consider a case where the product part of the mixture is orthogonal to the maximally entangled part. Specifically let us consider the state

$$\tau_{AB} = p|\Psi^{\pm}\rangle\langle\Psi^{\pm}| + (1-p)|11\rangle\langle 11|, \tag{5.41}$$

which we will call an R state. We note that up to a local X or XZ gate this state is exactly the state in Eq. (5.10) that we considered in the filtering example in Section 5.3.1 (this local flip on one side will be helpful when discussing remote entanglement generation in the following section).

This type of state is interesting for two reasons. The first one is "mathematical". The above R state is a simple example of a state that as expressed in [42] possesses local information, in the sense that the reduced state on Alice and Bob individually is not a maximally mixed state. This local information can also be seen in the non-zero off-diagonal elements when the state is expressed in the Bell basis. Since for the DEJMPS and BBPSW protocols the output fidelity and probability of success are completely independent of those off-diagonal coefficients, this local information is completely neglected in those protocols. Hence one could expect that for these states there exist distillation strategies that utilize this local information and in this way possibly outperform the DEJMPS protocol.

As observed in [20] this is indeed the case, since for any value of $0 < p \leq 1$ it is possible to extract a perfect Bell state from two copies of the R state by performing a bilateral CNOT, measuring the target copy in the standard basis and post-selecting the events for which both Alice and Bob measured the target copy to be one. In such a scenario

of applying this protocol to two copies of the R state the fidelity of $F = 1$ is achieved with probability of success $p_{\text{succ}} = p^2/2$. Note that depending on the value of p the R state might actually have fidelity to any maximally entangled state smaller than or equal to half. This shows a fundamental difference with respect to the protocols that do not utilize this local information like DEJMPS or BBPSSW for which it is required that the initial fidelity to some maximally entangled state is larger than 0.5 *.

The second reason for considering these states is experimental. These states arise in certain protocols for remote entanglement generation that use a single photon detection scheme in the presence of photon loss [7, 13, 45]. In particular, [7] describes an entanglement generation procedure that generates two copies of a state closely related to the R state (see the next section for more details) and then performs the above described distillation protocol proposed in [20] to combat the effect of photon loss. Since the authors refer to this entire entanglement generation scheme as the Extreme Photon Loss scheme (EPL), here we will refer to this distillation protocol used within the EPL procedure as EPL-D. As already mentioned and as we will discuss in the next section, the R state is still only an idealisation of the actual raw state generated within the remote entanglement generation schemes described in [7, 13]. In particular the R state includes only noise due to the photon loss while all realistic implementations will also suffer from other types of noise.

NUMERICAL EXAMPLES

We first look at filtering a single copy of the R state, since as stated in Section 5.3.1, there exists a well-known protocol for filtering those states. Optimal filtering schemes have been studied in the literature [44, 46, 47], but not in the context of the optimal tradeoff of fidelity and probability of success.

First, we note that the filtering scheme described in Section 5.3.1 (here we assume that before filtering, Alice applies an X or XZ operation to bring the R state to the form in Eq. (5.10)) clearly cannot increase the fidelity deterministically, while from [44] we know that for all $p < 2/3$ there exists a way of deterministically increasing the fidelity of the R state by running a probabilistic filtering protocol and outputting a product state of fidelity half in case of failure. Inspired by this result we consider here a modified version of the discussed filtering scheme in which for certain larger values of the desired success probability for R states with $p < 2/3$, conditioned on the failure of that original scheme Alice and Bob probabilistically output a state of fidelity half. The details of this modification are discussed in Appendix 5.6.2.2. In FIG. 5.6 and in FIG. 5.7 we compare this modified filtering scheme with our numerical bounds. We consider one example for which the input fidelity is larger and one for which it is smaller than half.

The original filtering scheme allows us to choose the desired probability of success by making a suitable choice of the ϵ parameter, while in our modified scheme success probability can also be varied by changing the probability of outputting a product state in case of failure of the original scheme (here we maximise the fidelity over those two parameters for each probability of success). We note that independently of the value of

*It must be noted that there also exists a general procedure for distilling any inseparable two-qubit state, and in particular any two-qubit state whose fidelity to any maximally entangled state is smaller than or equal to half and which therefore cannot be distilled using DEJMPS or BBPSSW, see [43, 44].

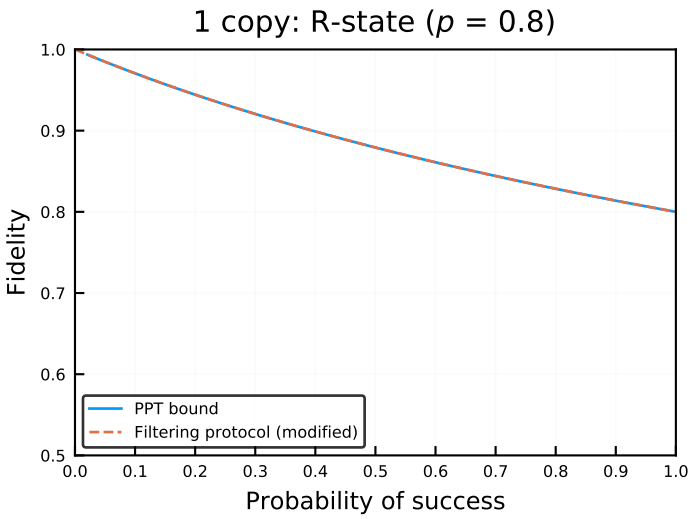

Figure 5.6: Filtering R state τ_{AB} with $D = 2$ and $p = 0.8$ in Eq. (5.41) to a two-qubit state. The fidelity of the input copy is $F_{\text{in}} = 0.8$ and in accordance with [44] we observe that deterministic filtering (with $p_{\text{succ}} = 1$) is not possible for this state. We see that the filtering scheme perfectly overlaps with the PPT bound, which proves its optimality for this state. The 1-BSE bound is not included because it overlaps with the PPT bound.

5

the parameter p (provided that it is non-zero), in the limit of zero success probability, this filtering scheme allows for obtaining a state that is arbitrarily close to a maximally entangled state. From the numerical results we observe that for the considered values of p, we have that for all probabilities of success our PPT bound perfectly overlaps with the modified filtering scheme, proving that no higher fidelity can be achieved for the fixed value of probability of success than already achieved by our modified filtering scheme. Hence the modified filtering scheme is in fact optimal for these states.

We also present two numerical examples for distillation from two to one copies of the R state in FIG. 5.8 and in FIG. 5.9. In FIG. 5.8 we consider two copies of the R state with input fidelity of 0.8. We see that while our achievable interpolation scheme cannot deterministically increase fidelity for this state, the non-trivial numerical bounds still allow for this possibility. We also see that for this state the PPT operations allow for distilling a state very close to a maximally entangled state for much larger probability of success than the achievable interpolation scheme. In FIG. 5.9 we consider two copies of the R state whose input fidelity is smaller than half. In this case the interpolation scheme allows for deterministic increase of fidelity above 0.5 (as discussed in the previous paragraph, for this value of p that is possible even with just the modified filtering, but the interpolation scheme performs better). We see that here the PPT operations do not allow for distilling a state with fidelity close to one for probabilities of success much larger than that of the EPL-D protocol.

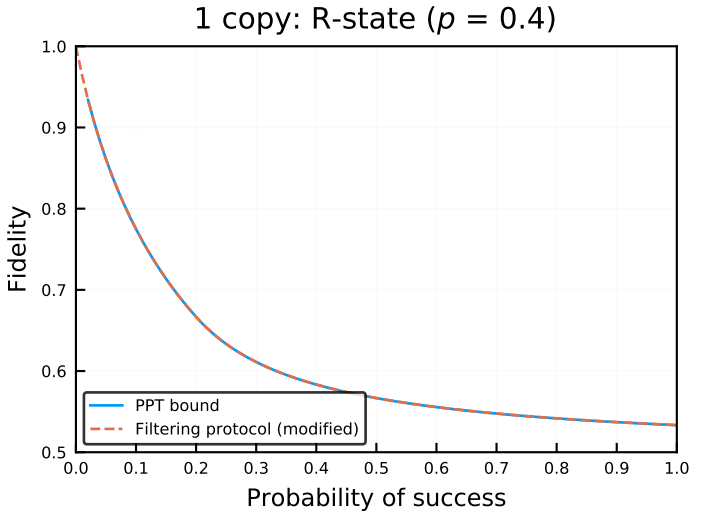

Figure 5.7: Filtering R state τ_{AB} with $D = 2$ and $p = 0.4$ in Eq. (5.41) to a two-qubit state. The fidelity of the input copy is $F_{\text{in}} = 0.4$. As first shown in [44], we observe that for the smaller values of p deterministic filtering of R states is possible and can be achieved with our scheme. We also see that the filtering scheme perfectly overlaps with the PPT bound, which proves its optimality for this state. The 1-BSE bound is not included because it overlaps with the PPT bound.

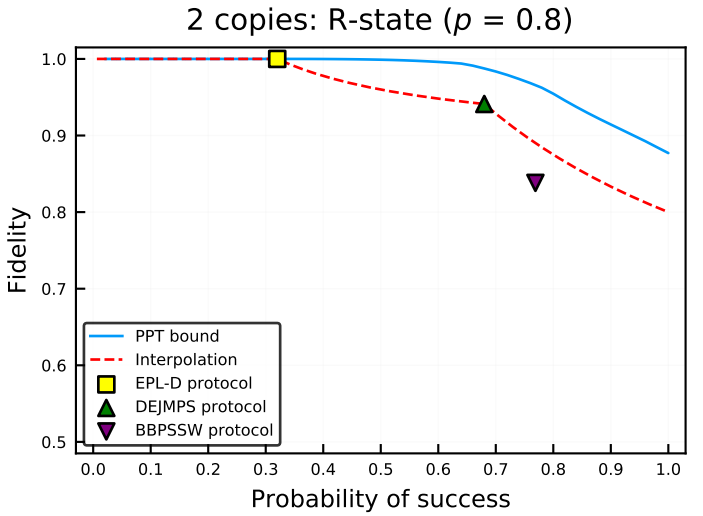

Figure 5.8: Distilling the R states $\tau_{ab}^{\otimes 2}$ with $D = 2$ and $p = 0.8$ in Eq. (5.41) to a two-qubit state. The fidelity of the input copy is $F_{\text{in}} = 0.8$ and we observe that while the extrapolation from DEJMPS does not allow for deterministic distillation (with $p_{\text{succ}} = 1$) in this case, the PPT bound still allows for this possibility. We also see that EPL-D allows for achieving unit fidelity. The 1-BSE bound is not included because it overlaps with the PPT bound.

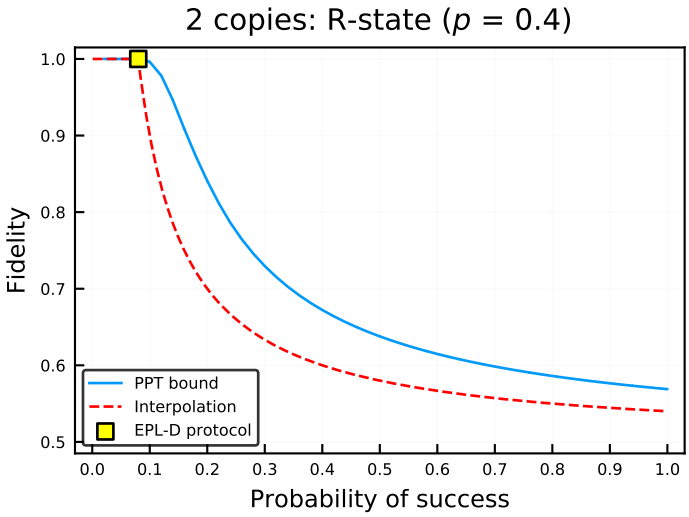

Figure 5.9: Distilling the R states $\tau_{ab}^{\otimes 2}$ with $D = 2$ and $p = 0.4$ in Eq. (5.41) to a two-qubit state. The fidelity of the input copy is $F_{\text{in}} = 0.4$ and we observe that deterministic distillation (with $p_{\text{succ}} = 1$) which achieves output fidelity larger than half is easily achievable for two copies of this state. We also see that EPL-D allows for achieving unit fidelity even if $p \leq 0.5$. The 1-BSE bound is not included because it overlaps with the PPT bound.

5

5.4.4. REMOTE ENTANGLEMENT GENERATION

Here we expand on the experimentally relevant ideas described in the previous section on R states to reliably model the remote entanglement generation through distillation, including most of the experimentally relevant sources of noise as described in [7] and as realised experimentally in [18]. Specifically, in most experimental implementations of this specific entanglement generation scheme the actual state that is created will be of the form

$$\rho_{AB}(p) = \frac{1}{2\pi}\int d\phi \tau_{A1B1}(\phi, p) \otimes \tau_{A2B2}(\phi, p), \tag{5.42}$$

where

$$\tau_{AB}(\phi, p) = p|\Psi^+(\phi)\rangle\langle\Psi^+(\phi)| + (1-p)|11\rangle\langle 11|, \tag{5.43}$$

and

$$|\Psi^+(\phi)\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + e^{i\phi}|10\rangle\right), \tag{5.44}$$

$$|\Psi^-(\phi)\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - e^{i\phi}|10\rangle\right). \tag{5.45}$$

Here ϕ is a phase that arises due to the optical apparatus and in most cases is completely unknown. We see that the complete lack of knowledge of the phase ϕ leads to the uniform averaging over that phase. However, if the system is stable over the duration of generation of the two copies of ρ, one can assume that both of those copies are correlated in that phase.

In the next step we make this model even more precise by acknowledging the fact that the first copy of ρ will actually undergo dephasing while trying to generate the second copy. Moreover, the phase will in general not be exactly the same for both copies since in any realistic setting it could drift with respect to the first copy. Mathematically, those two effects can be combined together into a single dephasing process that affects one of the two copies

$$\rho_{AB}(p, p_d) = \frac{1}{2\pi} \int d\phi \tau_{A1B1}(\phi, p, p_d) \otimes \tau_{A2B2}(\phi, p, 1), \tag{5.46}$$

where

$$\begin{aligned} \tau_{AB}(\phi, p, p_d) = p \big(& p_d |\Psi^+(\phi)\rangle\langle\Psi^+(\phi)| \\ & + (1-p_d)|\Psi^-(\phi)\rangle\langle\Psi^-(\phi)|\big) + (1-p)|11\rangle\langle 11|. \end{aligned} \tag{5.47}$$

Here we shall refer to the state in Eq. (5.46) as "R-state correlated phase". In this scenario the successful implementation of the EPL-D distillation protocol (followed by a local rotation) leads to the output state

$$\eta_{\hat{A}\hat{B}}(p_d) = p_d |\Phi^+\rangle\langle\Phi^+| + (1-p_d)|\Phi^-\rangle\langle\Phi^-|, \tag{5.48}$$

with probability of success $p_{\text{succ}} = p^2/2$. We also provide a more detailed description of this remote entanglement generation scheme in Appendix 5.6.2.1.

NUMERICAL EXAMPLES

We present two numerical examples for applying distillation to the state $\rho_{AB}(p, p_d)$ in FIG. 5.10 and in FIG. 5.11. We observe that EPL-D saturates the bound by achieving the highest possible fidelity with the highest possible probability of success. Moreover, we observe that extrapolating from EPL-D to higher values of probability of success also achieves the highest possible fidelity for the corresponding value of the probability of success.

OPTIMAL FIDELITY AND PROBABILITY OF SUCCESS

The numerical examples suggest that the EPL-D protocol is optimal for distilling states $\rho_{AB}(p, p_d)$ given in Eq. (5.46) both in terms of output fidelity and probability of success. This means that the EPL scheme utilizes the optimal distillation protocol in this respect.

Theorem 5.4.2. *Given a state of the form $\rho_{AB}(p, p_d)$ given in Eq.* (5.46) *and distillation towards the target maximally entangled state with $D = 2$, there is no protocol that achieves a larger fidelity than EPL-D and there is no protocol that achieves this fidelity with a larger success probability than EPL-D.*

It turns out that in this case it is possible to analytically prove this optimality in a simple way without using the SDP formulation. Specifically, see Appendix 5.6.8 for the proof, that after performing the integration over the phase ϕ, the state $\rho_{AB}(p, p_d)$ is actually block diagonal in the standard basis, where one of the blocks is of size two and all the other blocks are of size one. Clearly the blocks of size one correspond to separable states. Hence, output fidelity is maximised by projecting onto the size two block.

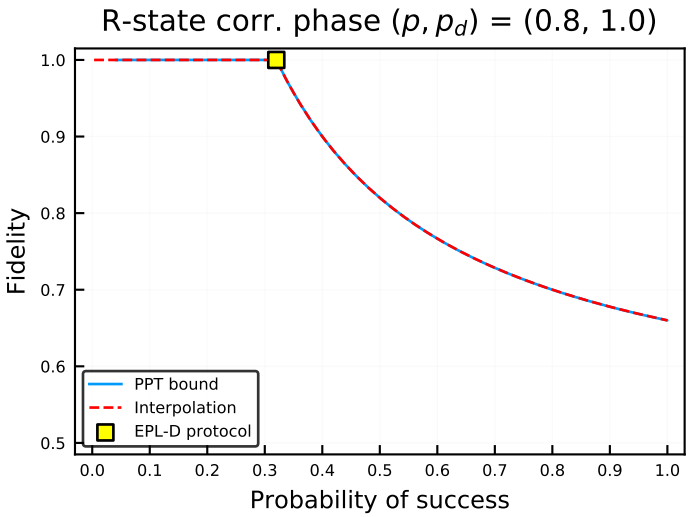

Figure 5.10: Distilling the R-state correlated phase $\rho_{AB}(p, p_d)$ given in Eq. (5.46) with $D = 2$ and $p = 0.8, p_d = 1$ to a two-qubit state. We see that EPL-D is an optimal distillation protocol for the EPL remote entanglement generation scheme. The red extrapolation curve perfectly overlaps with the PPT bounds which means that the protocols arising by extrapolating EPL-D to higher values of probability of success are also optimal and achieve the maximum possible fidelity for the corresponding probability of success. The 1-BSE bound is not included because it overlaps with the PPT bound.

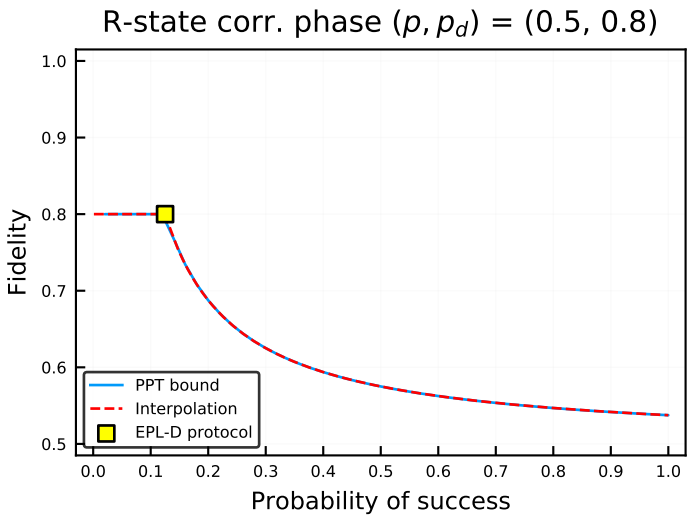

Figure 5.11: Distilling the R-state correlated phase $\rho_{AB}(p, p_d)$ given in Eq. (5.46) with $D = 2$ and $p = 0.5, p_d = 0.8$ to a two-qubit state. EPL-D is an optimal distillation protocol for the EPL remote entanglement generation scheme. The red extrapolation curve perfectly overlaps with the PPT bounds which means that the protocols arising by extrapolating EPL-D to higher values of probability of success are also optimal and achieve the maximum possible fidelity for the corresponding probability of success. The 1-BSE bound is not included because it overlaps with the PPT bound.

Finally, this block is equivalent up to a local relabelling to the state $\eta_{\hat{A}\hat{B}}(p_d)$ in Eq. (5.48). Since this state is non-filterable in the sense that even probabilistically no LOCC scheme can increase its fidelity [44], the optimal protocol cannot achieve fidelity higher than p_d which is achieved by EPL-D within the EPL scheme.

The same argument also implies that within EPL, EPL-D achieves fidelity p_d with maximum probability. More concretely, the probability of the projection onto the size-two block succeeds with probability at most $p^2/2$ which is the success probability of EPL-D within EPL.

OPTIMALITY WITH RESPECT TO DISTILLABLE ENTANGLEMENT

Recall that the distillable entanglement of a state is defined as the optimal asymptotic rate at which it is possible to transform copies of the state into copies of the maximally entangled state. It turns out that within EPL, EPL-D is also optimal for distillable entanglement. More concretely:

Theorem 5.4.3. *Given a state of the form $\rho_{AB}(p, p_d)$ given in Eq.* (5.46)*, there is no protocol with the success probability of EPL-D that outputs a state with larger distillable entanglement. Equally there is no protocol that outputs a state with the same distillable entanglement as EPL-D and succeeds with larger probability.*

We defer the proof of Theorem 5.4.3 to Appendix 5.6.8. The informal argument relies on the fact that the distillable entanglement of the output of a distillation protocol

multiplied by the rate of successful distillation cannot be larger than the distillable entanglement of the original state; that is, we must have that

$$p_{\text{succ,EPL}} E_D(\eta_{\hat{A}\hat{B}}(p_d)) \leq E_D((\rho_{AB}(p,p_d)). \tag{5.49}$$

In the case of EPL, the distillable entanglement of the state $\rho_{AB}(p,p_d)$ equals $p_{\text{succ,EPL}}(1-h(p_d))$ (see Appendix 5.6.8) while the distillable entanglement of the output state of EPL-D, $\eta_{\hat{A}\hat{B}}(p_d)$, is $1-h(p_d)$, where $h(x) = -x\log x-(1-x)\log(1-x)$ is the binary entropy function [48]. This proves that we actually have equality in Eq. (5.49). The result is stronger in the case that there is no dephasing, i.e. $p_d = 1$. In this case, EPL-D outputs perfect EPR pairs at the distillable entanglement rate. Hence, EPL-D is then by definition optimal within EPL.

5.4.5. S STATES

We have already looked at the R state, a simple mixture of a Bell state with a product state. However, we have only considered the scenario when the product state is orthogonal to the given Bell state. As we have already seen those states are easy to both distil and filter. Specifically, we have seen that from two copies of such a state we can obtain a perfect maximally entangled state with finite probability of success and even from a single copy in the limit of zero probability of success, a perfect maximally entangled state can also be filtered. It is now interesting to see what happens if this product noise is not orthogonal to that Bell state. Hence we will now consider the state

$$\tau_{AB} = p|\Phi^+\rangle\langle\Phi^+| + (1-p)|11\rangle\langle 11|, \tag{5.50}$$

which we will call an S state.

NUMERICAL EXAMPLES

The first property of this S state that we have verified numerically is that it is less filterable than the R state, meaning that even at the expense of the probability of success it is not possible to achieve arbitrarily high output fidelity through local filtering. However, we show here that by applying the seesaw optimisation from existing schemes to such local filtering of the S state, we find a new protocol that is more suited to those states. Namely, we start from the filtering scheme described in Section 5.3.1. We see in FIG. 5.12 that the seesaw method improves the output fidelity of the original filtering protocol designed to perform well on states given in Eq. (5.10). We observe that the new protocol obtained using the seesaw method overlaps with the PPT bound which proves its optimality for the considered state.

We then investigate distillation on two copies of such an S state. We plot our numerical results in FIG. 5.13. We see that distilling these states is harder than distilling R states in the sense that the output fidelity of one is no longer achievable for any probability of success. Moreover, our interpolation scheme does not allow for deterministic increase of fidelity which we see is possible using PPT operations. The numerical results also suggest that DEJMPS protocol is optimal for distilling these states, such that it allows us to achieve the highest possible output fidelity for this protocol's probability of success when operating on these states.

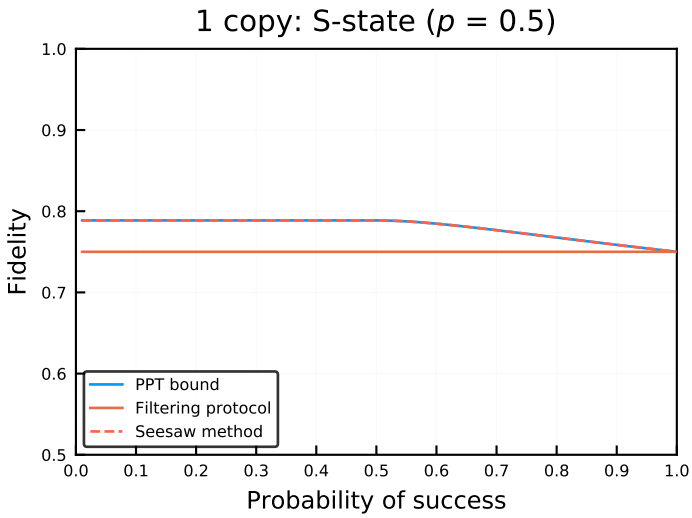

Figure 5.12: Filtering S state τ_{AB} with $D = 2$ and $p = 0.5$ in Eq. (5.50) to a two-qubit state. The fidelity of the input copy is $F_{\text{in}} = 0.75$. We see that deterministic increase of fidelity ($p_{\text{succ}} = 1$) is not possible. We also observe that the filtering scheme designed to work well for states given in Eq. (5.10) is not able to improve the fidelity of the S state for any value of the probability of success. However, after applying the seesaw method to this protocol we obtain a new filtering protocol that allows for increasing fidelity of this state. Since the curve corresponding to that protocol overlaps with the PPT bound, we see that this protocol is in fact optimal for this state. The 1-BSE bound is not included because it overlaps with the PPT bound.

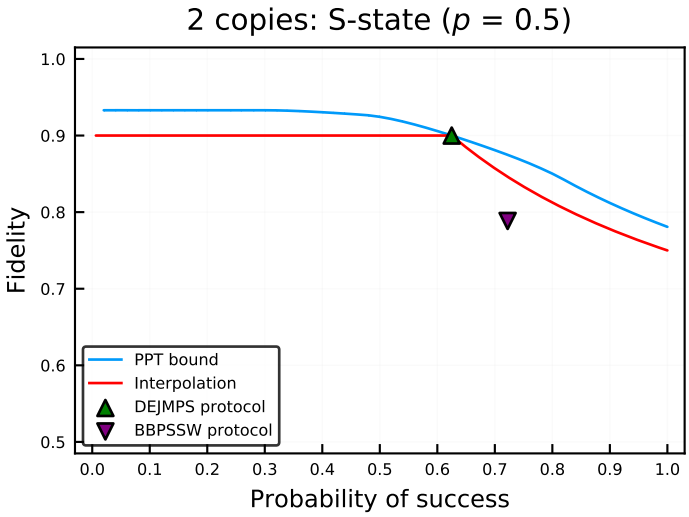

Figure 5.13: Distilling the S states $\tau_{ab}^{\otimes 2}$ with $D = 2$ and $p = 0.6$ in Eq. (5.50) to a two-qubit state. The fidelity of the input copy is $F_{\text{in}} = 0.75$ and we observe that while the extrapolation from DEJMPS does not allow for deterministic distillation (with $p_{\text{succ}} = 1$) in this case, the PPT bound still allows for this possibility. We also observe that DEJMPS allows us to achieve the highest fidelity for the corresponding probability of success. The 1-BSE bound is not included because it overlaps with the PPT bound.

5.5. DISCUSSION

We have provided and studied several methods to understand the trade-off between fidelity and probability of success in practical entanglement distillation schemes. The fidelity is thereby of interest not only because it is a commonly estimated measure in experiment, but most significantly because it bears a direct relation to the possible fidelity of teleportation using the entanglement generated [49]. Given that the deterministic transmission of qubits in present day systems relies on the heralded generation of entanglement, followed by deterministic teleportation (see e.g. [50]), the fidelity is thus of central interest in a quantum network. Evidently, it is an interesting open question to derive tradeoffs between the success probability and different entanglement measures.

Looking at the method of Bose symmetric extensions employed here, one might wonder whether one might also employ methods based on ϵ nets (see, e.g., [51]) in order to tackle our optimisation problem. Here an ϵ net is placed on the set of operations, and every point in this ϵ net is checked. Whereas this "try everything" approach seems rather trivial it does actually (in terms of ϵ) not lead to a computationally (in terms of k) more expensive optimisation than the methods of k Bose symmetric extensions when optimising over the set of separable states. We remark that while this comparison is evidently very interesting and fruitful from a complexity theoretic perspective, it is not of great practical interest for the small values of k for which it is feasible to evaluate the SDP. Here, the corresponding ϵ of the net is still very large, meaning we try out only relatively few points, leading to uninteresting solutions. In contrast, the method of k Bose

symmetric extensions actually performs not so badly even for $k = 1$ in a more practical fashion. We remark that the method of ϵ nets can of course be used to optimize over MX operations directly. It is straightforward to adapt the methods of [51] to derive conditions for optimising over the set of Choi states instead of all states, and then explore the resulting ϵ net to optimize. This evidently leads to statements on the complexity of optimising over Choi states, but does not lead to a practically realizable method which is the interest of the present article.

One might also wonder whether there exist good heuristic methods based on semidefinite programming in order to derive actual distillation schemes other than using the seesaw method starting from an existing scheme. This indeed may sound quite appealing given heuristics for imposing rank constraints on SDP variables: in our case, we could make explicit a potential ancilla that Alice and Bob may use in their distillation scheme. Fixing an ancilla of a desired maximum size, the Choi state is then pure if we include the purifying ancilla. As such, heuristics such as [52] that confine the rank of the entire state including the ancilla to be 1, approximate the set of pure states, and could thus give rise to a heuristic method for optimising over MX operations directly. In our situation, however, an implementation of [52] did not lead to any interesting results, which is why this method is omitted from this article. Nevertheless, it is an interesting open question to find good heuristic methods for optimising over the set of MX operations.

5.6. APPENDIX

5.6.1. PPT CHOI STATES

In this appendix we briefly discuss the connection between the PPT channels and PPT Choi states. The connection between the PPT channels and Jamiolkowski operator has been discussed in [21]; however here we are interested in the Choi isomorphism and so for clarity we describe this connection for the Choi isomorphism.

Following [35], we first recall the definition of a PPT operation:

Definition 5.6.1. *A quantum operation $\Psi_{AB\to\hat{A}\hat{B}}$ is a PPT operation if the superoperator $\Psi^{\Gamma}_{AB\to\hat{A}\hat{B}}$ is completely positive. Here, $\Psi^{\Gamma}_{AB\to\hat{A}\hat{B}}$ is defined such that:*

$$\Psi^{\Gamma}_{AB\to\hat{A}\hat{B}} : \rho_{AB} \to (\Psi_{AB\to\hat{A}\hat{B}}(\rho_{AB}^{\Gamma_B}))^{\Gamma_{\hat{B}}}, \tag{5.51}$$

with Γ_B and $\Gamma_{\hat{B}}$ denoting partial transposes on systems B and $\hat{B}$.

Now we can easily prove that a PPT Choi state corresponds to a PPT operation.

Lemma 5.6.2. *A quantum operation $\Psi_{AB\to\hat{A}\hat{B}}$ is a PPT operation if and only if its Choi state $C_{\hat{A}\hat{B}A'B'}(\Psi)$ is PPT.*

Proof. We use without proof the following simple observation: for every linear map $\Psi_{A\to\hat{A}}$, it follows

$$(\Psi_{A\to\hat{A}}\otimes\mathbb{1}_B)(\Phi_{AB}) = (\mathbb{1}_{\hat{A}}\otimes T_B\circ(\Psi_{\hat{B}\to B})^{\dagger}\circ T_{\hat{B}})(\Phi_{\hat{A}\hat{B}}) \tag{5.52}$$

where T denotes the transpose map and $\Psi^{\dagger}$ is the adjoint of Ψ (i.e., the unique linear map satisfying $\mathrm{tr}\left(\rho\Psi(\sigma)\right) = \mathrm{tr}\left(\sigma\Psi^{\dagger}(\rho)\right)$).

Consider the Choi matrix of the map Ψ^Γ:

$$C_{\hat{A}\hat{B}A'B'}(\Psi^\Gamma) = (\Psi^\Gamma_{AB\to\hat{A}\hat{B}} \otimes \mathbb{1}_{A'B'})\Phi_{ABA'B'} = (T_{\hat{B}} \circ \Psi_{AB\to\hat{A}\hat{B}} \circ T_B \otimes \mathbb{1}_{A'B'})\Phi_{ABA'B'} \quad (5.53)$$

$$= (T_{\hat{B}} \circ \Psi_{AB\to\hat{A}\hat{B}} \otimes T_{A'B'} \circ (T_{B'})^\dagger \circ T_{A'B'})\Phi_{ABA'B'} \quad (5.54)$$

It can be easily verified that $(T_{B'})^\dagger = T_{B'}$, so that

$$C_{\hat{A}\hat{B}A'B'}(\Psi^\Gamma) = (T_{\hat{B}} \otimes T_{B'})C_{\hat{A}\hat{B}A'B'}(\Psi) = C_{\hat{A}\hat{B}A'B'}(\Psi))^{\Gamma_{\hat{B}B'}} \quad (5.55)$$

Now it can be clearly seen that

$$(C_{\hat{A}\hat{B}A'B'}(\Psi))^{\Gamma_{\hat{B}B'}} \geq 0 \iff C_{\hat{A}\hat{B}A'B'}(\Psi^\Gamma) \geq 0 \iff \Psi^\Gamma \text{ is a completely positive map} \quad (5.56)$$

which concludes the proof. □

5.6.2. BACKGROUND: MODIFIED DISTILLATION PROTOCOLS

The well-known distillation protocols from the literature which we compare to our PPT and 1-BSE bounds have already been introduced in Section 3.3.2 in Chapter 3. However, in this chapter we have considered a more realistic version of the EPL remote entanglement generation protocol introduced in Section 3.3.2 in Chapter 3 which additionally to all the sources of noise introduced before, also includes additional dephasing noise. Hence, we restate that protocol here in this more accurate form. We also describe how we can interpolate or extrapolate new schemes from those existing ones in order to obtain schemes that allow us to succeed with arbitrary desired probability.

MODIFIED NOISE MODEL FOR EPL

In this section we will reconsider the EPL protocol described in Algorithm 4 in Section 3.3.2 in Chapter 3. In particular, here we also consider possible additional dephasing noise due to decoherence of the memories or possible drifts in the optical phase of the apparatus between the generation of the two copies. We describe the whole procedure in detail below.

Algorithm 6 EPL entanglement generation scheme

1: Generate node-photon entanglement at both remote nodes, where the photonic qubit is encoded in the presence-absence of a photon.
2: Send the photonic qubit towards a beam-splitter station in the middle.
3: Conditioned on the detection of a single photon, store the resulting state in quantum memories.
4: Repeat the above procedure to generate the second copy.
5: Assuming stability of the experimental apparatus over the time of generating those two copies, Alice and Bob share then an effective state:

$$\rho_{AB}(p,p_d) = \frac{1}{2\pi}\int d\phi \tau_{A1B1}(\phi,p,p_d)\otimes\tau_{A2B2}(\phi,p,1),$$

where

$$\tau_{AB}(\phi,p,p_d) = p\left(p_d|\Psi^+(\phi)\rangle\langle\Psi^+(\phi)| + (1-p_d)|\Psi^-(\phi)\rangle\langle\Psi^-(\phi)|\right) + (1-p)|11\rangle\langle 11|.$$

The dephasing noise corresponds to the decoherence of the quantum memories storing the first copy, while attempting to generate the second one and to the possible small drifts in the phase ϕ between the two copies.
6: Apply EPL-D distillation scheme.
7: **if** EPL-D succeeds (this occurs with probability $p_{\text{succ}} = p^2/2$) **then**
8: After Alice applies additional local rotation, we obtain a state:

$$\eta_{\hat{A}\hat{B}}(p_d) = p_d|\Phi^+\rangle\langle\Phi^+| + (1-p_d)|\Phi^-\rangle\langle\Phi^-|,$$

with fidelity p_d.
9: **return**

INTERPOLATING AND EXTRAPOLATING BETWEEN AND FROM THE FIXED SCHEMES

We note that having access to shared randomness, Alice and Bob can also apply a mixture of existing schemes. Consider two protocols with probability of success given by p_1 for the first one and p_2 for the second one. Also let the output fidelity conditioned on success be given by F_1 and F_2 for the two protocols respectively. Then if Alice and Bob share a classical coin with probability distribution $(r, 1-r)$, i.e., with probability r the coin outputs head and with probability $1-r$ it outputs tail, then they can construct a new protocol in which they first toss the coin and depending on the outcome they apply either the first or the second scheme. This new scheme has a probability of success given by:

$$p_{\text{succ}} = r\,p_1 + (1-r)\,p_2, \tag{5.57}$$

and the output fidelity conditioned on success will now be given by:

$$F = \frac{1}{p_{\text{succ}}}\left(r\,p_1F_1 + (1-r)\,p_2F_2\right). \tag{5.58}$$

It is also possible to easily extrapolate from an existing scheme. Consider a protocol that succeeds with probability p_1 with the output fidelity conditioned on success given

by F_1. Then one can also trivially achieve the same fidelity for any smaller value of p_{succ} by first performing that protocol, then conditioned on its success throwing a coin and effectively accepting the output of the protocol only for one of the outcomes of the coin.

It is also possible to extrapolate in the direction of higher probability of success. For all the considered states apart from the scenario of remote entanglement generation and R states with smaller values of the p parameter, we consider the following extrapolation scheme from a fixed protocol $\mathscr{P}$ when considering distillation from two to one copies. Alice and Bob first throw a coin with probability distribution $(r, 1-r)$ and depending on the outcome they either apply the protocol $\mathscr{P}$, which upon success occurring with probability p outputs a state of fidelity F_{out}, or they output one of the input copies of fidelity F_{in}. This scheme has a probability of success

$$p_{\text{succ}} = r\,p + (1-r), \tag{5.59}$$

and the output fidelity conditioned on success will now be given by:

$$F = \frac{1}{p_{\text{succ}}}\left(r\,p F_{\text{out}} + (1-r)F_{\text{in}}\right). \tag{5.60}$$

In the case of remote entanglement generation using EPL, the state from which we distill is not a simple tensor product of two copies and therefore the above extrapolation scheme could not be applied in this case. Hence, we then apply a different scheme. In this case Alice and Bob first apply the EPL-D protocol which upon success occurring with probability p outputs a state of fidelity F_{out}. In the case in which EPL-D fails, they throw a coin with probability distribution $(r, 1-r)$. Then for one of the coin outcomes Alice and Bob output a separable state of fidelity $1/2$, and declare failure for the other outcome. This gives

$$p_{\text{succ}} = p + (1-p)r, \tag{5.61}$$

with the output fidelity given by:

$$F = \frac{1}{p_{\text{succ}}}\left(p F_{\text{out}} + (1-p)\,r\,\frac{1}{2}\right). \tag{5.62}$$

It also turns out that for R states with $F_{\text{in}} < 2-\sqrt{2}$ it is also better in terms of output fidelities to apply this extrapolation scheme to EPL-D without interpolating with DEJMPS at all.

Finally we also describe the extrapolation-based modified filtering protocol which we apply to the states defined in Eq. (5.10) (rotated R states). In this scheme Alice and Bob apply the filtering protocol as described in Algorithm 5 in Section 3.3.2 in Chapter 3, but in the case of failure they throw a coin with probability distribution $(r, 1-r)$ and depending on the outcome they either output a state of fidelity half or declare a failure. This leads to the new overall probability of success given by $p_{\text{succ}} = p\epsilon + (1-p)\epsilon^2 + (1 - p\epsilon - (1-p)\epsilon^2)\,r$ and new output fidelity given by $F = [2p\epsilon + (1 - p\epsilon - (1-p)\epsilon^2)\,r]/2p_{\text{succ}}$. For fixed value of the probability of success one can then optimize the fidelity over ϵ and r. The result shows that the modification (throwing a coin with non zero probability of outputting a product state) helps for $p < 2/3$ for larger values of the success probability.

In particular after fixing p_{succ} the optimal output fidelity that can be obtained using this protocol is given by

$$F = \begin{cases} \frac{1}{2}\left(1+\frac{p^2}{4p_{\text{succ}}(1-p)}\right) & p \leq \frac{2}{3} \wedge p_{\text{succ}} \geq \frac{3p^2}{4(1-p)}, \\ \frac{2p}{p+\sqrt{p^2+4p_{\text{succ}}(1-p)}} & \text{otherwise.} \end{cases} \tag{5.63}$$

We note that it is the first parameter regime of the above function where probabilistically adding the product noise of fidelity half helps. The second regime corresponds to just applying the original filtering scheme. We also note that setting $p_{\text{succ}} = 1$ in the above expression we recover the result of [44] for maximum fidelity obtainable from a single copy of the R state using trace preserving LOCC operations.

5.6.3. SYMMETRY REDUCTION

If the structure of the SDP optimisation exhibits a certain symmetry we can exploit this to simplify the optimisation before actually evaluating it numerically. Inspired by the observation of Rains [21] we make a similar symmetry reduction to the main SDP in this section. Specifically, note that the target maximally entangled state Φ_D satisfies

$$\forall U, \quad U_{\hat{A}} \otimes U^*_{\hat{B}}(\Phi_D)(U_{\hat{A}} \otimes U^*_{\hat{B}})^\dagger = \Phi_D \,. \tag{5.64}$$

Let $\mathscr{T}(\cdot)$ be the twirling operation defined as

$$\mathscr{T}(\rho_{\hat{A}\hat{B}}) = \int dU (U_{\hat{A}} \otimes U^*_{\hat{B}})\rho_{AB}(U_{\hat{A}} \otimes U^*_{\hat{B}})^\dagger. \tag{5.65}$$

We can then re-express the symmetry in Eq. (5.64) as $\mathscr{T}(\Phi_D) = \Phi_D$. This means that without loss of generality our optimal solution exhibits the same symmetry, because both the constraints and objective function of the SDP in Optimisation Program 8 are invariant under the symmetry:

$$\begin{aligned} &\text{objective:} \\ \frac{|A||B|}{\delta}\operatorname{tr}\left(|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}} \otimes \rho^T_{A'B'}\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}\right) &= \frac{|A||B|}{\delta}\operatorname{tr}\left(\left(\mathscr{T}(|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}}) \otimes \rho^T_{A'B'}\right)\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}\right) \\ &= \frac{|A||B|}{\delta}\operatorname{tr}\left(\left(|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}} \otimes \rho^T_{A'B'}\right)\mathscr{T}^\dagger(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'})\right) \\ &= \frac{|A||B|}{\delta}\operatorname{tr}\left(\left(|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}} \otimes \rho^T_{A'B'}\right)\mathscr{T}(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'})\right), \\ &\text{constraints:} \\ |A||B|\operatorname{tr}\left[\left(\mathbb{I}_{\hat{A}\hat{B}} \otimes \rho^T_{A'B'}\right)\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}\right] &= |A||B|\operatorname{tr}\left[\left(\mathbb{I}_{\hat{A}\hat{B}} \otimes \rho^T_{A'B'}\right)\mathscr{T}(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'})\right] \,, \end{aligned} \tag{5.66}$$

and similarly for the other constraints. In other words, if $\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}$ is an optimal solution, then so is

$$\mathscr{T}(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}) = \int dU (U_{\hat{A}} \otimes U^*_{\hat{B}} \otimes \mathbb{I}_{A'B'})\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}(U_{\hat{A}} \otimes U^*_{\hat{B}} \otimes \mathbb{I}_{A'B'})^\dagger \,, \tag{5.67}$$

and it is intuitive that $\mathcal{T}(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'})$ contains a smaller number of variables compared to $\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}$. Thus, declaring and optimising over the variable $\mathcal{T}(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'})$ is a more efficient approach.

In order to explicitly write down the symmetry-reduced optimisation, we need to understand the structure of the twirling operation (5.65). Using the tools from representation theory of the unitary group [53] we can write

$$\begin{aligned}\mathcal{T}(\rho_{\hat{A}\hat{B}}) = \operatorname{tr}_{\hat{A}\hat{B}}\left[\rho_{\hat{A}\hat{B}}|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}}\right]|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}} \\ + \operatorname{tr}_{\hat{A}\hat{B}}\left[\rho_{\hat{A}\hat{B}}\left(\mathbb{I}-|\Phi_D\rangle\langle\Phi_D|\right)_{\hat{A}\hat{B}}\right]\frac{\mathbb{I}_{\hat{A}\hat{B}}-|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}}}{D^2-1}.\end{aligned} \tag{5.68}$$

This gives us the new form of our optimisation variable as follows

$$\begin{aligned}\mathcal{T}(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}) = \operatorname{tr}_{\hat{A}\hat{B}}\left[\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}(|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}}\otimes\mathbb{I}_{A'B'})\right]\otimes|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}} \\ + \operatorname{tr}_{\hat{A}\hat{B}}\left[\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}\left(\left(\mathbb{I}-|\Phi_D\rangle\langle\Phi_D|\right)_{\hat{A}\hat{B}}\otimes\mathbb{I}_{A'B'}\right)\right]\otimes\frac{\mathbb{I}_{\hat{A}\hat{B}}-|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}}}{D^2-1}.\end{aligned} \tag{5.69}$$

With the definitions

$$M_{A'B'} := \operatorname{tr}_{\hat{A}\hat{B}}\left[\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}(|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}}\otimes\mathbb{I}_{A'B'})\right], \tag{5.70}$$

$$E_{A'B'} := \operatorname{tr}_{\hat{A}\hat{B}}\left[\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}\left(\left(\mathbb{I}-|\Phi_D\rangle\langle\Phi_D|\right)_{\hat{A}\hat{B}}\otimes\mathbb{I}_{A'B'}\right)\right], \tag{5.71}$$

we have

$$\mathcal{T}(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}) = M_{A'B'}\otimes|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}} + E_{A'B'}\otimes\frac{\mathbb{I}_{\hat{A}\hat{B}}-|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}}}{D^2-1}\,, \tag{5.72}$$

and it is evident that we have reduced the number of variables to those contained in $M_{A'B'}$ and $E_{A'B'}$.

Now we are ready to derive the form of our SDP in terms of the new variables $M_{A'B'}$ and $E_{A'B'}$. Using (5.72) in the objective function gives

$$\frac{|A||B|}{\delta}\operatorname{tr}\left[\left(|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}}\otimes\rho^T_{A'B'}\right)\mathcal{T}\left(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}\right)\right] = \frac{|A||B|}{\delta}\operatorname{tr}\left[\rho^T_{A'B'}M_{A'B'}\right]\,. \tag{5.73}$$

Similarly, the equality constraint transforms as

$$|A||B|\operatorname{tr}\left[\left(\mathbb{I}_{\hat{A}\hat{B}}\otimes\rho^T_{A'B'}\right)\mathcal{T}(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'})\right] = |A||B|\operatorname{tr}\left[\rho^T_{A'B'}\left(M_{A'B'}+E_{A'B'}\right)\right] = \delta\,. \tag{5.74}$$

The inequality constraint $\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'}\geq 0$ becomes two inequality constraints $M_{A'B'}\geq 0$ and $E_{A'B'}\geq 0$. The PPT relaxation constraint $\hat{C}^{\Gamma}_{\checkmark,\hat{A}A'\hat{B}B'}\geq 0$ becomes

$$\begin{aligned}\mathcal{T}(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'})^{\Gamma} &= |\Phi_D\rangle\langle\Phi_D|^{\Gamma}_{\hat{A}\hat{B}}\otimes M^{\Gamma}_{A'B'} + \frac{(\mathbb{I}_{\hat{A}\hat{B}}-|\Phi_D\rangle\langle\Phi_D|_{\hat{A}\hat{B}})^{\Gamma}}{D^2-1}\otimes E^{\Gamma}_{A'B'} \\ &= \frac{1}{D}(P_{S_{\hat{A}\hat{B}}}-P_{A_{\hat{A}\hat{B}}})\otimes M^{\Gamma}_{A'B'} + \frac{\left(1-\frac{1}{D}\right)P_{S_{\hat{A}\hat{B}}}+\left(1+\frac{1}{D}\right)P_{A_{\hat{A}\hat{B}}}}{D^2-1}\otimes E^{\Gamma}_{A'B'} \\ &= P_{S_{\hat{A}\hat{B}}}\otimes\left(\frac{1}{D}M^{\Gamma}_{A'B'}+\frac{1-\frac{1}{D}}{D^2-1}E^{\Gamma}_{A'B'}\right)+P_{A_{\hat{A}\hat{B}}}\otimes\left(-\frac{1}{D}M^{\Gamma}_{A'B'}+\frac{1+\frac{1}{D}}{D^2-1}E^{\Gamma}_{A'B'}\right)\geq 0\,,\end{aligned} \tag{5.75}$$

5

where we have used $\Phi^\Gamma = (P_S - P_A)/D$ and $\mathbb{I}^\Gamma = P_S + P_A$, where P_S and P_A are projectors onto the symmetric and anti-symmetric subspace, respectively. The orthogonality of P_S and P_A allows us to read off this constraint as two inequality constraints

$$M^\Gamma_{A'B'} + \frac{1}{D+1} E^\Gamma_{A'B'} \geq 0\,, \quad -M^\Gamma_{A'B'} + \frac{1}{D-1} E^\Gamma_{A'B'} \geq 0\,. \tag{5.76}$$

Finally, the last two inequality constraints of SDP in Optimisation Program 8 become

$$M_{A'B'} + E_{A'B'} = \mathrm{tr}_{\hat{A},\hat{B}}(\mathscr{T}(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'})) = \hat{C}_{\checkmark,A'B'} \leq \frac{\mathbb{I}_{A',B'}}{|A||B|}\,, \tag{5.77}$$

$$M^\Gamma_{A'B'} + E^\Gamma_{A'B'} = (\mathrm{tr}_{\hat{A},\hat{B}}(\mathscr{T}(\hat{C}_{\checkmark,\hat{A}A'\hat{B}B'})))^\Gamma = \hat{C}^\Gamma_{\checkmark,A'B'} \leq \frac{\mathbb{I}_{A',B'}}{|A||B|}\,. \tag{5.78}$$

In summary, putting things together we obtain the following simplified SDP optimisation problem, as stated in Optimisation Program 9 in the main text:

$$\begin{array}{ll} \text{maximise} & \frac{|A||B|}{\delta}\,\mathrm{tr}\left[\rho^T_{A'B'} M_{A'B'}\right] \\ \text{subject to} & M_{A'B'} \geq 0,\, E_{A'B'} \geq 0\,, \\ & M_{A'B'} + E_{A'B'} \leq \frac{\mathbb{I}_{A'B'}}{|A||B|}\,, \\ & M^\Gamma_{A'B'} + E^\Gamma_{A'B'} \leq \frac{\mathbb{I}_{A'B'}}{|A||B|}\,, \\ & |A||B|\,\mathrm{tr}\left[\rho^T_{A'B'}(M_{A'B'} + E_{A'B'})\right] = \delta\,, \\ & M^\Gamma_{A'B'} + \frac{1}{D+1} E^\Gamma_{A'B'} \geq 0\,, \\ & -M^\Gamma_{A'B'} + \frac{1}{D-1} E^\Gamma_{A'B'} \geq 0\,. \end{array}$$

Optimisation Program 11.

5.6.4. DERIVATIONS OF DUAL SDPS

In this appendix we will use the duality relations between the primal and dual programs as explained in Section 2.3 to derive the form of the dual SDPs for optimising fidelity and probability of success.

OPTIMISING FIDELITY

The SDP in Optimisation Program 9 for finding the optimal output fidelity can be written in the primal form presented in Section 2.3 by defining:

$$A = \frac{|A||B|}{\delta}\begin{pmatrix}\rho^T & 0\\ 0 & 0\end{pmatrix},\; X = \begin{pmatrix}M & X_{12}\\ X_{12}^\dagger & E\end{pmatrix},\; B_1 = \delta,\; B_2 = \begin{pmatrix}\frac{\mathbb{I}}{|A||B|} & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & \frac{\mathbb{I}}{|A||B|}\end{pmatrix},$$

$$\Phi_1(X) = |A||B|\,\mathrm{tr}[\rho^T(M+E)], \tag{5.79}$$

$$\Phi_2(X) = \begin{pmatrix}M+E & 0 & 0 & 0\\ 0 & -M^\Gamma - \frac{1}{D+1}E^\Gamma & 0 & 0\\ 0 & 0 & M^\Gamma - \frac{1}{D-1}E^\Gamma & 0\\ 0 & 0 & 0 & M^\Gamma + E^\Gamma\end{pmatrix}.$$

Observe that the SDP induced by this choice is equivalent to the original SDP in Optimisation Program 9 because the constraint $X \geq 0$ reduces to $M \geq 0$ and $E \geq 0$ without loss of generality. More precisely, the $X \geq 0$ implies $M \geq 0$ and $E \geq 0$ so the optimum of the original SDP in Optimisation Program 9 is at least as large as the optimum of the SDP defined here. Conversely, for any feasible pair M, E of the original SDP in Optimisation Program 9 we can define a feasible X of the above SDP by setting $X_{12} = 0$ so the optimum of the original SDP in Optimisation Program 9 is at most the optimum of the above SDP.

Now in order to dualize, we need to calculate $\Phi_1^\dagger$ and $\Phi_2^\dagger$. Since Φ_1 maps to a scalar, we conclude that $Y_1 = y$ is a scalar and we must have, by definition of adjoint,

$$\operatorname{tr}[\Phi_1(X)Y_1] = |A||B|\operatorname{tr}[\rho^T(M+E)]y = \operatorname{tr}\left[X\Phi_1^\dagger(Y_1)\right], \tag{5.80}$$

from which we conclude that

$$\Phi_1^\dagger(Y_1) = |A||B|\begin{pmatrix} \rho^T y & 0 \\ 0 & \rho^T y \end{pmatrix}. \tag{5.81}$$

Turning now to Φ_2, we note that Y_2 will be a 4-by-4 block matrix and we will label the blocks as Y_2^{ij}. Observe that

$$\begin{aligned}
\operatorname{tr}[\Phi_2(X)Y_2] &= \operatorname{tr}[(M+E)Y_2^{11}] + \operatorname{tr}\left[\left(-M^\Gamma - \frac{1}{D+1}E^\Gamma\right)Y_2^{22}\right] \\
&\quad + \operatorname{tr}\left[\left(M^\Gamma - \frac{1}{D-1}E^\Gamma\right)Y_2^{33}\right] + \operatorname{tr}[(M^\Gamma + E^\Gamma)Y_2^{44}] \\
&= \operatorname{tr}[(M+E)Y_2^{11}] + \operatorname{tr}\left[\left(-M - \frac{1}{D+1}E\right)(Y_2^{22})^\Gamma\right] \\
&\quad + \operatorname{tr}\left[\left(M - \frac{1}{D-1}E\right)(Y_2^{33})^\Gamma\right] + \operatorname{tr}[(M+E)(Y_2^{44})^\Gamma].
\end{aligned} \tag{5.82}$$

With $\Phi_2^\dagger(Y_2)$ expressed as a 2-by-2 block matrix

$$\Phi_2^\dagger(Y_2) = \begin{pmatrix} W_1 & W_2 \\ W_2^\dagger & W_4 \end{pmatrix}, \tag{5.83}$$

we have

$$\operatorname{tr}\left[X\Phi_2^\dagger(Y_2)\right] = \operatorname{tr}[MW_1] + \operatorname{tr}[X_{12}^\dagger W_2] + \operatorname{tr}[X_{12}W_2^\dagger] + \operatorname{tr}[EW_4]. \tag{5.84}$$

The definition of the adjoint map, namely $\operatorname{tr}[\Phi_2(X)Y_2] = \operatorname{tr}\left[X\Phi_2^\dagger(Y_2)\right]$, allows us to directly compare (5.82) and (5.84) and read off

$$\begin{aligned}
W_1 &= Y_2^{11} - (Y_2^{22})^\Gamma + (Y_2^{33})^\Gamma + (Y_2^{44})^\Gamma, \\
W_2 &= 0, \\
W_3 &= 0, \\
W_4 &= Y_2^{11} - \frac{1}{D+1}(Y_2^{22})^\Gamma - \frac{1}{D-1}(Y_2^{33})^\Gamma + (Y_2^{44})^\Gamma.
\end{aligned} \tag{5.85}$$

Therefore, using the definition of the dual as stated in Section 2.3, the dual program becomes:

$$\begin{aligned} \text{minimize} \quad & y\delta + \tfrac{\mathrm{tr}[Y_2^{11}+Y_2^{44}]}{|A||B|} \\ \text{subject to} \quad & \begin{pmatrix} |A||B| y\rho^T + W_1 & 0 \\ 0 & |A||B| y\rho^T + W_4 \end{pmatrix} \geq \begin{pmatrix} \frac{|A||B|}{\delta}\rho^T & 0 \\ 0 & 0 \end{pmatrix}, \\ & y \in \mathbb{R}, \\ & Y_2 \geq 0 \ . \end{aligned}$$

Optimisation Program 12.

For ease of notation we will define $J = Y_2^{11}, G = Y_2^{22}, H = Y_2^{33}, K = Y_2^{44}$. The off-diagonal blocks of the matrix variable Y_2 can always be chosen to be zero and thus the dual SDP can be written as follows without loss of generality:

$$\begin{aligned} \text{minimize} \quad & y\delta + \tfrac{\mathrm{tr}[J+K]}{|A||B|} \\ \text{subject to} \quad & J, G, H, K \geq 0, y \in \mathbb{R}, \\ & |A||B|\left(y - \tfrac{1}{\delta}\right)\rho^T + J - G^\Gamma + H^\Gamma + K^\Gamma \geq 0, \\ & |A||B| y\rho^T + J - \tfrac{1}{D+1} G^\Gamma - \tfrac{1}{D-1} H^\Gamma + K^\Gamma \geq 0 . \end{aligned}$$

Optimisation Program 13.

Here all the matrices are on registers $A'B'$. Thus we have obtained the form of the dual semidefinite program for the optimal output fidelity.

OPTIMISING PROBABILITY OF SUCCESS

Similarly, we can now find the dual of the SDP in Optimisation Program 10 for optimising probability of success. Again, using the form specified in [54], we obtain:

$$A = |A||B| \begin{pmatrix} \rho^T & 0 \\ 0 & \rho^T \end{pmatrix}, \ X = \begin{pmatrix} M & X_{12} \\ X_{12}^\dagger & E \end{pmatrix}, \ B_1 = 0, \ B_2 = \begin{pmatrix} \frac{\mathbb{I}}{|A||B|} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{\mathbb{I}}{|A||B|} \end{pmatrix},$$

$$\Phi_1(X) = (1-F)\,\mathrm{tr}[\rho^T M] - F\,\mathrm{tr}[\rho^T E], \tag{5.86}$$

$$\Phi_2(X) = \begin{pmatrix} M+E & 0 & 0 & 0 \\ 0 & -M^\Gamma - \frac{1}{D+1}E^\Gamma & 0 & 0 \\ 0 & 0 & M^\Gamma - \frac{1}{D-1}E^\Gamma & 0 \\ 0 & 0 & 0 & M^\Gamma + E^\Gamma \end{pmatrix}.$$

Now we need to calculate $\Phi_1^\dagger$ and $\Phi_2^\dagger$. Since Φ_1 maps to a scalar, we conclude that $Y_1 = y$ is a scalar and we must have, by definition of adjoint:

$$\mathrm{tr}\left[\Phi_1(X), Y_1\right] = \left((1-F)\,\mathrm{tr}[\rho^T M] - F\,\mathrm{tr}[\rho^T E]\right) y = \mathrm{tr}\left[X \Phi_1^\dagger(Y_1)\right], \tag{5.87}$$

from which we conclude that:

$$\Phi_1^\dagger(Y_1) = \begin{pmatrix} (1-F) y\rho^T & 0 \\ 0 & -F y\rho^T \end{pmatrix}. \tag{5.88}$$

Turning now to Φ_2, we note that it is the same as in the program for optimising fidelity, see Eq. (5.79). Hence $\Phi_2^\dagger(Y_2)$ remains the same as given in Eq. (5.83) and in Eq. (5.85).

Therefore the dual problem becomes:

$$\begin{array}{ll} \text{minimize} & \frac{\mathrm{tr}[Y_2^{11}+Y_2^{44}]}{|A||B|} \\ \text{subject to} & \begin{pmatrix} (1-F)y\rho^T + W_1 & 0 \\ 0 & -Fy\rho^T + W_4 \end{pmatrix} \geq |A||B| \begin{pmatrix} \rho^T & 0 \\ 0 & \rho^T \end{pmatrix}, \\ & y \in \mathbb{R}, \\ & Y_2 \geq 0 \ . \end{array}$$

Optimisation Program 14.

This SDP can be rewritten as

$$\begin{array}{ll} \text{minimize} & \frac{\mathrm{tr}[J+K]}{|A||B|} \\ \text{subject to} & J, G, H, K \geq 0, y \in \mathbb{R}, \\ & [(1-F)y - |A||B|]\rho^T + J - G^\Gamma + H^\Gamma + K^\Gamma \geq 0, \\ & [-Fy - |A||B|]\rho^T + J - \frac{1}{D+1}G^\Gamma - \frac{1}{D-1}H^\Gamma + K^\Gamma \geq 0 . \end{array}$$

Optimisation Program 15.

5.6.5. k BOSE SYMMETRIC EXTENSIONS

This section details the calculations leading to the 1-BSE optimisation program mentioned in the main text. We first explain how the variable is defined for a k-BSE. Considering $\hat{C}_{(\hat{A}A')\hat{B}B'}$ to be k-BSE means that there exists $\hat{C}_{(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})\hat{B}B'}$ satisfying the BSE constraints. We are changing the optimisation variable from the former to the latter, which lives only on the symmetric subspace of $(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})$. The full Hilbert space of Alice decomposes as

$$\mathcal{H}_{(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})} = \mathcal{H}_{\mathrm{Sym}} \oplus \mathcal{H}_{\mathrm{Sym}}^\perp, \tag{5.89}$$

into symmetric subspace and its orthogonal complement. Hence, the joint Hilbert space of Alice and Bob's systems has the corresponding form

$$\mathcal{H}_{(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})\hat{B}B'} = (\mathcal{H}_{\mathrm{Sym}} \oplus \mathcal{H}_{\mathrm{Sym}}^\perp) \otimes \mathcal{H}_{\hat{B},B'} = (\mathcal{H}_{\mathrm{Sym}} \otimes \mathcal{H}_{\hat{B},B'}) \oplus (\mathcal{H}_{\mathrm{Sym}}^\perp \otimes \mathcal{H}_{\hat{B},B'}). \tag{5.90}$$

Under this decomposition, the operator $\hat{C}_{(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})\hat{B}B'}$ has the simple form

$$\hat{C}_{(\hat{A}_1A'_1)\ldots(\hat{A}_{k+1}A'_{k+1})\hat{B}B'} = \begin{pmatrix} W_s & 0 \\ 0 & 0 \end{pmatrix}, \tag{5.91}$$

with W_s being some operator acting on $\mathcal{H}_{\mathrm{Sym}} \otimes \mathcal{H}_{\hat{B},B'}$. Since our derivations in the main text are performed in the standard basis, let $U_{\mathrm{Sym}\to\mathrm{Std}}$ be the change of basis from the

"symmetric" basis to the computational basis of Alice's systems. We finally obtain the form of our new variable in the standard basis

$$\hat{C}_{(\hat{A}_1 A_1')\ldots(\hat{A}_{k+1}A_{k+1}')\hat{B}B'} = U_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B},B'} \begin{pmatrix} W_s & 0 \\ 0 & 0 \end{pmatrix} U^{\dagger}_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B},B'}. \tag{5.92}$$

In the final SDP which will be presented at the end of this section, we will only declare and optimize over the smaller variable W_s.

Now we specialize to the case of 1-BSE. Considering $\hat{C}_{(\hat{A}A')\hat{B}B'}$ to be 1-BSE means that there exists $\hat{C}_{(\hat{A}_1 A_1')(\hat{A}_2 A_2')\hat{B}B'}$ satisfying the BSE constraints. Since we have only two subsystems on Alice's side (corresponding to the indices 1 and 2), the orthogonal complement $\mathscr{H}^{\perp}_{\mathrm{Sym}}$ turns out to be the subspace consisting of antisymmetric vectors $\mathscr{H}_{\mathrm{ASym}}$. We need to compute the change of basis operator in

$$\hat{C}_{\hat{A}_1 A_1' \hat{A}_2 A_2' \hat{B}B'} = U_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B},B'} \begin{pmatrix} W_s & 0 \\ 0 & 0 \end{pmatrix} U^{\dagger}_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B},B'}. \tag{5.93}$$

In the case when the input dimensions of Alice and Bob are the same and the target is the maximally entangled state of dimension D, we have dimensions $|\hat{A}_1| = |\hat{A}_2| = |\hat{B}| = D$ and $|A_1'| = |A_2'| = |B'| = C$, so Alice's first $(\hat{A}_1 A_1')$ and second $(\hat{A}_2 A_2')$ subsystems each have dimension CD. We can construct the change of basis $U_{\mathrm{Sym}\to\mathrm{Std}}$ for $\mathbb{C}^{CD} \otimes \mathbb{C}^{CD}$ using standard techniques. Let $\{|i\rangle : i = 0,\ldots,CD\}$ denote the standard basis of a CD-dimensional system. Then the basis for the symmetric subspace on $(A_1 A_1')(A_2 A_2')$ consists of the vectors in $V_s = V_1 \cup V_2$ where

$$\begin{aligned} V_1 &= \left\{ |i\rangle_{A_1 A_1'} \otimes |i\rangle_{A_2 A_2'} \,|\, i = 0,1,\ldots,CD \right\}, \\ V_2 &= \left\{ \frac{1}{\sqrt{2}} \left(|i\rangle_{A_1 A_1'} \otimes |j\rangle_{A_2 A_2'} + |j\rangle_{A_1 A_1'} \otimes |i\rangle_{A_2 A_2'} \right) |\, i,j = 0,1,\ldots,CD \text{ and } j > i \right\}. \end{aligned} \tag{5.94}$$

Similarly, the basis for the antisymmetric subspace on $(A_1 A_1')(A_2 A_2')$ consists of the vectors in

$$V_a = \left\{ \frac{1}{\sqrt{2}} \left(|i\rangle_{A_1 A_1'} \otimes |j\rangle_{A_2 A_2'} - |j\rangle_{A_1 A_1'} \otimes |i\rangle_{A_2 A_2'} \right) |\, i,j = 0,1,\ldots,CD \text{ and } j > i \right\}. \tag{5.95}$$

The coefficients of these vectors form the entries of the matrix $U_{\mathrm{Sym}\to\mathrm{Std}}$.

We are now left with rewriting the optimisation in terms of W_s, a $\frac{(CD)^2(CD+1)}{2} \times \frac{(CD)^2(CD+1)}{2}$ matrix. The objective function

$$\frac{|A||B|}{\delta} \mathrm{tr}\left(\left(\mathbb{I}_{\hat{A}_1 A_1'} \otimes |\Phi_D\rangle\langle\Phi_D|_{\hat{A}_2,\hat{B}} \otimes \rho^{T}_{A_2' B'} \right) \left(U_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B},B'} \begin{pmatrix} W_s & 0 \\ 0 & 0 \end{pmatrix} U^{\dagger}_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B}B'} \right) \right) \tag{5.96}$$

can be rewritten as (since the trace is cyclic under permutation of operators)

$$\mathrm{tr}\left(X \begin{pmatrix} W_s & 0 \\ 0 & 0 \end{pmatrix} \right), \tag{5.97}$$

where we convert the input data written in standard basis to the "symmetric" basis

$$X = \frac{|A||B|}{\delta} U^{\dagger}_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B}B'} \left(\mathbb{I}_{\hat{A}_1 A_1'} \otimes |\Phi_D\rangle\langle\Phi_D|_{\hat{A}_2\hat{B}} \otimes \rho^{T}_{A_2' B'} \right) U_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B}B'}. \tag{5.98}$$

This means that only X_s, the component of X living in the symmetric subspace, i.e. the first $\frac{(CD)^2(CD+1)}{2}$ rows and columns of X, will appear in the objective function and the objective function becomes $\mathrm{tr}(X_s W_s)$. Similarly, the constraint on the probability of success can be rewritten as $\mathrm{tr}(Y_s W_s) = \delta$, where

$$Y = |A||B| U^\dagger_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B}B'} \left(\mathbb{I}_{\hat{A}_1 A'_1} \otimes \mathbb{I}_{\hat{A}_2\hat{B}} \otimes \rho^T_{A'_2 B'} \right) U_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B}B'}, \tag{5.99}$$

and again Y_s is just a matrix that consists of the first $\frac{(CD)^2(CD+1)}{2}$ rows and columns of Y. All other constraints become unaffected so the SDP becomes

$$\begin{aligned}
\text{maximise} \quad & \mathrm{tr}\left(X_{s\,\hat{A}_1 A'_1 \hat{A}_2 A'_2 \hat{B} B'} W_{s\,\hat{A}_1 A'_1 \hat{A}_2, A'_2, \hat{B}, B'} \right) \\
\text{subject to} \quad & \mathrm{tr}\left(Y_{s\,\hat{A}_1 A'_1 \hat{A}_2 A'_2 \hat{B} B'} W_{s\,\hat{A}_1 A'_1 \hat{A}_2 A'_2 \hat{B} B'} \right) = \delta \ , \\
& W_{s\,\hat{A}_1 A'_1 \hat{A}_2 A'_2 \hat{B} B'} \geq 0 \ , \\
& \mathrm{tr}_{\hat{A}_1 A'_1} \left(U_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B},B'} \begin{pmatrix} W_s & 0 \\ 0 & 0 \end{pmatrix} U^\dagger_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B},B'} \right)^\Gamma \geq 0 \ , \\
& \mathrm{tr}_{\hat{A}_1 A'_1 \hat{A}_2 \hat{B}} \left(U_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B}B'} \begin{pmatrix} W_s & 0 \\ 0 & 0 \end{pmatrix} U^\dagger_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B},B'} \right) \leq \frac{\mathbb{I}_{A'_2 B'}}{|A||B|} \ , \\
& \mathrm{tr}_{\hat{A}_1 A'_1 \hat{A}_2 \hat{B}} \left(U_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B}B'} \begin{pmatrix} W_s & 0 \\ 0 & 0 \end{pmatrix} U^\dagger_{\mathrm{Sym}\to\mathrm{Std}} \otimes \mathbb{I}_{\hat{B},B'} \right)^\Gamma \leq \frac{\mathbb{I}_{A'_2 B'}}{|A||B|} \ .
\end{aligned}$$

Optimisation Program 16.

In the scenario most frequently considered in this paper, that is of distillation from two to one copies of a two-qubit state, we have that $C = 4$ and $D = 2$ and so our variable W_s is a 288×288 matrix.

5.6.6. DEFINITIONS OF OPTIMALITY

In this section we introduce certain terminology that will later allow us to make precise optimality claims of the different distillation protocols. We also introduce and prove specific lemmas that later allow us to prove our optimality claims with respect to the EPL-D protocol in Appendix 5.6.8.

Let Λ denote the map corresponding to a distillation protocol and $P_\checkmark$ be the projector on the success space of the flags. We introduce the following shorthands:

$$\Psi(\Lambda, P_\checkmark, \rho) = \mathrm{tr}_F \left((\mathbb{I}_{\hat{A}\hat{B}} \otimes P_\checkmark) \Lambda_{AB\to\hat{A}\hat{B}F}(\rho) \right), \tag{5.100}$$

$$\eta(\Lambda, P_\checkmark, \rho) = \frac{\Psi(\Lambda, P_\checkmark, \rho)}{p(\Lambda, P_\checkmark, \rho)}, \tag{5.101}$$

where

$$p(\Lambda, P_\checkmark, \rho) = \mathrm{tr}(\Psi(\Lambda, P_\checkmark, \rho)). \tag{5.102}$$

That is, Ψ, η are, respectively, the unnormalised and normalised output state conditioned on success. We introduce two additional shorthands for the fidelity of Ψ and η to $|\Phi^+\rangle = |\Phi_2\rangle$, which for simplicity we will now denote as simply Φ:

$$g(\Lambda, P_\checkmark, \rho) = F\left(\Psi(\Lambda, P_\checkmark, \rho), \Phi\right), \tag{5.103}$$

$$f(\Lambda, P_\checkmark, \rho) = F\left(\eta(\Lambda, P_\checkmark, \rho), \Phi\right). \tag{5.104}$$

Note that $\eta(\Lambda, P_{\checkmark}, \rho)$ and $f(\Lambda, P_{\checkmark}, \rho)$ are defined only if $p(\Lambda, P_{\checkmark}, \rho) > 0$.

We define the optimal output fidelity $f_{\text{opt}}(\rho)$ and the optimal success probability $p_{\text{opt}}(\rho)$ when optimized over all LOCC distillation operations Λ and success projectors $P_{\checkmark}$ as follows:

$$f_{\text{opt}}(\rho) = \sup_{\Lambda \in \text{LOCC}, P_{\checkmark} | p(\Lambda, P_{\checkmark}, \rho) > 0} f(\Lambda, P_{\checkmark}, \rho) \tag{5.105}$$

and

$$p_{\text{opt}}(\rho) = \sup_{\Lambda \in \text{LOCC}, P_{\checkmark} | p(\Lambda, P_{\checkmark}, \rho) > 0 \text{ and } f(\Lambda, P_{\checkmark}, \rho) = f_{\text{opt}}(\rho)} p(\Lambda, P_{\checkmark}, \rho) \,. \tag{5.106}$$

With this notation, we introduce two different definitions of optimality:

Definition 5.6.3. *We call a protocol Λ with the success projector $P_{\checkmark}$ fidelity-optimal with respect to the quantum state ρ if*

$$f(\Lambda, P_{\checkmark}, \rho) = f_{\text{opt}}(\rho) \tag{5.107}$$

and

$$p(\Lambda, P_{\checkmark}, \rho) = p_{\text{opt}}(\rho). \tag{5.108}$$

5

We emphasise here that the above definition concerns distillation towards the maximally entangled state with $D = 2$, but it can be easily generalised to higher values of D.

Definition 5.6.4. *We call a protocol Λ with the success projector $P_{\checkmark}$ distillation-optimal with respect to the quantum state ρ if*

$$p(\Lambda, P_{\checkmark}, \rho) E_D(\eta(\Lambda, P_{\checkmark}, \rho)) = E_D(\rho), \tag{5.109}$$

where $E_D(\rho)$ is the distillable entanglement of ρ.

Note that our definition of a protocol being distillation optimal implies that no protocol can achieve a better tradeoff between success probability and distillable entanglement of the output state (Lemma 5.6.7). We recall that the distillable entanglement is defined as an optimisation over arbitrary distillation protocols and, in general, can only be achieved if Alice and Bob hold an infinite number of copies of the state ρ.

In the following, we prove several basic facts of these definitions.

Lemma 5.6.5. *Let $\rho = \sum_i \lambda_i \rho_i$ such that $\forall i, \lambda_i > 0$ and $\sum_i \lambda_i = 1$. Then,*

$$f_{\text{opt}}\left(\sum_i \lambda_i \rho_i\right) \leq \max_i f_{\text{opt}}(\rho_i). \tag{5.110}$$

Proof.

$$\begin{aligned} f_{\text{opt}}\left(\sum_i \lambda_i \rho_i\right) &= \sup_{\Lambda \in \text{LOCC}, P_{\checkmark} | p(\Lambda, P_{\checkmark}, \rho) > 0} \frac{g\left(\Lambda, P_{\checkmark}, \sum_i \lambda_i \rho_i\right)}{p\left(\Lambda, P_{\checkmark}, \sum_j \lambda_j \rho_j\right)} \\ &= \sup_{\Lambda \in \text{LOCC}, P_{\checkmark} | p(\Lambda, P_{\checkmark}, \rho) > 0} \frac{\sum_{i | p(\Lambda, P_{\checkmark}, \rho_i) > 0} \lambda_i f\left(\Lambda, P_{\checkmark}, \rho_i\right) p\left(\Lambda, P_{\checkmark}, \rho_i\right)}{\sum_j \lambda_j p\left(\Lambda, P_{\checkmark}, \rho_j\right)} \\ &\leq \max_i f_{\text{opt}}(\rho_i). \end{aligned} \tag{5.111}$$

□

Lemma 5.6.6. *Let $\rho = \sum_i \lambda_i \rho_i$ such that $\forall i, \lambda_i > 0$ and $\sum_i \lambda_i = 1$, let Λ and $P_{\checkmark}$ correspond to a distillation protocol such that $f(\Lambda, P_{\checkmark}, \rho) = f_{\text{opt}}(\rho) = \max_i f_{\text{opt}}(\rho_i)$ and let the index k be such that $f(\Lambda, P_{\checkmark}, \rho_k) = \max_i f(\Lambda, P_{\checkmark}, \rho_i)$ is unique. Then,*

$$p\left(\Lambda, P_{\checkmark}, \rho\right) \leq \lambda_k. \tag{5.112}$$

Proof. From Lemma 5.6.5 we see that we must have

$$f(\Lambda, P_{\checkmark}, \rho_k) = f_{\text{opt}}(\rho) = \max_i f_{\text{opt}}(\rho_i) = f_{\text{opt}}(\rho_k). \tag{5.113}$$

Then:

$$\begin{aligned} f_{\text{opt}}(\rho_k) &= f\left(\Lambda, P_{\checkmark}, \sum_i \lambda_i \rho_i\right) \\ &= \frac{\sum_{i|p(\Lambda,P_{\checkmark},\rho_i)>0} \lambda_i f\left(\Lambda, P_{\checkmark}, \rho_i\right) p\left(\Lambda, P_{\checkmark}, \rho_i\right)}{p\left(\Lambda, P_{\checkmark}, \rho\right)} \\ &= \frac{\lambda_k p\left(\Lambda, P_{\checkmark}, \rho_k\right)}{p\left(\Lambda, P_{\checkmark}, \rho\right)} f_{\text{opt}}(\rho_k) + \sum_{\substack{i \neq k \\ p(\Lambda,P_{\checkmark},\rho_i)>0}} \frac{\lambda_i p\left(\Lambda, P_{\checkmark}, \rho_i\right)}{p\left(\Lambda, P_{\checkmark}, \rho\right)} f(\Lambda, P_{\checkmark}, \rho_i). \end{aligned} \tag{5.114}$$

Now note that $\sum_i \lambda_i p(\Lambda, P_{\checkmark}, \rho_i)/p(\Lambda, P_{\checkmark}, \rho) = 1$ and $\forall i \neq k, f(\Lambda, P_{\checkmark}, \rho_i) < f_{\text{opt}}(\rho_k)$. That is we have a convex combination of $f_{\text{opt}}(\rho_k)$ and all the other $f(\Lambda, P_{\checkmark}, \rho_i)$ that are smaller than $f_{\text{opt}}(\rho_k)$. As this convex combination needs to equal $f_{\text{opt}}(\rho_k)$, we require that $\frac{\lambda_k p(\Lambda,P_{\checkmark},\rho_k)}{p(\Lambda,P_{\checkmark},\rho)} = 1$ and $\forall i \neq k, p\left(\Lambda, P_{\checkmark}, \rho_i\right) = 0$. This means that

$$p\left(\Lambda, P_{\checkmark}, \rho\right) = \lambda_k p\left(\Lambda, P_{\checkmark}, \rho_k\right) \leq \lambda_k. \tag{5.115}$$

□

Lemma 5.6.7. *Given a bipartite state ρ and an LOCC protocol $\Lambda_{AB\to\hat{A}\hat{B}F}$ together with a projector $P_{\checkmark}$, it holds that*

$$p(\Lambda, P_{\checkmark}, \rho) E_D(\eta(\Lambda, P_{\checkmark}, \rho)) \leq E_D(\rho). \tag{5.116}$$

Proof. Suppose that there exists $\Lambda_{AB\to\hat{A}\hat{B}F}$ together with a projector $P_{\checkmark}$ such that

$$p(\Lambda, P_{\checkmark}, \rho) E_D(\eta(\Lambda, P_{\checkmark}, \rho)) > E_D(\rho). \tag{5.117}$$

Then it would be possible to take n copies of ρ, obtain approximately $np(\Lambda, P_{\checkmark}, \rho)$ copies of $\eta(\Lambda, P_{\checkmark}, \rho)$, and for large enough n distill $np(\Lambda, P_{\checkmark}, \rho)E_D(\eta(\Lambda, P_{\checkmark}, \rho))$ EPR pairs which would be strictly larger than $nE_D(\rho)$. However, this is not possible since by definition $E_D(\rho)$ is the maximum rate at which EPR pairs can be distilled from ρ_{AB} by LOCC. □

5.6.7. BELL DIAGONAL STATES

In Section 5.4.2.2, we stated Theorem 5.4.1 and argued that the DEJMPS distillation protocol is optimal for distilling two copies of rank three Bell diagonal states. In this appendix we make this argument rigorous. The formal statement that we show is as follows:

Theorem 5.6.8. *DEJMPS is fidelity-optimal with respect to the state $\rho = \tau^{\otimes 2}$, where*

$$\tau = p_1|\Phi^+\rangle\langle\Phi^+| + p_2|\Psi^+\rangle\langle\Psi^+| + (1-p_1-p_2)|\Phi^-\rangle\langle\Phi^-|\,, \tag{5.118}$$

with $p_1 > 0.5$ and $p_1 > p_2 \geq 1 - p_1 - p_2$.

Remark 5.6.9. *Every Bell diagonal state of rank up to three can be transformed to the form in Eq. 5.118 using only local Clifford operations, hence Theorem 5.6.8 effectively applies to all Bell diagonal states of rank up to three.*

The proof is structured as follows. In Appendix 5.6.7.1, we prove some basic properties of Bell diagonal states. In Appendix 5.6.7.2, we show that DEJMPS protocol achieves $f(\text{DEJMPS}, \rho) = f_{\text{opt}}(\rho)$ for states of the form in Eq. (5.118) and we complete the argument in Appendix 5.6.7.3, where we show that the success probability for these states is $p(\text{DEJMPS}, \rho) = p_{\text{opt}}(\rho)$.

PROPERTIES OF THE BELL DIAGONAL STATES

Consider the Bell diagonal states

$$\tau = p_1|\Phi^+\rangle\langle\Phi^+| + p_2|\Psi^+\rangle\langle\Psi^+| + p_3|\Phi^-\rangle\langle\Phi^-| + (1-p_1-p_2-p_3)|\Psi^-\rangle\langle\Psi^-|. \tag{5.119}$$

Given the parameters (p_1, p_2, p_3) we have that $\text{tr}[\tau] = 1$ and the eigenvalues of τ are positive so long as $p_1, p_2, p_3 \geq 0$ and $1 - p_1 - p_2 - p_3 \geq 0$. Geometrically the set of Bell diagonal states forms a tetrahedron. Notice that $p_1 = \text{tr}\left[|\Phi^+\rangle\langle\Phi^+|\tau\right]$ and so on.

We can give an alternative parameterization for τ as follows:

$$\tau = \frac{1}{4}(\mathbb{III} + r_1 XX + r_2 YY + r_3 ZZ)\,, \tag{5.120}$$

where for Pauli matrices P_i we use the shorthand notation $P_i \otimes P_j = P_i P_j$. Notice that $r_1 = \text{tr}[XX\tau]$ and so on. The convenience of this parameterization is that

$$\tau^\Gamma = \frac{1}{4}(\mathbb{III} + r_1 XX - r_2 YY + r_3 ZZ)\,, \tag{5.121}$$

so that in these coordinates the partial transpose is a reflection. (This follows because $Y^T = -Y$ and other Pauli matrices are unaffected by transpose.) Notice that the partial transpose of a Bell diagonal state is a Bell diagonal matrix.

We can use the definitions to find

$$\begin{aligned} p_1 &= (1 + r_1 - r_2 + r_3)/4, && (5.122)\\ p_2 &= (1 + r_1 + r_2 - r_3)/4, && (5.123)\\ p_3 &= (1 - r_1 + r_2 + r_3)/4, && (5.124)\\ 1 - p_1 - p_2 - p_3 &= (1 - r_1 - r_2 - r_3)/4. && (5.125) \end{aligned}$$

These formulas make it possible to tell when τ is positive even if it is expressed in terms

of the parameters r_i. Now if we have two copies of τ we of course have

$$\begin{aligned}\tau\otimes\tau &= \frac{1}{4}(\mathbb{III}+r_1XX+r_2YY+r_3ZZ)\otimes\frac{1}{4}(\mathbb{III}+r_1XX+r_2YY+r_3ZZ)\\ &= \frac{1}{16}\big[\mathbb{IIIIII}+r_1(\mathbb{III}XX+XX\mathbb{III})+r_2(\mathbb{III}YY+YY\mathbb{III})+r_3(\mathbb{III}ZZ+ZZ\mathbb{III})\\ &+r_1^2XXXX+r_1r_2(XXYY+YYXX)+r_1r_3(XXZZ+ZZXX)\\ &+r_2^2YYYY+r_2r_3(YYZZ+ZZYY)\big].\end{aligned} \tag{5.126}$$

In the dual SDP we will restrict attention to dual variables V that have the same symmetry as the matrices $\tau\otimes\tau$; specifically,

$$\begin{aligned}V = \frac{1}{16}[&v_0\mathbb{IIIIII}+v_1(\mathbb{III}XX+XX\mathbb{III})+v_2(\mathbb{III}YY+YY\mathbb{III})+v_3(\mathbb{III}ZZ+ZZ\mathbb{III})\\ &+v_{11}XXXX+v_{12}(XXYY+YYXX)+v_{13}(XXZZ+ZZXX)\\ &+v_{22}YYYY+v_{23}(YYZZ+ZZYY)]\end{aligned} \tag{5.127}$$

and so

$$\begin{aligned}V^\Gamma = \frac{1}{16}[&v_0\mathbb{IIIIII}+v_1(\mathbb{III}XX+XX\mathbb{III})-v_2(\mathbb{III}YY+YY\mathbb{III})+v_3(\mathbb{III}ZZ+ZZ\mathbb{III})\\ &+v_{11}XXXX-v_{12}(XXYY+YYXX)+v_{13}(XXZZ+ZZXX)\\ &+v_{22}YYYY-v_{23}(YYZZ+ZZYY)]\ .\end{aligned} \tag{5.128}$$

Here Γ denotes the transpose on Bob's systems, that is on the second and fourth Pauli matrices. Notice that in this parameterization $v_{13}=\mathrm{tr}[(XXZZ)V]$ and so on. Alternatively we can expand V in terms of projections on the Bell states as follows:

$$\begin{aligned}V = &w_1|\Phi^+\rangle\langle\Phi^+||\Phi^+\rangle\langle\Phi^+|+w_2(|\Phi^+\rangle\langle\Phi^+||\Psi^+\rangle\langle\Psi^+|+|\Psi^+\rangle\langle\Psi^+||\Phi^+\rangle\langle\Phi^+|)\\ &+w_3|\Psi^+\rangle\langle\Psi^+||\Psi^+\rangle\langle\Psi^+|+w_4|\Phi^-\rangle\langle\Phi^-||\Phi^-\rangle\langle\Phi^-|\\ &+w_5(|\Phi^+\rangle\langle\Phi^+||\Phi^-\rangle\langle\Phi^-|+|\Phi^-\rangle\langle\Phi^-||\Phi^+\rangle\langle\Phi^+|)\\ &+w_6(|\Psi^+\rangle\langle\Psi^+||\Phi^-\rangle\langle\Phi^-|+|\Phi^-\rangle\langle\Phi^-||\Psi^+\rangle\langle\Psi^+|)\\ &+w_7|\Psi^-\rangle\langle\Psi^-||\Psi^-\rangle\langle\Psi^-|+w_8(|\Phi^+\rangle\langle\Phi^+||\Psi^-\rangle\langle\Psi^-|+|\Psi^-\rangle\langle\Psi^-||\Phi^+\rangle\langle\Phi^+|)\\ &+w_9(|\Psi^+\rangle\langle\Psi^+||\Psi^-\rangle\langle\Psi^-|+|\Psi^-\rangle\langle\Psi^-||\Psi^+\rangle\langle\Psi^+|)\\ &+w_{10}(|\Phi^-\rangle\langle\Phi^-||\Psi^-\rangle\langle\Psi^-|+|\Psi^-\rangle\langle\Psi^-||\Phi^-\rangle\langle\Phi^-|).\end{aligned} \tag{5.129}$$

Here we use a shorthand notation $|\psi\rangle\langle\psi|\otimes|\phi\rangle\langle\phi| = |\psi\rangle\langle\psi||\phi\rangle\langle\phi|$. In terms of this parameterization $V\geq 0$ if and only if $w_i\geq 0$ for all i.

In constructing a dual semidefinite program in the main text we consider a restricted set of V such that $V^\Gamma = V$. It is clear from Eq. (5.127) and Eq. (5.128) that the condition $V^\Gamma = V$ is equivalent to $v_2 = 0 = v_{12} = v_{23}$. Thus we require the following three conditions

$$v_2 = -w_1+w_3+w_4+2w_6-w_7-2w_8=0, \tag{5.130}$$

$$v_{12} = -w_1+w_3-w_4+2w_5+w_7-2w_9=0, \tag{5.131}$$

$$v_{23} = -w_1+2w_2-w_3+w_4+w_7-2w_{10}=0. \tag{5.132}$$

In the main text we construct a dual feasible solution for the SDP that arises in the restricted case of a Bell diagonal state where $1-p_1-p_2-p_3=0$, and therefore $p_3 = 1-p_1-p_2$. Making the definitions

$$\lambda_1 = p_1^2,\ \lambda_2 = p_1p_2,\ \lambda_3 = p_2^2,\ \lambda_4 = (1-p_1-p_2)^2,\ \lambda_5 = p_1(1-p_1-p_2),\ \lambda_6 = p_2(1-p_1-p_2), \tag{5.133}$$

we obtain

$$\begin{aligned}\tau\otimes\tau = {} & \lambda_1|\Phi^+\rangle\langle\Phi^+||\Phi^+\rangle\langle\Phi^+| + \lambda_2(|\Phi^+\rangle\langle\Phi^+||\Psi^+\rangle\langle\Psi^+| + |\Psi^+\rangle\langle\Psi^+||\Phi^+\rangle\langle\Phi^+|)\\ & + \lambda_3|\Psi^+\rangle\langle\Psi^+||\Psi^+\rangle\langle\Psi^+| + \lambda_4|\Phi^-\rangle\langle\Phi^-||\Phi^-\rangle\langle\Phi^-|\\ & + \lambda_5(|\Phi^+\rangle\langle\Phi^+||\Phi^-\rangle\langle\Phi^-| + |\Phi^-\rangle\langle\Phi^-||\Phi^+\rangle\langle\Phi^+|)\\ & + \lambda_6(|\Psi^+\rangle\langle\Psi^+||\Phi^-\rangle\langle\Phi^-| + |\Phi^-\rangle\langle\Phi^-||\Psi^+\rangle\langle\Psi^+|).\end{aligned} \tag{5.134}$$

OPTIMAL FIDELITY OF DEJMPS

We will first show that $f(\text{DEJMPS},\rho) = f_{\text{opt}}(\rho)$, when ρ consists of two copies of some Bell diagonal state of rank up to three. The dual SDP for maximizing fidelity has the form:

$$\begin{array}{ll}\text{minimize} & d(y,J,G,H,K) = y\delta + \frac{\text{tr}[J+K]}{|A||B|}\\ \text{subject to} & J,G,H,K\geq 0, y\in\mathbb{R}\,,\\ & |A||B|\left(y-\frac{1}{\delta}\right)\rho^T + J - G^\Gamma + H^\Gamma + K^\Gamma \geq 0\,,\\ & |A||B|y\rho^T + J - \frac{1}{D+1}G^\Gamma - \frac{1}{D-1}H^\Gamma + K^\Gamma \geq 0\,,\end{array}$$

Optimisation Program 17.

For rank-two and rank-three Bell diagonal states, the output fidelity of DEJMPS is $F = p_1' = p_1^2/N$, where $N = p_1^2 + (1-p_1)^2$ is the probability that the protocol succeeds. Hence we require a feasible solution of the dual program whose objective function takes the value p_1'. Here we find such a solution that is valid for all all $\delta\in(0,1]$. As an ansatz consider a solution with $y = \frac{p_1'}{\delta}$ and $J=G=K=0$. This means that the objective function takes the value p_1'. We now need to show that there exists a matrix H such that

$$H\geq 0, \tag{5.135}$$

$$\frac{|A||B|}{\delta}(p_1'-1)\rho^T + H^\Gamma \geq 0, \tag{5.136}$$

$$\frac{|A||B|}{\delta}p_1'\rho^T - H^\Gamma \geq 0, \tag{5.137}$$

To make it simpler we can assume that $H = \frac{|A||B|}{\delta}V$ and so now we need to find the matrix V such that

$$V\geq 0, \tag{5.138}$$

$$(p_1'-1)\rho^T + V^\Gamma \geq 0, \tag{5.139}$$

$$p_1'\rho^T - V^\Gamma \geq 0. \tag{5.140}$$

Since the input state in our SDP is $\rho = \tau \otimes \tau$ given by Eq. (5.134), we further restrict V by requiring that $V = V^\Gamma$. We can also ignore the transpose on $\rho_{A'B'}$ in the above equations as here we work with the Bell diagonal states. The chosen dual variable V that satisfies the above conditions can be specified as follows in terms of the coefficients in Eq. (5.129):

$$\begin{aligned} w_1 = p_1'(1-p_1)^2,\ w_2 = p_1'(1-p_1)p_2,\ w_3 = p_1' p_2^2,\ w_4 = p_1'(1-p_1-p_2)^2, \\ w_5 = p_1'(1-p_1)(1-p_1-p_2),\ w_6 = p_1' p_2(1-p_1-p_2),\ w_7 = 0 = w_8 = w_9 = w_{10}. \end{aligned} \tag{5.141}$$

Clearly $V \geq 0$ since $w_i \geq 0$ for all i. It is straightforward to check that each of equations (5.130-5.132) are satisfied and therefore $V = V^\Gamma$. Since V^Γ is diagonal in the same basis as $\rho_{A'B'}$, to verify the conditions (5.139) and (5.140) we just need to verify a set of scalar equations:

$$(p_1' - 1)\lambda_i + w_i \geq 0, \tag{5.142}$$

$$p_1'\lambda_i - w_i \geq 0, \tag{5.143}$$

where the coefficients λ_i are defined in Eq. (5.133). It is straightforward to determine that each of these equations is satisfied so long as $p_1 \geq 1/2$ as was specified originally. This shows that V defined through Eq. (5.129) and Eq. (5.141) satisfies Eq. (5.139) and Eq. (5.140) and therefore we have found a feasible solution of the dual problem for which the objective function takes the value p_1' for all values of $\delta \in (0,1]$. This proves that for all those values of δ there exists no protocol that can achieve higher fidelity than p_1', and hence DEJMPS protocol achieves the highest fidelity for two copies of all Bell diagonal states of rank up to three, when optimising over all LOCC protocols.

OPTIMAL PROBABILITY OF SUCCESS OF DEJMPS

Now we will show that DEJMPS also satisfies the second condition required for being fidelity-optimal, namely $p(\text{DEJMPS}, \rho) = p_{\text{opt}}(\rho)$. In other words, we will show that it is also not possible to achieve the output fidelity of DEJMPS with probability of success larger than that of DEJMPS. We recall that the dual SDP for the probability of success reads

$$\begin{array}{ll} \text{minimize} & \frac{\text{tr}[J+K]}{|A||B|} \\ \text{subject to} & J, G, H, K \geq 0, y \in \mathbb{R}\,, \\ & [(1-F)y - |A||B|]\rho^T + J - G^\Gamma + H^\Gamma + K^\Gamma \geq 0\,, \\ & [-Fy - |A||B|]\rho^T + J - \frac{1}{D+1}G^\Gamma - \frac{1}{D-1}H^\Gamma + K^\Gamma \geq 0\,. \end{array}$$

Optimisation Program 18.

As an ansatz we consider a solution with $J = |A||B|R$, $y = |A||B|s$ and $G = K = 0$, where

$$\begin{aligned} R = \big[& p_1^2 |\Phi^+\rangle\langle\Phi^+||\Phi^+\rangle\langle\Phi^+| + p_2^2 |\Psi^+\rangle\langle\Psi^+||\Psi^+\rangle\langle\Psi^+| + (1-p_1-p_2)^2 |\Phi^-\rangle\langle\Phi^-||\Phi^-\rangle\langle\Phi^-| \\ & + p_2(1-p_1-p_2)\left(|\Psi^+\rangle\langle\Psi^+||\Phi^-\rangle\langle\Phi^-| + |\Phi^-\rangle\langle\Phi^-||\Psi^+\rangle\langle\Psi^+|\right)\big] \end{aligned} \tag{5.144}$$

and

$$s = -\frac{N}{(1-p_1)(2p_1-1)}. \tag{5.145}$$

This means that the objective function takes the value N. We now need to show that there exists a matrix H such that

$$H \geq 0, \tag{5.146}$$

$$[(1-F)y - |A||B|]\rho^T + J + H^\Gamma \geq 0, \tag{5.147}$$

$$[-Fy - |A||B|]\rho^T + J - \frac{1}{D-1}H^\Gamma \geq 0. \tag{5.148}$$

To make it simpler we can assume that $H = |A||B|V$ and so now we need to find the matrix V such that

$$V \geq 0, \tag{5.149}$$

$$[(1-F)s - 1]\rho^T + R + V^\Gamma \geq 0, \tag{5.150}$$

$$[-Fs - 1]\rho^T + R - \frac{1}{D-1}V^\Gamma \geq 0. \tag{5.151}$$

5

Here $F = p_1'$ is the output fidelity of DEJMPS and $N = p_1^2 + (1-p_1)^2$. Again, since we work in the Bell basis with Bell diagonal states, we can ignore the transpose in the above equations. We specify the Bell coefficients of V as

$$\begin{aligned} w_1 = \frac{(1-p_1)p_1^2}{2p_1-1},\ w_2 = \frac{p_1^2 p_2}{2p_1-1},\ w_3 = \frac{p_1^2 p_2^2}{(1-p_1)(2p_1-1)},\ w_4 = \frac{p_1^2(1-p_1-p_2)^2}{(1-p_1)(2p_1-1)}, \\ w_5 = \frac{p_1^2(1-p_1-p_2)}{2p_1-1},\ w_6 = \frac{p_1^2 p_2(1-p_1-p_2)}{(1-p_1)(2p_1-1)},\ w_7 = w_8 = w_9 = w_{10} = 0. \end{aligned} \tag{5.152}$$

where w's are the Bell coefficients as expressed in the definition Eq (5.129). Now we will show that these variables satisfy all the constraints. Clearly $V \geq 0$ since $w_i \geq 0$ for all i. It is straightforward to check that each of equations (5.130-5.132) are satisfied and therefore $V = V^\Gamma$. Since V^Γ is diagonal in the same basis as $\rho_{A'B'}$, to verify the conditions (5.150) and (5.151) we just need to verify a set of scalar equations:

$$[(1-F)s - 1]\lambda_i + [R]_{ii} + w_i \geq 0, \tag{5.153}$$

$$(-Fs - 1)\lambda_i + [R]_{ii} - w_i \geq 0. \tag{5.154}$$

where the coefficients λ_i are again defined in Eq. (5.133) and $[R]_{ii}$ are the diagonal entries of R in the Bell basis.

We can easily check that for $p_1 > 0.5$, all the constraints are satisfied and so we have found a feasible solution to the dual SDP for probability of success. The value of the objective function is $\frac{\mathrm{tr}[J]}{|A||B|} = N$. Hence we have found a feasible solution of the dual minimisation problem (that provides upper bounds for achievable probability of success) that can be in fact achieved with DEJMPS. That is, we have proven that DEJMPS is also optimal with respect to probability of success. That is, for Bell diagonal states of rank up to three, it is impossible to achieve the output fidelity of DEJMPS with probability of success larger than that of DEJMPS. This concludes the proof that DEJMPS is fidelity-optimal for two copies of all Bell diagonal states of rank up to three.

5.6.8. REMOTE ENTANGLEMENT GENERATION THROUGH EPL SCHEME

Here, we show that EPL-D is the optimal distillation protocol within the EPL remote entanglement generation scheme according to our two definitions. That is, we formally state and prove Theorems 5.4.2 and 5.4.3 which we now formulate as one theorem:

Theorem 5.6.10. *EPL-D is both fidelity-optimal and distillation-optimal for states of the form:*

$$\rho_{AB}(p,p_d) = \frac{1}{2\pi}\int d\phi \tau_{A1B1}(\phi,p,p_d)\otimes\tau_{A2B2}(\phi,p,1), \tag{5.155}$$

where

$$\tau_{AB}(\phi,p,p_d) = p\left(p_d|\Psi^+(\phi)\rangle\langle\Psi^+(\phi)| + (1-p_d)|\Psi^-(\phi)\rangle\langle\Psi^-(\phi)|\right) + (1-p)|11\rangle\langle 11|. \tag{5.156}$$

We postpone the proof of fidelity-optimal to Appendix 5.6.8.1 and the proof of distillation-optimal to Appendix 5.6.8.2.

EPL-D IS FIDELITY-OPTIMAL

We note that for states of the form Eq. (5.46) the integration over the phase can be performed analytically:

$$\begin{aligned}\rho_{AB}(p,p_d) = &\frac{p^2}{4}\left[P_{\text{odd}_{A1B1}}\otimes P_{\text{odd}_{A2B2}} + (2p_d-1)(|01\rangle\langle 10|_{A1B1}\otimes|10\rangle\langle 01|_{A2B2}\right.\\ &\left.+|10\rangle\langle 01|_{A1B1}\otimes|01\rangle\langle 10|_{A2B2})\right]\\ &+\frac{(1-p)p}{2}\left[|11\rangle\langle 11|_{A1B1}\otimes P_{\text{odd}_{A2B2}} + P_{\text{odd}_{A1B1}}\otimes|11\rangle\langle 11|_{A2B2}\right]\\ &+(1-p)^2|11\rangle\langle 11|_{A1B1}\otimes|11\rangle\langle 11|_{A2B2},\end{aligned} \tag{5.157}$$

where $P_{\text{odd}} = |01\rangle\langle 01| + |10\rangle\langle 10|$ is the projector on the odd-parity subspace of the two-qubit space. Let us now permute the order of the registers to $A1A2B1B2$. After the permutation, ρ takes the following diagonal form in the standard basis:

$$\rho_{AB}(p,p_d) = \begin{pmatrix} 0_3 & & & & & & & & & & & & & & & \\ & a & & & & & & & & & & & & & & \\ & & 0_2 & & & & & & & & & & & & & \\ & & & Q & & & & & & & & & & & & \\ & & & & & 0_1 & & & & & & & & & & \\ & & & & & & & b & & & & & & & & \\ & & & & & & & & & a & & & & & & \\ & & & & & & & & & & b & & & & & \\ & & & & & & & & & & & & b & & & \\ & & & & & & & & & & & & & & c & \end{pmatrix}, \tag{5.158}$$

where 0_i denotes an $i\times i$ zero matrix, all the non filled elements are 0, and the shorthands Q, a, b, c and d stand for

$$Q = \begin{pmatrix} a & 0 & 0 & ad \\ 0 & b & 0 & 0 \\ 0 & 0 & 0 & 0 \\ ad & 0 & 0 & a \end{pmatrix}, \tag{5.159}$$

$$a = \frac{p^2}{4}, \tag{5.160}$$

$$b = \frac{1}{2}(1-p)p, \tag{5.161}$$

$$c = (1-p)^2, \tag{5.162}$$

$$d = 2p_d - 1, \tag{5.163}$$

Let

$$L(p,p_d) = \begin{pmatrix} 0_3 & & & & & & & \\ & a & & & & & & \\ & & 0_7 & & & & & \\ & & & b & & & & \\ & & & & a & & & \\ & & & & & b & & \\ & & & & & & b & \\ & & & & & & & c \end{pmatrix},$$

$$I(p,p_d) = \begin{pmatrix} 0_6 & & & & & \\ & 0 & 0 & 0 & 0 & \\ & 0 & b & 0 & 0 & \\ & 0 & 0 & 0 & 0 & \\ & 0 & 0 & 0 & 0 & \\ & & & & & 0_6 \end{pmatrix}, \tag{5.164}$$

$$F(p,p_d) = \begin{pmatrix} 0_6 & & & & & \\ & a & 0 & 0 & ad & \\ & 0 & 0 & 0 & 0 & \\ & 0 & 0 & 0 & 0 & \\ & ad & 0 & 0 & a & \\ & & & & & 0_6 \end{pmatrix}.$$

Now we can rewrite ρ as a function of L, I and F:

$$\rho_{AB}(p,p_d) = \mathrm{tr}[L]\rho^L + \mathrm{tr}[I]\rho^I + \mathrm{tr}[F]\rho^F, \tag{5.165}$$

where:

$$\rho^L = \frac{1}{\mathrm{tr}[L]}L,\ \rho^I = \frac{1}{\mathrm{tr}[I]}I,\ \rho^F = \frac{1}{\mathrm{tr}[F]}F. \tag{5.166}$$

Both ρ^L and ρ^I are diagonal in the standard basis. In consequence, the output fidelity on these states is upper bounded by 0.5. Hence by Lemma 5.6.5 we see that:

$$f_{\mathrm{opt}}\left(\rho_{AB}(p,p_d)\right) \leq f_{\mathrm{opt}}(\rho^F). \tag{5.167}$$

Note that ρ^F only has support on a bipartite two-qubit subspace:

$$\begin{aligned}\rho^F = \frac{1}{2}\,&(|01\rangle\langle 01|_A \otimes |10\rangle\langle 10|_B + d|01\rangle\langle 10|_A \otimes |10\rangle\langle 01|_B \\ &+ d|10\rangle\langle 01|_A \otimes |01\rangle\langle 10|_B + |10\rangle\langle 10|_A \otimes |01\rangle\langle 01|_B)\,.\end{aligned} \tag{5.168}$$

Hence, Alice and Bob can redefine their state according to:

$$\begin{aligned} |01\rangle_A &\to |0\rangle_A, \\ |10\rangle_A &\to |1\rangle_A, \\ |01\rangle_B &\to |1\rangle_B, \\ |10\rangle_B &\to |0\rangle_B. \end{aligned} \tag{5.169}$$

Under such local relabeling the state ρ^F becomes

$$\rho^F = p_d|\Phi^+\rangle\langle\Phi^+| + (1-p_d)|\Phi^-\rangle\langle\Phi^-|. \tag{5.170}$$

We know from [44] that it is not possible to increase the fidelity of the state in Eq. (5.170) through local filtering. In consequence,

$$f_{\text{opt}}\left(\rho_{AB}(p,p_d)\right) \leq p_d. \tag{5.171}$$

Since the output fidelity of EPL-D is exactly p_d, EPL-D achieves the optimal fidelity. Now we show that it achieves this output fidelity with the highest possible probability of success. From Lemma 5.6.6, it follows that this probability of success is upper bounded by the relative weight of ρ_F in $\rho_{AB}(p,p_d)$, which is $p^2/2$. Since EPL-D achieves the output fidelity of p_d with success probability $p^2/2$, we can conclude that it is also optimal with respect to probability of success. Hence EPL-D is fidelity-optimal for the EPL remote entanglement generation.

5

EPL-D IS DISTILLATION-OPTIMAL

Let us consider the distillable entanglement of the state in Eq. (5.157). Unfortunately, there is no straightforward way of calculating distillable entanglement. However, distillable entanglement is upper bounded by the relative entropy of entanglement [55]:

$$E_R(\rho) = \min_{\sigma\in\text{SEP}} S(\rho||\sigma), \tag{5.172}$$

where $S(\rho||\sigma)$ is the relative entropy defined as

$$S(\rho||\sigma) = \text{tr}[\rho\log\rho] - \text{tr}[\rho\log\sigma]. \tag{5.173}$$

Moreover, $S(\rho||\sigma)$ for any $\sigma \in$ SEP is an upper bound on $E_R(\rho)$ and, in consequence, on $E_D(\rho)$. Consider the separable state

$$\sigma^{\text{SEP}}_{AB}(p) = \frac{p^2}{4}P_{\text{odd}_{A1B1}} \otimes P_{\text{odd}_{A2B2}} + \frac{(1-p)p}{2}\left[|11\rangle\langle 11|_{A1B1} \otimes P_{\text{odd}_{A2B2}}\right. \tag{5.174}$$

$$\left. + P_{\text{odd}_{A1B1}} \otimes |11\rangle\langle 11|_{A2B2}\right] + (1-p)^2|11\rangle\langle 11|_{A1B1} \otimes |11\rangle\langle 11|_{A2B2}. \tag{5.175}$$

Then we can calculate

$$S(\rho_{AB}(p,p_d)||\sigma^{\text{SEP}}_{AB}(p)) = \frac{p^2}{2}(1-h(p_d)), \tag{5.176}$$

where h denotes the binary entropy function. We can conclude that $E_D(\rho_{AB}(p,p_d)) \leq \frac{p^2}{2}(1-h(p_d))$.

Now, we note that a possible distillation scheme would be to first perform the EPL-D protocol on the individual copies of the state in Eq. (5.157) and then perform the optimal achievable distillation procedure on the output states. Hence it is possible to distil EPR states from the states in Eq. (5.157) at a rate given by

$$R = p_{\text{succ,EPL-D}} E_D\left(\eta_{\hat{A}\hat{B}}(p_d)\right). \tag{5.177}$$

The success probability of EPL-D is $\frac{p^2}{2}$ and the distillable entanglement of rank-two Bell diagonal states is [48]

$$E_D\left(\eta_{\hat{A}\hat{B}}(p_d)\right) = 1 - h(p_d). \tag{5.178}$$

Hence we can conclude that $E_D(\rho_{AB}(p,p_d)) = \frac{p^2}{2}(1-h(p_d))$ and so $E_D(\rho_{AB}(p,p_d)) = p_{\text{succ,EPL-D}} E_D\left(\eta_{\hat{A}\hat{B}}(p_d)\right)$. This proves that EPL-D is distillation-optimal for EPL remote entanglement generation scheme.

REFERENCES

[1] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum repeaters: The role of imperfect local operations in quantum communication,* Physical Review Letters **81**, 5932 (1998).

[2] S. Bratzik, S. Abruzzo, H. Kampermann, and D. Bruß, *Quantum repeaters and quantum key distribution: The impact of entanglement distillation on the secret key rate,* Physical Review A **87**, 062335 (2013).

[3] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, *Rate-loss analysis of an efficient quantum repeater architecture,* Physical Review A **92**, 022357 (2015).

[4] K. G. H. Vollbrecht, C. A. Muschik, and J. I. Cirac, *Entanglement distillation by dissipation and continuous quantum repeaters,* Physical Review Letters **107**, 120502 (2011).

[5] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, *Inside quantum repeaters,* Selected Topics in Quantum Electronics, IEEE Journal of **21**, 1 (2015).

[6] N. H. Nickerson, Y. Li, and S. C. Benjamin, *Topological quantum computing with a very noisy network and local error rates approaching one percent,* Nature Communications **4**, 1756 (2013).

[7] N. H. Nickerson, J. F. Fitzsimons, and S. C. Benjamin, *Freely scalable quantum technologies using cells of 5-to-50 qubits with very lossy and noisy photonic links,* Physical Review X **4**, 041041 (2014).

[8] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, *Purification of noisy entanglement and faithful teleportation via noisy channels,* Physical Review Letters **76**, 722 (1996).

[9] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *Quantum privacy amplification and the security of quantum cryptography over noisy channels,* Physical Review Letters **77**, 2818 (1996).

[10] Z. Zhao, J.-W. Pan, and M. Zhan, *Practical scheme for entanglement concentration,* Physical Review A **64**, 014301 (2001).

[11] T. Yamamoto, M. Koashi, and N. Imoto, *Concentration and purification scheme for two partially entangled photon pairs,* Physical Review A **64**, 012304 (2001).

[12] J.-W. Pan, C. Simon, Č. Brukner, and A. Zeilinger, *Entanglement purification for quantum communication,* Nature **410**, 1067 (2001).

[13] E. T. Campbell and S. C. Benjamin, *Measurement-based entanglement under conditions of extreme photon loss,* Physical Review Letters **101**, 130502 (2008).

[14] P. G. Kwiat, S. Barraza-Lopez, A. Stefanov, and N. Gisin, *Experimental entanglement distillation and hidden non-locality,* Nature **409**, 1014 (2001).

[15] Z. Zhao, T. Yang, Y.-A. Chen, A.-N. Zhang, and J.-W. Pan, *Experimental realization of entanglement concentration and a quantum repeater,* Physical Review Letters **90**, 207901 (2003).

[16] R. Reichle, D. Leibfried, E. Knill, J. Britton, R. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, *Experimental purification of two-atom entanglement,* Nature **443**, 838 (2006).

[17] H. Takahashi, J. S. Neergaard-Nielsen, M. Takeuchi, M. Takeoka, K. Hayasaka, A. Furusawa, and M. Sasaki, *Entanglement distillation from gaussian input states,* Nature Photonics **4**, 178 (2010).

[18] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. 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**, 928 (2017).

[19] W. Dür and H. J. Briegel, *Entanglement purification and quantum error correction,* Reports on Progress in Physics **70**, 1381 (2007).

[20] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed-state entanglement and quantum error correction,* Physical Review A **54**, 3824 (1996).

[21] E. M. Rains, *A semidefinite program for distillable entanglement,* IEEE Transactions on Information Theory **47**, 2921 (2001).

[22] G. Vidal and R. F. Werner, *Computable measure of entanglement,* Physical Review A **65**, 032314 (2002).

[23] M. B. Plenio, *Logarithmic negativity: a full entanglement monotone that is not convex,* Physical Review Letters **95**, 090503 (2005).

[24] X. Wang and R. Duan, *Improved semidefinite programming upper bound on distillable entanglement,* Physical Review A **94**, 050301 (2016).

[25] M. Tomamichel, M. Berta, and J. M. Renes, *Quantum coding with finite resources,* Nature Communications **7**, 11419 (2016).

[26] F. Buscemi and N. Datta, *Distilling entanglement from arbitrary resources,* Journal of Mathematical Physics **51**, 102201 (2010).

[27] K. Fang, X. Wang, M. Tomamichel, and R. Duan, *Non-asymptotic entanglement distillation,* arXiv preprint arXiv:1706.06221 (2017).

[28] F. G. Brandao and N. Datta, *One-shot rates for entanglement manipulation under non-entangling maps,* IEEE Transactions on Information Theory **57**, 1754 (2011).

[29] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, *Long-distance quantum communication with atomic ensembles and linear optics,* Nature **414**, 413 (2001).

[30] S. D. Barrett and P. Kok, *Efficient high-fidelity quantum computation using matter qubits and linear optics,* Physical Review A **71**, 060310 (2005).

[31] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, *A complete family of separability criteria,* Physical Review A **69**, 022308 (2004).

[32] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, *Distinguishing separable and entangled states,* Physical Review Letters **88**, 187904 (2002).

[33] *EntanglementDist Julia package,* `https://github.com/StephanieWehner/EntanglementDist.jl`.

[34] N. Gisin, *Hidden quantum nonlocality revealed by local filters,* Physics Letters A **210**, 151 (1996).

[35] E. M. Rains, *Bound on distillable entanglement,* Physical Review A **60**, 179 (1999).

[36] E. M. Rains, *Rigorous treatment of distillable entanglement,* Physical Review A **60**, 173 (1999).

[37] M. Navascues, M. Owari, and M. B. Plenio, *Power of symmetric extensions for entanglement detection,* Physical Review A **80**, 052306 (2009).

[38] A. C. Doherty, *Entanglement and the shareability of quantum states,* Journal of Physics A: Mathematical and Theoretical **47**, 424004 (2014).

[39] M. M. Wolf, *Quantum channels and operations, guided tour,* (2012), available online: `https://www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/MichaelWolf/QChannelLecture.pdf`.

[40] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, *Local permutations of products of Bell states and entanglement distillation,* Physical Review A **67**, 022310 (2003).

[41] L. Ruan, W. Dai, and M. Z. Win, *Adaptive recurrence quantum entanglement distillation for two-kraus-operator channels,* Physical Review A **97**, 052332 (2018).

[42] E. T. Campbell, *How to exploit local information when distilling entanglement,* International Journal of Quantum Information **8**, 161 (2010).

[43] M. Horodecki, P. Horodecki, and R. Horodecki, *Inseparable two spin-1/2 density matrices can be distilled to a singlet form,* Physical Review Letters **78**, 574 (1997).

[44] F. Verstraete and H. Verschelde, *Optimal teleportation with a mixed state of two qubits,* Physical Review Letters **90**, 097901 (2003).

[45] C. Cabrillo, J. Cirac, P. Garcia-Fernandez, and P. Zoller, *Creation of entangled states of distant atoms by interference,* Physical Review A **59**, 1025 (1999).

[46] A. Kent, N. Linden, and S. Massar, *Optimal entanglement enhancement for mixed states,* Physical Review Letters **83**, 2656 (1999).

[47] F. Verstraete, J. Dehaene, and B. DeMoor, *Local filtering operations on two qubits,* Physical Review A **64**, 010101 (2001).

[48] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Fundamental limits of repeaterless quantum communications,* Nature Communications **8**, 15043 (2017).

[49] M. Horodecki, P. Horodecki, and R. Horodecki, *General teleportation channel, singlet fraction, and quasidistillation,* Physical Review A **60**, 1888 (1999).

[50] W. Pfaff, B. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, *et al.*, *Unconditional quantum teleportation between distant solid-state quantum bits,* Science **345**, 532 (2014).

[51] Y. Shi and X. Wu, *Epsilon-net method for optimizations over separable states,* Theoretical Computer Science **598**, 51 (2015).

[52] J. Datorro, *Convex Optimization and Euclidean Distance Geometry* (Meboo Publishing, 2015).

[53] J. Emerson, R. Alicki, and K. Życzkowski, *Scalable noise estimation with random unitary operators,* Journal of Optics B: Quantum and Semiclassical Optics **7**, S347 (2005).

[54] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).

[55] M. Horodecki, P. Horodecki, and R. Horodecki, *Limits for entanglement measures,* Physical Review Letters **84**, 2014 (2000).

6

PARAMETER REGIMES FOR A SINGLE SEQUENTIAL QUANTUM REPEATER

Filip Rozpędek [*], Kenneth Goodenough [*], Jeremy Ribeiro, Norbert Kalb, Valentina Caprara Vivoli, Andreas Reiserer, Ronald Hanson, Stephanie Wehner and David Elkouss

Quantum key distribution allows for the generation of a secret key between distant parties connected by a quantum channel such as optical fibre or free space. Unfortunately, the rate of generation of a secret key by direct transmission is fundamentally limited by the distance. This limit can be overcome by the implementation of so-called quantum repeaters. Here, we assess the performance of a specific but very natural setup called a single sequential repeater for quantum key distribution. We offer a fine-grained assessment of the repeater by introducing a series of benchmarks. *The benchmarks, which should be surpassed to claim a working repeater, are based on finite-energy considerations, thermal noise and the losses in the setup. In order to boost the performance of the studied repeaters we introduce two methods. The first one corresponds to the concept of a* cut-off, *which reduces the effect of decoherence during storage of a quantum state by introducing a maximum storage time. Secondly, we supplement the standard classical post-processing with an* advantage distillation *procedure. Using these methods, we find realistic parameters for which it is possible to achieve rates greater than each of the benchmarks, guiding the way towards implementing quantum repeaters.*

The results of this chapter have been published in Quantum Sci. Technol. 3, 034002 (2018).
[*]These authors contributed equally.

6.1. INTRODUCTION

In Chapter 3 we have already discussed that assessing quantum repeaters with respect to their ability of generating secret key provides a very natural quantification of the performance of such a quantum network. In this chapter, we evaluate a realistic setup of a so-called single sequential quantum repeater on how it performs for this specific task of quantum key distribution. The setup considers two parties which we call Alice and Bob who are spatially separated, and want to generate a shared secret key. The setup that we will investigate here was originally proposed in [1], where the authors were inspired by the memory-assisted measurement-device-independent QKD setup (MA-MDI QKD) [2]. Alice and Bob use a single sequential quantum repeater located between them, where both of them are connected to the quantum repeater by optical fibre. The repeater is composed of two quantum memories, both of which have the ability to become entangled with a photon, see FIG. 6.1. However, the repeater has a single photonic interface, which means that it can only address Alice and Bob in a sequential fashion. Examples where only one of the qubit memories has an interface to the photonic channel include modular ion traps [3] and nitrogen-vacancy centres in diamond [4–6]. The situation is similar for atoms or ions trapped in a single cavity [7]. In this case, both memories can have a photonic interface. However, typically only one of the interfaces can be active at a given moment.

As discussed in Chapter 3, the figure of merit that we have chosen to evaluate the repeater is the secret-key rate. That is, the ratio between the number of generated secret bits and the number of uses of the quantum channel connecting the two parties. The secret-key rate is a very natural quantifier of the performance of the studied scheme for the task of the secret key generation. It depends both on the success rate of the protocol as well as on the quality of the transmission. We compare the secret-key rate achievable with the repeater with a set of benchmarks that we introduce here. The most strict of these benchmarks is the capacity of the channel [8]. That is, the optimal secret-key rate achievable over optical fibre unassisted by a quantum repeater [9] as discussed in Chapter 3. The other benchmarks correspond to the optimal rates achievable with additional restrictions. In consequence, these benchmarks form a set of stepping stones towards the first quantum repeater able to produce a secure key over large distances.

The idea of assessing quantum repeaters by comparing with the optimal unassisted rates [9–16] has spurred a significant amount of research devoted to developing sophisticated repeater proposals. Analysis of practical systems that utilise only parametric down-conversion sources and optical measurement setups [17] has shown that such systems do not allow for overcoming the channel capacity, which hints at the importance of quantum memories in repeater architectures. Specific architectures that utilise entangled-photon pair sources together with multimode quantum memories have also been considered in this context [18, 19]. Their analysis suggests that the required efficiency of those entangled-photon pair sources and number of storage modes might be experimentally very challenging for implementation in the very near future. Finally, the so called all-optical repeaters that do not require quantum memories but allow to overcome the channel capacity have been proposed [20]. However, they necessitate the ability to create large photonic cluster states which are beyond current experimental capabilities.

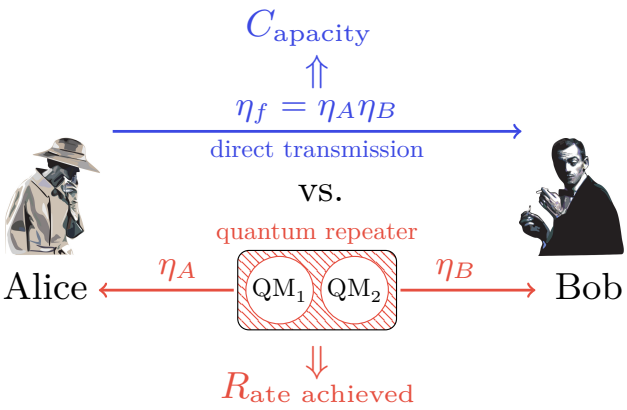

Figure 6.1: The quantum repeater will send photons entangled with the QM_1 to Alice through the optical fibre of transmissivity η_A. After receiving one photon she will perform a BB84 or six-state measurement. After Alice has measured a photon and communicated her success to the quantum repeater, the quantum repeater tries to send a photon entangled with the QM_2 to Bob through the optical fibre of transmissivity η_B. If Bob does not receive a photon within some pre-defined amount of trials (i.e. the cut-off), Alice and Bob will abort the round. This is done to prevent the state in the QM_1 from decohering excessively. If Bob does succeed, the quantum repeater performs a Bell state measurement on the two quantum memories.

A detailed analysis of a realistic, single-node proof of principle repeater that includes all the specific system imperfections has been recently performed [1]. In particular, the analysis identified parameter regimes where it would be possible to surpass the optimal direct transmission rates with a repeater scheme that is close to experimental implementation. We build upon the analysis of [1] by introducing two methods that allow us to achieve higher rates. The first of these methods is the introduction of a maximum storage time for the memories in the quantum repeater. This restriction effectively reduces the effect of decoherence. We derive tight analytical bounds for the secret-key rate as a function of the maximum storage time. In this way we can perform efficient optimisation of the secret-key rate over the maximum storage time. The second of these methods is advantage distillation [21], a two-way classical post-processing technique that allows for distilling secret key at a higher rate than achievable with only one-way post-processing.

The structure of the paper is as follows. In Section 6.2 we detail our key distribution protocol. The sources of errors, such as losses in the apparatus and noisy operations and storage, are discussed in Section 6.3. In Section 6.4, we calculate the secret-key rate that the single sequential quantum repeater would achieve. We define the benchmarks in Section 6.5, and in Section 7.6 we numerically explore the parameter regimes for which the quantum repeater implementation overcomes each benchmark and determine how the secret-key rate of the proposed protocol scales as a function of the distance. We end in Section 7.7 with some concluding remarks.

6.2. PROTOCOL FOR A SINGLE SEQUENTIAL QUANTUM REPEATER

A quantum key distribution protocol consists of two main parts. First, Alice and Bob exchange quantum signals over a quantum channel and measure them to obtain a raw key that is post-processed in a second, purely classical part into a secure key [22]. Here, we focus our interest on the entanglement-based version of the BB84 [23] and the six-state [24] protocols. In this section, we describe the first part of both key distribution protocols.

The physical setup consists of two spatially separated parties Alice and Bob connected to an intermediate repeater via optical fibre channels. We note that such a repeater does not need to be positioned exactly half-way between Alice and Bob. The repeater is composed of two qubit quantum memories which we denote by QM_1 and QM_2. The repeater is then able to generate memory-photon entanglement, where the photonic degree of freedom in which the qubits are encoded is assumed to be time-bin. Alice and Bob each have an optical detector setup that performs a BB84 or a six-state measurement. For technical reasons (see Section 6.3.2), we consider slightly different setups for BB84 and six-state. More concretely, for BB84 we consider an active setup that switches randomly between the two measurement bases, while in the six-state protocol we consider a passive setup that chooses between the three measurement bases by a passive optical construction [25].

Let us now describe a first version of the protocol without a maximum storage time. First, the quantum repeater attempts to generate an entangled qubit-qubit state between a photon and the first quantum memory QM_1, after which the photon is sent through a fibre to Alice. Such a *trial* is attempted repeatedly until a photon arrives at Alice's side, after which Alice performs either a BB84 or a six-state measurement. Second, the quantum repeater attempts to do the same on Bob's side with the second quantum memory QM_2 while the state in QM_1 is kept stored. We denote the number of trials performed until a photon arrives at Alice's and Bob's sides n_A and n_B respectively. After Bob has received and measured a photon, a Bell state measurement is performed on the two states in QM_1 and QM_2. We denote by p_{bsm} the probability that the measurement succeeds. The classical outcome of the Bell state measurement is communicated to Bob. This concludes a single *round* of the protocol. We note that in this protocol every round ends with a successful generation of one bit of raw key. Such a protocol is closely related to the memory-assisted measurement-device-independent QKD setup (MA-MDI QKD) [2]. We discuss this connection in Appendix 6.9.3.

One of the main problems in a quantum repeater implementation is that a quantum state will decohere when it is stored in a quantum memory. This means that if it takes Bob a large amount of trials to receive a photon, the state in the quantum memory QM_1 will have significantly decohered, preventing the generation of secret key. This motivates the introduction of a *cut-off*. A cut-off is a limit on the amount of trials that Bob can attempt to receive a photon. We denote this maximum number by $n^\star$.

The protocol that we consider here modifies the protocol above as follows: if in a given round Bob reaches the cut-off without success, the round is interrupted and a new round starts from the beginning with the quantum repeater again attempting to send a photon to Alice. In this scheme a large number of rounds might be required until a single bit of raw key is successfully generated. See Algorithm 7 for a description of the modified

protocol with the cut-off.

Algorithm 7 Generation of a bit of raw key with a single sequential quantum repeater

Initialize:
  $n_A \leftarrow 0,\ n_B \leftarrow 0,\ k \leftarrow 0$
loop
  $k \leftarrow k+1$ ▷ Increment the number of rounds
  repeat
    $n_A \leftarrow n_A + 1$ ▷ Increment the number of Alice's channel uses
    Generate entangled photon-QM_1 pair
    Send entangled photon through fibre towards Alice
  until Alice receives photon
  Alice performs a BB84 or a six-state measurement, stores result
  repeat
    $n_B \leftarrow n_B + 1$ ▷ Increment the number of Bob's channel uses
    Generate entangled photon-QM_2 pair
    Send entangled photon through fibre towards Bob
  until Bob receives photon or $n_B = kn^\star$
  if Bob received photon **then**
    Bob performs a BB84 or a six-state measurement, stores result
    Perform the Bell state measurement on the memories, communicate result
    Store $\max(n_A, n_B)$ ▷ Store channel uses
    return

6.3. SOURCES OF ERRORS

In this section, we model the different elements in the setup to identify the sources of losses and noise. The losses in the system are not only due to the transmissivity of the fibre; depending on the implementation a significant amount of photons is lost before they enter the fibre or due to the non-unit detector efficiency. The causes of noise are the experimental imperfections of the operations, measurements and quantum memories.

6.3.1. LOSSES

We model the process of generating and sending an entangled photon through a fibre as follows (see FIG. 6.2). First, the photon has to be generated at some photon source and be captured in the fibre. This process happens with probability p_{em}. Depending on the experimental implementation, only a fraction p_{ps} of the photons entering the fibre can be used for secret key generation. This can occur for any number of reasons, for instance photons might be filtered according to frequency or a certain time-window [6, 7]. The filtering can happen either before or after the transmission through the fibre. The fibre losses are modelled as an exponential decay of the transmissivity η_f with the distance L, i.e. $\eta_f = \exp(-\frac{L}{L_0})$ for some fibre attenuation length L_0. We denote by η_A the fibre losses on Alice's side and by η_B the fibre losses on Bob's side. Finally, the arriving photons

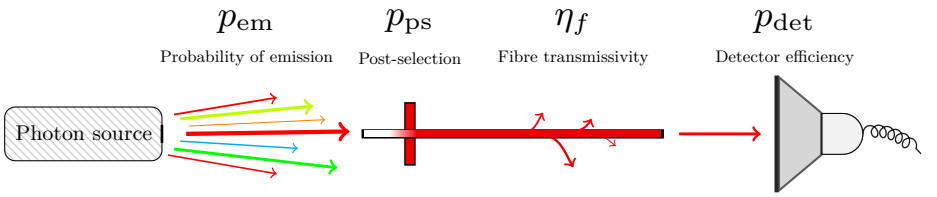

Figure 6.2: General model of all photon losses occurring in the repeater setup. p_{em} is the probability of generating and capturing a photon into the fibre. For experimental reasons a fraction $(1-p_{\text{ps}})$ of photons are additionally filtered out. The fibre has a transmissivity η_f. After exiting the fibre, the photons produce a click in the detector with probability p_{det}. The total efficiency of the apparatus is described by one parameter, $p_{\text{app}} = p_{\text{em}} p_{\text{det}}$.

will be captured by the detectors with an efficiency p_{det}. This probability of detecting a photon will be increased by the presence of dark counts (which will also inevitably add noise to the system), see the discussion of the dark counts at the bottom of this section and in Appendix 6.9.1. We define the quantity $p_{\text{app}} = p_{\text{em}} p_{\text{det}}$ describing the total efficiency of our apparatus.

6.3.2. NOISE

We model all noise processes either by the action of a dephasing channel in the Z-basis with parameter λ_1 or that of a depolarising channel with parameter λ_2 as defined in Section 2.1 in Chapter 2, specifically in Eqs. (2.7) and (2.5).

The noise processes occur due to imperfect operations, decoherence of the state while stored in QM_1 and dark counts in the detectors.

The noise from imperfect quantum operations is captured by two parameters: F_{prep} and F_{gm}. F_{prep} is a dephasing parameter which corresponds to the preparation fidelity of the memory-photon entangled state [26]. F_{gm} is a depolarising parameter that describes the noise introduced by the imperfect gates and measurements performed on the two quantum memories during the protocol [27, 28]. Hence, the noise can be modelled by a dephasing and a depolarising channel with $\lambda_1 = F_{\text{prep}}$ and $\lambda_2 = F_{\text{gm}}$.

The decoherence is modelled by a decay of the fidelity in the number of trials n. This decoherence is caused by two distinct effects. Firstly, there is the decoherence due to the time that the quantum repeater has to wait between sending photons. This time is the time it takes to confirm whether the photon got lost plus the time it takes to generate a photon entangled with the memory. We model this effect through an exponential decay of fidelity with time [29], which is expected whenever excess dephasing is suppressed (e.g. by dynamical decoupling [30]). However, we note that this is not the only possible model of decay, in several experiments a Gaussian decay has been observed [3, 31–33]. Secondly, attempting to generate an entangled photon-memory pair at QM_2 might also decohere the state stored in the QM_1. For example, this effect is the most prominent decoherence mechanism in nitrogen-vacancy implementations [5], where an exponential decay of fidelity with the number of trials was observed. This is also how we model that effect here.

The quantum state ρ that is subjected to those effects undergoes an evolution given by the dephasing and depolarising channels with $\lambda_1 = (1+e^{-an})/2$ and $\lambda_2 = e^{-bn}$. The two parameters a and b are given by

$$a = a_0 + a_1\left(\frac{2n_{\text{ri}}L_B}{c} + t_{\text{prep}}\right), \tag{6.1}$$

$$b = b_0 + b_1\left(\frac{2n_{\text{ri}}L_B}{c} + t_{\text{prep}}\right), \tag{6.2}$$

where n_{ri} is the refractive index of the fibre, c is the speed of light in vacuum, L_B the distance from the quantum repeater to Bob and t_{prep} is the time it takes to prepare for the emission of an entangled photon. Here a_0 and b_0 quantify the noise due to a single attempt at generating an entangled state and a_1 and b_1 quantify the noise during storage per second. Finally, the dark counts in the detectors introduce depolarising noise. This model is justified for the two quantum key distribution protocols that we consider, see [25, 34]. We let $\alpha_{A/B}$ denote the corresponding depolarising parameter on Alice's/Bob's side. The details of this model are presented in Appendix 6.9.1.

6.4. SECRET-KEY RATE OF A SINGLE SEQUENTIAL QUANTUM REPEATER

The secret-key rate R is defined as the amount of secret-key bits generated by a protocol divided by the number of channel uses and the number of optical modes. In the particular case of our sequential quantum repeater, the secret-key rate is given by

$$R = \frac{Y}{2}r\,. \tag{6.3}$$

The yield Y of the protocol is defined as the rate of raw bits per channel use. The secret-key fraction r is defined as the average amount of secret key that can be extracted from a single raw bit. The factor of a half is due to the fact that the encoding uses two optical modes. Since we consider two possible quantum key distribution protocols we take

$$r = \max\{r_{\text{BB84}}, r_{\text{six-state}}\}. \tag{6.4}$$

where r_{BB84} and $r_{\text{six-state}}$ are the secret-key fractions of the BB84 and six-state protocols, respectively (see Eq. (6.10) and Appendix 6.9.4).

6.4.1. YIELD

The yield can be calculated as p_{bsm} (i.e. the success probability of the Bell state measurement) divided by the (average) number of channel uses needed for the successful detection of a photon by both Alice and Bob in the same round. With a single sequential quantum repeater it is not obvious how to count the number of channel uses. As in [1], we count the *maximum* of the two channel uses on Alice's and Bob's sides respectively,

$$Y = \frac{p_{\text{bsm}}}{\mathbb{E}[N]} = \frac{p_{\text{bsm}}}{\mathbb{E}[\max(N_A, N_B)]}\,. \tag{6.5}$$

where N, N_A and N_B are the random variables that model the number of channel uses, the number of channel uses at Alice's side and the number of channel uses at Bob's side, respectively.

Without the cut-off, it is possible to obtain an analytical formula for the average number of channel uses [1, 2],

$$\mathbb{E}[\max(N_A, N_B)] = \frac{1}{p_A} + \frac{1}{p_B} - \frac{1}{p_A + p_B - p_A p_B}\,, \tag{6.6}$$

where p_A and p_B depend on the quantum key distribution protocol and are given by the following equations (see Appendix 6.9.1),

$$p_{A/B,\text{BB84}} = 1 - (1 - p_{\text{app}} p_{\text{ps}} \eta_{A/B})(1 - p_d)^2\,, \tag{6.7}$$

$$p_{A/B,\text{six-state}} = 1 - (1 - p_{\text{app}} p_{\text{ps}} \eta_{A/B})(1 - p_d)^6\,. \tag{6.8}$$

Here p_d is the probability of measuring a dark count.

Every time that Bob reaches $n^\star$ trials, Alice and Bob restart the round and start over again. The cut-off thus increases the average number of channel uses. We have developed an analytic approximation of $\mathbb{E}[N]$ which is essentially tight (see Appendix 6.9.5 for the derivation and error bounds)

$$\mathbb{E}[\max(N_A, N_B)] \approx \begin{cases} \frac{1}{p_A\left(1-(1-p_B)^{n^\star}\right)} & \frac{1}{p_A} > n^\star \\ \frac{1}{p_A} + \frac{1}{p_B} - \frac{1}{p_A + p_B - p_A p_B} & \frac{1}{p_A} \leq n^\star\,. \end{cases} \tag{6.9}$$

6

6.4.2. SECRET-KEY FRACTION

Here we consider the secret-key fraction of the BB84 and six-state protocols. As we discussed previously, we consider the BB84 protocol with an active measuring scheme and the six-state protocol with a passive one. Moreover, we consider a fully asymmetric version of BB84 and a fully symmetric version of six-state. Fully symmetric means that all bases are used with equal probability while fully asymmetric means that the ratio at which one of the bases is used is arbitrarily close to one. Finally, we consider a one-way key distillation scheme for BB84 [22] while for the six-state protocol we consider the advantage distillation scheme in [35]. Advantage distillation [21] is a classical post-processing technique that allows to increase the secret-key fraction at all levels of noise.

The reasons for not analysing the BB84 protocol with advantage distillation and the fully asymmetric six-state with advantage distillation are technical. In the case of BB84, computing the rate with advantage distillation requires the optimisation over a free parameter. The combination of the optimisation over the cut-off together with the extra free parameter was computationally too intensive to consider here.

For the six-state protocol there is, to our knowledge, no security proof that can deal with the asymmetric six-state protocol with photonic qubits without introducing extra noise [25, 36]. However, these protocol choices do not have a strong impact on our analysis. Advantage distillation does not significantly increase the amount of distillable key for low error rates. Hence, asymmetric BB84 without advantage distillation is only slightly suboptimal. For higher error rates, where advantage distillation plays a role, the symmetric six-state protocol with advantage distillation is a factor of three away from the asymmetric version.

The expression for the secret-key fraction of both protocols depends on the error rates in the X, Y and Z bases, which we denote by e_X, e_Y and e_Z. In the case of the BB84 protocol, [22, 37] it is given by

$$r_{\text{BB84}} = 1 - h(e_Z) - h(e_X)\,, \tag{6.10}$$

where $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function. The expression for $r_{\text{six-state}}$ is more complex; we leave its discussion to Appendix 6.9.4.

We can directly evaluate the error rates in each basis as a function of the general parameters of Section 6.3.2. For the single sequential quantum repeater these average errors are

$$e_X = e_Y = e_{XY} = \frac{1}{2} - \frac{1}{2}F_{\text{gm}}\alpha_A\alpha_B\left(2F_{\text{prep}} - 1\right)^2\left\langle e^{-(a+b)n}\right\rangle\,, \tag{6.11}$$

$$e_Z = \frac{1}{2} - \frac{1}{2}F_{\text{gm}}\alpha_A\alpha_B\langle e^{-bn}\rangle\,. \tag{6.12}$$

where $\langle e^{-cn}\rangle$ is the average of the exponential e^{-cn} over a geometric distribution over the first $n^\star$ trials. The detailed derivation of the error expressions is presented in Appendix 6.9.2.

6.5. BENCHMARKS FOR THE ASSESSMENT OF QUANTUM REPEATERS

We introduce a set of benchmarks to assess the performance of a quantum repeater implementation.

The first benchmark that we consider is the rate that would be achieved with the same parameters for the system losses and dark counts and for the same protocol but without a quantum repeater. Overcoming this benchmark gives the first indication that the repeater setup is useful; it means that the repeater setup outperforms the setup without repeater. We call this benchmark the direct transmission benchmark.

The remaining benchmarks represent the optimal secret-key rate that Alice and Bob could achieve if they were to communicate over the same quantum channel without a repeater under some constraints.

The optimal secret-key rate without a repeater highly depends on the channel model. The first modelling decision is the placement of the boundary between Alice's and Bob's laboratories and the quantum channel. This is because it is not *a priori* clear where the channel begins and ends. However, this decision has a strong impact on the optimal achievable rate; if the channel includes most of Alice's and Bob's laboratories, then the channel is more lossy and noisy and the benchmark is easier to overcome. If, on the other hand, the channel is just the optical fibre cable the benchmark becomes more difficult to overcome.

We consider three cases in terms of the individual lossy components of our setup (see FIG. 6.1, FIG. 6.2 and their captions):

Case 1: Fibre only, in this case the transmissivity is: $\eta = \eta_{\text{f}} = \eta_A\eta_B$.

Case 2: Fibre and different filters, then the channel transmissivity becomes: $\eta = \eta_{\text{f}}p_{\text{ps}}$.

Case 3: Fibre, filters and Alice's and Bob's apparatus, then the transmissivity becomes: $\eta = \eta_f p_{\text{ps}} p_{\text{app}}$.

Note that although in the experimental implementation of the repeater the terms p_{ps} and p_{app} appear twice in the expression of the transmissivity, they appear only once in the benchmarks which include them. The reason is that in a scenario without a repeater the emission inefficiency and the filters only affect the transmissivity once.

The second design parameter for these benchmarks is the type of channel. Transmission of photons through fibres is modelled as a pure-loss channel [38], where only a fraction η of the input photons reach the end of the channel. The first type of channel that we consider is the pure-loss channel without any additional restriction. The optimal achievable rate over one mode of the pure-loss channel is given by the secret-key capacity [9]

$$-\log_2(1-\eta)\ . \tag{6.13}$$

This is the maximum secret-key rate achievable, meaning that even if Alice and Bob had perfect unbounded quantum computers and memories, they could not generate secret key at a larger rate. If, by using a quantum repeater setup, a higher rate can be achieved than $-\log_2(1-\eta_f)$, we are certain our quantum repeater setup allowed us to do something that would be impossible with direct transmission. Surpassing the secret-key capacity has been widely used as a defining feature of a quantum repeater [1, 9–11, 17–20, 39–41]. Note that for high losses the scaling of this capacity with distance is proportional to $\eta_f = \exp\left(-\frac{L}{L_0}\right)$. At the same time with an ideal (noiseless) single quantum repeater placed half-way between Alice and Bob, the expected secret-key rate would scale proportionally to $\sqrt{\eta_f} = \exp(-\frac{L}{2L_0})$ [1].

The second type of channel that we consider is the pure-loss channel when the transmitter has a limitation in the energy that can be introduced into the channel. There has been some recent work studying the optimal rate per mode of the finite-energy pure-loss channel [11, 12, 39]. However, the optimal rate remains unknown. The bound that we consider here [39] is given by

$$g\left((1+\eta)P/2\right) - g\left((1-\eta)P/2\right)\ , \tag{6.14}$$

where $g(x) := (x+1)\log_2(x+1) - x\log_2 x$ and P is the mean photon number. In our repeater setup, the finite energy restriction arises from the fact that, on average, only a fraction of a photon enters the fibre in each trial. More precisely, the average photon number satisfies $P = p_{\text{em}}$ in cases 1 and 2 above and $P = 1$ in case 3. Unfortunately, since Eq. (6.14) is an upper bound, it is only strictly smaller than the capacity of the pure-loss channel for small mean photon number. Expanding the bounds from equations Eq. (6.13) and Eq. (6.14) around $\eta = 0$ shows that the cross-over between the two bounds occurs when $p_{\text{em}}\log_2\left(\frac{p_{\text{em}}+2}{p_{\text{em}}}\right) = \frac{1}{\ln 2}$. In other words, for high losses the finite-energy bound is tighter when $p_{\text{em}} \lesssim 0.796$. This implies that the finite-energy bound does not yield an interesting benchmark in case 3.

The third type of channel that we consider is the thermal-loss channel. An upper bound on the capacity of the thermal-loss channel is

$$-\log_2[(1-\eta)\eta^{\overline{n}}] - g\left(\overline{n}\right), \tag{6.15}$$

if $\overline{n} < \frac{\eta}{1-\eta}$ and zero otherwise [9]. Here, $\overline{n}$ is the average number of thermal photons per channel use [38]. The secret-key capacity of the thermal channel has been studied extensively [9, 11, 40–45]. This is an interesting channel because the effect of dark counts can be seen as caused by the thermal photons. Hence this type of channel becomes relevant for case 3, where detectors, and therefore also the dark counts, are regarded as part of the channel. The details of the dark count model are presented in Appendix 6.9.1. There we also show how to easily convert the experimentally relevant dark count rate of the detector and the duration of the detection window t_w into $\overline{n}$ and p_d, the probability of getting a dark count within the given time-window.

The combinations of a channel boundary together with a channel type give us a set of benchmarks. Not all combinations yield interesting benchmarks. In Table 6.1, we summarise the benchmarks that we consider.

	Infinite	Finite	Thermal	Direct transmission
Case 1: η_f	1a	1b	–	–
Case 2: $\eta_f p_{ps}$	2a	2b	–	–
Case 3: $\eta_f p_{ps} p_{app}$	–	–	3c	3d

Table 6.1: Labels of the benchmarks that we use to assess the performance of a quantum repeater. These labels are frequently referred to in the numerical results. Each row corresponds to a different channel boundary, which translates into an effective channel transmissivity. Each column corresponds to a different type of channel: pure loss, pure loss with energy constraint and thermal channel, and the final column corresponds to the direct transmission benchmark.

6.6. IMPLEMENTATION BASED ON NITROGEN-VACANCY CENTRE SETUP

Our model is fully general and can be applied to a wide range of physical platforms. To illustrate its performance we will now consider one of such potential near-term realisations of a single sequential quantum repeater. For this particular example we choose to base our system on Nitrogen-Vacancy (NV) centres in diamond. NVs are a prime candidate for this task due to their optical interface featuring high-fidelity single-shot readout [46] and their recently demonstrated capabilities to distribute spin-photon entanglement while faithfully storing quantum states [28].

In the following we expand on the required experimental techniques (see Fig. 6.3). The NV centre itself can be readily used as a generator of spin-photon entanglement at cryogenic temperatures [47]. Firstly, we generate spin-photon entanglement and send the emitted photon off to Alice who reports successful detection events back to the repeater station. Note that electron spin decoherence during communication rounds is negligible since second-long coherence times have been demonstrated by employing XY8 dynamical decoupling sequences [48].

Upon success the optical interface of the NV is reused for communication with Bob. To this end, the NV spin state that is correlated with Alice's measurement outcome is stored on a ^{13}C nuclear spin in the vicinity of the electron spin, which itself is then reinitialised [28]. We choose a configuration in which the always-on magnetic hyperfine coupling between both spins is weak (on the order of a few kHz). This configuration has

been experimentally shown to result in a highly-addressable quantum memory [49].

The protocol then proceeds as described in Section 6.2 by communicating with Bob. We note that the ^{13}C nuclear spin memory can retain coherence for thousands of remote entangling attempts despite stochastic electron spin reset operations, quasi static noise and microwave control infidelities during the subsequent probabilistic entanglement generation attempts [5, 50]. Nevertheless, these repeated communication attempts will eventually decohere the memory state due to the always-on hyperfine interaction between the two spins. This constitutes the main source of error in this system (parametrised by a_0 and b_0, see Section 6.3.2).

After a successful state transmission to Bob, we conduct a sequential two-step Bell state measurement. Specifically, in the NV node containing both the electron and carbon nuclear spin it is possible to perform a deterministic Bell-state measurement on the two spins. A combination of two nuclear-electron spin gates and two sequential electron spin state measurements reads out the combined nuclear-electron spin state in the Z- and X-bases, enabling us to discriminate all four Bell states [47].

For an NV center in free space, only ~ 3% of photons are emitted in the *zero-phonon-line* (ZPL) that can be used for secret-key generation. This poses a key challenge for a repeater implementation, since this means that the probability of successfully detecting an emitted photon is low. Therefore, we consider a setup in which the NV center is embedded in an optical cavity with a high ratio of quality factor Q to mode volume V to enhance this probability via the Purcell effect in the weak coupling regime [51]. This directly translates into a lower optical excited state lifetime that is beneficial to shorten the time-window during which we detect ZPL photons after the beam splitter, reducing the impact of dark counts on the entangled state. Additionally, a cavity introduces a preferential mode into which the ZPL photons are emitted that can be picked up efficiently. This leads to a higher expected collection efficiency than the non-cavity case [52]. Enhancement of the ZPL has been successfully implemented for different cavity architectures, including photonic crystal cavities [53–60], microring resonators [61], whispering gallery mode resonators [62, 63] and open, tunable cavities [64–66]. However, cavity-assisted entanglement generation has not yet been demonstrated for these systems, limited predominantly by broad optical lines of surface-proximal NV centers. Therefore, we focus on the open, tunable microcavity approach [67], since it has the potential of incorporating micron-scale diamond slabs inside the cavity, while allowing to keep high Q/V values and providing in-situ spatial and spectral tunability [68]. In these diamond slabs, an NV centre can be microns away from surfaces, potentially allowing to maintain bulk like optical and spin properties as needed for the considered repeater protocols. We note here that as no particular low-loss cavity design has been implemented with NVs yet, we rely purely on the aforementioned ZPL enhancement. However, more specific cavity configurations that allow for reflection based mechanisms rely on the realisation of a low-loss overcoupled cavity to be efficient [69] and might become available in the future.

6.7. NUMERICAL RESULTS

In this section, we perform a numerical analysis of our model applied to the physical system based on NV centres as described in Section 6.6. All numerical results have been

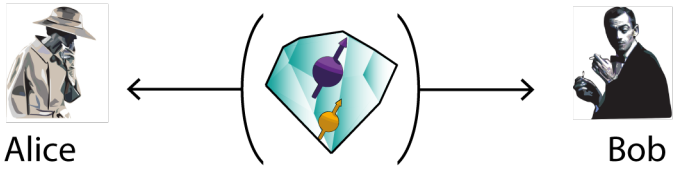

Figure 6.3: Single sequential quantum repeater based on an electron spin associated with an NV (purple) and ^{13}C nuclear spin (orange) in diamond. The previous quantum memories $QM_{1,2}$ are now represented by the electron and nuclear spin respectively. The optical interface of the NV is strongly Purcell-enhanced by an optical cavity with low-mode volume and allows for efficient photon transmission to Alice and Bob.

obtained using a Mathematica notebook. [70]. Unless specified otherwise, we use the following parameters that we call "expected parameters". These parameters represent best-case scenarios from the chosen references. These experimental capabilities do not fundamentally contradict or exclude each other and seem therefore achievable in a single experimental NV setup.

- a_0 (dephasing due to interaction) = $\frac{1}{2000}$ per attempt [5, 50],
- a_1 (dephasing with time) = $\frac{1}{3}$ per second [71],
- b_0 (depolarisation due to interaction) = $\frac{1}{5000}$ per attempt [5],
- b_1 (depolarisation with time) = $\frac{1}{3}$ per second [71],
- t_{prep} (memory-photon entanglement preparation time) = 6 μs [72],
- F_{gm} (depolarising parameter for gates and measurements) = 0.9 [28],
- F_{prep} (dephasing parameter for the memory-photon state preparation) = 0.99 [72],
- p_{em} (probability of emission) = 0.49 [52, 72],
- p_{ps} (post-selection) = 0.46 [66],
- p_{det} (detector efficiency) = 0.8 [72],
- p_{bsm} (Bell state measurement success probability) = 1 [47],
- Dark count rate = 10 per second [72],
- t_{w} (detection window) = 30 ns [72],
- L_0 (attenuation length) = 0.542 km [72],
- n_{ri} (refractive index of the fibre) = 1.44 [73].

Before we present the results, we note that the emission frequency of the nitrogen-vacancy centres results in a relatively low L_0 which in turn does not allow to achieve large distances. In practical quantum key distribution networks, assuming that dedicated fibres are used for which one can choose which frequency mode one wants to transmit at, this problem might be overcome using the frequency conversion of the emitted photons into a telecom frequency, which will yield an increased L_0. Note that the benchmarks in Table 6.1 will scale accordingly. There is a range of frequencies used in fibre-based communication and for each of those frequencies the attenuation length varies greatly depending on the type of the fibre used. To give some examples, the best fibres at 1560 nm have losses of 0.1419 dB/km ($L_0 \approx 30.6$ km) [74], while at 1310 nm standard single-mode fibres exhibit losses of 0.4 dB/km ($L_0 \approx 10.9$ km) [75]. Clearly our model is general and can be applied to a channel with any value of L_0. Here, throughout most of this section, we consider the transmission through the channel at the same wavelength as the emission line of the NV-centre setup, as such a channel for this specific physical system has been realised in an experiment [72] using fibre with losses of 8 dB/km ($L_0 = 0.542$ km as given in the list of parameters above). At the end we present an additional plot describing the scenario in which a telecom channel with the commonly used in the quantum repeater community attenuation length of $L_0 \approx 22$ km is available. In this case the frequency conversion of the emitted photons to telecom is applied.

Tightness of the error bounds for the secret-key rate. We have derived upper and lower bounds on the yield, and thus also on the secret-key rate, for the two studied protocols. In FIG. 6.4, we plot both the upper and the lower bound on the achieved rate with the current and improved parameters ($p_{\text{ps}} = p_{\text{em}} = 0.6$ and $F_{\text{gm}} = 0.97$) and optimised cut-off as a function of the distance in units of L_0. There are two regimes visible on the plot. This is a consequence of the fact that our bounds have a different analytical form in the two regimes (see Appendix 6.9.5). Since for practical purposes our bounds are essentially tight, from now on we will refer to the upper bound as the expected secret-key rate, and will omit the lower bound for the legibility of the plots.

The impact of the cut-off on the secret-key rate. In FIG. 6.5 we plot the secret-key rate versus the cut-off for different sets of parameters. The repeater is assumed to be positioned half-way between Alice and Bob. We observe a strong dependency of the secret-key rate on the cut-off. In particular, for large cut-off the secret-key rate drops to zero. This is due to the inclusion of rounds where the state has significantly decohered. This implies that the cut-off is essential for generating a key at large distances. Moreover, we observe that the optimal cut-off highly depends on the explored parameter regime.

Optimal positioning of the repeater. The asymmetry of the studied sequential protocol raises the question of whether it is best to position the repeater half-way between Alice and Bob. In fact, in the absence of a cut-off this is not the case [1]. For sufficiently large distances, shifting the repeater towards Bob can increase both the secret-key rate and the distance over which the secret-key rate is non-zero in the presence of dark counts. Specifically, the optimal positioning remains a fixed distance away from Bob independently of the actual total distance. Here, we find that with the cut-off and for the parameters considered this phenomenon disappears. We see in FIG. 6.6 that the optimal position with the cut-off optimisation appears to be exactly in the middle of Alice and Bob. Nevertheless, we note that the bounds for the yield derived in Appendix 6.9.5

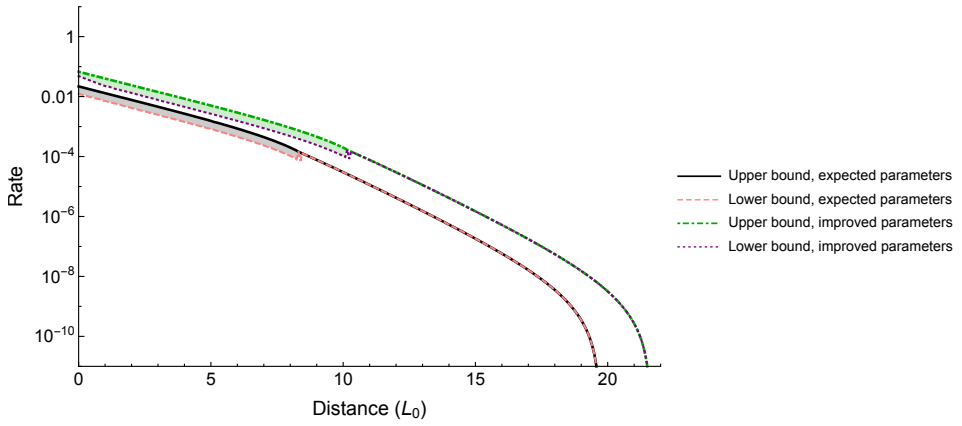

Figure 6.4: Upper- and lower bounds on the secret-key rate rate with a quantum repeater as a function of the distance in units of $L_0 = 0.542$ km. The repeater is positioned half-way between Alice and Bob. The curves correspond to the expected and improved parameters with optimised cut-off. The improved parameters correspond to setting $p_{\text{ps}} = p_{\text{em}} = 0.6$ and $F_{\text{gm}} = 0.97$. For high losses, the upper- and lower bounds become essentially tight. For this reason, the upper bound on the achieved rate forms a reliable estimate of the secret-key rate.

are valid under the condition $\eta_B \geq \eta_A$. This means that we can only study the effect of moving the repeater towards Bob. However, we do not expect any benefit in shifting the repeater towards Alice as this could only increase the noise due to decoherence. From now on for the scenarios with the cut-off optimisation, we always consider the repeater to be placed half-way between Alice and Bob. Interestingly, in FIG. 6.6 we also see that the rates for the two scenarios with and without the cut-off start to coincide after the quantum repeater is shifted within a certain distance of Bob. Intuitively this happens when the probability of Bob getting a photon is large enough so that the significance of the cut-off becomes marginal.

Cut-off versus no cut-off. Having established the optimal positioning of the repeater, we can now compare the two scenarios: optimised cut-off with middle positioning of the repeater and no cut-off with optimised positioning. We find that in the absence of dark counts the scaling with distance of both schemes is the same, with a small advantage of the cut-off scheme. However, the cut-off is more robust against dark counts. Hence, for imperfect detectors the cut-off allows distributing keys at larger distances. These results can be seen in FIG. 6.7 and FIG. 6.8, which show the secret-key rate as a function of distance for detectors without and with dark counts, together with the channel capacity of the optical fibre (i.e. benchmark 1a). We plot the data for the expected and improved parameters ($p_{\text{ps}} = p_{\text{em}} = 0.6$ and $F_{\text{gm}} = 0.97$).

In FIG. 6.7 where we assume no dark counts, we see that for small distances the rate scales approximately with the square root of the transmissivity for both scenarios. That is, they are proportional to the theoretical optimum [1] of $\sqrt{\eta_f} = e^{-L/2L_0}$. For sufficiently

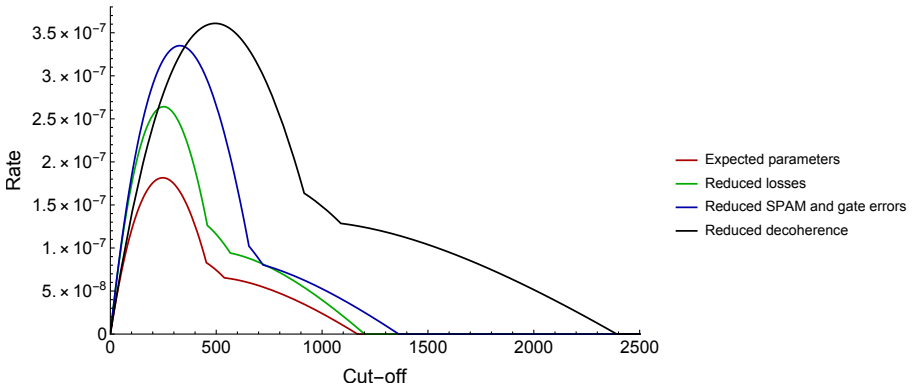

Figure 6.5: Secret-key rate as a function of the cut-off for the expected parameters with the repeater positioned half-way between Alice and Bob. The reduced losses are for $p'_{\text{app}} = (p_{\text{app}})^{0.9}$ and $p'_{\text{ps}} = (p_{\text{ps}})^{0.9}$, the reduced SPAM (state preparation and measurement) and gate errors are for $F'_{\text{gm}} = (F_{\text{gm}})^{0.7}$ and $F'_{\text{prep}} = (F_{\text{prep}})^{0.7}$ and the reduced decoherence is for $a' = a/2$ and $b' = b/2$. The optimal $n^\star$ shifts depending on the parameters. The kinks arise due to the fact that we optimise over two protocols: fully asymmetric BB84 and symmetric six-state protocol with advantage distillation which itself consists of two subprotocols. The optimal protocol depends on the bit error rates. The data have been plotted for the distance of $15L_0$, where $L_0 = 0.542$ km.

large distances time-dependent decoherence of the memory QM_1 becomes a problem. Both schemes overcome it at the expense of reducing the yield. As a result, the scaling becomes proportional to $\eta_f = e^{-L/L_0}$ for both schemes. In FIG. 6.8 however we see that the presence of dark counts affects the two schemes quite differently. While for both schemes the effect of dark counts becomes the dominant source of noise after a certain distance, this distance is shorter for the no cut-off scheme than for the scheme with the cut-off. In other words, we see that the cut-off is more robust towards dark counts than the repositioning method. This fact can be explained by noting that shifting the repeater towards Bob increases the losses on Alice's side and as a result makes the Alice-repeater link vulnerable to dark counts. With the cut-off however, the repeater remains in the middle making both of the individual links Alice-repeater and repeater-Bob shorter than the Alice-repeater link in the no cut-off scheme. As a result the setup with the cut-off and with the improved parameters allows us to overcome the channel capacity (1a) more confidently and over larger range of distances, than without the cut-off.

Comparison with the proposed benchmarks. Let us now investigate the secret-key rate achievable with the expected parameters and how it compares with the proposed benchmarks. The comparison is depicted in FIG. 6.9. The benchmarks corresponding to direct transmission (3d), the thermal-loss channel (3c) and the pure-loss channel with energy constraint and inclusion of post-selection (2b) are outperformed. The achievable secret-key rate is also very close to the pure-loss channel benchmark with post-selection

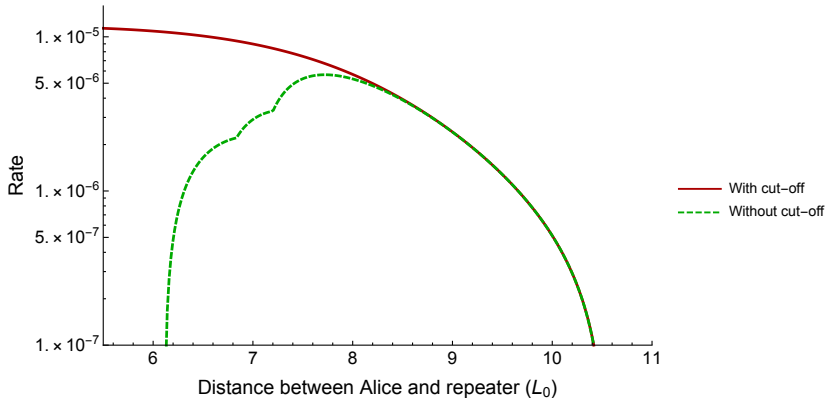

Figure 6.6: Secret-key rate with and without the cut-off as a function of the distance in units of $L_0 = 0.542$ km between Alice and quantum repeater. The total distance between Alice and Bob is fixed to $11L_0$. We see that with the cut-off optimisation, positioning the repeater half-way between Alice and Bob is optimal. This behaviour was also observed for other parameter regimes. This result contrasts with the optimal positioning for the no cut-off scenario, for which we see that shifting the repeater towards Bob is beneficial. We also note that the two rates overlap when the repeater is shifted towards Bob.

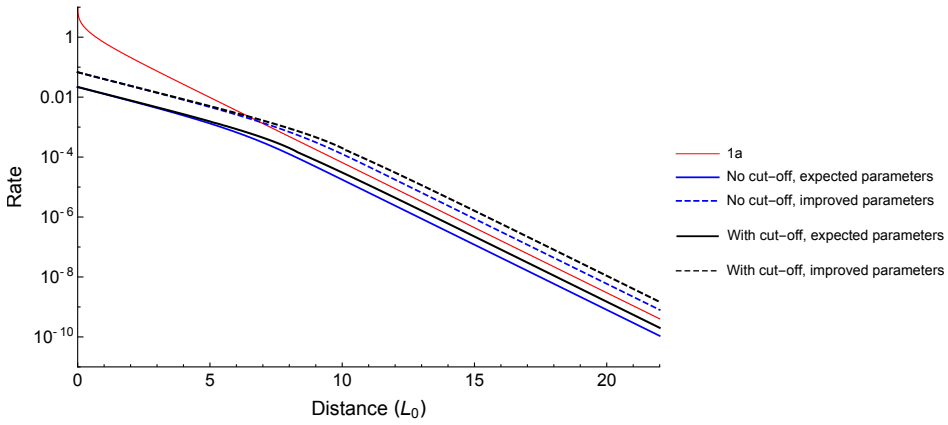

Figure 6.7: Secret-key rate as a function of the distance in units of $L_0 = 0.542$ km, assuming detectors without dark counts. The black lines correspond to the protocol with cut-off and the blue lines to the protocol without the cut-off but with optimised positioning of the repeater. We plot the data for both the expected and improved parameters. The improved parameters correspond to setting $p_{\text{ps}} = p_{\text{em}} = 0.6$ and $F_{\text{gm}} = 0.97$. Finally, the channel capacity (1a) is also included for comparison. It can be seen that both the cut-off and repositioning of the repeater allows to generate key for all distances.

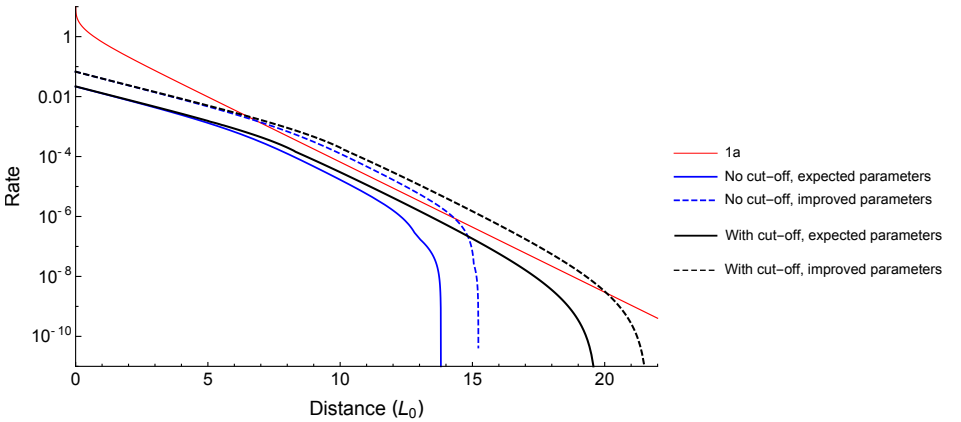

Figure 6.8: Secret-key rate as a function of the distance in units of $L_0 = 0.542$ km with dark counts. The black lines correspond to the protocol with cut-off and the blue lines to the protocol without the cut-off but with optimised positioning of the repeater. We plot the data for both the expected and improved parameters. The improved parameters correspond to setting $p_{\text{ps}} = p_{\text{em}} = 0.6$ and $F_{\text{gm}} = 0.97$. Finally, the channel capacity (1a) is also included for comparison. It can be seen that the protocol with the cut-off is more robust against dark counts than the protocol without the cut-off.

(2a). The other benchmarks are not overcome but are within experimental reach.

Parameter trade-off. Let us now give a general overview of how good the improved parameters need to be in order to overcome individual benchmarks. This information is presented on two contour plots. In FIG. 6.10, we study the parameter regions for which it is possible to beat the benchmarks in Table 6.1 as a function of p_{ps} and p_{em}. A similar plot as a function of F_{gm} and p_{em} can be seen in FIG. 6.11. We omit here the direct transmission benchmark which, as we have already seen, can be easily surpassed with the expected parameters. Moreover, we note that the capacity of the thermal channel in the benchmark (3c) goes to zero for very low p_{ps} and p_{em} for which it is still possible to generate key with the quantum repeater. Hence it is trivially easy to beat this benchmark for low p_{ps} and p_{em}. In that sense this benchmark is not so interesting in that regime. It is for this reason that this regime is not depicted on the contour plots. In both FIG. 6.10 and FIG. 6.11 we observe a crossing between the finite energy benchmarks (1b) and (2b) and their infinite energy counterparts (1a) and (2a) at $p_{\text{em}} \approx 0.796$, as discussed in Section 6.5.

Comparison with the proposed benchmarks for a commonly used telecom channel. Let us now again investigate the secret-key rate achievable with the expected parameters and how it compares with the proposed benchmarks, but this time assuming that we have an available channel at the commonly used telecom wavelength with attenuation length $L_0 = 22$ km. Hence in this case the frequency conversion of the emitted light into telecom would be applied. We consider such a conversion process with effi-

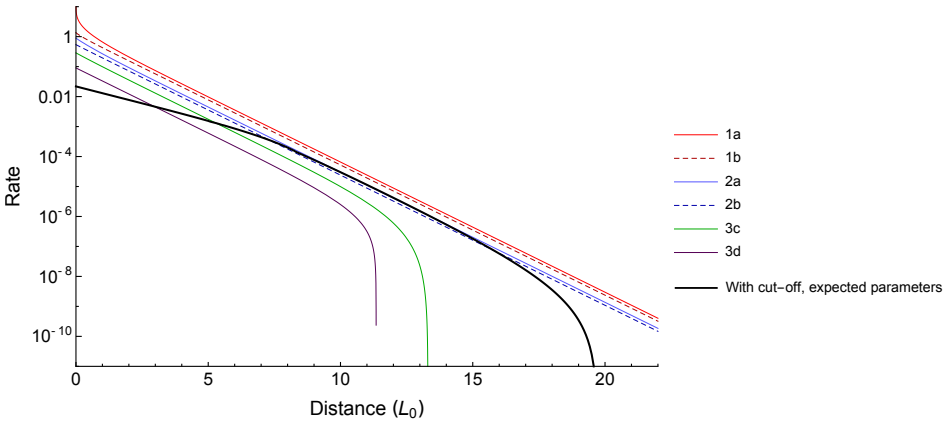

Figure 6.9: Secret-key rate with the quantum repeater implementation for the expected parameters with optimised cut-off as a function of the distance in units of $L_0 = 0.542$ km. The rate is compared to all the benchmarks defined in Table 6.1.

ciency of 30% [76]. This parameter can be added to p_{em} so that we define $p'_{\text{em}} = 0.3\, p_{\text{em}}$. We note here that the assumed value of this parameter is a choice based on the specific experimental implementation. However, higher conversion efficiencies are in principle achievable. The comparison is depicted in FIG. 6.12. We see that for this choice of the direct channel, the benchmarks are more difficult to overcome. In particular only the benchmarks corresponding to direct transmission (3d) and the thermal-loss channel (3c) can be outperformed. The other benchmarks seem to be far from near-term experimental reach.

6.8. CONCLUSIONS

In this work, we have analysed numerically a realistic quantum repeater implementation for quantum key distribution. We have introduced two methods for improving the rates of the repeater with respect to previous proposals: advantage distillation and the cut-off. Advantage distillation is a classical post-processing method that increases the secret-key rate at all levels of noise. The cut-off on the other hand allows for a trade-off between the channel uses required and the secret-key fraction. Utilising the cut-off results in three benefits with respect to the previous scheme for the single sequential quantum repeater [1]. Firstly, the cut-off method achieves a higher rate for all distances. Secondly, the protocol is more robust against dark counts, in the sense that non-zero secret key can be generated over larger distances. Finally, the cut-off can be adjusted on the fly, unlike the repositioning of the repeater [1]. This is especially convenient in the scenario where the experimental setup might be modified. With the previous scheme for example, improving the coherence times of the memories would lead to a new optimal position. The repositioning of the repeater node would be both costly and time-inefficient, while modifying the cut-off corresponds to a simple change in the programming of the devices.

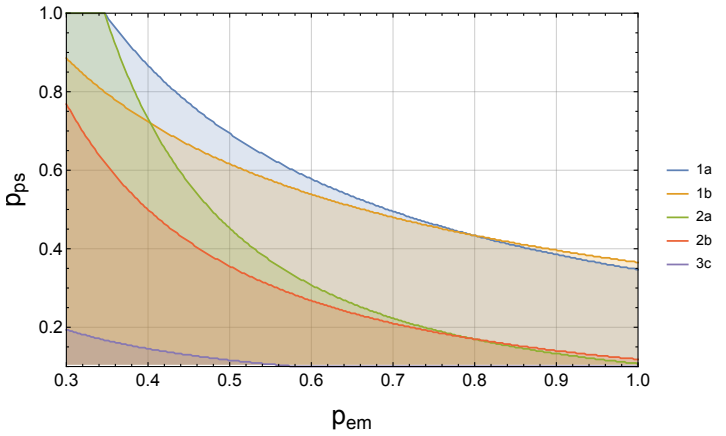

Figure 6.10: Contour plot of regions of p_{em} versus p_{ps} with the expected parameters where the benchmarks listed in Table 6.1 can be surpassed. The contour lines correspond to the parameters that achieve the corresponding benchmarks while the parameter regimes above the curves allow us to surpass them. The data is plotted for the distance of $9.6L_0$, where $L_0 = 0.542$ km.

We note here that one could also use the secret-key rate *per unit time* to assess the performance of a quantum repeater. The secret-key rate per unit time can be calculated by multiplying the secret-key fraction with the inverse of the (average) time it takes to generate a single raw bit between Alice and Bob. This time will depend on the travel time of the photons from the quantum repeater to Alice and Bob, the generation time of the entangled photon-memory pairs and the time it takes to perform the required operations such as the Bell state measurement. To compare the secret-key rate per unit time to the benchmarks, the benchmarks too must then be re-expressed in the secret-key rate per unit time. This can be achieved by multiplying the benchmarks with a fixed emission rate of a photon source [77]. Note that there is now an ambiguity in the benchmarks, as they depend on the fixed emission rate. Since the emission rate is limited by engineering constraints, the benchmarks are dependent on current technologies and cannot be claimed to be fundamental.

By optimising over the cut-off, we have found realistic parameter regions where it is possible to surpass several different benchmarks including the secret-key capacity. These benchmarks are relevant milestones towards claiming a quantum repeater, and thus form an important step in the creation of the first large-scale quantum networks. To make our arguments concrete, we have chosen a specific parameter set induced by some recent experimental results. However, other platforms or technological advances might allow to improve upon our results and predict particularly simple setups for performing the first quantum repeater experiment. For example, our work could be extended by including other types of encoding, such as polarisation encoding, in which case additional depolarising noise in the fibre could become relevant. We leave the investigation of other parameter regimes open. In this respect our model has a very broad functionality, as it allows us to perform efficient optimisation of the secret-key rate over the cut-off for any

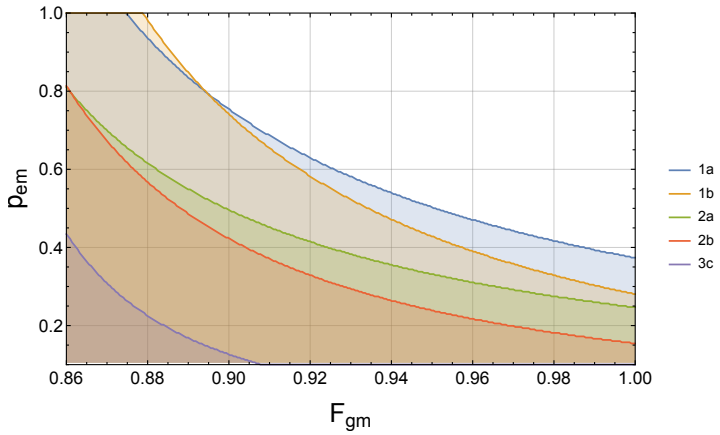

Figure 6.11: Contour plot of regions of F_{gm} versus p_{em} with the expected parameters where the benchmarks listed in Table 6.1 can be surpassed. The contour lines correspond to the parameters that achieve the corresponding benchmarks while the parameter regimes above the curves allow us to surpass them. The data is plotted for the distance of $9.6L_0$, where $L_0 = 0.542$ km.

set of parameters. We achieve this functionality by finding tight analytical bounds for the number of channel uses needed to generate one bit of raw key as a function of the cut-off. Our numerical package is freely available for further exploration [70].

6.9. APPENDIX

6.9.1. DARK COUNTS

In this section we detail the effect of dark counts in the detectors of Alice and Bob on our protocol. In particular, we briefly go over the concept of so-called *squashing models* [25, 34], after which we will be able to calculate the induced depolarising noise. We conclude with explaining how dark counts increase the yield.

Quantum states of light are naturally described by operators on an infinite-dimensional Hilbert space. However, a significant number of optical experiments have been performed where the infinite-dimensional states and operations are approximated by a lower dimensional description. An example of this is where the state of light is assumed to lie within a two-dimensional subspace spanned by the vacuum state and a single-photon excitation. Such an approximation is valid in the sense that the theoretical predictions of measurement statistics correspond accurately to those that are observed experimentally.

However, in cryptographic contexts one usually has to make unconditional statements about the information held by a third party. This third party might be malicious and all-powerful, and her measurement statistics are, by definition, unknown. This implies that there is not necessarily a bound on the information held by a malicious third party, despite the fact that the truncation of the Hilbert space is a good approximation for experimental statistics.

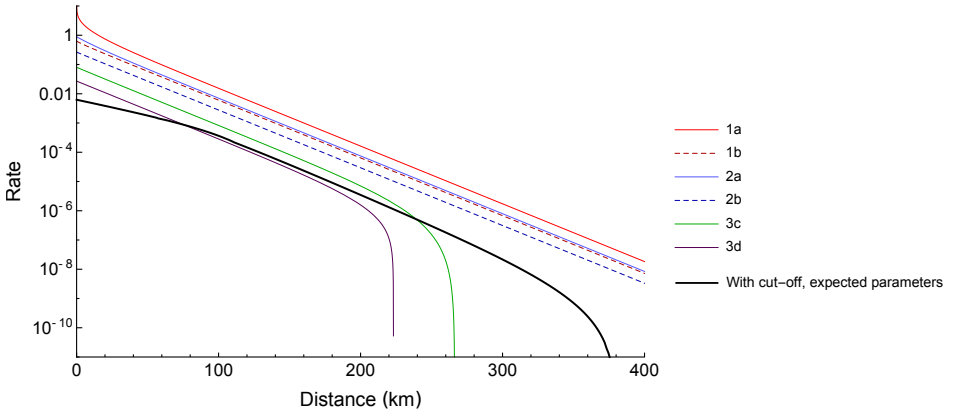

Figure 6.12: Secret-key rate for the telecom channel with $L_0 = 22$ km with the quantum repeater implementation for the expected parameters with optimised cut-off as a function of the distance in units of km. The rate is compared to all the benchmarks defined in Table 6.1.

Since the theoretical analysis in an infinite-dimensional Hilbert space is difficult, one would prefer to be able to bound the information held by a third party, while at the same time applying a truncation to the finite-dimensional Hilbert space. This can be done if a so-called squashing model exists, which is a way of relating measurements performed on a high-dimensional state to a truncated space. As an approximation we consider here the squashing models for measurements of qubits encoded in the polarisation of photons. In this case squashing models exist for both the fully asymmetric BB84 protocol and the symmetric six-state protocol (with only passive measurements), implying that one can, without loss of generality, perform the fully asymmetric BB84 and symmetric (passive) six-state protocol with photons [25, 34]. The squashing model also dictates how multiple clicks in different detectors give rise to noise in the truncated space. In the next section, we discuss how to map the dark counts in the detectors to depolarising noise according to the corresponding squashing model.

The parameters typically used to quantify detectors are the dark counts per second and the detection window t_w, which is the duration of the integration period of the detectors. The number of thermal photons $\overline{n}$ relevant for the thermal benchmark is given by t_{int} times the dark counts per second. Assuming a Poisson distribution of the dark counts, it follows that the probability p_d of getting at least a single dark count click within the time-window of awaiting the signal photon is given by $p_d = 1 - \exp(-\overline{n}) \approx \overline{n}$ for small $\overline{n}$.

The noise caused by the dark counts at Alice's or Bob's detector can then be modelled by a depolarising channel, where the depolarising parameter $\alpha_{A/B}$ depends on the

implemented protocol,

$$\alpha_{A/B,\,\mathrm{BB84}} = \frac{p_{\mathrm{app}} p_{\mathrm{ps}} \eta_{A/B}(1-p_d)}{1-(1-p_{\mathrm{app}} p_{\mathrm{ps}} \eta_{A/B})(1-p_d)^2}\,, \tag{6.16}$$

$$\alpha_{A/B,\,\text{six-state}} = \frac{p_{\mathrm{app}} p_{\mathrm{ps}} \eta_{A/B}(1-p_d)^5}{1-(1-p_{\mathrm{app}} p_{\mathrm{ps}} \eta_{A/B})(1-p_d)^6}\,. \tag{6.17}$$

That is, conditioned on a click in at least one of the detectors, Alice or Bob receive the desired state if they receive the signal photon and no other detector was triggered. Due to the squashing map all other events can be mapped onto a maximally mixed state [25, 34]. To explain the exponents, we note that the active BB84 protocol requires an optical measurement setup with two detectors, while for the six-state protocol such a measurement setup will consist of six detectors.

Furthermore, independent of the existence of a squashing map, the dark counts increase the total probability that Alice or Bob gets a click. This probability depends on whether the BB84 or six-state protocol is implemented, and is given by

$$p_{A/B,\,BB84} = 1-(1-p_{\mathrm{app}} p_{\mathrm{ps}} \eta_{A/B})(1-p_d)^2\,, \tag{6.18}$$

$$p_{A/B,\,\text{six-state}} = 1-(1-p_{\mathrm{app}} p_{\mathrm{ps}} \eta_{A/B})(1-p_d)^6\,. \tag{6.19}$$

6.9.2. QUANTUM BIT ERROR RATE

In this appendix we derive the expressions for the average quantum bit error rate in the X, Y and Z basis as a function of the experimental parameters. It is given by

$$\langle e_X\rangle = \langle e_Y\rangle = \frac{1}{2} - \frac{1}{2} F_{\mathrm{gm}} \alpha_A \alpha_B \left(2F_{\mathrm{prep}}-1\right)^2 \left\langle e^{-(a+b)n}\right\rangle\,, \tag{6.20}$$

$$\langle e_Z\rangle = \frac{1}{2} - \frac{1}{2} F_{\mathrm{gm}} \alpha_A \alpha_B \langle e^{-b\cdot n}\rangle\,, \tag{6.21}$$

where the average is performed over the geometric distribution with only the first $n^\star$ trials. That is, the average of the exponential e^{-cn} is given by

$$\begin{aligned}\langle e^{-cn}\rangle &= \frac{\sum_{n=1}^{n^\star} p_B \left(1-p_B\right)^{n-1} e^{-cn}}{\sum_{n=1}^{n^\star} p_B \left(1-p_B\right)^{n-1}} \\ &= \frac{p_B e^{-c}}{1-\left(1-p_B\right)^{n^\star}} \frac{1-\left(1-p_B\right)^{n^\star} e^{-cn^\star}}{1-\left(1-p_B\right)e^{-c}}\,.\end{aligned} \tag{6.22}$$

To derive these quantum bit error rates, let us firstly define the two-qubit Bell states as

$$|\psi(\mathrm{x},\mathrm{z})\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0+\mathrm{x}\rangle + (-1)^{\mathrm{z}}|1\rangle|1+\mathrm{x}\ (\mathrm{mod}\,2)\rangle), \tag{6.23}$$

for $\mathrm{x},\mathrm{z}\in\{0,1\}$. The noise in the preparation can be modelled as dephasing noise [26]. The initially generated entangled state between the quantum memory and the state of the photon flying to Alice is then

$$\rho_{AR} = F_{\mathrm{prep}}|\psi(1,0)\rangle\langle\psi(1,0)| + (1-F_{\mathrm{prep}})|\psi(1,1)\rangle\langle\psi(1,1)|\,, \tag{6.24}$$

where F_{prep} is the preparation fidelity of this state. The state in the first quantum memory is now kept stored there. During this time, a second entangled photon-memory is attempted to be generated at the second quantum memory. During these attempts, the state stored in the first quantum memory decoheres through time-dependent dephasing and depolarising noise acting on it. This means that at the time when the second copy is generated, the first copy will have decohered. This second copy will be of the same form as the first one. The decohered first copy is of the form

$$\begin{aligned}\rho'_{AR} = F_{T_1}[F_{\text{prep}}(F_{T_2}|\psi(1,0)\rangle\langle\psi(1,0)| + (1-F_{T_2})|\psi(1,1)\rangle\langle\psi(1,1)|) \\ + (1-F_{\text{prep}})\left(F_{T_2}|\psi(1,1)\rangle\langle\psi(1,1)| + (1-F_{T_2})|\psi(1,0)\rangle\langle\psi(1,0)|\right)] + (1-F_{T_1})\frac{\mathbb{I}}{4},\end{aligned} \tag{6.25}$$

where F_{T_1}, F_{T_2} are respectively the depolarising and dephasing parameters due to the decoherence processes on the stored state in the first memory. The fidelity decays exponentially with the number of attempts [5] and hence these parameters can be written as

$$F_{T_1} = e^{-b\cdot n}, \tag{6.26}$$

$$F_{T_2} = \frac{1+e^{-a\cdot n}}{2}. \tag{6.27}$$

Here n is the number of attempts that have been performed on the second memory to successfully generate the repeater-Bob entanglement and the decay rates a and b are defined in the main text. Hence we can rewrite the state of ρ'_{AR} as

$$\rho'_{AR} = F_{T_1}(F_{\text{deph},AR}|\psi(1,0)\rangle\langle\psi(1,0)| + (1-F_{\text{deph},AR})|\psi(1,1)\rangle\langle\psi(1,1)|) + (1-F_{T_1})\frac{\mathbb{I}}{4}. \tag{6.28}$$

where

$$F_{\text{deph},AR} = \frac{1+(2F_{\text{prep}}-1)e^{-an}}{2}. \tag{6.29}$$

The entanglement swapping is performed at the two memories at the repeater node. Since the situation is symmetric for all the four measurement outcomes, without loss of generality we can consider the resulting state on AB as if the repeater measured $|\psi(1,0)\rangle$. If a different Bell state was measured, a Pauli rotation could be used to bring the state to this form. The state that we obtain is

$$\begin{aligned}\rho''_{AB} = F_{T_1}\Big(\left[F_{\text{deph},AR}F_{\text{prep}} + (1-F_{\text{deph},AR})(1-F_{\text{prep}})\right]|\psi(1,0)\rangle\langle\psi(1,0)| \\ + \left[F_{\text{deph},AR}(1-F_{\text{prep}}) + (1-F_{\text{deph},AR})F_{\text{prep}}\right]|\psi(1,1)\rangle\langle\psi(1,1)|\Big) + \left(1-F_{T_1}\right)\frac{\mathbb{I}}{4}.\end{aligned} \tag{6.30}$$

Finally we note that the operations such as Bell state measurements or any other required gates performed on the memories are also noisy. We will model them by the depolarising channel here [27]. The depolarising channel commutes with the dephasing channel. For the two copies of the Bell-diagonal state, it also commutes with the entanglement swapping, in the sense that applying it to one of our memory qubits is mathematically equivalent to applying the same channel to one of the photons flying to Alice

or Bob. Hence independently of when exactly in the protocol those gates or measurements on the memories are applied, we can add the resulting depolarisation to the final state shared between Alice and Bob, so that we obtain

$$\rho''_{AB} = F_{\text{gm}}\alpha_A\alpha_B F_{T_1}\left(\left[F_{\text{deph},AR}F_{\text{prep}} + (1-F_{\text{deph},AR})(1-F_{\text{prep}})\right]|\psi(1,0)\rangle\langle\psi(1,0)| \right. \tag{6.31}$$
$$\left. + \left[F_{\text{deph},AR}(1-F_{\text{prep}}) + (1-F_{\text{deph},AR})F_{\text{prep}}\right]|\psi(1,1)\rangle\langle\psi(1,1)|\right) + \left(1-F_{\text{gm}}\alpha_A\alpha_B F_{T_1}\right)\frac{\mathbb{I}}{4}\,.$$

Here by F_{gm} we denote the product of all the depolarising parameters corresponding to all noisy gates and measurements and $\alpha_{A/B}$ corresponds to the noise caused by the dark counts on Alice's/Bob's side. From the final state it follows that

$$\langle e_X\rangle = \langle e_Y\rangle = \frac{1}{2} - \frac{1}{2}F_{\text{gm}}\alpha_A\alpha_B\left(2F_{\text{prep}}-1\right)^2\left\langle e^{-(a+b)n}\right\rangle\,, \tag{6.32}$$

$$\langle e_Z\rangle = \frac{1}{2} - \frac{1}{2}F_{\text{gm}}\alpha_A\alpha_B\langle e^{-b\cdot n}\rangle\,. \tag{6.33}$$

where the average is over the geometric distribution with only the first $n^\star$ trials. This is due to the fact that, by construction, the state is never allowed to decohere more than $n^\star$ trials.

6.9.3. COMPARISON WITH MEMORY-ASSISTED MEASUREMENT-DEVICE-INDEPENDENT QKD SCHEMES

The setup of the proof of principle repeater analysed in this paper bears close resemblance to the memory-assisted measurement-device-independent QKD (MA-MDI QKD) setups proposed in [2], which were analysed in more detail in the particular context of NV centres in [78]. However, in contrast to our focus on key per channel use, these schemes were mostly assessed on their performance of generating key per unit time. In this section, we will briefly discuss these schemes and their advantages and disadvantages in comparison to the scheme analysed in this paper. In particular, we will focus both on their relevance in the context of secret-key generation per channel use, and on the complexity of their experimental implementation.

The three schemes that we compare with can be found in Figure 6.13. These schemes have the advantage of high expected rate per unit time, since heralding of the successful events now takes place at the repeater. Thus, after a failed attempt the repeater can immediately prepare for receiving another photon, without the need for waiting on any classical communication from Alice and Bob. Furthermore, these schemes are secure against detector side-channel attacks [79], since in each scheme there is no quantum information sent from the repeater to Alice or Bob.

However, these advantages, while relevant in practical QKD setups, might not necessarily translate directly in higher secret-key rate per channel use for proof of principle repeaters. Moreover, there are experimental challenges that make these MA-MDI QKD schemes more difficult to implement than the sequential quantum repeater that we consider. This is particularly important, since the goal of this paper is to analyse a protocol that would be simple from the implementation perspective, and would have the capability to exceed the benchmarks in Section 6.5.

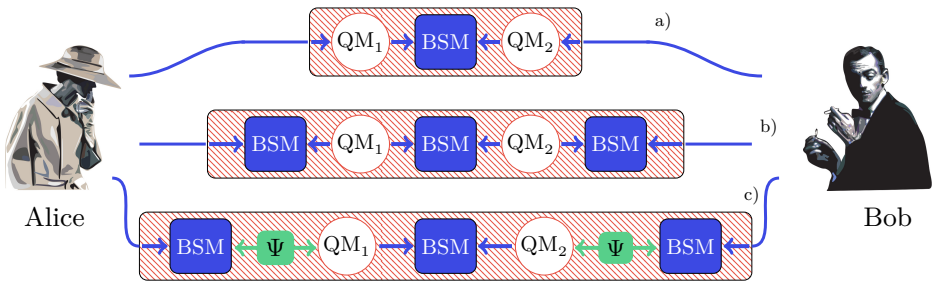

Figure 6.13: Three different setups for the memory-assisted measurement-device-independent quantum key distribution (MA-MDI QKD). Here, BSM stands for Bell state measurement. The first setup a) corresponds to the scheme of MA-MDI QKD with direct heralding. Specifically, the implementation of this setup requires that a photonic state can be transferred into a quantum memory QM_1 and QM_2 in a heralded fashion. That is, following the transfer attempt, one obtains the information whether the state of the photon emitted at Alice or Bob has been successfully transferred to the desired quantum memory. The second setup b) with indirect heralding is a modification of the first one. Here the requirement of the heralded state transfer has been dropped, at the cost of probabilistic Bell state measurements between two photonic qubits at the outer BSM stations. Finally, the setup in c) is a modification of b), which uses sources of entangled photons (Ψ). In this way, the attempt to transfer the quantum state of the photon into the memory is performed only after a successful Bell state measurement. This can increase the rate per unit time, since writing unto and resetting the memory is a time-consuming process.

Let us now go over each of these schemes. Firstly, let us consider the first scheme a). This scheme seems to require a similar number of components as our proposed scheme, with the exception that the two detector setups have now been replaced with the sources of BB84 states. The main difficulty with implementing such a scheme lies in the requirement of heralded quantum state transfer from a single photon into the quantum memory. We have already discussed in Section 3.3.1 in Chapter 3 that this is a great challenge from the experimental perspective.

Due to the reasons explained in Section 3.3.1 in Chapter 3, scheme b) seems more realistic than scheme a) with the current state-of-the-art technology. However, a larger number of components is needed and the two additional optical Bell state measurements will reduce the rate by a factor of four. In particular, photonic states need to be emitted both from the quantum memories and the BB84 sources. These need to be synchronised such that the Bell state measurements can be performed on both of them. While there is nothing fundamentally challenging with this scheme, it requires larger number of components and is more complicated than the scheme analysed in this paper. Similar conclusions apply to the more complex scheme proposed in c), which adds sources of entangled photons (denoted here by Ψ) into the scheme of b). A comparison of the achieved secret-key rate with the secret-key capacity, for a variant of scheme c), has been performed in [80].

6.9.4. SECRET-KEY FRACTION AND ADVANTAGE DISTILLATION

In this section the secret-key fraction formula for the six-state protocol with advantage distillation of [35] is briefly reviewed. We note here that while the analysis in Appendix 6.9.2 has the state $|\psi(1,0)\rangle$ as the target state, here we follow the analysis of [35] for which $|\psi(0,0)\rangle$ is the target state. This doesn't affect the overall analysis as the final state from Appendix 6.9.2 can be rotated locally such that $|\psi(0,0)\rangle$ could be made the target state. The secret key fraction can be expressed in terms of the Bell coefficients of the Bell diagonal state

$$\rho_{AB} = \sum_{x,z\in\{0,1\}} P_{XZ}(x,z)|\psi(x,z)\rangle\langle\psi(x,z)| \,. \tag{6.34}$$

Here P_{XZ} is a probability distribution and we will abbreviate $P_{XZ}(x,z)$ as p_{xz}. For the description of the advantage distillation protocol we refer the reader to [35]. It is shown there that the secret-key fraction can be written as

$$r_{\text{six-state}} = \frac{1}{3}\max\left[1 - H(P_{XZ}) + \frac{P_{\tilde{X}}(1)}{2} h\left(\frac{p_{00}p_{10}+p_{01}p_{11}}{(p_{00}+p_{01})(p_{10}+p_{11})}\right), \frac{P_{\tilde{X}}(0)}{2}(1 - H(P'_{XZ}))\right] \tag{6.35}$$

where

$$P_{\bar{\mathsf{X}}}(0) = (p_{00}+p_{01})^2+(p_{10}+p_{11})^2\,, \tag{6.36}$$
$$P_{\bar{\mathsf{X}}}(1) = 2(p_{00}+p_{01})(p_{10}+p_{11})\,, \tag{6.37}$$
$$P'_{\mathsf{XZ}}(0,0) = \frac{p_{00}^2+p_{01}^2}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}, \tag{6.38}$$
$$P'_{\mathsf{XZ}}(1,0) = \frac{2p_{00}p_{01}}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}, \tag{6.39}$$
$$P'_{\mathsf{XZ}}(0,1) = \frac{p_{10}^2+p_{11}^2}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}, \tag{6.40}$$
$$P'_{\mathsf{XZ}}(1,1) = \frac{2p_{10}p_{11}}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}\,, \tag{6.41}$$

and $H(P_{\mathsf{XZ}})$ is the Shannon entropy of the distribution P_{XZ}. The factor of a third arises from the fact that for a symmetric six-state protocol only a third of the measurements will be performed in the same basis by Alice and Bob.

In our model we only consider depolarising noise and dephasing noise in standard basis. Hence for the six-state protocol the error rates in X and Y basis will be the same. Therefore

$$p_{10}+p_{11} = e_Z\,, \tag{6.42}$$
$$p_{01}+p_{11} = e_{XY}\,, \tag{6.43}$$
$$p_{01}+p_{10} = e_{XY}\,, \tag{6.44}$$
$$p_{00}+p_{01}+p_{10}+p_{11} = 1\,. \tag{6.45}$$

Hence

$$p_{00} = 1-\frac{e_Z}{2}-e_{XY}\,, \tag{6.46}$$
$$p_{01} = e_{XY}-\frac{e_Z}{2}\,, \tag{6.47}$$
$$p_{10} = p_{11} = \frac{e_Z}{2}\,. \tag{6.48}$$

And so

$$P_{\bar{\mathsf{X}}}(0) = 1-2e_Z+2e_Z^2\,, \tag{6.49}$$
$$P_{\bar{\mathsf{X}}}(1) = 2(1-e_Z)e_Z\,. \tag{6.50}$$

6.9.5. YIELD

In this appendix we derive the analytical approximation for the yield with the cut-off $n^\star$. The yield Y is given by

$$Y = \frac{p_{\text{bsm}}}{\mathbb{E}[N]} = \frac{p_{\text{bsm}}}{\mathbb{E}[\max(N_A,N_B)]}\,. \tag{6.51}$$

The approximation used for $\mathbb{E}[\max(N_A,N_B)]$ is

$$\mathbb{E}[\max(N_A,N_B)] \approx \begin{cases} \frac{1}{p_A\left(1-(1-p_B)^{n^\star}\right)} & \frac{1}{p_A} \geq n^\star \\ \frac{1}{p_A}+\frac{1}{p_B}-\frac{1}{p_A+p_B-p_Ap_B} & \frac{1}{p_A} < n^\star, \end{cases} \tag{6.52}$$

where p_A and p_B are defined in Eq. (6.18) for BB84 and in Eq. (6.19) for the six-state protocol. In the rest of this appendix, we will motivate this approximation by finding tight analytical lower and upper bounds on $\mathbb{E}[N]$.

We note that we consider separately two parameter regimes. One of them is the regime where on average the dominant number of channel uses per round is on Alice's side $\left(\frac{1}{p_A} > n^\star\right)$. This corresponds to the high-loss regime since the number of channel uses per round on Bob's side is upper bounded by the cut-off. The other regime is the low-loss regime $\left(\frac{1}{p_A} \leq n^\star\right)$. In this regime we will show that the cut-off does not play any significant role, so that in this regime the formula for the yield with no cut-off [1, 2] can be used. Moreover, for our derivation to be valid we require an additional constraint to be satisfied, namely $p_B \geq p_A$. This means that we cannot consider scenarios when the repeater is positioned closer to Alice than to Bob. Such a constraint is well-justified since the time-dependent decoherence in quantum memory QM_1 would only increase by shifting the repeater towards Alice.

HIGH-LOSS REGIME

The high-loss regime is the regime where the losses on Alice's side together with the cut-off on Bob's side ensure that the predominant number of channel uses is almost always on Alice's side, i.e. $\mathbb{E}[N] = \mathbb{E}[\max(N_A, N_B)] \approx \mathbb{E}[N_A]$. This regime is described by the condition $p_A n^\star < 1$. More specifically, as we will show in this section, if

$$\frac{1}{p_A} := \mu = \beta n^\star,\ \beta > 1\,, \tag{6.53}$$

then

$$\mathbb{E}[N_A] \leq \mathbb{E}[N] \leq \left(g_{\mathrm{err}}(p_A, p_B, n^\star) + 1\right)\mathbb{E}[N_A]\,, \tag{6.54}$$

where $\mathbb{E}[N_A] = \frac{1}{p_A(1-(1-p_B)^{n^\star})}$ (see Eq. (6.62)) and $g_{\mathrm{err}}(p_A, p_B, n^\star) = \mathcal{O}\left(\frac{1}{\beta^2}\right)$ is a function defined in Eq. (6.81). This implies that for β large enough, $\mathbb{E}[N]$ can be accurately approximated by $\frac{1}{p_A(1-(1-p_B)^{n^\star})}$.

We start the proof of Eq. (6.54) by first noticing that $\mathbb{E}[N_A] \leq \mathbb{E}[N]$. It is, thus, only necessary to find an upper bound for $\mathbb{E}[N]$. Now, let $p(K=k) = (1-p_r)^{k-1}p_r$ be the probability that Bob succeeds in round k. Here $p_r = 1-(1-p_B)^{n^\star}$ is the probability that Bob succeeds in a given round. Then

$$\begin{aligned}\mathbb{E}[N] &= \mathbb{E}[\max(N_A, N_B)] \\ &= \sum_{k=1}^{\infty} p(K=k)\left(\sum_{n_A=k}^{\infty}\left(\sum_{n_B=(k-1)n^\star+1}^{kn^\star} p(N_A = n_A \wedge N_B = n_B | K=k)\max(n_A, n_B)\right)\right).\end{aligned} \tag{6.55}$$

One can split the sum over n_A in two, depending on whether n_A is greater than n_B or

vice versa. We get

$$\mathbb{E}[N] = \sum_{k=1}^{\infty} p(k) \left(\sum_{n_B=(k-1)n^\star+1}^{kn^\star} \left(\sum_{n_A=k}^{n_B} p(n_A \wedge n_B|k) n_B \right) + \sum_{n_B=(k-1)n^\star+1}^{kn^\star} \left(\sum_{n_A=n_B+1}^{\infty} p(n_A \wedge n_B|k) n_A \right) \right), \tag{6.56}$$

where $p(k) = p(K = k)$, and $p(n_A \wedge n_B|k) = p(N_A = n_A \wedge N_B = n_B|K = k)$. The first term of Eq. (6.56) can be upper bounded noticing that $n_B \leq kn^\star$, i.e.

$$\sum_{k=1}^{\infty} p(k) \left(\sum_{n_B=(k-1)n^\star+1}^{kn^\star} \left(\sum_{n_A=k}^{n_B} p(n_A \wedge n_B|k) n_B \right) \right) \leq \sum_{k=1}^{\infty} p(k)\, p\left(N_A \leq N_B|K = k\right) kn^\star. \tag{6.57}$$

The second term of Eq. (6.56) can be upper bounded in the following way

$$\sum_{k=1}^{\infty} p(k) \left(\sum_{n_B=(k-1)n^\star+1}^{kn^\star} \left(\sum_{n_A=n_B+1}^{\infty} p(n_A \wedge n_B|k) n_A \right) \right) \leq \sum_{k=1}^{\infty} p(k) \left(\sum_{n_A=k}^{\infty} p(n_A|k) n_A \right) \tag{6.58}$$

$$= \sum_{k=1}^{\infty} p(k) \sum_{n_A=1}^{\infty} p(n_A|k) n_A \tag{6.59}$$

$$= \sum_{n_A=1}^{\infty} p(n_A) n_A = \mathbb{E}[N_A]\,. \tag{6.60}$$

Inputting Eq. (6.57) and Eq. (6.60) back into Eq. (6.56), we obtain

$$\mathbb{E}[N] \leq \left(\frac{n^\star}{\mathbb{E}[N_A]} \sum_{k=1}^{\infty} p(k)\, p\left(N_A \leq N_B|k\right) k + 1 \right) \mathbb{E}[N_A]\,. \tag{6.61}$$

Let N_A^i be the random variable describing the number of trials on Alice's side in round i. Since $p(N_A^i = n_A^i) = (1-p_A)^{n_A^i - 1} p_A$, we clearly have that $\mathbb{E}[N_A^i] = \frac{1}{p_A} = \mu$. Then we note that

$$\begin{aligned} \mathbb{E}[N_A] &= \sum_{k=1}^{\infty} p(k) \sum_{i=1}^{k} \sum_{n_A^i=1}^{\infty} p(n_A^i) n_A^i = \sum_{k=1}^{\infty} p(k) \sum_{i=1}^{k} \mathbb{E}[N_A^i] = \mu \sum_{k=1}^{\infty} p(k) k \\ &= \mathbb{E}[K]\mu = \frac{1}{p_A p_r} = \frac{1}{p_A(1-(1-p_B)^{n^\star})}\,. \end{aligned} \tag{6.62}$$

Here, we first express $\mathbb{E}[N_A]$ by calculating the average number of trials in each of the k rounds. Then, we sum the k averages together, and finally, we average over the total number of rounds k. Since all the rounds are independent, we replace each $\mathbb{E}[N_A^i]$ by μ as stated above. By inputting Eq. (6.62) into Eq. (6.61), we get

$$\mathbb{E}\left[N_A\right] \leq \mathbb{E}\left[N\right] \leq \left(\frac{1}{\mathbb{E}[K]\beta} \sum_{k=1}^{\infty} p(k)\, p\left(N_A \leq N_B|k\right) k + 1 \right) \mathbb{E}[N_A]\,. \tag{6.63}$$

We now upper bound the $p\,(N_A \leq N_B|k)$ term. Note that

$$p\,(N_A \leq N_B|k) = p\left(\sum_{i=1}^{k} N_A^i \leq \sum_{i=1}^{k} N_B^i \Big| k\right). \tag{6.64}$$

We note that conditioned on $K=k$, we have that $\sum_{i=1}^{k} N_B^i = (k-1)n^\star + N_B^k$. It then follows that

$$p\,(N_A \leq N_B|k) = p\left(\sum_{i=1}^{k} N_A^i \leq (k-1)n^\star + N_B^k \Big| k\right) \leq p\left(\sum_{i=1}^{k} N_A^i \leq kn^\star \Big| k\right). \tag{6.65}$$

Condition Eq. (6.53) and $-\sum_{i=1}^{k} N_A^i \geq -kn^\star$ is equivalent to $k\mu - \sum_{i=1}^{k} N_A^i \geq k(\beta-1)n^\star$. Hence,

$$p\left(\sum_{i=1}^{k} N_A^i \leq kn^\star \Big| k\right) = p\left(k\mu - \sum_{i=1}^{k} N_A^i \geq k(\beta-1)n^\star \Big| k\right). \tag{6.66}$$

We can use the Chernoff bound to upper bound this probability. The Chernoff bound for a random variable X is

$$p(X \geq a) \leq \frac{\mathbb{E}[e^{tX}]}{e^{ta}},\ t>0\,. \tag{6.67}$$

Let X be the sum of k random variables $X_1, X_2, \ldots, X_k$, where

$$X_i = \mu - N_A^i\,, \tag{6.68}$$

i.e. $X = \sum_{i=1}^{k} X_i = k\mu - \sum_{i=1}^{k} N_A^i$. From this we can now bound the desired probability. Using (6.67) and $a = k(\beta-1)n^\star$, we obtain the inequality

$$p\left(k\mu - \sum_{i=1}^{k} N_A^i \geq k(\beta-1)n^\star \Big| k\right) \leq \frac{\mathbb{E}\left[\exp\left(t\left(k\mu - \sum_{i=1}^{k} N_A^i\right)\right)\Big| k\right]}{e^{tk(\beta-1)n^\star}} \tag{6.69}$$

$$= \exp\left[tk\left(\mu - (\beta-1)n^\star\right)\right]\mathbb{E}\left[\Pi_{i=1}^{k} e^{-tN_A^i}|k\right]\,. \tag{6.70}$$

Let us now focus on $\mathbb{E}\left[\prod_{i=1}^{k} e^{-tN_A^i}|k\right]$,

$$\mathbb{E}\left[\prod_{i=1}^{k} e^{-tN_A^i}|k\right] = \prod_{i=1}^{k}\mathbb{E}\left[e^{-tN_A^i}|k\right] = \prod_{i=1}^{k}\left(\sum_{n_A^i=1}^{\infty} p_A(1-p_A)^{n_A^i-1}\, e^{-tn_A^i}\right) = \left(\frac{p_A e^{-t}}{1-(1-p_A)e^{-t}}\right)^k. \tag{6.71}$$

Here, after the first equality sign we have used the fact that the random variables N_A^i are independent for different i's. After the second equality we note that all of them have exactly the same geometric distribution over the k rounds. Specifically, it is now important to note that this holds provided that k is the value of K on which we have conditioned, i.e., the success on Bob's side occurs exactly in the k'th round. Furthermore, the common ratio $(1-p_A)e^{-t}$ satisfies the convergence condition $\left|(1-p_A)e^{-t}\right| < 1$ for all $t>0$. This yields

$$p\,(N_A \leq N_B|K=k) \leq \left(\exp\left[t\left(\frac{1}{p_A} - (\beta-1)n^\star\right)\right]\frac{p_A e^{-t}}{1-(1-p_A)e^{-t}}\right)^k. \tag{6.72}$$

Let's define the function $f(t)$ as

$$f(t) := \exp\left[t\left(\frac{1}{p_A} - (\beta-1)n^\star\right)\right]\frac{p_A e^{-t}}{1-(1-p_A)e^{-t}}\,. \tag{6.73}$$

This function should be minimised subject to $t>0$ to obtain the tightest bound. A single stationary point is analytically found at

$$t_0 = \ln\left(\frac{(1-p_A)(p_A(\beta-1)n^\star-1)}{p_A(\beta-1)n^\star+p_A-1}\right). \tag{6.74}$$

We now want to make sure that t_0 always satisfies the condition $t>0$, necessary for applying the Chernoff bound. By condition Eq. (6.53), the denominator of the above expression inside the logarithm is $p_A(\beta-1)n^\star+p_A-1 = 1-p_An^\star+p_A-1 = p_A(1-n^\star)<0$ as long as $n^\star>1$. From this it follows that $t_0>0$ if and only if

$$(1-p_A)(p_A(\beta-1)n^\star-1) < p_A(\beta-1)n^\star+p_A-1\,. \tag{6.75}$$

Clearly this condition is equivalent to $-p_A^2(\beta-1)n^\star<0$ which is satisfied for $\beta>1$. This means that $t_0>0$ is always satisfied. Now note that $f(t=0)=1$. Moreover, one can also easily verify that $f'(t=0)=n^\star(1-\beta)<0$ for $\beta>1$, and that $\lim_{t\to\infty}f(t)\to\infty$ as long as $n^\star>1$. These properties of $f(t)$, together with the continuity of $f(t)$, prove that $t=t_0$ corresponds to the global minimum of this function in the regime $t>0$ and that $f(t_0)<1$. Hence, we can now calculate $f(t_0)$ which gives

$$f(t_0) = \left(\frac{(p_A(\beta-1)n^\star-1)(1-p_A)}{p_A(\beta-1)n^\star+p_A-1}\right)^{\frac{1}{p_A}-(\beta-1)n^\star-1}(1-p_A(\beta-1)n^\star)\,. \tag{6.76}$$

This formula can be simplified by substituting the condition Eq. (6.53) to eliminate β

$$f(t_0) = p_An^\star\left(\frac{n^\star(1-p_A)}{n^\star-1}\right)^{n^\star-1}. \tag{6.77}$$

$\mathbb{E}[N]$ can now be upper bounded by an expression that depends on $f(t_0)$, that is

$$\mathbb{E}[N] \le \left(\frac{1}{\mathbb{E}[K]\beta}\sum_{k=1}^{\infty}p(K=k)f(t_0)^k k+1\right)\mathbb{E}[N_A]\,. \tag{6.78}$$

We can now average over the number of rounds k,

$$\sum_{k=1}^{\infty}\frac{p_r}{(1-p_r)}\left[(1-p_r)f(t_0)\right]^k k = \frac{p_r f(t_0)}{\left[1-(1-p_r)f(t_0)\right]^2}\,. \tag{6.79}$$

Moreover, $\mathbb{E}[K]=\frac{1}{p_r}$ and again removing β through condition Eq. (6.53) yields

$$\mathbb{E}[N] \le \left(\frac{p_r^2p_An^\star f(t_0)}{\left[1-(1-p_r)f(t_0)\right]^2}+1\right)\mathbb{E}[N_A] = \left(\frac{(1-(1-p_B)^{n^\star})^2p_An^\star f(t_0)}{\left[1-(1-p_B)^{n^\star}f(t_0)\right]^2}+1\right)\mathbb{E}[N_A]\,. \tag{6.80}$$

Now by taking the number of channel uses to be $\mathbb{E}[N_A]$, we can define the relative error $g_{\text{err}}(p_A, p_B, n^\star)$,

$$g_{\text{err}}(p_A, p_B, n^\star) := \frac{(1-(1-p_B)^{n^\star})^2 p_A n^\star f(t_0)}{\left[1-(1-p_B)^{n^\star} f(t_0)\right]^2}\,, \tag{6.81}$$

with $f(t_0)$ given in Eq. (6.77), so that

$$\mathbb{E}[N_A] \leq \mathbb{E}[N] \leq \left(g_{\text{err}}(p_A, p_B, n^\star)+1\right)\mathbb{E}[N_A]\,, \tag{6.82}$$

where the conditions required to satisfy the above formula are $n^\star > 1$ and $p_A n^\star < 1$. Finally, we can now show how $g_{\text{err}}(p_A, p_B, n^\star)$ scales with β. Note that

$$f(t_0) \leq p_A n^\star \left(1+\frac{1}{n^\star-1}\right)^{n^\star-1} \leq p_A n^\star e\,. \tag{6.83}$$

This together with $f(t_0) < 1$ gives

$$g_{\text{err}}(p_A, p_B, n^\star) < \frac{p_r^2 (p_A n^\star)^2 e}{p_r^2} = \frac{e}{\beta^2}\,. \tag{6.84}$$

Therefore $g_{\text{err}}(p_A, p_B, n^\star) = \mathcal{O}\left(\frac{1}{\beta^2}\right)$, implying that the bounds in the high-loss regime are good enough to tightly bound the achieved yield.

6

LOW-LOSS REGIME

Now we consider the complementary low-loss regime characterised by the condition $p_A n^\star \geq 1$. Firstly, since in our protocol there is never any benefit in placing the repeater closer to Alice than to Bob, we also have that $p_B \geq p_A$. This implies that $\frac{1}{p_B} \leq \frac{1}{p_A} = \mathbb{E}[N_A^i] \leq n^\star$. This is the regime where the cut-off is large in comparison with the average number of channel uses required to detect a single photon on Bob's side. That is,

$$\frac{\beta'}{p_B} = n^\star,\ n^\star \geq \beta' \geq 1\,. \tag{6.85}$$

As we will show in this section, in this region we can approximate $\mathbb{E}[N] = \mathbb{E}[\max(N_A, N_B)]$ by N_{NC}, where

$$N_{NC} = \frac{1}{p_A} + \frac{1}{p_B} - \frac{1}{p_A + p_B - p_A p_B}\,, \tag{6.86}$$

is the average number of channel uses in the no cut-off (NC) scenario [1, 2]. Intuitively, this is because Alice and Bob almost never have to restart due to Bob reaching the cut-off. More specifically, we show that

$$N_{NC} \leq \mathbb{E}[N] \leq \left(\tilde{g}_{\text{err}}(p_A, p_B, n^\star)+1\right) N_{NC}\,, \tag{6.87}$$

where $\tilde{g}_{\text{err}}(p_A, p_B, n^\star)$ is defined in Eq. (6.99). Since $\tilde{g}_{\text{err}}(p_A, p_B, n^\star) = \mathcal{O}\left(\beta' e^{-\beta'}\right)$, for sufficiently large β' the expectation value $\mathbb{E}[N]$ can be accurately approximated by N_{NC}.

Here we detail a proof of Eq. (6.87). We note that the presence of the cut-off increases the number of needed channel uses with respect to the no cut-off scenario, i.e. $N_{NC} \leq \mathbb{E}[N]$. For the upper bound we can write now

$$\mathbb{E}[N] = \mathbb{E}[\max(N_A, N_B)] \tag{6.88}$$

$$= \sum_{k=1}^{\infty} p(K=k) \left(\sum_{n_A=k}^{\infty} \left(\sum_{n_B=(k-1)n^\star+1}^{kn^\star} p(n_A \wedge n_B | K=k) \max(n_A, n_B) \right) \right) \tag{6.89}$$

$$= p(K=1) \sum_{n_B=1}^{n^\star} \sum_{n_A=1}^{\infty} p(n_A|K=1) p(n_B|K=1) \max(n_A, n_B)$$

$$+ \sum_{k=2}^{\infty} p(K=k) \left(\sum_{n_B=(k-1)n^\star+1}^{kn^\star} \left(\sum_{n_A=k}^{\infty} p(n_A \wedge n_B|k) \max(n_A, n_B) \right) \right) . \tag{6.90}$$

In Eq. (6.90) we split the sum over k into two terms, one with $k=1$ and the other with $k>1$. Since the first term has fixed $k=1$, the variables N_A and N_B are independent here (there is only one round in which Bob for sure succeeds, so the value of n_B doesn't affect the value of n_A). Moreover, the geometric distribution of N_B is normalised over the interval $[1,\ldots,n^\star]$.

$$\mathbb{E}[N] \leq p(K=1) N_{NC} + \sum_{k=2}^{\infty} p(K=k) \left(\sum_{n_B=(k-1)n^\star+1}^{kn^\star} \left(\sum_{n_A=k}^{\infty} p(n_A \wedge n_B|k) \max(n_A, kn^\star) \right) \right) . \tag{6.91}$$

We have upper bounded the first term of Eq. (6.90) by upper bounding the sum $\sum_{n_B=1}^{n^\star}$ with $\sum_{n_B=1}^{\infty}$. In this case the expression after $p(K=1)$ in the first term becomes N_{NC}. In the second term we upper bound n_B by $kn^\star$. Since the second term does not depend on n_B anymore we upper bound it by removing the constraints on N_B completely from the probabilities $p(n_A \wedge n_B|K=k)$, i.e.

$$\mathbb{E}[N] \leq p(K=1) N_{NC} + \sum_{k=2}^{\infty} p(K=k) \sum_{n_A=k}^{\infty} p(n_A|K=k) \max(n_A, kn^\star)$$

$$= p(K=1) N_{NC} + \sum_{k=2}^{\infty} p(K=k) \left(\sum_{n_A=k}^{kn^\star} p(n_A|K=k) kn^\star + \sum_{n_A=kn^\star+1}^{\infty} p(n_A|K=k) n_A \right) , \tag{6.92}$$

where in the last line of Eq. (6.92) we split the second term into two terms corresponding to the regime where $kn^\star$ is larger than n_A and vice versa. Since $kn^\star$ does not depend on n_A, we upper bound this term by removing the constraints on n_A,

$$\mathbb{E}[N] \leq p(K=1) N_{NC} + \sum_{k=2}^{\infty} p(K=k) kn^\star + \sum_{k=2}^{\infty} p(K=k) \sum_{n_A=k}^{\infty} p(n_A|K=k) n_A . \tag{6.93}$$

Eq. (6.93) can be greatly simplified. We can perform the sum over n_A in the third term obtaining $k\mu$. Then the sums over k can also be easily evaluated so that the right hand

side of Eq. (6.93) can be rewritten as

$$p(K=1)N_{NC} + \sum_{k=2}^{\infty} p(K=k)kn^\star + \sum_{k=2}^{\infty} p(K=k)k\mu \tag{6.94}$$

$$= p(K=1)N_{NC} + (n^\star + \mu)(\mathbb{E}(K) - p(K=1)) \tag{6.95}$$

$$= \left(p_r + \frac{n^\star + \mu}{N_{NC}}\left(\frac{1}{p_r} - p_r\right)\right)N_{NC} \tag{6.96}$$

$$= \left(p_r + \left(\frac{n^\star + \mu}{N_{NC}}\right)\left(\frac{1-p_r^2}{p_r}\right)\right)N_{NC}\,. \tag{6.97}$$

Hence we have that

$$N_{NC} \leq \mathbb{E}[N] \leq \left(\tilde{g}_{\text{err}}(p_A, p_B, n^\star) + 1\right)N_{NC}\,, \tag{6.98}$$

where $\tilde{g}_{\text{err}}(p_A, p_B, n^\star)$ is defined as

$$\tilde{g}_{\text{err}}(p_A, p_B, n^\star) := (1-p_B)^{n^\star}\left[\left(\frac{n^\star + \mu}{N_{NC}}\right)\left(\frac{2-(1-p_B)^{n^\star}}{1-(1-p_B)^{n^\star}}\right) - 1\right]\,. \tag{6.99}$$

We now show that $\tilde{g}_{\text{err}}(p_A, p_B, n^\star)$ is small compared to the other quantities in Eq. (6.98). Observe that

$$(1-p_B)^{n^\star} = \left(1 - \frac{\beta'}{n^\star}\right)^{n^\star} \leq e^{-\beta'}\,. \tag{6.100}$$

From Eq. (6.99) it follows that

$$\tilde{g}_{\text{err}}(p_A, p_B, n^\star) \leq e^{-\beta'}\left[\frac{n^\star + \frac{1}{p_A}}{N_{NC}}\left(\frac{2}{1-e^{-\beta'}}\right) - 1\right]\,. \tag{6.101}$$

To upper bound the relative error, we start by upper bounding the first term inside the brackets, namely

$$\frac{n^\star + \frac{1}{p_A}}{N_{NC}} = \frac{n^\star + \frac{1}{p_A}}{\frac{1}{p_A} + \frac{1}{p_B} - \frac{1}{p_A + p_B - p_A p_B}} \leq \frac{n^\star + \frac{1}{p_A}}{\frac{1}{p_A} + \frac{1}{p_B} - \frac{1}{p_A + p_B - p_A}} = p_A n^\star + 1\,. \tag{6.102}$$

$\tilde{g}_{\text{err}}(p_A, p_B, n^\star)$, then, is upper bounded by

$$\tilde{g}_{\text{err}}(p_A, p_B, n^\star) \leq e^{-\beta'}\left[(p_A n^\star + 1)\left(\frac{2}{1-e^{-\beta'}}\right) - 1\right] \tag{6.103}$$

$$= \frac{e^{-\beta'}}{1-e^{-\beta'}}(2p_A n^\star + 1 + e^{-\beta'}) \tag{6.104}$$

$$\leq \frac{e^{-\beta'}}{1-e^{-\beta'}}(2\beta' + 1 + e^{-\beta'}) \tag{6.105}$$

$$= e^{-\beta'}\left(\frac{2\beta'}{1-e^{-\beta'}} + \coth\left(\frac{\beta'}{2}\right)\right) \tag{6.106}$$

$$< e^{-\beta'}\left(\frac{2\beta'}{1-e^{-1}} + \coth\left(\frac{1}{2}\right)\right) \tag{6.107}$$

$$< e^{-\beta'}\coth\left(\frac{1}{2}\right)(2\beta' + 1) \tag{6.108}$$

$$< 3\coth\left(\frac{1}{2}\right)\beta' e^{-\beta'}\,. \tag{6.109}$$

Therefore $\tilde{g}_{\text{err}}(p_A, p_B, n^\star) = \mathcal{O}\left(\beta' e^{-\beta'}\right)$.

REFERENCES

[1] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, *Overcoming lossy channel bounds using a single quantum repeater node,* Applied Physics B **122**, 96 (2016).

[2] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, *Memory-assisted measurement-device-independent quantum key distribution,* New Journal of Physics **16**, 043005 (2014).

[3] D. Hucul, I. Inlek, G. Vittorini, C. Crocker, S. Debnath, S. Clark, and C. Monroe, *Modular entanglement of atomic qubits using photons and phonons,* Nature Physics **11**, 37 (2015).

[4] M. Blok, N. Kalb, A. Reiserer, T. Taminiau, and R. Hanson, *Towards quantum networks of single spins: analysis of a quantum memory with an optical interface in diamond,* Faraday Discussions **184**, 173 (2015).

[5] A. Reiserer, N. Kalb, M. S. Blok, K. J. van Bemmelen, T. H. Taminiau, R. Hanson, D. J. Twitchen, and M. Markham, *Robust quantum-network memory using decoherence-protected subspaces of nuclear spins,* Physical Review X **6**, 021040 (2016).

[6] W. Gao, A. Imamoglu, H. Bernien, and R. Hanson, *Coherent manipulation, measurement and entanglement of individual solid-state spins using optical fields,* Nature Photonics **9**, 363 (2015).

[7] A. Reiserer and G. Rempe, *Cavity-based quantum networks with single atoms and optical photons,* Reviews of Modern Physics **87**, 1379 (2015).

[8] M. M. Wilde, *Quantum information theory* (Cambridge University Press, 2013).

[9] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Fundamental limits of repeaterless quantum communications,* Nature Communications **8**, 15043 (2017).

[10] M. Takeoka, S. Guha, and M. M. Wilde, *Fundamental rate-loss tradeoff for optical quantum key distribution,* Nature Communications **5**, 5235 (2014).

[11] K. Goodenough, D. Elkouss, and S. Wehner, *Assessing the performance of quantum repeaters for all phase-insensitive gaussian bosonic channels,* New Journal of Physics **18**, 063005 (2016).

[12] M. M. Wilde and H. Qi, *Energy-constrained private and quantum capacities of quantum channels,* IEEE Transactions on Information Theory **64**, 7802 (2018).

[13] M. M. Wilde, M. Tomamichel, and M. Berta, *Converse bounds for private communication over quantum channels,* IEEE Transactions on Information Theory **63**, 1792 (2017).

[14] S. Pirandola and R. Laurenza, *General benchmarks for quantum repeaters,* arXiv preprint arXiv:1512.04945 (2015).

[15] M. Christandl and A. Müller-Hermes, *Relative entropy bounds on quantum, private and repeater capacities,* Communications in Mathematical Physics **353**, 821 (2017).

[16] B. R. Bardhan and M. M. Wilde, *Strong converse rates for classical communication over thermal and additive noise bosonic channels,* Physical Review A **89**, 022302 (2014).

[17] A. Khalique and B. C. Sanders, *Practical long-distance quantum key distribution through concatenated entanglement swapping with parametric down-conversion sources,* JOSA B **32**, 2382 (2015).

[18] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, *Rate-loss analysis of an efficient quantum repeater architecture,* Physical Review A **92**, 022357 (2015).

[19] H. Krovi, S. Guha, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, *Practical quantum repeaters with parametric down-conversion sources,* Applied Physics B **122**, 52 (2016).

[20] M. Pant, H. Krovi, D. Englund, and S. Guha, *Rate-distance tradeoff and resource costs for all-optical quantum repeaters,* Physical Review A **95**, 012304 (2017).

[21] D. Gottesman and H.-K. Lo, *Proof of security of quantum key distribution with two-way classical communications,* IEEE Transactions on Information Theory **49**, 457 (2003).

[22] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution,* Reviews of Modern Physics **81**, 1301 (2009).

[23] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* in *International Conference on Computer System and Signal Processing, IEEE, 1984* (1984) pp. 175–179.

[24] D. Bruß, *Optimal eavesdropping in quantum cryptography with six states,* Physical Review Letters **81**, 3018 (1998).

[25] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, *Squashing model for detectors and applications to quantum-key-distribution protocols,* Physical Review A **89**, 012325 (2014).

[26] E. Togan, Y. Chu, A. Trifonov, L. Jiang, J. Maze, L. Childress, M. G. Dutt, A. S. Sørensen, P. Hemmer, A. Zibrov, *et al.*, *Quantum entanglement between an optical photon and a solid-state spin qubit,* Nature **466**, 730 (2010).

[27] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau, *Repeated quantum error correction on a continuously encoded qubit by real-time feedback,* Nature Communications **7**, 11526 (2016).

[28] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. 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**, 928 (2017).

[29] K. Nemoto, M. Trupke, S. J. Devitt, B. Scharfenberger, K. Buczak, J. Schmiedmayer, and W. J. Munro, *Photonic quantum networks formed from nv- centers,* Scientific Reports **6** (2016).

[30] G. De Lange, Z. Wang, D. Riste, V. Dobrovitski, and R. Hanson, *Universal dynamical decoupling of a single solid-state spin from a spin bath,* Science **330**, 60 (2010).

[31] H. P. Specht, C. Nölleke, A. Reiserer, M. Uphoff, E. Figueroa, S. Ritter, and G. Rempe, *A single-atom quantum memory,* Nature **473**, 190 (2011).

[32] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, *Quantum repeaters based on atomic ensembles and linear optics,* Reviews of Modern Physics **83**, 33 (2011).

[33] C. Thiel, T. Böttger, and R. Cone, *Rare-earth-doped materials for applications in quantum information storage and signal processing,* Journal of Luminescence **131**, 353 (2011).

[34] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, *Squashing models for optical measurements in quantum communication,* Physical Review Letters **101**, 093601 (2008).

[35] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, *Key rate of quantum key distribution with hashed two-way classical communication,* Physical Review A **76**, 032312 (2007).

[36] M. A. Ballester, S. Wehner, and A. Winter, *State discrimination with post-measurement information,* IEEE Transactions on Information Theory **54**, 4183 (2008).

[37] H.-K. Lo, H. F. Chau, and M. Ardehali, *Efficient quantum key distribution scheme and a proof of its unconditional security,* Journal of Cryptology **18**, 133 (2005).

[38] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian quantum information,* Reviews of Modern Physics **84**, 621 (2012).

[39] M. Takeoka, S. Guha, and M. M. Wilde, *The squashed entanglement of a quantum channel,* Information Theory, IEEE Transactions on **60**, 4987 (2014).

[40] E. Kaur and M. M. Wilde, *Upper bounds on secret-key agreement over lossy thermal bosonic channels,* Physical Review A **96**, 062318 (2017).

[41] K. Sharma, M. M. Wilde, S. Adhikari, and M. Takeoka, *Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic gaussian channels,* New Journal of Physics **20**, 063025 (2018).

[42] N. Davis, M. E. Shirokov, and M. M. Wilde, *Energy-constrained two-way assisted private and quantum capacities of quantum channels,* Physical Review A **97**, 062310 (2018).

[43] C. Ottaviani, R. Laurenza, T. P. Cope, G. Spedalieri, S. L. Braunstein, and S. Pirandola, *Secret key capacity of the thermal-loss channel: Improving the lower bound,* in *Quantum Information Science and Technology II*, Vol. 9996 (International Society for Optics and Photonics, 2016) p. 999609.

[44] R. Laurenza, S. L. Braunstein, and S. Pirandola, *Finite-resource teleportation stretching for continuous-variable systems,* Scientific Reports **8**, 15267 (2018).

[45] R. Laurenza, S. Tserkis, S. L. Braunstein, T. C. Ralph, and S. Pirandola, *Tight finite-resource bounds for private communication over gaussian channels,* arXiv preprint arXiv:1808.00608 (2018).

[46] L. Robledo, L. Childress, H. Bernien, B. Hensen, P. F. A. Alkemade, and R. Hanson, *High-fidelity projective read-out of a solid-state spin quantum register,* Nature **477**, 574 (2011).

[47] W. Pfaff, B. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, *et al.*, *Unconditional quantum teleportation between distant solid-state quantum bits,* Science **345**, 532 (2014).

[48] M. H. Abobeih, J. Cramer, M. A. Bakker, N. Kalb, M. Markham, D. J. Twitchen, and T. H. Taminiau, *One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment,* Nature Communications **9**, 2552 (2018).

[49] T. H. Taminiau, J. Cramer, T. van der Sar, V. V. Dobrovitski, and R. Hanson, *Universal control and error correction in multi-qubit spin registers in diamond,* Nature Nanotechnology **9**, 171 (2014).

[50] N. Kalb, P. Humphreys, J. Slim, and R. Hanson, *Dephasing mechanisms of diamond-based nuclear-spin memories for quantum networks,* Physical Review A **97**, 062330 (2018).

[51] E. M. Purcell, H. C. Torrey, and R. V. Pound, *Resonance Absorption by Nuclear Magnetic Moments in a Solid,* Physical Review **69**, 37 (1946).

[52] S. Bogdanović, S. B. van Dam, C. Bonato, L. C. Coenen, A.-M. J. Zwerver, B. Hensen, M. S. Liddy, T. Fink, A. Reiserer, M. Lončar, *et al.*, *Design and low-temperature characterization of a tunable microcavity for diamond-based quantum networks,* Applied Physics Letters **110**, 171103 (2017).

[53] D. Englund, B. Shields, K. Rivoire, F. Hatami, J. Vučković, H. Park, and M. D. Lukin, *Deterministic coupling of a single nitrogen vacancy center to a photonic crystal cavity,* Nano Letters **10**, 3922 (2010).

[54] J. Wolters, A. W. Schell, G. Kewes, N. Nüsse, M. Schoengen, H. Döscher, T. Hannappel, B. Löchel, M. Barth, and O. Benson, *Enhancement of the zero phonon line emission from a single nitrogen vacancy center in a nanodiamond via coupling to a photonic crystal cavity,* Applied Physics Letters **97**, 141108 (2010).

[55] T. Van Der Sar, J. Hagemeier, W. Pfaff, E. C. Heeres, S. M. Thon, H. Kim, P. M. Petroff, T. H. Oosterkamp, D. Bouwmeester, and R. Hanson, *Deterministic nanoassembly of a coupled quantum emitter-photonic crystal cavity system,* Applied Physics Letters **98**, 193103 (2011).

[56] A. Faraon, C. Santori, Z. Huang, V. M. Acosta, and R. G. Beausoleil, *Coupling of nitrogen-vacancy centers to photonic crystal cavities in monocrystalline diamond,* Physical Review Letters **109**, 2 (2012).

[57] B. J. Hausmann, B. J. Shields, Q. Quan, Y. Chu, N. P. De Leon, R. Evans, M. J. Burek, A. S. Zibrov, M. Markham, D. J. Twitchen, H. Park, M. D. Lukin, and M. Loncar, *Coupling of NV centers to photonic crystal nanobeams in diamond,* Nano Letters **13**, 5791 (2013).

[58] J. C. Lee, D. O. Bracher, S. Cui, K. Ohno, C. A. McLellan, X. Zhang, P. Andrich, B. Alemán, K. J. Russell, A. P. Magyar, I. Aharonovich, A. Bleszynski Jayich, D. Awschalom, and E. L. Hu, *Deterministic coupling of delta-doped nitrogen vacancy centers to a nanobeam photonic crystal cavity,* Applied Physics Letters **105**, 261101 (2014).

[59] L. Li, T. Schröder, E. H. Chen, M. Walsh, I. Bayn, J. Goldstein, O. Gaathon, M. E. Trusheim, M. Lu, J. Mower, M. Cotlet, M. L. Markham, D. J. Twitchen, and D. Englund, *Coherent spin control of a nanocavity-enhanced qubit in diamond,* Nature Communications **6**, 6173 (2015).

[60] J. Riedrich-Möller, S. Pezzagna, J. Meijer, C. Pauly, F. Mücklich, M. Markham, A. M. Edmonds, and C. Becher, *Nanoimplantation and Purcell enhancement of single nitrogen-vacancy centers in photonic crystal cavities in diamond,* Applied Physics Letters **106**, 221103 (2015).

[61] A. Faraon, P. E. Barclay, C. Santori, K. M. C. Fu, and R. G. Beausoleil, *Resonant enhancement of the zero-phonon emission from a colour centre in a diamond cavity,* Nature Photonics **5**, 301 (2011).

[62] P. E. Barclay, K. M. C. Fu, C. Santori, A. Faraon, and R. G. Beausoleil, *Hybrid nanocavity resonant enhancement of color center emission in diamond,* Physical Review X **1**, 1 (2011).

[63] M. Gould, E. R. Schmidgall, S. Dadgostar, F. Hatami, and K. M. C. Fu, *Efficient Extraction of Zero-Phonon-Line Photons from Single Nitrogen-Vacancy Centers in an Integrated GaP-on-Diamond Platform,* Physical Review Applied **6**, 2 (2016).

[64] H. Kaupp, C. Deutsch, H. C. Chang, J. Reichel, T. W. Hänsch, and D. Hunger, *Scaling laws of the cavity enhancement for nitrogen-vacancy centers in diamond,* Physical Review A **88**, 1 (2013).

[65] S. Johnson, P. R. Dolan, T. Grange, A. A. Trichet, G. Hornecker, Y. C. Chen, L. Weng, G. M. Hughes, A. A. Watt, A. Auffèves, and J. M. Smith, *Tunable cavity coupling of the zero phonon line of a nitrogen-vacancy defect in diamond,* New Journal of Physics **17**, 122003 (2015).

[66] D. Riedel, I. Söllner, B. J. Shields, S. Starosielec, P. Appel, E. Neu, P. Maletinsky, and R. J. Warburton, *Deterministic enhancement of coherent photon generation from a nitrogen-vacancy center in ultrapure diamond,* Physical Review X **7**, 031040 (2017).

[67] D. Hunger, T. Steinmetz, Colombe, Y., C. Deutsch, T. W. Hänsch, and J. Reichel, *A fiber Fabry-Perot cavity with high finesse,* New Journal of Physics **12**, 065038 (2010).

[68] E. Janitz, M. Ruf, M. Dimock, A. Bourassa, J. Sankey, and L. Childress, *Fabry-Perot microcavity for diamond-based photonics,* Physical Review A **92**, 1 (2015).

[69] L.-M. Duan and H. Kimble, *Scalable photonic quantum computation through cavity-assisted interactions,* Physical Review Letters **92**, 127902 (2004).

[70] Available on request.

[71] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham, *et al.*, *Room-temperature quantum bit memory exceeding one second,* Science **336**, 1283 (2012).

[72] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, *et al.*, *Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres,* Nature **526**, 682 (2015).

[73] R. Paschotta, *Article on 'fibers' in* Encyclopedia of Laser Physics and Technology, `https://www.rp-photonics.com/fibers.html`.

[74] Y. Tamura, H. Sakuma, K. Morita, M. Suzuki, Y. Yamamoto, K. Shimada, Y. Honma, K. Sohma, T. Fujii, and T. Hasegawa, *Lowest-ever 0.1419-db/km loss optical fiber,* in *Optical Fiber Communication Conference* (Optical Society of America, 2017) pp. Th5D–1.

[75] G. Keiser, *Optical Fiber Communications*, 4th ed. (McGraw-Hill, 2011).

[76] S. Zaske, A. Lenhard, C. A. Keßler, J. Kettler, C. Hepp, C. Arend, R. Albrecht, W.-M. Schulz, M. Jetter, P. Michler, *et al.*, *Visible-to-telecom quantum frequency conversion of light from a single quantum emitter,* Physical Review Letters **109**, 147404 (2012).

[77] N. L. Piparo, M. Razavi, and W. J. Munro, *Memory-assisted quantum key distribution with a single nitrogen-vacancy center,* Physical Review A **96**, 052313 (2017).

[78] N. L. Piparo, M. Razavi, and W. J. Munro, *Measurement-device-independent quantum key distribution with nitrogen vacancy centers in diamond,* Physical Review A **95**, 022338 (2017).

[79] H.-K. Lo, M. Curty, and B. Qi, *Measurement-device-independent quantum key distribution,* Physical Review Letters **108**, 130503 (2012).

[80] N. L. Piparo, N. Sinclair, and M. Razavi, *Memory-assisted quantum key distribution resilient against multiple-excitation effects,* Quantum Science and Technology **3**, 014009 (2017).

7

NEAR-TERM QUANTUM-REPEATER EXPERIMENTS WITH NV CENTERS: OVERCOMING THE LIMITATIONS OF DIRECT TRANSMISSION

Filip Rozpędek [*], Raja Yehia [*], Kenneth Goodenough [*], Maximilian Ruf, Peter Humphreys, Ronald Hanson, Stephanie Wehner and David Elkouss

Quantum channels enable the implementation of communication tasks inaccessible to their classical counterparts. The most famous example is the distribution of secret keys. However, in the absence of quantum repeaters the rate at which these tasks can be performed is dictated by the losses in the quantum channel. In practice, channel losses have limited the reach of quantum protocols to short distances. Quantum repeaters have the potential to significantly increase the rates and reach beyond the limits of direct transmission. However, no experimental implementation has overcome the direct transmission threshold. Here, we propose three quantum repeater schemes and assess their ability to generate secret key when implemented on a setup using NV centers in diamond with near-term experimental parameters. We find that one of these schemes - the so-called single-photon scheme, requiring no quantum storage - has the ability to surpasses the capacity - the highest secret-key rate achievable with direct transmission - by a factor of seven, establishing it as a prime candidate for the first experimental realization of a quantum repeater.

The results of this chapter have been published in Phys. Rev. A **99**, 052330 (2019).
[*]These authors contributed equally.

7.1. INTRODUCTION

In this chapter we build upon the ideas presented in the previous chapter to devise further proof of principle repeater schemes. Specifically, in this chapter we propose three such new schemes and together with the fourth scheme analyzed before in [1] and Chapter 6, we assess their performance for generating secret key. We again consider their implementation based on nitrogen-vacancy centers in diamond (NV centers), a system which has properties making it an excellent candidate for long-distance quantum communication applications [2–10].

The four considered schemes are: the "single sequential quantum repeater node" (first proposed and studied in [1], then further analyzed in Chapter 6), the single-photon scheme (proposed originally in the context of remote entanglement generation [11] as introduced in Chapter 3, also studied in the context of secret-key generation without quantum memories [12]), and two schemes which are a combination of the first two. See Fig. 7.1 for a schematic overview of the repeater proposals considered in this work.

We compare the *secret-key rate* of each of these schemes to the highest theoretically achievable secret-key rate using direct transmission, the *secret-key capacity of the pure-loss channel* [13]. We show that one of these schemes, the *single-photon scheme*, can surpass the secret-key capacity by a factor of seven for a distance of ≈ 9.2 km with near-term parameters. This shows the viability of this scheme for the first experimental implementation of a quantum repeater.

In Section 7.2 we discuss and detail the different repeater proposals that will be assessed in this work. In Section 7.3 we expand on how the different components of the repeater proposals would be implemented experimentally. Section 7.4 details how to calculate the secret-key rate achieved with the quantum repeater proposals from the modeled components. In Section 7.5 we discuss how to assess the performance of a quantum repeater. The comparison of the different repeater proposals is performed in Section 7.6, which allows us to conclude with our results in Section 7.7. The numerical results of this article were produced with a Python and a Mathematica script, which are available upon request.

7.2. QUANTUM REPEATER SCHEMES

In the following section we present the quantum repeater schemes that will be assessed in this work. All these schemes use NV center based setups which involve memory nodes consisting of an electron spin qubit acting as an optical interface and possibly an additional carbon ^{13}C nuclear spin qubit acting as a long-lived quantum memory. Specifically, the optical interface of the electron spin allows for the generation of spin-photon entanglement, where the photonic qubits can then be transmitted over large distances. The carbon nuclear spin acts as a long-lived memory, but can be accessed only through the interaction with the electron spin. Here, we briefly go over all the proposed schemes, motivate why they are interesting from an experimental perspective and discuss their advantages and disadvantages. The first scheme of the Single Sequential Quantum Repeater (SiSQuaRe) has already been introduced in Chapter 6.

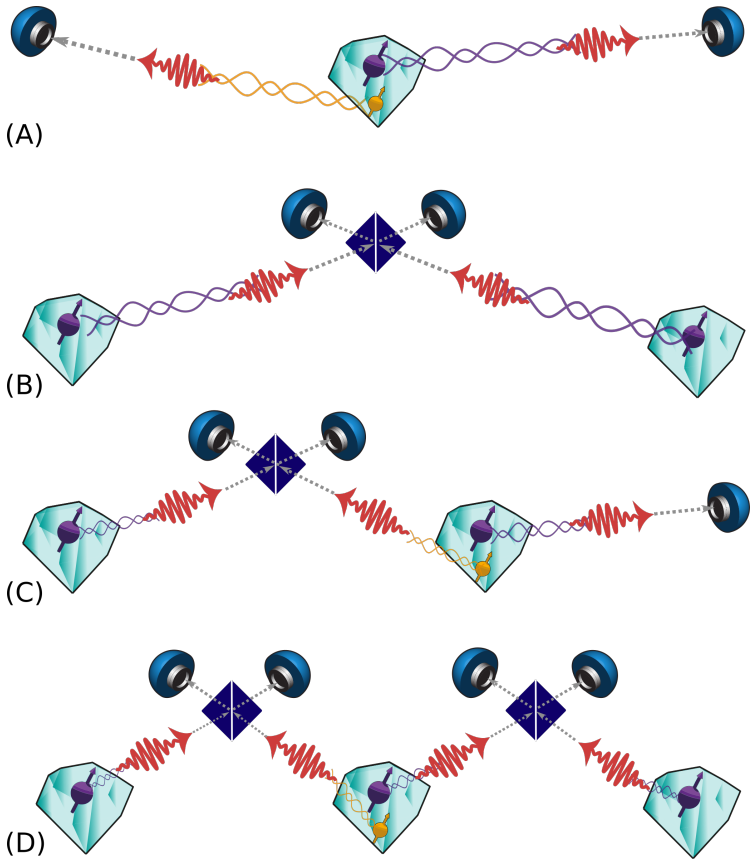

Figure 7.1: Schematic overview of the four quantum repeater schemes assessed in this chapter. From top to bottom: the Single Sequential Quantum Repeater (SiSQuaRe) scheme (A), the single-photon scheme (B), the Single-Photon with Additional Detection Setup (SPADS) scheme (C) and the Single-Photon Over Two Links (SPOTL) scheme (D). The purple particles represent NV electron spins capable of emitting photons (red wiggly arrows) while the yellow particles represent carbon ^{13}C nuclear spins. Dark blue squares depict the beam splitters used to erase the which-way information of the photons, followed by blue photon detectors. For more details on the different proposals, see Section 7.2.

7.2.1. THE SINGLE-PHOTON SCHEME

Let us now recall the single-photon scheme introduced in Section 3.3.1 in Chapter 3. This scheme devised by Cabrillo et al. [11] is a procedure that allows for the heralded generation of entanglement between a separated pair of matter qubits (their proposal discusses specific implementation with single atoms, but the scheme can also be applied to other platforms such as NV centers or quantum dots) using linear optics. For the atomic ensemble platform this scheme also forms a building block of the DLCZ quantum repeater scheme, named after the authors Duan, Lukin, Cirac, and Zoller [14]. The requirement of successful transmission of only a single photon from one node to the middle heralding station makes it possible for this scheme to qualify as a quantum repeater (see below for more details).

Recall, that the basic setup of the single-photon scheme consists of placing a beam splitter and two detectors between Alice and Bob, with both parties simultaneously sending a photonic quantum state towards the beam splitter. The transmitted quantum state is entangled with a quantum memory, and the state space of the photon is spanned by the two states corresponding to the presence and absence of a photon. Immediately after transmitting their photons through the fiber, both Alice and Bob measure their quantum memories in a BB84 or six-state basis (see the discussion of which quantum key distribution protocol is optimal for each scheme in Section 7.4.2 and in Section 7.6.1). Note that this is equivalent to preparing a specific state of the photonic qubit and therefore is closely linked to the measurement device independent quantum key distribution (MDI QKD) [15] as discussed in Appendix 7.8.9. However, preparing specific states that involve the superposition of the presence and absence of a photon on its own is generally experimentally challenging. The NV-implementation allows us to achieve this task precisely by preparing spin-photon entanglement and then measuring the spin qubit. Afterwards, by conditioning on the click of a single detector only, Alice and Bob can use the information of which detector clicked to generate a single raw bit of key, see Appendix 7.8.5 and [11] for more information.

The main motivation of this scheme is that, informally, we only need one photon to travel half the distance between the two parties to get an entangled state. This thus effectively reduces the effects of losses, and in the ideal scenario the secret-key rate would scale with the square root of the total transmissivity η, as opposed to linear scaling in η (which is the optimal scaling without a quantum repeater [16]).

However, as discussed in Section 3.3.1 in Chapter 3, one problem that one faces when implementing this scheme is that the fiber induces a phase shift on the transmitted photons. This shift can change over time, e.g. due to fluctuations in the temperature and vibrations of the fiber. The uncertainty of the phase shift induces dephasing noise on the state, reducing the quality of the state.

To overcome this problem, a two-photon scheme was proposed by Barrett and Kok [17] which we have also already introduced in Section 3.3.1 in Chapter 3. We have shown there that this scheme does not place such high requirement on the optical stability of the setup. Specifically, in the Barrett and Kok scheme the problem of optical phase fluctuations is overcome by requiring two consecutive clicks and performing additional spin flip operations on both of the remote memories. The Barrett and Kok scheme has seen implementation in many experiments [18–21]. However, the requirement of two consec-

utive clicks implies that a setup using only the Barrett and Kok scheme with two memory nodes will never be able to satisfy the demands of a quantum repeater. Specifically, the probability of getting two consecutive clicks will not be higher than the transmissivity of the fiber between the two parties and therefore will not surpass the secret-key capacity.

In the single-photon scheme, on the other hand, the dephasing caused by the unknown optical phase shift is overcome by using active *phase-stabilization* of the fiber to reduce the fluctuations in the induced phase. This technique has been used in the experimental implementations of the single-photon scheme for remote entanglement generation using quantum dots [22, 23], NV centers [2] and atomic ensembles [24]. For experimental details relating to NV-implementation, we refer the reader to Section 7.3. This phase-stabilization technique effectively reduces the uncertainty in the phase, allowing us to significantly mitigate the resulting dephasing noise, see Appendix 7.8.1 for mathematical details.

In contrast to the Barrett and Kok scheme, the single-photon scheme cannot produce a perfect maximally entangled state, even in the case of perfect operations and perfect phase-stabilization. This is because losses in the channel result in a significant probability of having both nodes emitting a photon which can also lead to a single click in one of the detectors, yet the memories will be projected onto a product state as discussed in Section 3.3.1 in Chapter 3. This noise can be traded versus the probability of success of the scheme by reducing the weight of the photon-presence term in the generated spin-photon entangled state. This is also discussed in more detail below and the full analysis is presented in Appendix 7.8.5.

The single-photon scheme with phase-stabilization is a promising candidate for a near-term quantum repeater with NV centers. We note here that recently other QKD schemes that use the MDI framework have been proposed. These schemes, similarly to our proposal, use single-photon detection events to overcome the linear scaling of the secret-key rate with η [12, 25, 26]. In these proposals, in contrast to our single-photon scheme, no quantum memories are used, but instead Alice and Bob send phase-randomized optical pulses to the middle heralding station.

SETUP AND SCHEME

In the setup of the single-photon scheme Alice and Bob are separated by a fiber where in the center there is a beam splitter with two detectors (see Fig. 7.2). They will both create entanglement between a photonic qubit and a stored spin and send the photonic qubit to the beam splitter.

Alice and Bob thus perform the following,

1. Alice and Bob both prepare a state $|\psi\rangle = \sin\theta|\downarrow\rangle|0\rangle + \cos\theta|\uparrow\rangle|1\rangle$ where $|\downarrow\rangle/|\uparrow\rangle$ refers to the dark/bright state of the electron-spin qubit, $|0\rangle/|1\rangle$ indicates the absence/presence of a photon, and θ is a tunable parameter.

2. Alice and Bob attempt to both separately send the photonic qubit to the beam splitter.

3. Alice and Bob both perform a six-state measurement on their memories.

4. The previous steps are repeated until only one of the detectors between the parties clicks.

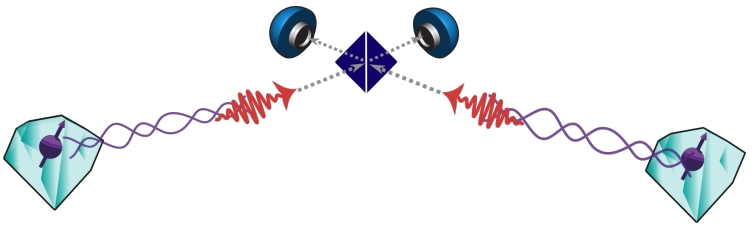

Figure 7.2: Schematic overview of the single-photon scheme. Alice and Bob simultaneously transmit a photonic state from their NV centers towards a balanced beam splitter in the center. This photonic qubit, corresponding to the presence and absence of a photon, is initially entangled with the NV electron spin. If only one of the detectors (which can be seen at the top of the figure) registers a click, Alice and Bob can use the information of which detector clicked to generate a single raw bit of key.

5. The information of which detector clicked gets sent to Alice and Bob for classical correction.

6. All the previous step are repeated until sufficient data have been generated.

The parameter θ can be chosen by preparing a non-uniform superposition of the dark and bright state of the electron spin $|\psi\rangle = \sin\theta|\downarrow\rangle + \cos\theta|\uparrow\rangle$ via coherent microwave pulses. This is done before applying the optical pulse to the electron which entangles it with the presence and absence of a photon. The parameter θ can then be tuned in such a way as to maximize the secret-key rate. In the next section, we will briefly expand on some of the issues arising when losses and imperfect detectors are present. We defer the full explanation and calculations until Appendix 7.8.5.

REALISTIC SETUP

In any realistic implementation of the single-photon scheme, a large number of attempts is needed before a photon detection event is observed. Furthermore, a single detector registering a click does not necessarily mean that the state of the memories is projected onto the maximally entangled state. This is due to multiple reasons, such as losing photons in the fiber or in some other loss process between the emission and detection, arrival of the emitted photons outside of the detection time-window and the fact that *dark counts* generate clicks at the detectors. Photon loss in the fiber effectively acts as amplitude-damping on the state of the photon when using the presence/absence state space [13, 27]. Dark counts are clicks in the detectors, caused by thermal excitations. These clicks introduce noise, since it is impossible to distinguish between clicks caused by thermal excitations and the photons traveling through the fiber if they arrive in the same time-window. All these sources of loss and noise acting on the photonic qubits are discussed in detail in Appendix 7.8.1. Finally we note that we assume here the application of non-number resolving detectors. This can lead to additional noise in the low loss regime, since the event in which two photons got emitted cannot be distinguished from the single-photon emission events even if no photons got lost. However, in any realistic loss regime this is not a problem, since the probability of two such photons arriving at the heralding station is quadratically suppressed with respect to events where only one

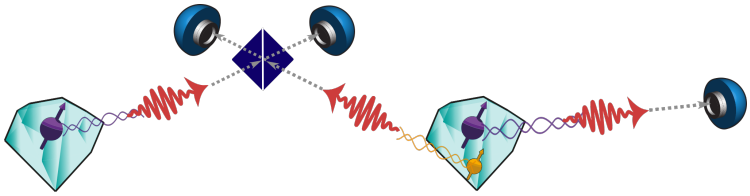

Figure 7.3: Schematic overview of the SPADS scheme. First, the two NV centers run the single-photon scheme, such that Alice measures her electron spin directly after every attempt. After success, the middle node swaps its state to the carbon spin. Then the middle node generates electron-photon entangled pairs where the photonic qubit is encoded in the time-bin degree of freedom and sent to Bob. This is attempted until Bob successfully measures the photon or until the cut-off is reached. If the cut-off is reached, the scheme gets restarted, otherwise the middle node performs an entanglement swapping on its two memories and communicates the classical outcome to Alice and Bob, who can correct their measurement outcomes to obtain a bit of raw key.

photon arrives. In the realistic regime, almost all the noise coming from the impossibility of distinguishing two-photon from single-photon emission events is the result of photon loss. Namely, if a two-photon emission event occurs and the detector registers a click, then with dominant probability it is due to only a single photon arriving, while the other one being lost. Hence the use of photon-number resolving detectors would not give any visible benefit with respect to the use of the non-number resolving ones. For a detailed calculation of the effects of losses and dark counts for the single-photon scheme, see Appendix 7.8.5.

7.2.2. SINGLE-PHOTON WITH ADDITIONAL DETECTION SETUP (SPADS) SCHEME

The third scheme that we consider here is the Single-Photon with Additional Detection Setup (SPADS) scheme, which is effectively a combination of the single-photon scheme and the SiSQuaRe scheme as shown in Fig. 7.3. If the middle node is positioned at two-thirds of the total distance away from Alice, the rate of this setup would scale, ideally, with the cube root of the transmissivity η.

This scheme runs as follows:

1. Alice and the repeater run the single-photon scheme until success, however, only Alice performs her spin measurement immediately after each spin-photon entanglement generation attempt. This measurement is either in a six-state or BB84 basis.

2. The repeater swaps the state of the electron spin onto the carbon spin.

3. The repeater runs the second part of the SiSQuaRe scheme with Bob. This means it generates spin-photon entanglement between an electron and the time-bin encoded photonic qubit. Afterwards, it sends the photonic qubit to Bob. This is repeated until Bob successfully measures his photon in a six-state or BB84 basis or until the cut-off n^* is reached in which case the scheme is restarted with step 1.

4. After Bob has received the photon and communicated this to the repeater, the repeater performs a Bell-state measurement on its two quantum memories and communicates the classical result to Bob.

5. All the previous steps are repeated until sufficient data have been generated.

The motivation for introducing this scheme is two-fold. Firstly, we note that by using this scheme we divide the total distance between Alice and Bob into three segments: two segments corresponding to the single-photon subscheme and the third segment over which the time-bin encoded photons are sent. This gives us one additional independent segment with respect to the single-photon or the SiSQuaRe scheme on their own. Hence, for distances where no cut-off is required, we expect the scaling of the secret-key rate with the transmissivity to be better than the ideal square root scaling of the previous two schemes. Furthermore, dividing the total distance into more segments should also allow us to reach larger distances before dark counts become significant. When considering the resources necessary to run this scheme, we note that the additional third node needs to be equipped only with a photon detection setup.

Secondly, we note that the SPADS scheme can also be naturally compared to the scenario in which an NV center is used as a single photon source for direct transmission between Alice and Bob. Both the setup for the SPADS scheme and such direct transmission involve Alice using an NV for emission and Bob having only a detector setup. Hence, the SPADS scheme corresponds to inserting a new NV-node (the repeater) between Alice and Bob without changing their local experimental setups at all. This motivates us to compare the achievable secret-key rate of the SPADS scheme and direct transmission. We perform this comparison on a separate plot in Section 7.6.

7.2.3. SINGLE-PHOTON OVER TWO LINKS (SPOTL) SCHEME

The final scheme that we study here is the Single-Photon Over Two Links (SPOTL) scheme, and it is another combination of the single-photon and SiSQuaRe schemes. A node is placed between Alice and Bob which tries to sequentially generate entanglement with their quantum memories by using the single-photon scheme (see Fig. 7.4). The motivation for this scheme is that, while using relatively simple components and without imposing stricter requirement on the memories than in the previous schemes, its secret-key rate would ideally scale with the fourth root of the transmissivity η.

SETUP AND SCHEME

The setup that we study is the following:

1. Alice and the repeater run the single-photon scheme until success with the tunable parameter $\theta = \theta_A$. However, only Alice performs her spin measurement immediately after each spin-photon entanglement generation attempt. This measurement is in a six-state basis.

2. The repeater swaps the state of the electron spin onto the carbon spin.

3. Bob and the repeater run the single-photon scheme until success or until the cut-off n^* is reached in which case the scheme is restarted with step 1. The tunable

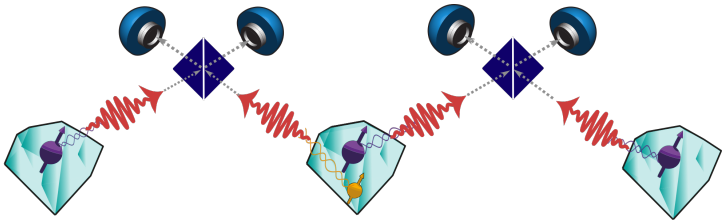

Figure 7.4: Schematic overview of the setup for the SPOTL scheme. This scheme is a combination of the SiSQuaRe and single-photon scheme. Instead of sending photons directly through the fiber as in the SiSQuaRe scheme, entanglement is established between the middle node and Alice/Bob using the single-photon scheme.

parameter is set here to $\theta = \theta_B$. Again, only Bob performs his spin measurement immediately after each spin-photon entanglement generation attempt and this measurement is in a six-state basis.

4. The quantum repeater performs a Bell-state measurement and communicates the result to Bob.

5. All the previous steps are repeated until sufficient data have been generated.

We note that for larger distances the optimal cut-off becomes smaller. Then, since we lose the independence of the attempts on both sides, the scaling of the secret-key rate with distance is expected to drop to $\sqrt{\eta}$, which is the same as for the single-photon scheme. However, the total distance between Alice and Bob is now split into four segments. Alice and Bob thus send photons over only one fourth of the total distance. Thus, this scheme should be able to generate key over much larger distances than the previous ones, as the dark counts will start becoming significant for larger distances only.

7.3. NV-IMPLEMENTATION

Having proposed different quantum repeater schemes, we now move on to describe their experimental implementation based on nitrogen-vacancy centers in diamond [28]. Most of the components are the same as required for the SiSQuRe scheme and therefore have already been described in Section 6.6 of Chapter 6. Here we describe the additional components utilised only by the three new schemes. We also refer the reader to Appendix 7.8.2 for details relating the noise model of the NV-based memory qubits.

By applying selective optical pulses and coherent microwave rotations, we first generate spin-photon entanglement at an NV center node [20]. To generate entanglement between two distant NV electron spins, these emitted photons are then overlapped on a central beam splitter to remove their which-path information. Subsequent detection of a single photon heralds the generation of a spin-spin entangled state [20]. For all schemes based on single-photon entanglement generation, we need to employ active phase-stabilization techniques to compensate for phase shifts of the transmitted photons, which will reduce the entangled state fidelity, as introduced in Section 7.2.1. These fluctuations arise from both mechanical vibrations and temperature induced changes in

optical path length, as well as phase fluctuations of the lasers used during spin-photon entanglement generation. This problem can be mitigated by using light reflected off the diamond surface to probe the phase of an effectively formed interferometer between the two NV nodes and the central beam splitter, and by feeding the acquired error signal back to a fiber stretcher that changes the relative optical path length [2].

7.4. CALCULATION OF THE SECRET-KEY RATE

With the modelling of each of the components of the different setups in hand, the performance of each setup can be estimated. The performance of a setup is again assessed by its ability to shared generate secret key between two parties Alice and Bob quantified by the secret-key rate, which allows us to make concrete information-theoretical statements about our ability to generate such secret key. We further discuss the significance of the secret-key rate and its relation to throughput in Section 7.6.5.

Recall, that the secret-key rate R is equal to

$$R = \frac{Y \cdot r}{N_{\text{modes}}}, \tag{7.1}$$

where Y and r are the yield and secret-key fraction, respectively. The yield Y is defined as the average number of raw bits generated per channel use and the secret-key fraction r is defined as the amount of secret key that can be extracted from a single raw bit (in the limit of asymptotically many rounds). Here N_{modes} is the number of optical modes needed to run the scheme. Time-bin encoding requires two modes while the single-photon scheme uses only one mode. Hence $N_{\text{modes}} = 2$ for all the schemes that use time-bin encoding in at least one of the arms of the setup. For the schemes that use only the single-photon subschemes as their building blocks we have that $N_{\text{modes}} = 1$.

In the remainder of this section, we will briefly detail how to calculate the yield and secret-key fraction, from which we can estimate the secret-key rate of each scheme.

7.4.1. YIELD

The yield depends not only on the used scheme, but also on the losses in the system. We model the general emission and transmission of photons through fibers from NV centers in diamond similarly as in Chapter 6. However, the modelled considered here is made more accurate than in the previous chapter by including also the element of variable detection time-window. Moreover, since here we consider exclusively the NV based implementation, we adjust the names of the parameters defined in Chapter 6 to reflect that fact. We represent the loss processes graphically in Fig. 7.5. Specifically, with probability p_{ce} spin-photon entanglement is generated and the photon is coupled into a fiber. The photons that successfully got coupled into the fiber might not be useful for quantum information processing since they are not coherent. Thus, we filter out those photons that are not emitted at the zero-phonon line, reducing the number of photons by a further factor of p_{zpl}. Then, over the length of the fiber, a photon gets lost with probability $1 - \eta_f = 1 - e^{-\frac{L}{L_0}}$, where L_0 is the attenuation length and η_f is the transmissivity. After exiting the fiber the photon gets registered as a click by the detector

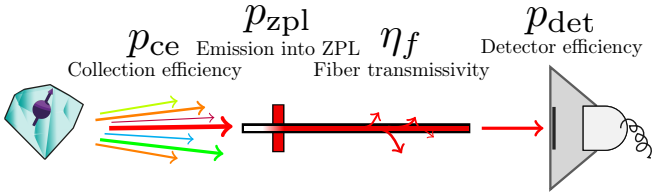

Figure 7.5: The model of photon loss proccesses occurring in our repeater setups. The parameter p_{ce} is the photon collection efficiency, which includes the probability that the photon is successfully coupled into the fiber. Only photons emitted at the zero phonon line (ZPL) can be used for quantum information processing. All non-ZPL photons are filtered out, such that a fraction p_{zpl} of the photons remains. The photons are then transmitted through a fiber with transmissivity η_f. Such successful transmissions are registered by the detector with probability p_{det}. Additionally, a significant fraction of photons can arrive in the detector outside of the detection time-window t_{w}. Such photons will effectively also get discarded. Here we describe the total efficiency of our apparatus by a single parameter, $p_{\text{app}} = p_{\text{ce}} p_{\text{zpl}} p_{\text{det}}$.

with probability p_{det}. Finally, the photon gets accepted as a successful click if the click happens within the time-window t_{w} of the detector (see Appendix 7.8.1 for more details).

Recall that the yield can then be calculated as the reciprocal of the expected number of channel uses needed to get one single raw bit,

$$Y = \frac{1}{\mathbb{E}[N]}\,, \tag{7.2}$$

with N being the random variable that models the number of channel uses needed for generating a single raw bit.

YIELD OF THE SINGLE-PHOTON SCHEME

The yield of the single-photon scheme is relatively easy to calculate, since the single condition heralding the success of the scheme is a single click in one of the detectors in the heralding station. Therefore the yield Y is simply the probability that an individual attempt will result in a single click in one of the detectors. This probability will depend on the losses in the system, dark counts and the angle θ. A full calculation of the yield is given in Appendix 7.8.5.

YIELD OF THE SISQUARE, SPADS AND SPOTL SCHEMES

The SiSQuaRe, SPADS and SPOTL schemes require two conditions for the heralding of the successful generation of a raw bit, namely the scheme needs to succeed both on Alice's and Bob's side independently. In this case we are going to take a very conservative perspective and assume the total number of channel uses to be the sum of the required channel uses on Alice's and Bob's side of the memory repeater node

$$\mathbb{E}[N] = \mathbb{E}[N_A + N_B]\,. \tag{7.3}$$

Moreover, every time Bob reaches n^* attempts, both parties start the scheme over again. The cut-off increases the average number of channel uses, thus decreasing the yield.

Denoting by p_A and p_B the probability that a single attempt of the subscheme on Alice's and Bob's side respectively succeeds, we find (see Appendix 7.8.3 for the derivation),

$$\mathbb{E}[N_A + N_B] = \frac{1}{p_A\left(1-\left(1-p_B\right)^{n^*}\right)} + \frac{1}{p_B}\,. \tag{7.4}$$

7.4.2. SECRET-KEY FRACTION

Similarly as in Chapter 6 we consider the same two asymptotic protocols for generating secret key: BB84 with standard one-way error correction and six-state with advantage distillation [29]. We recall that for technical reasons within our model it is not possible to run an asymmetric six-state protocol when time-bin encoded photons are to be measured by Alice or Bob, see Chapter 6. The expressions for the secret-key fraction for these protocols have already been discussed in Chapter 6. In Appendix 7.8.7 we elaborate on specific subtleties relating to the basis in which the key is extracted.

Now we can state explicitly which QKD protocols will be considered for each scheme, which in turn depends on the type of measurements that Alice and Bob perform in that scheme. There are two physical implementations of measurements that Alice and Bob perform, depending on the scheme under consideration. That is, they either measure a quantum state of a spin or of a time-bin encoded photons. Since the fully asymmetric six-state protocol with advantage distillation has higher efficiency than both symmetric and asymmetric BB84 protocol with one-way error correction, we will use this six-state protocol for both the single-photon and SPOTL scheme. The SiSQuaRe and SPADS schemes involve direct measurement on time-bin encoded photons. Hence, for these schemes we consider the maximum of the amount of key that can be obtained using the fully asymmetric BB84 protocol and the symmetric six-state protocol with advantage distillation (which can tolerate more noise, but has three times lower efficiency than the fully asymmetric BB84 protocol).

To estimate the QBER, we model all the noisy and lossy processes that take place during the protocol run. From this, we calculate the qubit error rates and yield, from which we can retrieve the secret-key fraction. We invite the interested reader to read about the details of these calculations in Appendices 7.8.5 and 7.8.6. The derivation of the QBER and the yield for the SiSQuaRe scheme is performed in Chapter 6. Moreover, in this work we introduce certain refinements to the model which we discuss in Appendix 7.8.4. With the QBER in hand, we can calculate the resulting secret-key fraction for the considered protocols as presented in Chapter 6 and in the Appendix 7.8.7.

We note here that we consider only the secret-key rate in the asymptotic limit, and that we thus do not have to deal with non-asymptotic statistics.

7.5. ASSESSING THE PERFORMANCE OF QUANTUM REPEATER SCHEMES

In this section we will detail four benchmarks that will be used to assess the performance of quantum repeaters. These benchmarks are analogous to the benchmarks used in Chapter 6.

Again, the considered benchmarks are defined with respect to the efficiencies of processes involving photon loss when emitting photons at NV centers, transmitting them through an optical fiber and detecting them at the end of the fiber as described in Section 7.4.1 and as shown in Fig. 7.5.

Having this picture in mind, we can now proceed to present the considered benchmarks. The first three of these benchmarks are inspired by fundamental limits on the maximum achievable secret-key rate if Alice and Bob are connected by quantum channels which model quantum key distribution over optical fiber without the use of a (possible) quantum repeater.

The first of these benchmarks is, similarly to Chapter 6, the *capacity of the pure-loss channel* [13], which models the losses occuring in the optical fiber with transmissivity η_f linking Alice and Bob. Unfortunately, as we have observed in Chapter 6, surpassing the capacity is experimentally challenging. This motivates the introduction of other, easier to surpass, benchmarks. These benchmarks are still based on (upper bounds on) the secret-key capacity of quantum channels which model realistic implementations of quantum communications over fibers.

The second benchmark is again built on the idea of including the losses of the apparatus into the transmissivity of the fiber. The resultant channel with all those losses included we call here *the extended channel*. The benchmark is thus equal to

$$-\log_2\left(1-\eta_f p_{\text{app}}\right). \tag{7.5}$$

Here p_{app} describes all the intrinsic losses of the devices used. That is, the collection efficiency p_{ce} at the emitting diamond, the probability that the emitted photon is within the zero-phonon-line p_{zpl} (which is necessary for generating quantum correlations) and photon detection efficiency p_{det}, so that $p_{\text{app}} = p_{\text{ce}} p_{\text{zpl}} p_{\text{det}}$. Note that this definition of p_{app} is different than in Chapter 6, where the p_{ps} corresponding here to p_{zpl} was not included in the definition of p_{app}.

The third benchmark we consider is again the *thermal channel bound*, which takes into account the effects of dark counts. We have already defined it in Chapter 6. We only note that the transmissivity of the channel η is here taken to be $\eta_f p_{\text{app}}$ similarly as in the second benchmark. We note here that the time-window of the detector t_{w} is not fixed in our model, but is optimized over for every distance in order to achieve the highest possible secret-key rate. Hence in this benchmark we fix $t_{\text{w}} = 5$ ns which is the shortest duration of the time-window that we consider in our secret-key rate optimization.

Finally, the secret-key rate achieved with *direct transmission using the same devices* can be seen as **a fourth benchmark**. Specifically, here we mean the secret-key rate achieved when Alice uses her electron spin to generate spin-photon entanglement and sends the time-bin encoded photon to Bob. She then measures her electron spin while Bob measures the arriving photon. However, to take a conservative view, we will only use this direct transmission benchmark for the SPADS scheme. This is motivated by the fact that for both the SPADS scheme and the direction transmission scheme the experimental setups on Alice's and Bob's side are the same, ensuring that the two rates can be compared fairly. We note that similarly as in the modeled secret-key rates achievable with our proposed repeater schemes, also for this direct transmission benchmark we optimize over the time-window t_{w} for each distance.

The secret-key capacity is the main benchmark that we consider. Surpassing it establishes the considered scheme as a quantum repeater. The two additional capacity bounds and the achieved rate with direct transmission are additional benchmarks, which guide the way towards implementation of a quantum repeater. We define all the considered benchmarks for the channel with the same fiber attenuation length L_0 as the channel used for the corresponding achievable secret-key rate.

7.6. NUMERICAL RESULTS

We now have a full model of the rate of the presented quantum repeater protocols as a function of the underlying experimental parameters. In this section we will firstly state all the parameters required by our model and then present the results and conclusions drawn from the numerical implementation of this model. In particular, in Section 7.6.1 we will first provide a deeper insight into the benefits of using the six-state protocol and advantage distillation in specific schemes. In Section 7.6.2 we determine the optimal positioning of the repeater nodes for our schemes and investigate the dependence of the secret-key rate achievable with those schemes on the photon emission angle θ and the cutoff n^* for the appropriate schemes. In Section 7.6.3 we then use the insights acquired in the previous section to compare the achievable secret-key rates for all the proposed repeater schemes with the secret-key capacity and other proposed benchmarks. In particular, we show that the single-photon scheme significantly outperforms the secret-key capacity and hence can be used to demonstrate a quantum repeater. Finally, in Section 7.6.4 we determine the duration of the experiment that would allow us to demonstrate such a quantum repeater with the single-photon scheme.

Here we will use the same parameters as stated in Chapter 6 with small modifications relating to the fact that the model used here has been made more accurate than in Chapter 6 (see Appendix 7.8.4) and certain parameters characterise specifically the single-photon scheme which has only been proposed in this chapter. We again emphasise that these are the parameters that have been achieved in an experiment, or correspond to expected parameters when the NV center is embedded in an optical Fabry-Perot microcavity. The additional parameters to those defined in Chapter 6 are:

- F_m (depolarizing parameter for the measurement of the electron spin) = 0.95 [2]
- F_g (depolarizing parameter for two qubit gates in quantum memories) = 0.98 [4]
- τ (characteristic time of the NV emission) = 6.48 ns [30, 31]
- $t_{\mathrm{w}}^{\mathrm{offset}}$ (detection window offset) = 1.28 ns [18]
- $\Delta\phi$ (optical phase uncertainty of the spin-spin entangled state) = 14.3° [2]

We note that the parameters F_m and F_g replace the parameter F_{gm} from Chapter 6 (see Appendix 7.8.4). As discussed, the parameters p_{em} and p_{ps} from Chapter 6 have been renamed to p_{ce} and p_{zpl} respectively but maintain their values from Chapter 6. Moreover, the detector time-window t_{w} which in Chapter 6 has been fixed is now a variable over which we optimise. Finally, note that the parameters that have not been discussed in the main text are discussed in the appendix.

7.6.1. COMPARING BB84 AND SIX-STATE ADVANTAGE DISTILLATION PROTOCOLS

We first investigate here when the BB84 or six-state advantage distillation protocol performs better. It was shown in Chapter 6 that in the SiSQuaRe scheme there is a trade-off - for the low noise regime (small distances) the fully asymmetric BB84 protocol is preferable, while in the high noise regime (large distances) the problem of noise can be overcome by using a six-state protocol supplemented with advantage distillation. This technique allows us to increase the secret-key fraction at the expense of reducing the yield by a factor of three, since a six-state protocol in which Alice and Bob perform measurements on photonic qubits does not allow for the (fully) asymmetric protocol within our model. Numerically, we find that for the SPADS and SPOTL scheme advantage distillation is *necessary* to generate non-zero secret-key at any distance. This is due to the fact that there is a significant amount of noise in these schemes. Thus, for the SPADS (SPOTL) scheme the (a)symmetric six-state protocol with advantage distillation is optimal.

To provide more insight into the performance of those different QKD schemes for different parameter regimes, we plot the achievable secret-key fraction for the SPADS and SPOTL schemes as a function of the depolarizing parameter due to imperfect electron spin measurement F_m in Figure 7.6 (see Appendix 7.8.2 for the discussion of the corresponding noise model). Noise due to imperfect measurements is one of the significant noise sources in our setup, since the SPADS scheme involves three and the SPOTL scheme four single-qubit measurements on the memory qubits. The data have been plotted for a fixed distance of $12.5L_0$, where $L_0 = 0.542$ km is the attenuation length of the fiber. Moreover, since on this plot we aim at maximizing only the secret-key fraction over the tunable parameters, we set the cutoff n^* to one and the detection time-window t_w to 5 ns (the smallest detection time-window we use) for both schemes. Furthermore, within the single-photon subscheme the heralding station is always placed exactly in the middle between the two memory nodes. We also consider the positioning of the memory repeater node to be two-thirds away from Alice for the SPADS scheme and in the middle for the SPOTL scheme as discussed in the next section. For the SPOTL scheme we also assume $\theta_A = \theta_B$ which we will justify in the next section.

We see that for the current experimental value of $F_m = 0.95$ both schemes can generate key only if the advantage distillation post-processing is used. As F_m increases, we observe that for the SPADS scheme firstly the six-state protocol without advantage distillation and then the BB84 protocol start generating key. For the SPOTL scheme the value of F_m at which the six-state protocol without advantage distillation starts generating key is much larger than the corresponding value of F_m for any of the studied protocols for the SPADS scheme. This is because the SPOTL scheme involves more noisy processes than the SPADS scheme. This also provides an approximate quantification of the benefit of using advantage distillation. Specifically, looking at the SPOTL scheme, it can be observed that while at the current experimental value of $F_m = 0.95$ advantage distillation allows for generating key, at a higher value of the depolarizing parameter $F_m = 0.97$, still no key can be generated with standard one-way post-processing. Moreover, we see that utilizing advantage distillation for the SPADS scheme allows for the generation of key, even with very noisy measurements when $F_m = 0.91$. We also observe two distinct scalings of the secret-key fraction with F_m in the regime where non-zero amount of key

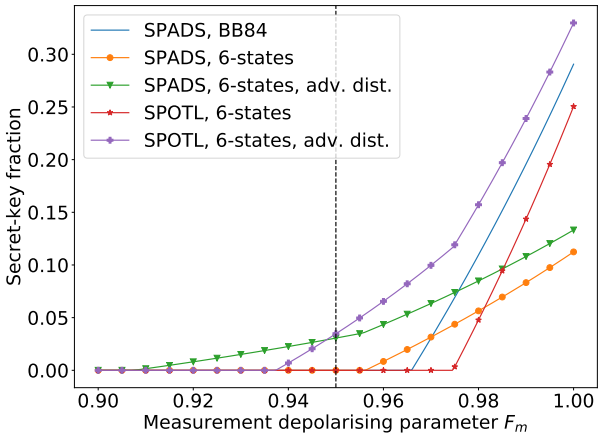

Figure 7.6: Secret-key fraction as a function of the depolarizing parameter due to noisy measurement F_m for the total distance of $12.5L_0$. We see that for the current experimental value of $F_m = 0.95$ (marked with a dashed black vertical line) both schemes can generate key only if the advantage distillation post-processing is used. As F_m increases the protocols that do not utilize advantage distillation also start generating key. We also see that the curves can be divided into two groups in terms of their slope in the regime where they generate non-zero amount of key. Those two groups correspond to the scenarios where a fully asymmetric (bigger slope) or a symmetric (smaller slope) protocol is used. For all the plotted protocols the cutoff n^* is set to one and $t_w = 5$ ns (the smallest detection time-window we use) to maximize the secret-key fraction. Moreover, for each value of F_m we optimize the secret-key fraction over the angle θ. For the SPOTL scheme we assume $\theta_A = \theta_B$. For the SPADS scheme we position the repeater node 2/3 away of the total distance from Alice and in the middle between Alice and Bob for the SPOTL scheme.

is generated. These two scalings depend on whether we use a symmetric or asymmetric protocol. Specifically, for the SPADS scheme the symmetric six-state protocol is used. Therefore the corresponding two curves have a slope that is approximately three times smaller than the other three curves corresponding to the protocols that run in the fully asymmetric mode.

7.6.2. OPTIMAL SETTINGS

We see that the above described repeater schemes include several tunable parameters. These parameters are the cut-off $n^\star$ for Bob's number of attempts until restart, the angle θ in the single-photon scheme and the positioning of the repeater. These parameters can be optimized to maximize the secret-key rate. Here we will approach this optimization in a consistent way - we gradually restrict the parameter space by making specific observations based on numerical evidence.

The first claim that we will make is in relation to the *optimal positioning of the repeater*. In Chapter 6 we have conjectured that for the SiSQuaRe scheme the middle positioning of the repeater is optimal. For the single-photon scheme we want the probability

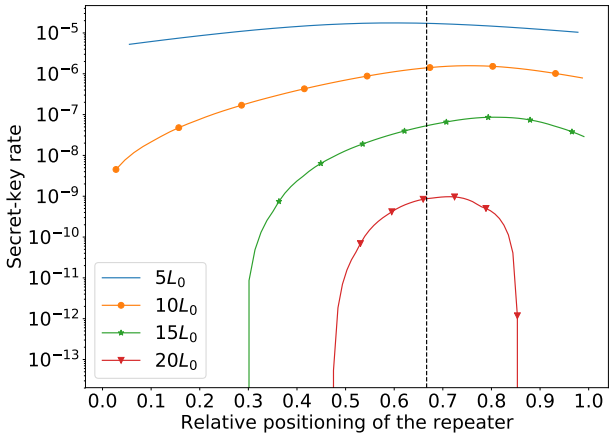

Figure 7.7: Secret-key rate as a function of the relative positioning of the repeater for few different total distances for the SPADS scheme. The total distances are expressed in terms of the fiber attenuation length $L_0 = 0.542$ km. We see that positioning the repeater two-thirds of the distance away from Alice (marked by the vertical black dashed line) is a good positioning for all the distances. For each total distance considered and each positioning the secret-key rate is optimized over the cutoff n^*, the angle θ and the time-window of the detector t_w.

of transmitting the photons from each of the two nodes to the beam splitter heralding station to be equal. This effectively sets the target state between the electron spins to be the maximally entangled state. Hence, if we restrict ourselves to the case where the emission angles θ of both Alice and Bob are the same, then it is natural to position the heralding station symmetrically in the middle between them. Hence, the only non-obvious optimal positioning is for the SPADS and SPOTL scheme.

For the SPADS scheme, positioning the repeater at two-thirds of the relative distance away from Alice could intuitively be expected to be optimal. This is due to the fact that the single-photon scheme runs on two segments: Alice-beam splitter, beam splitter-repeater, while the one half of the SiSQuaRe scheme runs only over a single segment between repeater and Bob. By segment we mean here a distance over which we need to be able to independently transmit a photon. In Fig. 7.7 we show the secret-key rate as a function of the relative positioning of the repeater for a set of different total distances. We see there that despite the fact that positioning the repeater at two-thirds is not always optimal, it is a good enough positioning for all distances for our purposes. For each data point on the plot we independently optimize over the cut-off n^*, the angle θ of the single-photon subscheme and the duration of the detector time-window t_w.

The SPOTL scheme has the same symmetry as the SiSQuaRe scheme, in the sense that the part of the scheme performed on Alice's side is exactly the same as on Bob's side. This symmetry is only broken by the sequential nature of the scheme. Since we have already observed that the middle positioning is optimal for the SiSQuaRe scheme,

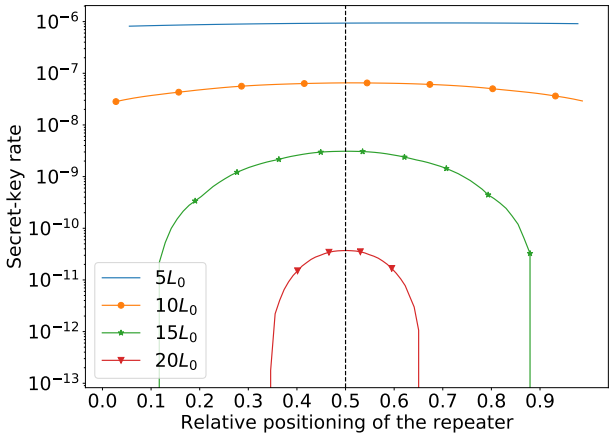

Figure 7.8: Secret-key rate as a function of the relative positioning of the repeater for few different total distances for the SPOTL scheme. The total distances are expressed in terms of the fiber attenuation length $L_0 = 0.542$ km. We see that positioning the repeater in the middle between Alice and Bob (marked by the vertical black dashed line) is a good positioning for all the distances. For each total distance considered and each positioning the secret-key rate is optimized over the cutoff n^*, the angles θ_A and θ_B and the time-window of the detector t_w.

we expect to see the same behavior for the SPOTL scheme. Indeed, we confirm this expectation numerically in Fig. 7.8. Here for each data point we independently optimize over the cut-off $n^\star$, the angle θ_A (θ_B) of the single-photon subscheme on Alice's (Bob's) side and the duration of the detection time-window.

To conclude, we will always place the heralding station within the single-photon (sub)protocol exactly in the middle between the two corresponding memory nodes. Moreover, we will also always place the memory repeater node in the middle for the SPOTL scheme and two-thirds of the distance away from Alice for the SPADS scheme.

Having established the optimal positioning of the repeater, we look into the relation between θ_A and θ_B for the SPOTL scheme. We observe that the relative error resulting from optimizing the secret-key rate over a single angle $\theta_A = \theta_B$ rather than two independent ones is smaller than 1% for all distances. Hence from now on we will restrict ourselves to optimizing only over one angle θ for the SPOTL scheme.

Having resolved the issues of the optimal positioning of the repeater for all schemes and reducing the number of angles to optimize over for the SPOTL scheme to one, we now investigate how our secret-key rate depends on the remaining parameters. These parameters are the angle θ, the cut-off $n^\star$ and the duration of the detection time-window t_w. The optimal time-window follows a simple behavior for all schemes: for short distances the probability of getting a dark count p_d is negligible compared to the probability of detecting the signal photon. Hence for those distances we can use a time-window of 30 ns to make sure that almost all the emitted photons which are not polluted by the

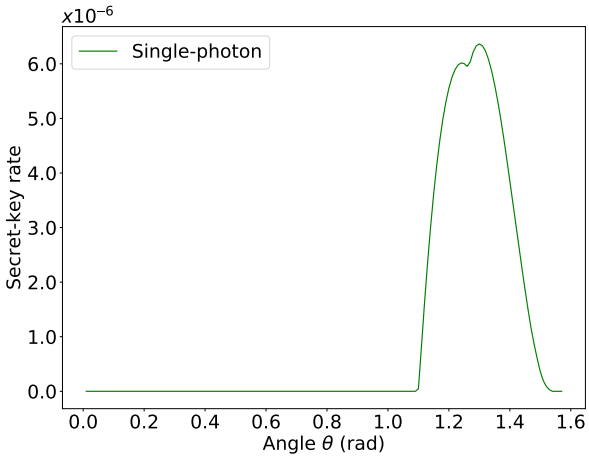

Figure 7.9: (Color online) Secret-key rate as a function of the θ angle for the single-photon scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that there is a relatively large range of angles for which non-zero amount of key can be generated. For each value of θ the secret-key rate is optimized over the time-window t_w. The kink on the plot is a consequence of the fact that the six-state protocol with advantage distillation involves optimization over of two subprotocols.

photons from the optical excitation pulse arrive inside the detection time-window. We always need to sacrifice the photons arriving within the time t_w^{offset} after the optical pulse has been applied to filter out the photons from that pulse, see Appendix 7.8.1 for details. Then, for larger distances where p_d starts to become comparable with the probability of detecting the signal photon, the duration of the time-window is gradually reduced. This reduces the effect of dark counts at the expense of having more and more photons arriving outside of the time-window. See Appendix 7.8.1 for the modeling of the losses resulting from photons arriving outside of the time-window.

The dependence of the secret-key rate on the angle θ, the tunable parameter that Alice and Bob choose in their starting state $|\psi\rangle = \sin\theta|\downarrow\rangle|0\rangle + \cos\theta|\uparrow\rangle|1\rangle$ in the single-photon scheme, is more complex. We observe that the optimal value of θ is closer to $\frac{\pi}{2}$ for schemes that involve more noisy processes. Informally, this means that Alice and Bob send 'less' photons towards the beam splitter, to overcome the noise coming from events in which both nodes emit a photon. At $\frac{\pi}{2}$ however, no photons are emitted and the rate drops down to zero. We illustrate this in Figs. 7.9, 7.10, and 7.11. We see that for the SPADS and SPOTL scheme, there is only a restricted regime of the angle θ for which one can generate non-zero amount of key. In particular, the SPOTL scheme requires a larger number of noisy operations, and therefore cannot tolerate much noise arising from the effect of photon loss in the single-photon subscheme. This means that there is only a small range of θ that allows for production of secret key. The single-photon scheme involves much less operations and can tolerate more noise, and so lower values of the parameter θ still allow for the generation of key.

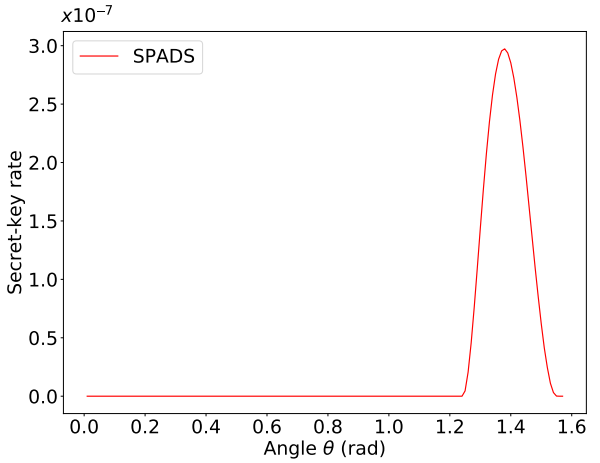

Figure 7.10: Secret-key rate as a function of the θ angle for the SPADS scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that due to more noisy processes the range of θ that allows us to generate key is much more restricted than for the single-photon scheme. For each value of θ the secret-key rate is optimized over the cutoff n^* and the time-window t_w.

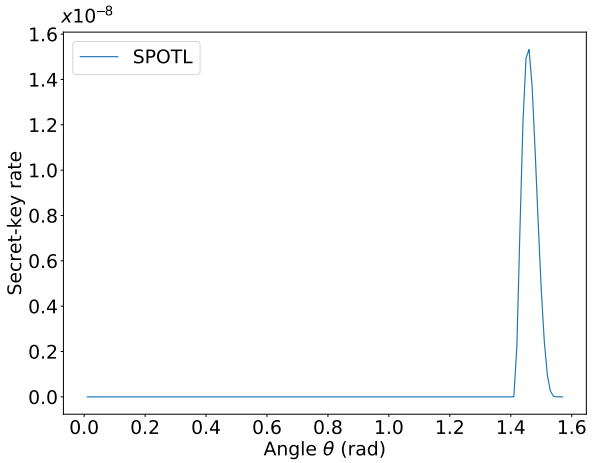

Figure 7.11: Secret-key rate as a function of the angle $\theta = \theta_A = \theta_B$ for the SPOTL scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that, due to the increased amount of noisy processes, this scheme requires θ to be in a much narrower regime than for the single-photon and SPADS schemes, as can be seen by comparing the plot with the plots in FIG. 7.9 and in FIG. 7.10. This corresponds to the overwhelming dominance of the dark state of the spin (no emission of the photon) in order to avoid any extra noise coming from the photon loss. For each value of θ the secret-key rate is optimized over the cutoff n^* and the time-window t_w.

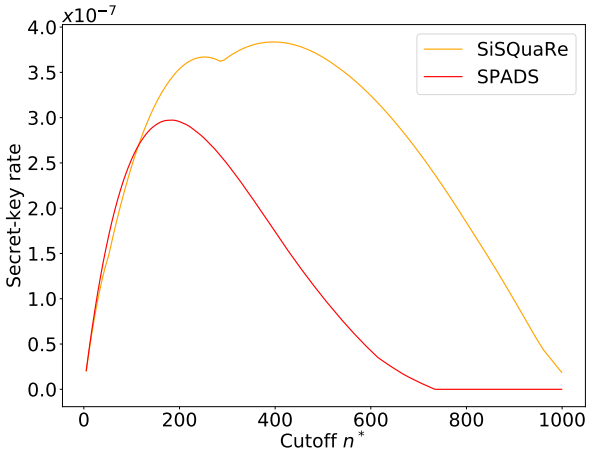

Figure 7.12: Secret-key rate as a function of the cut-off for the SiSQuaRe and SPADS scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that the SPADS scheme requires lower cut-off than the SiSQuaRe scheme because it involves more noisy operations. For each value of the cutoff n^* we optimize the secret-key rate over the time-window t_w and for the SPADS scheme also over the θ angle. The kink for the SiSQuaRe scheme arises because of the optimization over the fully asymmetric one-way BB84 protocol and symmetric six-state protocol with advantage distillation, which itself involves optimization over two subprotocols.

We also investigate the dependence of the rate on the cut-off. Both the SPADS and SPOTL scheme require a lower cut-off than the SiSQuaRe scheme, see Fig. 7.12 and 7.13. This is caused by the fact that each of them involves more noisy operations, and hence less noise tolerance is possible.

7.6.3. ACHIEVED SECRET-KEY RATES OF THE QUANTUM REPEATER PROPOSALS

Now we are ready to present the main results, the secret-key rate for all the considered schemes as a function of the total distance when optimized over θ, the cut-off $n^\star$ and the duration of the time-window t_w. We compare the rates to the benchmarks from Section 7.5.

In Fig. 7.14 we plot the rate of all four of the quantum repeater schemes as a function of the distance between Alice and Bob. We observe that already for realistic near-term parameters, the single-photon scheme can outperform the secret-key capacity of the pure-loss channel by a factor of seven for a distance of ≈ 9.2 km.

We have also investigated what improvements would need to be done in order for the SPADS and SPOTL schemes to also overcome the secret-key capacity. An example scenario in which the SPADS scheme outperforms this repeaterless bound includes better phase stabilization such that $\Delta\phi = 5°$ and reduction of the decoherence effects in the carbon spin during subsequent entanglement generation attempts such that $a_0 =$

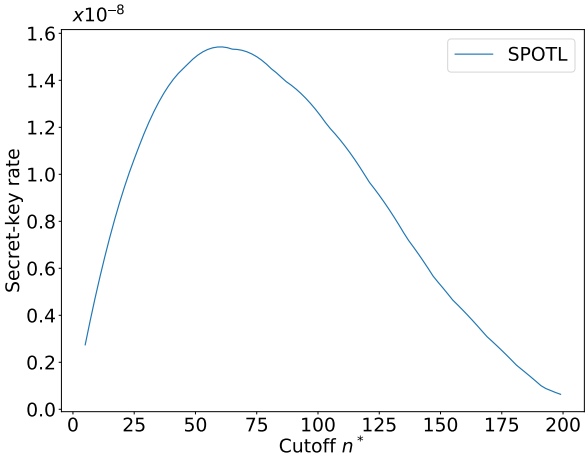

Figure 7.13: Secret-key rate as a function of the cut-off for the SPOTL scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that due to the large number of noisy operations, this scheme requires a low cut-off in order to be able to generate key. For each value of the cutoff n^* we optimize the secret-key rate over the time-window t_w and the θ angle.

$1/8000$ and $b_0 = 1/20000$. Further improvement of these effective coherence times to $a_0 = 1/20000$ and $b_0 = 1/50000$ allows the SPOTL scheme to also overcome the secret-key capacity. We note that maintaining coherence of the carbon-spin memory qubit for such large number of subsequent remote entanglement generation attempts is expected to be possible using the method of decoherence-protected subspaces [8, 32].

As mentioned before, the SPADS scheme can be naturally compared against the benchmark of the direct transmission using NV as a source. The results are depicted in Fig. 7.15. We see that the SPADS scheme easily overcomes the NV-based direct transmission and the thermal benchmark for larger distances for which these benchmarks drop to zero.

In Fig. 7.14 we observe that for the SPOTL scheme, the total distance over which key can be generated is significantly smaller than for the SPADS scheme. This is despite the fact that the full distance is divided into four segments. The rather weak performance of this scheme is due to the fact that it involves a larger number of noisy operations. As a result, the scheme can tolerate little noise from the single-photon subscheme, requiring the angle θ to be close to $\frac{\pi}{2}$ as can be seen in Fig. 7.11. Hence, the probability of photon emission becomes greatly diminished and so the distance after which dark counts start becoming significant is much smaller than for the SPADS scheme. To overcome this problem one would need to reduce the amount of noise in the system. One of the main sources of noise is the imperfect single-qubit measurement. Hence, we illustrate the achievable rates for the scenario with the boosted measurement depolarizing parameter $F_m = 0.98$ in Fig. 7.16. Additionally, in this plot we also consider the application of probabilistic frequency conversion to the telecom wavelength at which $L_0 = 22$ km. Frequency conversion has already been achieved experimentally in the single-photon

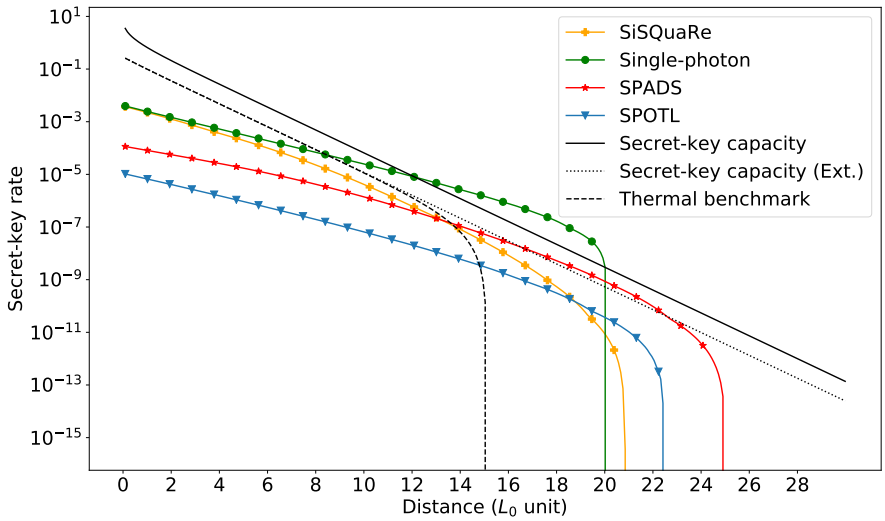

Figure 7.14: Rate of all studied quantum repeater schemes as a function of the distance between Alice and Bob, expressed in the units of $L_0 = 0.542$ km. We also plot the different benchmarks from Section 7.5. We see that the single-photon scheme outperforms the secret-key capacity. For the achievable rates the secret-key rate is optimized over the cutoff n^*, the angle θ and the time-window t_w independently for each distance.

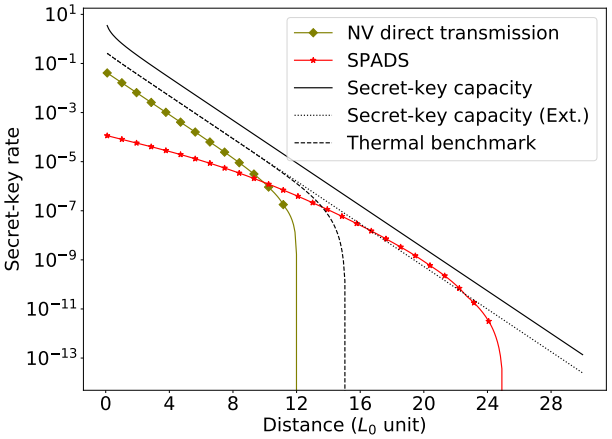

Figure 7.15: Comparison of the SPADS scheme with the rate achievable using the direct transmission, with NV being the photon source. The secret-key rates for those schemes are plotted as a function of the distance between Alice and Bob, expressed in the units of $L_0 = 0.542$ km. We also plot the different benchmarks. We see that the SPADS scheme easily overcomes the direct transmission and the thermal benchmark (see Section 7.5). For the secret-key rate achievable with the SPADS scheme we perform optimization over the cutoff n^*, the angle θ and the time-window t_w independently for each distance. Similarly, we also optimize the secret-key rate achievable with direct transmission over the time-window t_w.

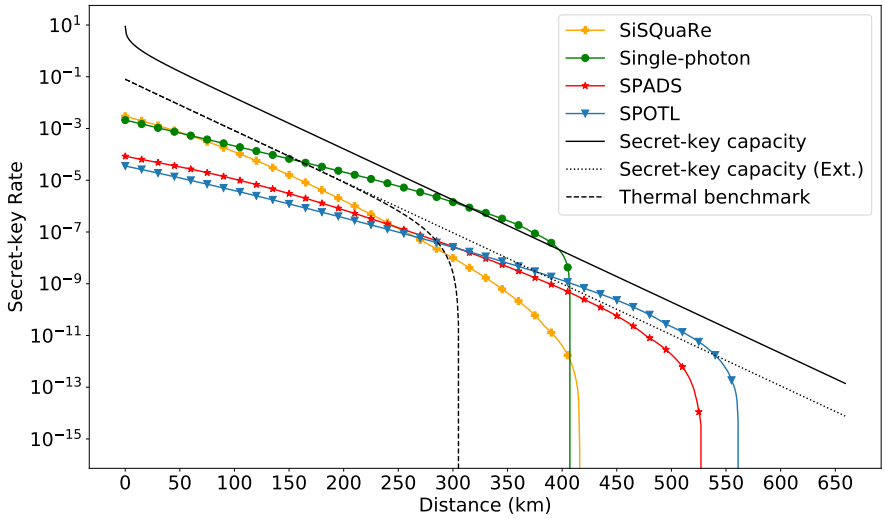

Figure 7.16: Secret-key rate as a function of distance in units of km for transmission at telecom channel with $L_0 = 22$ km, along with the benchmarks from Section 7.5. We consider an improved measurement depolarizing parameter of $F_m = 0.98$. The frequency conversion efficiency is assumed to be 0.3. We observe that the SPOTL scheme allows for the generation of secret-key over a distance of more than 550 km. For the achievable rates the secret-key rate is optimized over the cutoff n^*, the angle θ and the time-window t_w independently for each distance.

regime with success probability of 30% [33]. This is also the success probability that we consider here. The corresponding benchmarks have also been plotted for the new channel with $L_0 = 22$ km. We see in Fig. 7.16 that with the improved measurement and using frequency conversion, the SPOTL scheme allows now to generate secret key over more than 550 km. We also see that under those conditions the single-photon scheme can also overcome the secret-key capacity of the telecom channel.

7.6.4. RUNTIME OF THE EXPERIMENT

While the theoretical capability of an experimental setup to surpass the secret-key capacity is a necessary requirement to claim a working quantum repeater, it does not necessarily mean that this can be experimentally verified in practice. Indeed, if a quantum repeater proposal only surpasses the secret-key capacity by a narrow margin at a large distance, the running time of an experiment could be too long for practical purposes. In this section, we will discuss an experiment which can validate a quantum repeater setup and calculate the running time of such an experiment, where we demonstrate that the single-photon scheme could be validated to be a quantum repeater within twelve hours.

A straightforward way of validating a quantum repeater would consist of first generating secret-key, calculating the achieved (finite-size) secret-key rate and then compar-

ing the rate with the secret-key capacity. However, this requires a large number of raw bits to be generated, partially due to the loose bounds on finite-size secret-key generation. What we propose here is an experiment where the QBER and yield are separately estimated to lie within a certain confidence interval. Then, if with the (worst-case) values of the yield and the QBER the corresponding asymptotic secret-key rate still confidently beats the benchmarks, one could claim that, in the asymptotic regime, the setup would qualify as a quantum repeater.

As we show in Appendix 7.8.8, it is possible to run the single-photon scheme over a distance of $17L_0 \approx 9.2$ km for approximately twelve hours to find with high confidence ($\geq 1 - 1.5 \cdot 10^{-4}$) that the scheme beats the capacity (see Eq. (6.13)) at that distance by a factor of at least three.

7.6.5. DISCUSSION AND FUTURE OUTLOOK

It is worth noting that our figure of merit - the secret-key rate - is weakly impacted by the latency of transmission, which grows linearly with distance for the SiSQuaRe, SPADS and SPOTL schemes. Its only effect on the secret-key rate is the resulting decoherence time in the quantum memories while the memory nodes await the success/failure signals. This decoherence due to the waiting time is negligible in comparison to the noise due to interaction, arising from subsequent entanglement generation attempts. On the other hand, this latency would clearly be very visible in low throughput of these schemes. Single-photon scheme on the other hand has an advantage of the repetition rate being limited only by the local processing of the memory nodes which would result in a higher throughput. We observe this fact in the modest expected duration of the experiment, even in the high loss regime needed for overcoming the secret-key capacity. It is worth noting that while the single-photon scheme maintains constant latency for QKD, there exist schemes where such constant latency can be maintained also for remote entanglement generation, see e.g. [34]. It is hence clear that there are certain important properties of an efficient quantum repeater scheme that are not captured by the secret-key rate. However, achieving high throughputs for arbitrary distances would require almost all the components to be efficient in terms of rates and memories to be of high quality in terms of operational and long-storage fidelities. It is clear that demonstrating all these features together in a single experiment is still a future goal. The advantage of the secret-key rate is that overcoming the secret-key capacity would form a crucial step towards an implementation of an efficient and practical, long-distance quantum repeater architecture whose validity would carry an information-theoretic significance and will therefore be totally independent of any hardware-based reference scenario.

In our model we have identified significant amount of noise arising in the system. As a result, we find that it is not always beneficial to just divide the fixed distance into more elementary links. Hence, it is a natural question whether this noise could be eliminated e.g. using entanglement distillation. In fact for the noise arising due to photon loss in the single-photon scheme not only does there exist an efficient distillation procedure [35, 36], but it has also already been demonstrated in the NV-platform [4]. Moreover, in the ideal case of noiseless operations and storage, a scheme based on generating two entangled states through the single-photon scheme and then distilling them as demonstrated in [4] should effectively also be able to overcome the secret-key capacity

(see Chapter 4) and provide a significant boost by completely removing the noise due to photon loss. Furthermore, an implementation of such a distillation-based remote entanglement generation scheme would alleviate the requirement of the optical phase stabilisation of the system. Therefore this distillation based scheme could be a natural fifth candidate for a proof of principle repeater. Nevertheless, we believe that the fidelities of quantum operations and the effective coherence times of the memories used in this paper might need to be improved before this distillation would prove useful.

7.7. CONCLUSIONS

We analyzed four experimentally relevant quantum repeater schemes on their ability to generate secret key. More specifically, the schemes were assessed by contrasting their achievable secret-key rate with the secret-key capacity of the channel corresponding to direct transmission. The secret-key rates have been estimated using near-term experimental parameters for the NV center platform. The majority of these parameters have already been demonstrated across multiple experiments. A remaining challenging element of our proposed schemes is the implementation of optical cavities. These cavities would enable the enhancement of both the photon emission probability into the zero-phonon line and the photon collection efficiency to the desired level.

With these near-term experimental parameters, our assessment shows the viability of one of the schemes, the single-photon scheme, for the first experimental demonstration of a quantum repeater. In fact, the single-photon scheme achieves a secret-key rate more than seven times greater than the secret-key capacity. We also estimated the duration of an experiment to conclude that a rate larger than the secret-key capacity is achievable. The duration of the experiment would be approximately twelve hours.

Finally, we show that a scheme based on concatenating the single-photon scheme twice (i.e. the SPOTL scheme), has the capability to generate secret-key at large distances. However, this requires converting the frequency of the emitted photons to the telecom wavelength and modestly improving the fidelity at which measurements can be performed.

7.8. APPENDIX

7.8.1. LOSSES AND NOISE ON THE PHOTONIC QUBITS

In this appendix we describe how the losses and noise affect our photonic qubits. In particular, we first recall how the two types of encoding result in the losses acting as different quantum channels on the states. Then, we study the effects of a finite detector time-window. More specifically, we firstly show that the arrival of a photon outside the time-window is equivalent to all the other loss processes and secondly we calculate the probability of registering a dark count within the time-window. We also show how to model the noise arising from those dark counts for the SiSQuaRe and SPADS schemes. Finally, we calculate the dephasing induced by the unknown phase shift for the single-photon scheme.

EFFECTS OF LOSSES FOR THE DIFFERENT ENCODINGS

The physical process of probabilistically losing photons corresponds to different quantum channels depending on the qubit encoding. In our repeater schemes we use two types of encoding: time-bin and presence-absence of a photon. For a time-bin encoded qubit in the ideal scenario of no loss we always expect to obtain a click in one of the detectors. Hence loss of a photon resulting in a no-click event raises an erasure flag which carries the failure information. Therefore it is clear that for this encoding the physical photon loss process corresponds to an erasure channel with the erasure probability given by one minus the corresponding transmissivity,

$$D(\rho) = \eta\rho + (1-\eta)|\perp\rangle\langle\perp| . \tag{7.6}$$

Here $|\perp\rangle$ is the loss flag, corresponding to the non-detection of a photon. Since we are only interested in the quantum state of the system for the successful events when a detection event has occurred, we effectively post-select on the non-erasure events.

For presence-absence encoding the situation is different since now there is no flag available that could explicitly tell us whether a photon got lost or not. In fact for this encoding the photon loss results in an amplitude-damping channel applied to the photonic qubit. Here the damping parameter equals one minus the transmissivity of the channel [37].

EFFECTS OF THE DETECTOR TIME-WINDOW

The detector only registers clicks that fall within a certain time-window. It is *a priori* not clear what kind of noisy or lossy channel should be used to model the loss of information due to non-detection of photons arriving outside of the time-window. This is because in a typical loss process we have a probabilistic leakage of information to the environment. In the scenario considered here, the situation is slightly different as effectively no leakage occurs, but rather certain part of the incoming signal effectively gets discarded. Here we will show that despite this qualitative difference, within our model this process can effectively be modeled as any other loss process.

Now, let us provide a brief description of the physics of this process. Firstly, the detection time-window is chosen such that the probability of detecting a photon from the optical excitation pulse used to entangle the electron spin with the photonic qubit is negligible [18]. For that reason the detection time-window is opened after a fixed offset t_w^{offset} with respect to the beginning of the decay of the optical excited state of the electron spin. We note that for the considered enhancement of the ZPL-emission using the optical cavity we predict the characteristic time of the NV emission τ to be approximately a half of the corresponding value of τ if no cavity is used [18, 30, 31]. Therefore here we consider the scenario where the duration of the optical excitation pulse is made twice shorter with respect to the one used in [18]. This will allow us to filter out the unwanted photons from the excitation pulse by setting t_w^{offset} to half of the offset used in [18].

Secondly, we note that the detection time-window cannot last too long, specifically, it needs to be chosen such that there is a good trade-off between detecting coherent and non-coherent (i.e. dark counts) photons. In this subsection we will discuss the effects of photons arriving outside of this time-window and the effects of registering dark counts within this time-window.

LOSSES FROM THE DETECTOR TIME-WINDOW

The NV center emits a photon through an exponential decay process with characteristic time τ. Therefore the probability of detecting a photon during a time-window starting at $t_{\mathrm{w}}^{\mathrm{offset}}$ and lasting for t_{w} is

$$p_{\mathrm{in}}(t_{\mathrm{w}}) = \frac{1}{\tau}\int_{t_{\mathrm{w}}^{\mathrm{offset}}}^{t_{\mathrm{w}}^{\mathrm{offset}}+t_{\mathrm{w}}} \mathrm{d}t \exp(-\frac{t}{\tau}) = \exp(-\frac{t_{\mathrm{w}}^{\mathrm{offset}}}{\tau}) - \exp(-\frac{t_{\mathrm{w}}^{\mathrm{offset}}+t_{\mathrm{w}}}{\tau}) \,. \tag{7.7}$$

Clearly the process of a photon arriving outside of the time-window is qualitatively different from the loss process where the photons get lost to the environment. In the remainder of this section we will now look at the difference between these two phenomena in more detail.

The emission process of the NV center is a coherent process over time. Consider a generic scenario in which we divide the emission time into two intervals, denoted by "in" and "out", respectively. Coherent emission then means that the state of the photon emitted by the electron spin in state $|\uparrow\rangle$ will be

$$|\psi\rangle = \sqrt{p_{\mathrm{in}}}|1\rangle_{\mathrm{in}}|0\rangle_{\mathrm{out}} + \sqrt{1-p_{\mathrm{in}}}|0\rangle_{\mathrm{in}}|1\rangle_{\mathrm{out}} \,. \tag{7.8}$$

Now let us come back to our specific model, in which the "in" mode corresponds to the interval $[t_{\mathrm{w}}^{\mathrm{offset}},\ t_{\mathrm{w}}^{\mathrm{offset}}+t_{\mathrm{w}}]$ and the "out" mode to all the times $t \geq 0$ lying outside of this interval ($t = 0$ is the earliest possible emission time). Here, the emission into the "in" mode occurs with probability $p_{\mathrm{in}}(t_{\mathrm{w}})$. Hence the spin-photon state resulting from the emission by the $\alpha|\downarrow\rangle + \beta|\uparrow\rangle$ spin state is

$$|\psi\rangle = \alpha|\downarrow\rangle|0\rangle_{\mathrm{in}}|0\rangle_{\mathrm{out}} + \beta|\uparrow\rangle\left(\sqrt{p_{\mathrm{in}}(t_{\mathrm{w}})}|1\rangle_{\mathrm{in}}|0\rangle_{\mathrm{out}} + \sqrt{1-p_{\mathrm{in}}(t_{\mathrm{w}})}|0\rangle_{\mathrm{in}}|1\rangle_{\mathrm{out}}\right) . \tag{7.9}$$

If the presence-absence encoding is used, such a photonic qubit is then transmitted to the detector. Since only the spin and the "in" mode of the photon will be measured, we can now trace out the "out" mode

$$\rho = \left(|\alpha|^2 + |\beta|^2 p_{\mathrm{in}}(t_{\mathrm{w}})\right)|\phi\rangle\langle\phi| + |\beta|^2(1-p_{\mathrm{in}}(t_{\mathrm{w}}))|\uparrow\rangle\langle\uparrow| \otimes |0\rangle\langle 0|_{\mathrm{in}} \,, \tag{7.10}$$

where

$$|\phi\rangle = \frac{1}{\sqrt{|\alpha|^2 + |\beta|^2 p_{\mathrm{in}}(t_{\mathrm{w}})}}\left(\alpha|\downarrow\rangle|0\rangle_{\mathrm{in}} + \beta\sqrt{p_{\mathrm{in}}(t_{\mathrm{w}})}|\uparrow\rangle|1\rangle_{\mathrm{in}}\right) . \tag{7.11}$$

Note that this state can be obtained by passing the photonic qubit of the state

$$|\psi\rangle = \alpha|\downarrow\rangle|0\rangle + \beta|\uparrow\rangle|1\rangle \,, \tag{7.12}$$

through the amplitude-damping channel with the damping parameter given by $1-p_{\mathrm{in}}(t_{\mathrm{w}})$. Hence we can conclude that for the photon number encoding, the possibility of the photon arriving outside of the time-window of the detector can be modeled in the same way as any other photon loss process, namely an amplitude-damping channel applied to that photonic qubit.

In the case of time-bin encoding we effectively have four photonic qubits, since now we have an "in" and "out" mode for both the early (denoted by "e") and the late (denoted

by "l") time-window. We assume here that the slots do not overlap. That is, a photon emitted in the "out" mode of the early time-window is always distinct from any photon in the late time-window. This can be achieved by making the time gap between the "in" modes of the early and late window long enough. In this case the emission process results in a state

$$|\psi\rangle = \alpha|\downarrow\rangle\left(\sqrt{p_{\text{in}}(t_{\text{w}})}|1\rangle_{e,\text{in}}|0\rangle_{e,\text{out}}|0\rangle_{l,\text{in}}|0\rangle_{l,\text{out}} + \sqrt{1-p_{\text{in}}(t_{\text{w}})}|0\rangle_{e,\text{in}}|1\rangle_{e,\text{out}}|0\rangle_{l,\text{in}}|0\rangle_{l,\text{out}}\right) \tag{7.13}$$

$$+\beta|\uparrow\rangle\left(\sqrt{p_{\text{in}}(t_{\text{w}})}|0\rangle_{e,\text{in}}|0\rangle_{e,\text{out}}|1\rangle_{l,\text{in}}|0\rangle_{l,\text{out}} + \sqrt{1-p_{\text{in}}(t_{\text{w}})}|0\rangle_{e,\text{in}}|0\rangle_{e,\text{out}}|0\rangle_{l,\text{in}}|1\rangle_{l,\text{out}}\right). \tag{7.14}$$

Again, tracing out the "out" modes results in a state

$$\rho = p_{\text{in}}(t_{\text{w}})|\phi\rangle\langle\phi| + (1-p_{\text{in}}(t_{\text{w}}))\left(|\alpha|^2|\downarrow\rangle\langle\downarrow| + |\beta|^2|\uparrow\rangle\langle\uparrow|\right)\otimes|00\rangle\langle 00|_{e,l}\,, \tag{7.15}$$

where

$$|\phi\rangle = \alpha|\downarrow\rangle|1\rangle_e|0\rangle_l + \beta|\uparrow\rangle|0\rangle_e|1\rangle_l = \alpha|\downarrow\rangle|e\rangle + \beta|\uparrow\rangle|l\rangle\,. \tag{7.16}$$

Here $|00\rangle_{e,l}$ corresponds to the loss flag from which we see that for the time-bin encoding the possible arrival of a photon outside of the time-window results in an erasure channel with the erasure probability given by $(1-p_{\text{in}}(t_{\text{w}}))$. Hence this process can be also modeled as any other loss process for this encoding.

We have just shown that for both photon presence/absence and time-bin encodings the process of the photon arriving outside of the time-window can be modeled by the source which prepares photons in a coherent superposition of the "in" and "out" modes and the detector tracing out (losing) the "out" modes. We have also shown that those two elements combined together result effectively in a loss process corresponding to the same channel as any other loss process for that encoding (amplitude-damping for photon presence/absence and erasure channel for time-bin encoding).

However, between the source and the detector there are other lossy or noisy components resulting in other quantum channels that need to be applied before the tracing out of the "out" mode at the detector. Now we show that for all loss and noise processes that occur in our model, the tracing out of the "out" mode can be mathematically commuted through all those additional noise/lossy processes. This means that the tracing out can be applied directly after the source, such that the above described reductions to amplitude-damping or erasure channel can be applied.

Consider the quantum channels acting on the photonic qubits of the form

$$\mathcal{N} = \sum_i p_i \mathcal{N}^i_{\text{in}} \otimes \mathcal{N}^i_{\text{out}}\,. \tag{7.17}$$

Effectively these are the channels that do not couple the "in" and "out" modes. Since in reality "in" and "out" modes correspond to different time modes, their coupling would require some kind of memory inside the channel. Hence we can think of the above defined channels as channels without memory. Now it is clear that for a quantum state ρ

that among its registers includes both the "in" and the "out" mode, we have that

$$\mathrm{tr}_{\mathrm{out}}[\mathcal{N}(\rho)] = \mathrm{tr}_{\mathrm{out}}\left[\sum_i p_i \mathcal{N}_{\mathrm{in}}^i \otimes \mathcal{N}_{\mathrm{out}}^i(\rho)\right] = \sum_i p_i \mathcal{N}_{\mathrm{in}}^i(\rho_{\mathrm{in}})\,. \tag{7.18}$$

Now, firstly tracing out the "out" modes and then applying the channel $\mathcal{N}$ (only the "in" part can be applied now) also results in $\sum_i p_i \mathcal{N}_{\mathrm{in}}^i(\rho_{\mathrm{in}})$ at the output. Hence the tracing out of the "out" modes commutes with all the channels that are of the form (7.17), which correspond to channels without memory. Clearly the noise/loss processes that occur before the detection, such as photon loss or dephasing due to uncertainty in the optical phase of the photon, belong to this class of channels. In particular this means that for photon presence/absence the amplitude-damping due to photon loss in the channel and due to photon arrival outside of the time-window can be both combined into one channel with the single damping parameter given by $1-\eta p_{\mathrm{in}}(t_{\mathrm{w}})$ (η denotes the transmissivity due to the loss process e.g. the transmissivity of the fiber). The same applies to time-bin encoding where we now have a single erasure channel with erasure probability $1-\eta p_{\mathrm{in}}(t_{\mathrm{w}})$.

To conclude, the arrival of the photon outside of the time-window can be modeled in the same way as any other loss process for both photon encodings used and therefore we can now redefine the detector efficiency $p'_{\mathrm{det}} = p_{\mathrm{det}} \cdot p_{\mathrm{in}}(t_{\mathrm{w}})$ and the total apparatus efficiency $p'_{\mathrm{app}} = p_{\mathrm{ce}} p_{\mathrm{zpl}} p'_{\mathrm{det}}$. We can then define $\eta_{\mathrm{total}} = p'_{\mathrm{app}} \eta_f$ as the total transmissivity - with probability η_{total} a photon will be successfully transmitted from the sender to the receiver.

DARK COUNTS WITHIN THE DETECTOR TIME-WINDOW

Photon detectors are imperfect, and due to thermal excitations, they will register clicks that do not correspond to any incoming photons. These undesired clicks are called dark counts and can effectively be seen as a source of noise. The magnitude of this noise depends on the ratio between the probability of detecting the signal photon and measuring a dark count. Clearly, dark counts become a dominant source of noise when the probability of detecting the signal photon becomes comparable to the probability of a dark count click. The probability p_d of getting at least one dark count within the time-window t_{w} of awaiting the signal photon is given by $p_d = 1 - \exp(-t_{\mathrm{w}} \cdot \mathrm{DCpS})$, where DCpS is the number of dark counts per second of the detector, see Chapter 6.

In the SiSQuRe scheme Alice and Bob perform measurements on time-bin encoded photons. The same applies to Bob in the SPADS scheme. Since at least two detectors are required to perform this measurement, the presence of dark counts means that the outcome may lie outside of the qubit space. Moreover, this measurement needs to be trusted. In consequence, a squashing map needs to be used to process the multi-click events in a secure way. Here as an approximation we consider the squashing map for the polarization encoding [38] in the same way as described in Appendix 6.9.1 in Chapter 6. Hence this measurement can also be modeled as a perfect measurement preceded by a depolarizing channel with parameter α which depends on whether the BB84 or six-state

protocol is used. The parameter α is given by (see Chapter 6):

$$\alpha_{A/B,\,\mathrm{BB84}} = \frac{p'_{\mathrm{app}}\eta_B(1-p_d)}{1-(1-p'_{\mathrm{app}}\eta_{A/B})(1-p_d)^2}\,, \tag{7.19}$$

$$\alpha_{A/B,\,\text{six-state}} = \frac{p'_{\mathrm{app}}\eta_{A/B}(1-p_d)^5}{1-(1-p'_{\mathrm{app}}\eta_{A/B})(1-p_d)^6}\,. \tag{7.20}$$

Here $\eta_{A/B}$ denotes the transmissivity of the fiber between the memory repeater node and Alice's/Bob's detector setup. Finally we note that dark counts increase the probability of registering a successfull measurement event. For the optical measurement schemes utilising the squashing map the probability of registering a click in at least one detector is given by (see Chapter 6):

$$p_{A/B,\,BB84} = 1-(1-p'_{\mathrm{app}}\eta_{A/B})(1-p_d)^2\,, \tag{7.21}$$

$$p_{A/B,\,\text{six-state}} = 1-(1-p'_{\mathrm{app}}\eta_{A/B})(1-p_d)^6\,. \tag{7.22}$$

The effect of dark counts in the single-photon scheme, which carries over to the SPOTL scheme, is analyzed in Appendix 7.8.5.

NOISE DUE TO OPTICAL PHASE UNCERTAINTY

Another important noise process affecting photonic qubits is related to the fact that for the photon presence/absence encoding the spin-photon entangled state will also depend on the optical phase of the apparatus used. Specifically, it will depend on the phase of the lasers used to generate the spin photon entanglement as well as the optical phase acquired by the photons during the transmission of the photonic qubit. Knowledge about this phase is crucial for being able to generate entanglement through the single-photon scheme. In any realistic setup however, there would be a certain degree of the lack of knowledge about this phase acquired by the photons. Since in the end what matters is the knowledge about the relative phase between the two photons, we can model this source of noise as the lack of knowledge of the phase on only one of the incoming photonic qubits. This noise process can be effectively modeled as dephasing. In this section we will show that the phase uncertainty induces dephasing with a parameter λ equal to

$$\lambda = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{2I_0\left(\frac{1}{(\Delta\phi)^2}\right)} + \frac{1}{2}\,, \tag{7.23}$$

where $\Delta\phi$ is the uncertainty in the phase and $I_{0/1}$ is the Bessel function of order 0/1. Let us assume that for Alice, the local phase of the photonic qubit has a Gaussian-like distribution on a circle, with standard deviation $\Delta\phi$ as observed in [2]. This motivates us to model the distribution as a von Mises distribution [39]. The von Mises distribution reads

$$f(\phi) = \frac{e^{\kappa\cos(\phi-\mu)}}{2\pi I_0(\kappa)}\,. \tag{7.24}$$

Here μ is the measure of location, i.e. it corresponds to the center of the distribution, κ is a measure of concentration and can be effectively seen as the inverse of the variance and I_0 is the modified Bessel function of the first kind of order 0. One can then show [39] that

$$\int_{-\pi}^{\pi} \mathrm{d}\phi f(\phi) e^{\pm i\phi} = \frac{I_1(\kappa)}{I_0(\kappa)} e^{\pm i\mu} . \tag{7.25}$$

Since we are only interested in the noise arising from the lack of knowledge about the phase rather than the actual value of this phase, without loss of generality we can assume $\mu = 0$. Moreover, the experimental parameter that we use here is effectively the standard deviation of the distribution $\Delta\phi$ and therefore we can write $\kappa = \frac{1}{(\Delta\phi)^2}$.

Hence, let us write the spin-photon entangled state that depends on the optical phase ϕ.

$$|\psi^{\pm}(\phi)\rangle = \sin(\theta)|\downarrow 0\rangle \pm e^{i\phi}\cos(\theta)|\uparrow 1\rangle . \tag{7.26}$$

Now, the lack of knowledge about this phase leads to a mixed state:

$$\begin{aligned}\int_{-\pi}^{\pi} f(\phi)|\psi^{\pm}(\phi)\rangle\langle\psi^{\pm}(\phi)|\mathrm{d}\phi = \sin^2(\theta)|\downarrow 0\rangle\langle\downarrow 0| + \cos^2(\theta)|\uparrow 1\rangle\langle\uparrow 1| \\ \pm \sin(\theta)\cos(\theta)\int_{-\pi}^{\pi} f(\phi)(e^{i\phi}|\uparrow 1\rangle\langle\downarrow 0| + e^{-i\phi}|\downarrow 0\rangle\langle\uparrow 1|)\mathrm{d}\phi .\end{aligned} \tag{7.27}$$

Let us now try to map this state onto a dephased state

$$\begin{aligned}\lambda|\psi^{\pm}(0)\rangle\langle\psi^{\pm}(0)| + (1-\lambda)|\psi^{\mp}(0)\rangle\langle\psi^{\mp}(0)| = \sin^2(\theta)|\downarrow 0\rangle\langle\downarrow 0| + \cos^2(\theta)|\uparrow 1\rangle\langle\uparrow 1| \\ \pm \sin(\theta)\cos(\theta)(2\lambda-1)(|\uparrow 1\rangle\langle\downarrow 0| + |\downarrow 0\rangle\langle\uparrow 1|) .\end{aligned} \tag{7.28}$$

Hence, we observe that

$$2\lambda - 1 = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{I_0\left(\frac{1}{(\Delta\phi)^2}\right)} . \tag{7.29}$$

$$\rightarrow \lambda = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{2I_0\left(\frac{1}{(\Delta\phi)^2}\right)} + \frac{1}{2} . \tag{7.30}$$

7.8.2. NOISY PROCESSES IN NV-BASED QUANTUM MEMORIES

In our setups we use ^{13}C nuclear spins in diamond as long-lived memory qubits next to a Nitrogen Vacancy (NV) electron spin taking the role of a communication qubit. In this appendix, we will detail our model of the noisy processes in the NV. For most of these processes we use the model that has already been discussed in Section 6.3.2 of Chapter 6. However, certain small modifications apply for the three new schemes proposed in this chapter. Moreover, some of the noise processes are modelled in more detail in this chapter than in Chapter 6. Here we discuss all these modifications.

For all the schemes that utilise quantum storage in the carbon spin memory during subsequent entanglement generation attempts, we apply the noise model discussed in

Section 6.3.2 of Chapter 6, where the amount of noise is quantified by the dephasing parameter λ_1 and the depolarising parameter λ_2. Recall, that the parameters depend as follows on the number of attempts n,

$$\lambda_1 = F_{T_2} = \frac{1+e^{-an}}{2}\,, \tag{7.31}$$

$$\lambda_2 = F_{T_1} = e^{-bn}\,, \tag{7.32}$$

where a and b are given by

$$a = a_0 + a_1\left(L_s \cdot \frac{n_{ri}}{c} + t_{\text{prep}}\right), b = b_0 + b_1\left(L_s \cdot \frac{n_{ri}}{c} + t_{\text{prep}}\right). \tag{7.33}$$

Here n_{ri} is the refractive index of the fiber, c is the speed of light in vacuum, t_{prep} is the time it takes to prepare for the emission of an entangled photon and L_s is the distance the signal needs to travel before the repeater receives the information about failure or success of the attempt. Let L_B denote the distance between the memory repeater node and Bob. Then for the SiSQuaRe and SPADS schemes $L_s = 2L_B$ as in each attempt first the quantum signal needs to travel to Bob who then sends back to the middle node the classical information about success or failure. For the SPOTL scheme $L_s = L_B$ as in this case both the quantum and the classical signals need to travel only half of the distance between the middle node and Bob since the signals are exchanged with the heralding station which is located half-way between the middle memory node and Bob. The parameters a_0 and b_0 quantify the noise due to a single attempt at generating an entangled spin-photon, induced by stochastic electron spin reset operations, quasi static noise and microwave control infidelities. The parameters a_1 and b_1 quantify the noise during storage per second.

Gates and measurements in the quantum memory are also imperfect. We model those imperfections via two depolarizing channels. The first one acts on a single qubit with depolarizing parameter $\lambda_2 = F_m$ corresponding to the measurement of the electron spin. The second one acts on two qubits with depolarizing parameter $\lambda_2 = F_g$ corresponding to applying a two-qubit gate to both the electron spin and the ^{13}C spin. This means that every time a measurement is done on a e^- qubit of a quantum state ρ, it is actually done on $\mathscr{D}^{F_m}_{\text{depol}}(\rho)$. Also a swapping operation between the e^- spin and the nuclear spin (done experimentally via two two-qubit gates, see main text) leads to an error modeled by a depolarizing channel of parameter $F_{\text{swap}} = F_g^2$. Following the same logic, a Bell state measurement will cause the state to undergo an evolution given by a depolarizing channel. Specifically, following the decomposition of the Bell measurement into elementary gates for the NV-implementation as described in Section 6.6 in Chapter 6, this evolution will consist of a depolarizing channel with parameter F_g^2 acting on both of the measured qubits and the depolarizing channel with parameter F_m^2 acting only on the electron spin qubit.

7.8.3. EXPECTATION OF THE NUMBER OF CHANNEL USES WITH A CUT-OFF

In this appendix we derive an analytical formula for the expectation value of the number of channel uses between Alice and Bob needed to generate one bit of raw key for the

SiSQuaRe, SPADS and SPOTL schemes,

$$\mathbb{E}[N] = \frac{1}{p_A \cdot \left(1-(1-p_B)^{n^*}\right)} + \frac{1}{p_B} \,. \tag{7.34}$$

For these three schemes, we implement a cut-off which is used to prevent decoherence. Each time the number of channel uses between the repeater node and Bob reaches the cut-off n^*, the entire protocol restarts from the beginning. Here we take a conservative view and define the number of channel uses N between Alice and Bob as the sum $N_A + N_B$, where N_A (N_B) corresponds to the number of channel uses between Alice (Bob) and the middle node. From the linearity of the expectation value we have that

$$\mathbb{E}[N_A + N_B] = \mathbb{E}[N_A] + \mathbb{E}[N_B] \,. \tag{7.35}$$

We denote by p_A and p_B the probability of a successful attempt on Alice's and Bob's side respectively. Bob's number of channel uses follows a geometric distribution with parameter $p = p_B$, so that $\mathbb{E}[N_B] = \frac{1}{p_B}$. Without the cut-off, Alice's number of channel use would follow a geometric distribution with parameter $p = p_A$. However, the cut-off parameter adds additional channel uses on Alice side. Since the probability that Bob succeeds within n^* trials is $p_{\text{succ}} = 1-(1-p_B)^{n^*}$, we in fact have that Alice's number of channel uses follows a geometric distribution with parameter $p'_A = p_A \cdot p_{\text{succ}}$. Hence it is straightforward to see that

$$\mathbb{E}[N_A + N_B] = \frac{1}{p'_A} + \frac{1}{p_B} \tag{7.36}$$

$$= \frac{1}{p_A \cdot \left(1-(1-p_B)^{n^*}\right)} + \frac{1}{p_B} \,. \tag{7.37}$$

7.8.4. SiSQuaRe scheme analysis

The analysis of the SiSQuare scheme has been performed in Chapter 6. In this work we use the estimates of the yield and QBER as derived in Chapter 6 with the following modifications:

- For the calculation of the yield we now adopt a conservative perspective and calculate the number of channel uses as $\mathbb{E}[N_A+N_B]$, as derived in Appendix 7.8.3, rather than $\mathbb{E}[\max(N_A, N_B)]$. Note that $\mathbb{E}[\max(N_A, N_B)] \leq \mathbb{E}[N_A + N_B] \leq 2\mathbb{E}[\max(N_A, N_B)]$.

- The total depolarising parameter for gates and measurements F_{gm} defined in Chapter 6 is now decomposed into individual operations as described in Appendix 7.8.2. That is, in this work depolarisation due to imperfect operations on the memories is expressed in terms of depolarising parameter due to imperfect measurement, F_m, and imperfect two-qubit gate, F_g. Since in the analysis of the SiSQuaRe scheme we only deal with Bell diagonal states, the overall noise due to imperfect swap gate and the Bell measurement leads to $F_{\text{gm}} = F_g^4 F_m^2$.

- In Chapter 6 we have assummed the duration of the detection time-window to be fixed to 30 ns and assumed that all the emitted photons will fall into that time-window. Here, similarly as for other schemes, we perform a more refined analysis in which we include the trade-off between the duration of the time-window and the dark count probability as described in Appendix 7.8.1.

Additionally, we note that in Chapter 6 we assumed that the amount of key that can be generated in the Y- and X-basis will be the same as in the Z-basis for the advantage distillation scheme. This turns out not to be the case. In particular, here we find that for this scheme more key can be extracted in those two bases than in the Z-basis, giving an overall expression that achieves higher secret-key fraction than the expression used in Chapter 6. This point is discussed in more detail in Appendix 7.8.7.

7.8.5. SINGLE-PHOTON SCHEME ANALYSIS

In this appendix we provide a detailed analysis of the single-photon scheme between two remote NV-center nodes. This section is structured as follows. First, we describe the creation of the spin-photon entangled state followed by the action of the lossy channel on the photonic part of this state, including the noise due to the uncertainty in the phase of the state induced by the fiber. Second, we apply the optical Bell measurement. Then we evaluate the effect of dark counts which introduce additional errors to the generated state. Finally we calculate the yield of this scheme and extract the QBER from the resulting state.

SPIN-PHOTON ENTANGLEMENT AND ACTION OF A LOSSY FIBER ON THE PHOTONIC QUBIT

Firstly, both Alice and Bob generate spin-photon entangled states, parameterized by θ. As we will later see, this parameter allows for trading off the quality of the final entangled state of the two spins with the yield of the generation process. The ideal spin-photon state would then be described as

$$|\psi^+\rangle = \sin(\theta)|\downarrow\rangle|0\rangle + \cos(\theta)|\uparrow\rangle|1\rangle\,. \tag{7.38}$$

The preparation of the spin-photon entangled state is not ideal. That is, the spin-photon entangled state is not actually as described above, but rather of the form (see Appendix 7.8.2)

$$\rho = F_{\text{prep}}|\psi^+\rangle\langle\psi^+| + (1-F_{\text{prep}})(\mathbb{I}\otimes Z)|\psi^+\rangle\langle\psi^+|(\mathbb{I}\otimes Z) = F_{\text{prep}}|\psi^+\rangle\langle\psi^+| + (1-F_{\text{prep}})|\psi^-\rangle\langle\psi^-|\,. \tag{7.39}$$

Here

$$|\psi^-\rangle = \sin(\theta)|\downarrow\rangle|0\rangle - \cos(\theta)|\uparrow\rangle|1\rangle\,. \tag{7.40}$$

For the next step we need to consider two additional noise processes that affect the photonic qubits before the optical Bell measurement is performed. The first one is the loss of the photonic qubit. This can happen at the emission, while filtering the photons that are not of the required ZPL frequency, in the lossy fiber, in the imperfect detectors, or due to the arrival outside of the time-window in which detectors expect a click. All these losses can be combined into a single loss parameter

$$\eta = \eta_{\text{total}} = p_{\text{ce}}\, p_{\text{zpl}} \sqrt{\eta_f}\, p'_{\text{det}}\,, \tag{7.41}$$

with $\eta_f = \exp(-\frac{L}{L_0})$, where L is the distance between the two remote NV-center nodes in the scheme (see Fig. 7.5 and Appendix 7.8.1). Hence, a photon is successfully transmitted through the fiber and detected in the middle heralding station with probability η. Now we note that the action of the pure-loss channel on the qubit encoded in the presence or absence of a photon corresponds to the action of the amplitude-damping channel with the damping parameter $1-\eta$ [37].

The second process that effectively happens at the same time as loss, is the dephasing noise arising from the optical instability of the apparatus as described in Appendix 7.8.1. We note that the amplitude-damping and dephasing channel commute, hence it does not matter in which order we apply the two noise processes corresponding to the loss of the photonic qubit and unknown drifts of the phase of the photonic qubit in our model. Here we firstly apply the dephasing due to the lack of knowledge of the phase on Alice's photon and then amplitude-damping on both photons due to all the loss processes.

Following the model in Appendix 7.8.1, the lack of knowledge about the optical phase will effectively transform Alice's state to

$$\rho_A = \left(F_{\text{prep}}\lambda + (1-F_{\text{prep}})(1-\lambda)\right)|\psi^+\rangle\langle\psi^+| + \left((1-F_{\text{prep}})\lambda + F_{\text{prep}}(1-\lambda)\right)|\psi^-\rangle\langle\psi^-|\,. \quad (7.42)$$

where

$$\lambda = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{2I_0\left(\frac{1}{(\Delta\phi)^2}\right)} + \frac{1}{2}. \quad (7.43)$$

Now we can apply all the transmission losses modeled as the amplitude-damping channel. The action of this channel on the photonic part of the state ρ results in the state that we can describe as follows. Firstly, let us introduce two new states

$$|\psi_\eta^\pm\rangle = \frac{1}{\sqrt{\sin^2(\theta)+\eta\cos^2(\theta)}}\left(\sin(\theta)|\downarrow\rangle|0\rangle \pm \sqrt{\eta}\cos(\theta)|\uparrow\rangle|1\rangle\right). \quad (7.44)$$

Then, after the losses and before the Bell measurement, the state of Alice can be written as

$$\begin{aligned}\rho'_A = \left(\sin^2(\theta)+\eta\cos^2(\theta)\right)\Big(&\left(F_{\text{prep}}\lambda + (1-F_{\text{prep}})(1-\lambda)\right)|\psi_\eta^+\rangle\langle\psi_\eta^+| + \left((1-F_{\text{prep}})\lambda + \right.\\ &\left. F_{\text{prep}}(1-\lambda)\right)|\psi_\eta^-\rangle\langle\psi_\eta^-|\Big) + (1-\eta)\cos^2(\theta)|\uparrow\rangle\langle\uparrow||0\rangle\langle 0|\,,\end{aligned} \quad (7.45)$$

and for Bob

$$\rho'_B = \left(\sin^2(\theta)+\eta\cos^2(\theta)\right)\left(F_{\text{prep}}|\psi_\eta^+\rangle\langle\psi_\eta^+| + (1-F_{\text{prep}})|\psi_\eta^-\rangle\langle\psi_\eta^-|\right) + (1-\eta)\cos^2(\theta)|\uparrow\rangle\langle\uparrow||0\rangle\langle 0|\,. \quad (7.46)$$

STATES AFTER THE BELL MEASUREMENT

Now we need to perform a Bell measurement on the photonic qubits within the states ρ'_A and ρ'_B. Here we consider the scenario with non photon-number resolving detectors. Assuming for the moment the scenario without dark counts, we have at most two photons in the system. For this scenario, we have already derived in Section 3.3.1 in Chapter 3

the measurement operators $\{A_0, A_1, A_2\}$ corresponding to the three possible outcomes: left detector clicked, right detector clicked, none of the detectors clicked. The three corresponding outcomes occur with the following probabilities,

$$p_0 = p_1 = \eta\cos^2(\theta)\left(1 - \frac{\eta}{2}\cos^2(\theta)\right), \tag{7.47}$$

$$p_2 = (1 - \eta\cos^2(\theta))^2 . \tag{7.48}$$

The post-measurement state of the two spins for the outcome A_0 is

$$\rho_0 = \frac{2\sin^2(\theta)}{2 - \eta\cos^2(\theta)}\left(a|\Psi^+\rangle\langle\Psi^+| + b|\Psi^-\rangle\langle\Psi^-|\right) + \frac{\cos^2(\theta)(2-\eta)}{2-\eta\cos^2(\theta)}|\uparrow\uparrow\rangle\langle\uparrow\uparrow| . \tag{7.49}$$

Here

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|\downarrow\uparrow\rangle \pm |\uparrow\downarrow\rangle) , \tag{7.50}$$

$$a = \lambda(F_{\text{prep}}^2 + (1-F_{\text{prep}})^2) + 2F_{\text{prep}}(1-F_{\text{prep}})(1-\lambda) , \tag{7.51}$$

$$b = (1-\lambda)(F_{\text{prep}}^2 + (1-F_{\text{prep}})^2) + 2F_{\text{prep}}(1-F_{\text{prep}})\lambda . \tag{7.52}$$

For the outcome A_1 the post-measurement state of the spins is the same up to a local Z gate which Bob can apply following the trigger of the A_1 outcome. The post-measurement state of the spins for the outcome A_2, that is when none of the detector clicked, is

$$\begin{aligned}\rho_2 = \frac{1}{(1-\eta\cos^2(\theta))^2}\Big(&\sin^4(\theta)|\downarrow\downarrow\rangle\langle\downarrow\downarrow| + (1-\eta)\cos^2(\theta)\sin^2(\theta)\left(|\downarrow\uparrow\rangle\langle\downarrow\uparrow| + |\uparrow\downarrow\rangle\langle\uparrow\downarrow|\right)\\ &+(1-\eta)^2\cos^4(\theta)|\uparrow\uparrow\rangle\langle\uparrow\uparrow|\Big) .\end{aligned} \tag{7.53}$$

This is a separable state and so events corresponding to outcome A_2 (that is, no click in any of the detectors) will be discarded as failure. However, dark counts on our detectors can make us draw wrong conclusions about which of the three outcomes we actually obtained.

The effect of dark counts can be seen as follows

- We measured A_2 (no actual detection) but one of the detectors had a dark count. This event will happen with probability $2p_2p_d(1-p_d)$ and will make us accept the state ρ_2. Note that this is a classical state so application of the Z correction by Bob does not affect this state at all.

- We measured A_1 or A_2 but we also got a dark count in the other detector. This event will happen with probability $(p_0+p_1)\cdot p_d$. This will effectively lead us to rejection of the desired state ρ_0. Hence effectively ρ_0 will only be accepted if we measured A_1 or A_2 but the other detector did not have a dark count, which will happen with probability $(p_0+p_1)\cdot(1-p_d)$.

THE YIELD AND QBER

Taking dark counts into account, we see that the yield of the single-photon scheme, which is just the probability of registering a click in only one of the detectors, will be

$$Y = (p_0+p_1)(1-p_d)+2p_2p_d(1-p_d) = 2(1-p_d)\left[\eta\cos^2(\theta)\left(1-\frac{\eta}{2}\cos^2(\theta)\right)+(1-\eta\cos^2(\theta))^2 p_d\right]. \tag{7.54}$$

The effective accepted state after a click in one of the detectors will then be

$$\rho_{\text{out}} = \frac{1}{Y}\left((p_0+p_1)(1-p_d)\rho_0 + 2p_2p_d(1-p_d)\rho_2\right). \tag{7.55}$$

Note that both Alice and Bob perform a measurement on their electron spins immediately after each of the spin-photon entanglement generation events. This measurement causes an error modeled as a depolarizing channel of parameter F_m on each qubit, which means that after a successful run of the single-photon protocol, the effective state shared by Alice and Bob including the noise of their measurements will be given by

$$\rho_{AB} = F_m^2\rho_{\text{out}} + (1-F_m)F_m\left[\frac{\mathbb{I}_{2,A}}{2}\otimes \text{tr}_A[\rho_{\text{out}}] + \text{tr}_B[\rho_{\text{out}}]\otimes\frac{\mathbb{I}_{2,B}}{2}\right] + (1-F_m)^2\,\frac{\mathbb{I}_{4,AB}}{4}. \tag{7.56}$$

One can then extract the QBER for this state in all the three bases using the appropriate correlated/anti-correlated projectors such that:

$$e_z = \text{Tr}((|00\rangle\langle 00| + |11\rangle\langle 11|)\rho_{AB}), \tag{7.57}$$

$$e_{xy} = \text{Tr}((|+-\rangle\langle +-| + |-+\rangle\langle -+|)\rho_{AB}) = \text{Tr}((|0_y1_y\rangle\langle 0_y1_y| + |1_y0_y\rangle\langle 1_y0_y|)\rho_{AB}). \tag{7.58}$$

Here $|+\rangle$ and $|-\rangle$ denote the two eigenstates of X and $|0_y\rangle$ and $|1_y\rangle$ denote the two eigenstates of Y. We note that for our model of the single-photon scheme the QBER in X- and Y- bases are the same and therefore we denote both by a single symbol e_{xy}.

7.8.6. SPADS AND SPOTL SCHEMES ANALYSIS

In order to compute the quantum bit error rate (QBER) of the Single-Photon with Additional Detection Setup (SPADS) scheme and the Single-Photon Over Two Links (SPOTL) scheme, we derive step by step the quantum state shared between Alice and Bob. The following results have been found using Mathematica. Finally, we also calculate the yield of the SPADS and SPOTL schemes.

GENERATION OF ELEMENTARY LINKS

SINGLE-PHOTON SCHEME ON ALICE SIDE

The application of the single-photon scheme on Alice's side leads Alice and the quantum repeater to share a state given in Eq. (7.55). This state can be rewritten as

$$\rho_{\text{A-QR}^e} = A_1|\Psi^+\rangle\langle\Psi^+| + B_1|\Psi^-\rangle\langle\Psi^-| + C_1\,(|10\rangle\langle 10| + |01\rangle\langle 01|) + D_1|11\rangle\langle 11| + E_1|00\rangle\langle 00|, \tag{7.59}$$

with $A_1 = A(\theta_A, Y_A)$, $B_1 = B(\theta_A, Y_A)$, $C_1 = C(\theta_A, Y_A)$, $D_1 = D(\theta_A, Y_A)$ and $E_1 = E(\theta_A, Y_A)$. Here we have that

$$\begin{aligned}
A(\theta, Y) &= \frac{1}{Y} 2\cos^2(\theta)\sin^2(\theta)\eta(1-p_d)\left[(F_{\text{prep}}^2 + (1-F_{\text{prep}})^2)\lambda + 2F_{\text{prep}}(1-F_{\text{prep}})(1-\lambda)\right] , \\
B(\theta, Y) &= \frac{1}{Y} 2\cos^2(\theta)\sin^2(\theta)\eta(1-p_d)\left[(F_{\text{prep}}^2 + (1-F_{\text{prep}})^2)(1-\lambda) + 2F_{\text{prep}}(1-F_{\text{prep}})\lambda\right] , \\
C(\theta, Y) &= \frac{2}{Y} \cos^2(\theta)\sin^2(\theta) p_d(1-p_d)(1-\eta) , \\
D(\theta, Y) &= \frac{1}{Y} \cos^4(\theta)\left(2(1-\eta)\eta(1-p_d) + \eta^2(1-p_d) + 2(1-\eta)^2 p_d(1-p_d)\right) , \\
E(\theta, Y) &= \frac{2}{Y} \sin^4(\theta) p_d(1-p_d) .
\end{aligned} \tag{7.60}$$

In the above Y denotes the yield or the probability of success of the single-photon scheme and is given by Eq. (7.54). Subscript A indicates that in that expression for the yield and for each of the above defined coefficients we use $\theta = \theta_A$. Moreover, we have made here the following change of notation with respect to the Appendix 7.8.5, $|\downarrow\rangle \rightarrow |0\rangle$ and $|\uparrow\rangle \rightarrow |1\rangle$.

SWAP GATE IN THE MIDDLE NODE

In the next step a SWAP gate is applied in the middle node to transfer the electron state to the nuclear spin of the NV center. This causes a depolarizing noise of parameter $F_{\text{swap}} = F_g^2$ (see Appendix 7.8.1). The resulting state can then be written as

$$\rho_{\text{A-QR}^C} = F_{\text{swap}}\rho_{\text{A-QR}^e} + (1-F_{\text{swap}})\,\text{tr}_{\text{QR}}[\rho_{\text{A-QR}^e}] \otimes \frac{\mathbb{I}_{2,\text{QR}}}{2} . \tag{7.61}$$

THE PROCEDURE ON BOB'S SIDE

We now use the electron spin of the quantum repeater to generate the second quantum state. Here the procedures for the SPADS and SPOTL schemes diverge.

In the procedure for the SPADS scheme, the quantum repeater generates a spin-photon entangled state where the photonic qubit is encoded in the time-bin degree of freedom. Since the spin-photon entangled state is imperfect, the electron and the photon share a state

$$\rho_{\text{QR}^e-B} = F_{\text{prep}}|\Psi^+\rangle\langle\Psi^+| + (1-F_{\text{prep}})|\Psi^-\rangle\langle\Psi^-| . \tag{7.62}$$

Here we use the following labeling for time-bin encoded early and late mode of the photon: $|e\rangle = |1\rangle$, $|l\rangle = |0\rangle$. This photon is then sent towards Bob's detector. The lossy channel acts on such a time-bin encoded qubit as an erasure channel and so the quantum spin-photon state of the successful events in which the photonic qubit successfully arrives at the detector is unaffected by the lossy channel.

For the SPOTL scheme the repeater's electron spin and Bob's quantum memory generate a second state of the form given in Eq. (7.55). We can rewrite this state as

$$\rho_{\text{QR}^e-B} = A_2|\Psi^+\rangle\langle\Psi^+| + B_2|\Psi^-\rangle\langle\Psi^-| + C_2\left(|10\rangle\langle 10| + |01\rangle\langle 01|\right) + D_2|11\rangle\langle 11| + E_2|00\rangle\langle 00| , \tag{7.63}$$

with $A_2 = A(\theta_B, Y_B)$, $B_2 = B(\theta_B, Y_B)$, $C_2 = C(\theta_B, Y_B)$, $D_2 = D(\theta_B, Y_B)$ and $E_2 = E(\theta_B, Y_B)$.

DECOHERENCE IN THE QUANTUM MEMORIES

Decoherence of the carbon spin in the middle node can be modeled identically for both the SPADS and SPOTL scheme.

During the $n < n^*$ attempts to generate the state $\rho_{\text{QR}^e\text{-B}}$, the carbon spin in the middle node holding half of the state $\rho_{\text{A-QR}^C}$ will decohere. Using the decoherence model discussed in Appendix 7.8.2, decoherence of the carbon spin will thus give us

$$\rho'_{\text{A-QR}^C} = F_{T_1}(F_{T_2}\rho_{\text{A-QR}^C} + (1-F_{T_2})(\mathbb{I}_2 \otimes Z)\rho_{\text{A-QR}^C}(\mathbb{I}_2 \otimes Z)^\dagger) + (1-F_{T_1})\,\text{tr}_{\text{QR}}[\rho_{\text{A-QR}^C}] \otimes \frac{\mathbb{I}_{2,\text{QR}}}{2}\,. \tag{7.64}$$

For key generation, Alice (SPADS and SPOTL schemes) and Bob (SPOTL scheme) can actually measure their electron spin(s) immediately after the generation of spin photon entanglement, preventing the effect of decoherence on these qubit(s).

NOISE DUE TO MEASUREMENTS

MEASUREMENT OF THE QUBITS OF ALICE AND BOB

In the SPADS scheme Alice performs a measurement on her electron spin immediately after each of the spin-photon entanglement generation events to prevent any decoherence with time of this qubit. This measurement causes an error modeled as a depolarizing channel of parameter F_m. Bob on the other hand performs a measurement on a photonic qubit that is encoded in the time-bin degree of freedom. His measurement utilises the squashing map so that we can model the noise arising from this measurement as a depolarising channel with parameter α_B as described in Appendix 7.8.1. Hence the total state just before the Bell measurement is given by

$$\begin{aligned}\rho_{A-QR-B} = {} & F_m\alpha_B\rho'_{\text{A-QR}^C} \otimes \rho_{\text{QR}^e-B} + (1-F_m)\alpha_B\frac{\mathbb{I}_{2,A}}{2} \otimes \text{tr}_A[\rho'_{\text{A-QR}^C}] \otimes \rho_{\text{QR}^e-B} \\ & + (1-\alpha_B)F_m\rho'_{\text{A-QR}^C} \otimes \text{tr}_B[\rho_{\text{QR}^e-B}] \otimes \frac{\mathbb{I}_{2,B}}{2} \\ & + (1-F_m)(1-\alpha_B)\,\text{tr}_{AB}[\rho'_{\text{A-QR}^C} \otimes \rho_{\text{QR}^e-B}] \otimes \frac{\mathbb{I}_{4,AB}}{4}\,.\end{aligned} \tag{7.65}$$

For the SPOTL scheme, both Alice and Bob perform a measurement on their electron spins immediately after each of the spin-photon entanglement generation events. This measurement causes an error modeled as a depolarizing channel of parameter F_m on each qubit, which means that after both Alice and Bob succeeded in performing the single-photon scheme with the repeater, the total, four-qubit state just before the Bell-measurement and including the noise of the measurements of Alice and Bob will be given by

$$\begin{aligned}\rho_{A-QR-B} = {} & F_m^2\rho'_{\text{A-QR}^C} \otimes \rho_{\text{QR}^e-B} \\ & + (1-F_m)F_m\left[\frac{\mathbb{I}_{2,A}}{2} \otimes \text{tr}_A[\rho'_{\text{A-QR}^C}] \otimes \rho_{\text{QR}^e-B} + \rho'_{\text{A-QR}^C} \otimes \text{tr}_B[\rho_{\text{QR}^e-B}] \otimes \frac{\mathbb{I}_{2,B}}{2}\right] \\ & + (1-F_m)^2\,\text{tr}_{AB}[\rho'_{\text{A-QR}^C} \otimes \rho_{\text{QR}^e-B}] \otimes \frac{\mathbb{I}_{4,AB}}{4}\,.\end{aligned} \tag{7.66}$$

BELL STATE MEASUREMENT

Before the entanglement swapping, we have a total state ρ_{A-QR-B}. We now perform a Bell state measurement on the two qubits in the middle node. The error coming from this measurement is modeled by concatenation of depolarizing channels (see Appendix 7.8.1) which means that the measurement is actually performed on

$$\rho_{\text{fin}} = F_g^2 F_m^2 \rho_{A-QR-B} + F_g^2(1-F_m^2)\,\text{tr}_{QR^e}[\rho_{A-QR-B}]\otimes\frac{\mathbb{I}_{2,QR^e}}{2} + (1-F_g^2)\,\text{tr}_{QR}[\rho_{A-QR-B}]\otimes\frac{\mathbb{I}_{4,QR}}{4}\,. \tag{7.67}$$

While $\rho'_{\text{A-QR}^C}$ is not Bell diagonal for the SPADS scheme, ρ_{QR^e-B} is, and so we find that taking into account the classical correction (which will be performed on the measured bit-value by Alice and Bob) the four cases corresponding to different measurement outcomes are equivalent. This means that if we model the correction to be applied to the quantum state rather than the classical bit, then the four post-measurement bipartite states shared between Alice and Bob are exactly the same.

For the SPOTL scheme, both $\rho'_{\text{A-QR}^C}$ and ρ_{QR^e-B} are not Bell diagonal which means that the resulting state of qubits of Alice and Bob after the Bell state measurement depends on the outcome of this Bell measurement and those four corresponding states are not equivalent under local unitary corrections. In fact, the two states corresponding to the $\Phi^\pm$ outcomes and the two states corresponding to the $\Psi^\pm$ outcomes are pairwise equivalent under local Pauli corrections. Hence, we will derive two different QBER corresponding to the following different resulting states shared between Alice and Bob,

$$\rho_{\Phi,AB} = (\mathbb{I}_A\otimes U_{\Phi^\pm,B})\,\text{Tr}_{QR}\left[\frac{(\mathbb{I}\otimes|\Phi^\pm\rangle\langle\Phi^\pm|\otimes\mathbb{I})\rho_{\text{fin}}(\mathbb{I}\otimes|\Phi^\pm\rangle\langle\Phi^\pm|\otimes\mathbb{I})^\dagger}{\text{Tr}(\rho_{\text{fin}}(\mathbb{I}\otimes|\Phi^\pm\rangle\langle\Phi^\pm|\otimes\mathbb{I}))}\right](\mathbb{I}\otimes U_{\Phi^\pm,B})^\dagger\,, \tag{7.68}$$

$$\rho_{\Psi,AB} = (\mathbb{I}_A\otimes U_{\Psi^\pm,B})\,\text{Tr}_{QR}\left[\frac{(\mathbb{I}\otimes|\Psi^\pm\rangle\langle\Psi^\pm|\otimes\mathbb{I})\rho_{\text{fin}}(\mathbb{I}\otimes|\Psi^\pm\rangle\langle\Psi^\pm|\otimes\mathbb{I})^\dagger}{\text{Tr}(\rho_{\text{fin}}(\mathbb{I}\otimes|\Psi^\pm\rangle\langle\Psi^\pm|\otimes\mathbb{I}))}\right](\mathbb{I}\otimes U_{\Psi^\pm,B})^\dagger\,. \tag{7.69}$$

Here $U_{\Phi^\pm,B}$ and $U_{\Psi^\pm,B}$ denote the four Pauli corrections implemented by Bob after the corresponding outcome of the Bell measurement. Note that for the SPADS scheme $\rho_{\Phi,AB} = \rho_{\Psi,AB}$.

THE YIELD AND QBER

YIELD

For both SPADS and SPOTL scheme we calculate the yield as the inverse of the number of channel uses required to generate one bit of raw key, $Y = 1/\mathbb{E}[N]$, where $\mathbb{E}[N]$ is given by Eq. (7.34). For the SPOTL scheme in that formula we use $p_{A/B} = Y_{A/B}$, where $Y_{A/B}$ denotes the yield of the single-photon scheme on Alice's/Bob's side given by Eq. (7.54). For the SPADS scheme p_A takes the same form as for the SPOTL scheme (but is now calculated for two thirds of the total distance between Alice and Bob rather than half), while p_B is the probability of registering a click in Bob's optical detection setup as in the SiSQuaRe scheme.

EXTRACTION OF THE QUBIT ERROR RATES

By projecting these final corrected states onto the correct subspaces, we can obtain the qubit error rates e_z and e_{xy} (with our model we find that for both SPADS and SPOTL schemes the error rates in X and Y bases are the same). The state shared between Alice and Bob after the Pauli correction will always be the same for the SPADS scheme. Thus, there is only a single QBER e_z and e_{xy} independently of the outcome of the Bell measurement. For the SPOTL scheme that is not the case, there will be two set of QBER corresponding to the states $\rho_{\Phi,AB}$ and $\rho_{\Psi,AB}$.

$$e_{z,\Phi} = \mathrm{Tr}((|00\rangle\langle 00| + |11\rangle\langle 11|)\rho_\Phi)\,, \tag{7.70}$$

$$e_{z,\Psi} = \mathrm{Tr}((|00\rangle\langle 00| + |11\rangle\langle 11|)\rho_\Psi)\,, \tag{7.71}$$

$$e_{xy,\Phi} = \mathrm{Tr}((|+-\rangle\langle +-| + |-+\rangle\langle -+|)\rho_\Phi) = \mathrm{Tr}((|0_y1_y\rangle\langle 0_y1_y| + |1_y0_y\rangle\langle 1_y0_y|)\rho_\Phi)\,, \tag{7.72}$$

$$e_{xy,\Psi} = \mathrm{Tr}((|+-\rangle\langle +-| + |-+\rangle\langle -+|)\rho_\Psi) = \mathrm{Tr}((|0_y1_y\rangle\langle 0_y1_y| + |1_y0_y\rangle\langle 1_y0_y|)\rho_\Psi)\,. \tag{7.73}$$

Again, for the SPADS scheme $e_{z,\Phi} = e_{z,\Psi} = e_z$ and $e_{xy,\Phi} = e_{xy,\Psi} = e_{xy}$.

AVERAGING THE QUBIT ERROR RATES

We have now derived the qubit error rates as a function of the experimental parameters. For the SPOTL scheme we now average the QBER over the two outcomes to get the final average QBER

$$\langle e_z\rangle = \langle p_\Psi e_{z,\Psi} + p_\Phi e_{z,\Phi}\rangle\,, \tag{7.74}$$

$$\langle e_{xy}\rangle = \langle p_\Psi e_{xy,\Psi} + p_\Phi e_{xy,\Phi}\rangle\,, \tag{7.75}$$

where p_Ψ (p_Φ) is the probability of measuring one of the $|\Psi\rangle$ ($|\Phi\rangle$) states in the Bell measurement and $\langle ...\rangle$ is found by averaging the expression over the number of Bob's attempts n with the geometric distribution within the first n^* trials. For the SPADS scheme $\langle e_z\rangle$ and $\langle e_{xy}\rangle$ can be averaged directly. The dependence on n arises from the decoherence terms F_{T_1} and F_{T_2}. Indeed, those terms correspond to the decoherence in the middle node during the attempts on Bob's side. Denoting by p_B the probability that in a single attempt Bob generates entanglement with the quantum repeater using the single-photon scheme for the SPOTL scheme and using direct transmission of the time-bin encoded qubit from the repeater to Bob for the SPADS scheme, we have that the exponentials in those expressions can be averaged as follows (see Chapter 6)

$$\langle e^{-cn}\rangle = \frac{p_B e^{-c}}{1-(1-p_B)^{n^*}} \frac{1-(1-p)^{n^*}e^{-cn^*}}{1-(1-p_B)e^{-c}}\,. \tag{7.76}$$

7.8.7. SECRET-KEY FRACTION AND ADVANTAGE DISTILLATION

In this section we discuss certain subtleties relating to the differences between generating key from measurements in different bases in the scenario where the QBER is not uniform across all the bases. We also provide an expression for the asymptotic secret-key fraction with one-way postprocessing.

ONE-WAY BB84 PROTOCOL

For the fully asymmetric BB84 protocol with standard one-way post-processing, the secret-key fraction has been given in Section 6.4.2 in Chapter 6. Note that this formula is symmetric under the exchange of e_x and e_z - that is, the secret-key fraction is the same independently of whether we extract the key in the Z- or X-basis. As we will see later in this section, this is not the case for the six-state protocol with advantage distillation.

SIX-STATE PROTOCOL WITH ADVANTAGE DISTILLATION

Now we shall examine the six-state protocol with advantage distillation of [29]. In Appendix 6.9.4 in Chapter 6 we have already provided an expression for the secret-key fraction as a function of QBER for this protocol. We have used there that expression to approximate the amount of key that can be extracted from a single raw bit independently of the basis in which the key is generated. Here however, we note that this expression specifically describes only the secret-key fraction in the case when the key is extracted in the Z-basis.

It is important to note that for this advantage distillation scheme, the amount of generated secret key depends on the basis in which it is extracted, as has been shown in [40]. Let us now have a look at the amount of key that can be extracted in the X- and Y-bases. As has been shown in [40], the secret-key fraction in these cases is also given by Eq. (6.35) from Chapter 6 but now the Bell coefficients depend on QBER in the following way:

$$\begin{aligned} p_{00} &= 1 - \frac{e_z}{2} - e_{xy} \,, \\ p_{10} &= e_{xy} - \frac{e_z}{2} \,, \\ p_{01} &= p_{11} = \frac{e_z}{2} \,. \end{aligned} \tag{7.77}$$

And so

$$\begin{aligned} P_{\tilde{\mathrm{X}}}(0) &= 1 - 2e_{xy} + 2e_{xy}^2 \,, \\ P_{\tilde{\mathrm{X}}}(1) &= 2(1 - e_{xy})e_{xy} \,. \end{aligned} \tag{7.78}$$

We note that we have assumed here that in the case of key extraction in Y-basis, either Alice or Bob applies a local bit flip in the Y-basis to the shared state, as the target state $|\psi(0,0)\rangle$ is anti-correlated in that basis.

In [40] it has been also observed that in the considered case of having the QBER in the X- and Y-bases being equal, the six-state protocol with advantage distillation allows us to extract more key if it is extracted in the basis with higher QBER. This observation determines the basis that we use for extracting key for the single-photon and the SPOTL schemes that use fully asymmetric six-state protocol with advantage distillation. Specifically, for the single-photon scheme we observe higher QBER in the Z-basis, while for the SPOTL scheme the QBER is higher in the X- and Y-bases. Therefore these are the bases that we choose to use for extracting key for those schemes.

For the SiSQuaRe and SPADS schemes the symmetric six-state protocol is used, hence for those schemes we group the raw bits into three groups corresponding to three different key-extraction bases and we extract the key separately for each of these bases. Finally,

to obtain the final secret-key fraction, we note that for the symmetric six-state protocol we also need to include sifting, that is only one third of all the raw bits were obtained by Alice and Bob measuring in the same basis (the raw bits for the protocol runs in which they measured in different bases are discarded). Hence, if we denote by r_i the secret-key fraction obtained from the group of raw bits in which both Alice and Bob measured in the basis i, the final secret-key fraction for the six-state protocol for those schemes is given by

$$r = \frac{1}{3}\left(\frac{1}{3}r_x + \frac{1}{3}r_y + \frac{1}{3}r_z\right) . \tag{7.79}$$

Clearly in our case we have $r_x = r_y = r_{xy}$.

Since for the SiSQuRe scheme all the noise processes are modelled by the depolarising and the dephasing noise in Z-basis, we find there that $e_{xy} \geq e_z$ and therefore $r_{xy} \geq r_z$. This shows that approximating the amount of key that can be extracted in the X- and Y-bases by the secret-key fraction from the Z-basis as has been done in Chapter 6, provides actually a lower bound on the overall secret-key fraction. The actual expression given in Eq. (7.79) and used for this scheme in this chapter achieves larger values.

ONE-WAY SIX-STATE PROTOCOL

In Figure 7.6 we have also plotted the secret-key fraction for the one-way six-state protocol. For the fully asymmetric protocol and the case in which the key is extracted in the Z-basis, it is given by [41]

$$r = 1 - e_z h\left(\frac{1+(e_x-e_y)/e_z}{2}\right) - (1-e_z)h\left(\frac{1-(e_x+e_y+e_z)/2}{1-e_z}\right) - h(e_z) . \tag{7.80}$$

Although this formula does not appear to be symmetric under the permutation of e_x, e_y, e_z, it is in fact invariant under this permutation [42]. This means that for the symmetric one-way six-state protocol, in our case the final secret-key fraction is given by the expression in Eq. (7.80) multiplied by the sifting efficiency of one-third.

7.8.8. RUNTIME OF THE EXPERIMENT

In this section we will detail how to perform an experiment that will be able to establish that a setup can surpass the capacity of a quantum channel modeling losses in a fiber (see Eq. (6.13)). This experiment can validate a setup to qualify as a quantum repeater, without explicitly having to generate secret-key. We show then that, for the listed parameters in the main text, the single-photon scheme can be certified to be a quantum repeater within approximately twelve hours.

The experiment is based on estimating the yield of the scheme and the individual QBER of the generated states. More specifically, here we will calculate the probability that, assuming our model is accurate and each individual run is independent and identically distributed, the observed estimate of the yield and the individual QBER are larger and smaller, respectively, than some fixed threshold values. If, with these threshold values for the yield and QBER, the calculated asymptotic secret-key still surpasses the capacity, we can claim a working quantum repeater. The experiment consists of first performing n attempts at generating a state between Alice and Bob, from which the yield can be estimated by calculating the ratio of the successful attempts and n. Then, the

QBER in each basis is estimated by Alice and Bob measuring in the same basis in each of the successful attempts.

Central to our calculation is the fact that, for n instances of a Bernoulli random variable with probability p, the probability that the number of observed successes $S(n)$ is smaller or equal than some value k is equal to

$$P\left(S(n) \leq k\right) = \sum_{i=0}^{k} \binom{n}{i} p^i \left(1-p\right)^{n-i} . \tag{7.81}$$

Assuming the outcomes of our experiment are independent and identically distributed, the observed yield $\bar{Y}$ satisfies

$$P\left(\bar{Y} \leq (Y - t_Y)\right) = P\left(n\bar{Y} \leq n\left(Y - t_Y\right)\right) = \sum_{i=0}^{\lfloor n(Y-t_Y)\rfloor} \binom{n}{i} Y^i \left(1-Y\right)^{n-i} , \tag{7.82}$$

where $Y - t_Y$ is the lower threshold. Let us make this more concrete with a specific calculation. For a distance of $17L_0$ the yield is equal to $\approx 5.6 \cdot 10^{-6}$. Setting the maximum deviation in the yield to $\bar{Y} = Y - t_Y$ with $t_Y = 2.0 \cdot 10^{-7}$ and the number of attempts to $n = 5 \cdot 10^9$ (which corresponds to approximately a runtime of twelve hours assuming a single attempt takes $8.5 \cdot 10^{-6}$ s, corresponding to t_{prep} and a single-shot readout lasting $2.5 \cdot 10^{-6}$ s), we find that

$$P\left(\bar{Y} \leq (Y - t_Y)\right) \leq 9.2 \cdot 10^{-10} . \tag{7.83}$$

Similarly, for the individual errors $\{e_k\}_{k\in\{x,y,z\}}$ in the three bases we have that

$$P\left(\bar{e}_k \geq (e_k + t_k)\right) = P\left(m \cdot \bar{e}_k \geq m\left(e_k + t_k\right)\right) = \sum_{i=\lceil m(e_k+t_k)\rceil}^{m} \binom{m}{i} \left(e_k\right)^i \left(1-e_k\right)^{m-i} . \tag{7.84}$$

Here we set $m = \left\lfloor \frac{n}{3}\left(Y - t_Y\right)\right\rfloor$, which is an estimate for the number of raw bits that Alice and Bob obtain from measurements in each of the three bases, for the total n attempts of the protocol. All the raw bits from those three sets are then compared to estimate the QBER in each of the three bases. Note that we gather the same amount of samples for each basis, even when an asymmetric protocol would be performed. Setting $t_i = t = 0.015,\ \forall i \in \{x, y, z\}$ and, as before, $n = 5 \cdot 10^9$, we find, at a distance of $17L_0$ where $e_z \approx 0.171$ and $e_y = e_x \approx 0.141$, that

$$P\left(\bar{e}_z \geq (e_z + t)\right) \leq 9.0 \cdot 10^{-5} , \tag{7.85}$$

$$P\left(\bar{e}_y \geq \left(e_y + t\right)\right) = P\left(\bar{e}_x \geq (e_x + t)\right) \leq 2.7 \cdot 10^{-5} . \tag{7.86}$$

Then, with probability at least

$$\begin{aligned}\left(1 - P\left(\bar{e}_x \geq (e_x + t)\right)\right) \cdot \left(1 - P\left(\bar{e}_y \geq \left(e_y + t\right)\right)\right) \cdot \left(1 - P\left(\bar{e}_z \geq (e_z + t)\right)\right) \cdot \left(1 - P\left(\bar{Y} \leq (Y - t_Y)\right)\right) \\ \geq 1 - 1.5 \cdot 10^{-4} ,\end{aligned} \tag{7.87}$$

none of the observed QBER and yield exceed their threshold conditions. The corresponding lowest secret-key rate for these parameters (with a yield of $Y - t_Y$ and QBER of $e_x + t_x,\ e_y + t_y,\ e_z + t_z$) is $\approx 1.97 \cdot 10^{-7}$, which we observe is greater than the secret-key capacity by a factor ≈ 3.29 (see Eq.(6.13)) at a distance of $17L_0$, since the secret-key capacity equals $-\log_2\left(1 - e^{-17}\right) \lesssim 5.97 \cdot 10^{-8}$.

Thus, with high probability we can establish that the single-photon scheme achieves a secret-key rate significantly greater than the corresponding secret-key capacity for a distance of $17L_0 \approx 9.2$ kilometer within approximately twelve hours.

7.8.9. MDI QKD

We note here that the single-photon scheme for generating key is closely linked to the measurement device independent (MDI) QKD protocol [15]. In particular it is an entanglement-based version of a scheme in which Alice and Bob prepare and send specific photonic qubit states to the heralding station in the middle, where the qubits are encoded in the presence/absence of the photon. We note that in the ideal case of the single-photon scheme, the spin-photon state is given in Eq. (7.38). For the six-state protocol the spin part of this state is then measured in the X-, Y- or Z- basis at random according to a fixed probability distribution (this probability distribution dictates whether we use symmetric or asymmetric protocol). Considering the probabilities of the individual measurement outcomes, this is equivalent to the scenario in which Alice and Bob choose one of the three set of states at random according to the same probability distribution and prepare each of the two states from that set with the probability equal to the corresponding measurement outcome probability. These sets do not form bases, as the two states within each set are not orthogonal. We will therefore refer to these sets here as "pseudo-bases". Depending on the chosen pseudo-basis they prepare one of the six states encoding the bit value of "0" or "1" in that pseudo-basis. These states and the corresponding preparation probabilities are

- pseudo-basis 1: $\{|0\rangle, |1\rangle\}$ with probabilities $\{\sin^2\theta,\ \cos^2\theta\}$,
- pseudo-basis 2: $\{\sin\theta|0\rangle + \cos\theta|1\rangle,\ \sin\theta|0\rangle - \cos\theta|1\rangle\}$ with probabilities $\{\frac{1}{2}, \frac{1}{2}\}$,
- pseudo-basis 3: $\{\sin\theta|0\rangle + i\cos\theta|1\rangle,\ \sin\theta|0\rangle - i\cos\theta|1\rangle\}$ with probabilities $\{\frac{1}{2}, \frac{1}{2}\}$.

These states are then sent towards the beam splitter station. The station performs the standard photonic Bell-state measurement and sends the outcome to both Alice and Bob. Alice and Bob discard all the runs for which the beam splitter station measured A_2 (recall the measurement operators in Eq. (3.11) in Chapter 3). They then exchange the classical information about their pseudo-basis choice and keep only the data for the runs in which they both used the same basis. For those data they apply the following post-processing in order to obtain correlated raw bits

- pseudo-basis 1: for both outcomes A_0 and A_1 Bob flips the value of his bit.
- pseudo-basis 2: for the outcome A_0 they do nothing, for the outcome A_1 Bob flips the value of his bit.

- pseudo-basis 3: for the outcome A_0 they do nothing, for the outcome A_1 Bob flips the value of his bit.

In this way Alice and Bob have generated their strings of raw bits.

We note here that the direct preparation of the six states from the three pseudo-bases described above in the photonic presence/absence degree of freedom is experimentally hard. This is related to the fact that linear optics does not allow to easily perform single qubit rotations necessary to prepare these states. The use of memory-based NV-centers offers a great advantage here, as in these schemes the rotations that allow us to obtain the required amplitudes of the photonic states are performed on the electron spins rather than the photons themselves. There has also been proposed an alternative scheme that also benefits from single photon detection events in which Alice and Bob send coherent pulses to the heralding station [12, 25].

REFERENCES

[1] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, *Overcoming lossy channel bounds using a single quantum repeater node,* Applied Physics B **122**, 96 (2016).

[2] P. C. Humphreys, N. Kalb, J. P. Morits, R. N. Schouten, R. F. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, *Deterministic delivery of remote entanglement on a quantum network,* Nature **558**, 268 (2018).

[3] M. H. Abobeih, J. Cramer, M. A. Bakker, N. Kalb, M. Markham, D. J. Twitchen, and T. H. Taminiau, *One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment,* Nature Communications **9**, 2552 (2018).

[4] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. 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**, 928 (2017).

[5] T. H. Taminiau, J. Cramer, T. van der Sar, V. V. Dobrovitski, and R. Hanson, *Universal control and error correction in multi-qubit spin registers in diamond,* Nature Nanotechnology **9**, 171 (2014).

[6] M. Blok, N. Kalb, A. Reiserer, T. Taminiau, and R. Hanson, *Towards quantum networks of single spins: analysis of a quantum memory with an optical interface in diamond,* Faraday Discussions **184**, 173 (2015).

[7] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau, *Repeated quantum error correction on a continuously encoded qubit by real-time feedback,* Nature Communications **7**, 11526 (2016).

[8] A. Reiserer, N. Kalb, M. S. Blok, K. J. van Bemmelen, T. H. Taminiau, R. Hanson, D. J. Twitchen, and M. Markham, *Robust quantum-network memory using decoherence-protected subspaces of nuclear spins,* Physical Review X **6**, 021040 (2016).

[9] W. Gao, A. Imamoglu, H. Bernien, and R. Hanson, *Coherent manipulation, measurement and entanglement of individual solid-state spins using optical fields,* Nature Photonics **9**, 363 (2015).

[10] S. Bogdanović, S. B. van Dam, C. Bonato, L. C. Coenen, A.-M. J. Zwerver, B. Hensen, M. S. Liddy, T. Fink, A. Reiserer, M. Lončar, *et al., Design and low-temperature characterization of a tunable microcavity for diamond-based quantum networks,* Applied Physics Letters **110**, 171103 (2017).

[11] C. Cabrillo, J. Cirac, P. Garcia-Fernandez, and P. Zoller, *Creation of entangled states of distant atoms by interference,* Physical Review A **59**, 1025 (1999).

[12] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, *Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,* Nature **557**, 400 (2018).

[13] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Fundamental limits of repeaterless quantum communications,* Nature Communications **8**, 15043 (2017).

[14] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, *Long-distance quantum communication with atomic ensembles and linear optics,* Nature **414**, 413 (2001).

[15] H.-K. Lo, M. Curty, and B. Qi, *Measurement-device-independent quantum key distribution,* Physical Review Letters **108**, 130503 (2012).

[16] S. Pirandola, *Capacities of repeater-assisted quantum communications,* arXiv preprint arXiv:1601.00966 (2016).

[17] S. D. Barrett and P. Kok, *Efficient high-fidelity quantum computation using matter qubits and linear optics,* Physical Review A **71**, 060310 (2005).

[18] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, *et al.*, *Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres,* Nature **526**, 682 (2015).

[19] B. Hensen, N. Kalb, M. Blok, A. Dréau, A. Reiserer, R. Vermeulen, R. Schouten, M. Markham, D. Twitchen, K. Goodenough, *et al.*, *Loophole-free Bell test using electron spins in diamond: second experiment and additional analysis,* Scientific Reports **6** (2016).

[20] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. Blok, L. Robledo, T. Taminiau, M. Markham, D. Twitchen, L. Childress, *et al.*, *Heralded entanglement between solid-state qubits separated by three metres,* Nature **497**, 86 (2013).

[21] P. Maunz, D. Moehring, S. Olmschenk, K. Younge, D. Matsukevich, and C. Monroe, *Quantum interference of photon pairs from two remote trapped atomic ions,* Nature Physics **3**, 538 (2007).

[22] R. Stockill, M. Stanley, L. Huthmacher, E. Clarke, M. Hugues, A. Miller, C. Matthiesen, C. Le Gall, and M. Atatüre, *Phase-tuned entangled state generation between distant spin qubits,* Physical Review Letters **119**, 010503 (2017).

[23] A. Delteil, Z. Sun, W.-b. Gao, E. Togan, S. Faelt, and A. Imamoğlu, *Generation of heralded entanglement between distant hole spins,* Nature Physics **12**, 218 (2016).

[24] C. W. Chou, H. de Riedmatten, D. Felinto, S. V. Polyakov, S. J. van Enk, and H. J. Kimble, *Measurement-induced entanglement for excitation stored in remote atomic ensembles,* Nature **438**, 828 EP (2005).

[25] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, *Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound,* arXiv preprint arXiv:1805.05511 (2018).

[26] X. Ma, P. Zeng, and H. Zhou, *Phase-matching quantum key distribution,* Physical Review X **8**, 031043 (2018).

[27] J. S. Ivan, K. K. Sabapathy, and R. Simon, *Operator-sum representation for bosonic gaussian channels,* Physical Review A **84**, 042311 (2011).

[28] M. W. Doherty, N. B. Manson, P. Delaney, F. Jelezko, J. Wrachtrup, and L. C. L. Hollenberg, *The nitrogen-vacancy colour centre in diamond,* Physics Reports **528**, 1 (2013).

[29] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, *Key rate of quantum key distribution with hashed two-way classical communication,* Physical Review A **76**, 032312 (2007).

[30] D. Riedel, I. Söllner, B. J. Shields, S. Starosielec, P. Appel, E. Neu, P. Maletinsky, and R. J. Warburton, *Deterministic enhancement of coherent photon generation from a nitrogen-vacancy center in ultrapure diamond,* Physical Review X **7**, 031040 (2017).

[31] M. Fox, *Quantum optics: an introduction*, Vol. 15 (Oxford University Press, 2006).

[32] N. Kalb, P. Humphreys, J. Slim, and R. Hanson, *Dephasing mechanisms of diamond-based nuclear-spin memories for quantum networks,* Physical Review A **97**, 062330 (2018).

[33] S. Zaske, A. Lenhard, C. A. Keßler, J. Kettler, C. Hepp, C. Arend, R. Albrecht, W.-M. Schulz, M. Jetter, P. Michler, *et al.*, *Visible-to-telecom quantum frequency conversion of light from a single quantum emitter,* Physical Review Letters **109**, 147404 (2012).

[34] C. Jones, D. Kim, M. T. Rakher, P. G. Kwiat, and T. D. Ladd, *Design and analysis of communication protocols for quantum repeater networks,* New Journal of Physics **18**, 083015 (2016).

[35] E. T. Campbell and S. C. Benjamin, *Measurement-based entanglement under conditions of extreme photon loss,* Physical Review Letters **101**, 130502 (2008).

[36] N. H. Nickerson, J. F. Fitzsimons, and S. C. Benjamin, *Freely scalable quantum technologies using cells of 5-to-50 qubits with very lossy and noisy photonic links,* Physical Review X **4**, 041041 (2014).

[37] I. L. Chuang, D. W. Leung, and Y. Yamamoto, *Bosonic quantum codes for amplitude damping,* Physical Review A **56**, 1114 (1997).

[38] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, *Squashing model for detectors and applications to quantum-key-distribution protocols,* Physical Review A **89**, 012325 (2014).

[39] S. R. Jammalamadaka and A. Sengupta, *Topics in circular statistics*, Vol. 5 (World Scientific, 2001).

[40] G. Murta, F. Rozpędek, J. Ribeiro, D. Elkouss, and S. Wehner, In preparation (2019).

[41] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution,* Reviews of Modern Physics **81**, 1301 (2009).

[42] R. Renner, *ETH Zurich PhD Thesis*, arXiv preprint quant-ph/0512258 (2005).

8

QUANTUM PREPARATION UNCERTAINTY AND LACK OF INFORMATION

Filip Rozpędek, Jędrzej Kaniewski, Patrick Coles and Stephanie Wehner

The quantum uncertainty principle famously predicts that there exist measurements that are inherently incompatible, in the sense that their outcomes cannot be predicted simultaneously. In contrast, no such uncertainty exists in the classical domain, where all uncertainty results from ignorance about the exact state of the physical system. Here, we critically examine the concept of preparation uncertainty and ask whether similarly in the quantum regime, some of the uncertainty that we observe can actually also be understood as a lack of information (LOI), albeit a lack of quantum *information. We answer this question affirmatively by showing that for the well known measurements employed in BB84 quantum key distribution [1], the amount of uncertainty can indeed be related to the amount of available information about additional registers determining the choice of the measurement. We proceed to show that also for other measurements the amount of uncertainty is in part connected to a LOI. Finally, we discuss the conceptual implications of our observation to the security of cryptographic protocols that make use of BB84 states.*

The results of this chapter have been published in New J. Phys. 19, 023038 (2017).

8.1. INTRODUCTION

The uncertainty principle forms one of the cornerstones of quantum theory. As first observed by Heisenberg [2] and then rigorously proven by Kennard [3], it is impossible to perfectly predict the measurement outcomes of both position and momentum observables. This notion was generalised by Robertson to an arbitrary pair of observables [4] showing that uncertainty is an inherent feature of any non-commuting measurements in quantum mechanics. The described uncertainty is often referred to as preparation uncertainty, because it states that it is impossible to prepare a quantum state for which one could perfectly predict the measurement outcome of both observables.

A modern way of capturing the notion of preparation uncertainty is by means of a *guessing game* [5]. Such a game makes the concept of preparation uncertainty operational and is of great use in proving the security of quantum cryptographic protocols [6]. Fig. 8.1 summarises the game, which in its simplest form works as follows. Bob prepares system B in an arbitrary state ρ_B of his choosing and then passes it to Alice. Alice performs one of two incompatible measurements labeled by $r = 0$ and $r = 1$ according to a random coin flip contained in the register R and obtains measurement outcome X. She then informs Bob which measurement she performed by sending him the register R. Bob wins the game if he correctly guesses Alice's measurement outcome X.

To see why this captures the essence of the uncertainty principle, note that if the measurements are incompatible, then there exists no state ρ_B that Bob can prepare that would allow him to guess the outcomes for both choices of measurements with certainty. Uncertainty can thus be quantified by a bound on the average probability that Bob correctly guesses X. That is, a relation of the form

$$\begin{aligned} P_{\text{guess}}(X|\text{Bob}) = p(r=0)P_{\text{guess}}(X|\text{Bob}, r=0) \\ + p(r=1)P_{\text{guess}}(X|\text{Bob}, r=1) \leq 2^{-\zeta}, \end{aligned} \tag{8.1}$$

for all ρ_B. Equivalently, we can relate the above defined guessing probability to the min-entropy $H_{\min}(X|\text{Bob}) = -\log P_{\text{guess}}(X|\text{Bob})$ (in this article all logarithms are base 2), so that we obtain an inequality:

$$H_{\min}(X|\text{Bob}) \geq \zeta\,. \tag{8.2}$$

This expression forms an uncertainty relation as long as the RHS is non-trivial (i.e. $\zeta > 0$). Analogous relations exist for other entropies [6], but here we focus on the min-entropy since it is the relevant measure for quantum cryptography and randomness generation, and it quantifies the winning probability for the aforementioned guessing game.

In this work, we seek a deeper understanding of the uncertainty principle by considering a more general scenario than the typical guessing game and observing the conditions under which Bob's uncertainty vanishes. In particular, the generalisation we consider is to allow Bob to have additional information - possibly *quantum* information - about Alice's measurement choice. This generalisation is closely related to recent proposals for quantum control experiments [7, 8]. To elaborate, we note that Alice's random measurement choice in the guessing game can be implemented by preparing a qubit R in the maximally mixed state $\rho_R = \mathbb{I}/2$ and then performing a unitary operation on B conditioned on the state of R (see Fig. 8.2 below). In the generalised game that we

consider, we allow ρ_R to be a more general state, possibly with some coherence. As we discuss below, allowing for coherence in ρ_R corresponds to giving Bob more information.

Our motivation for considering this scenario is to distinguish between uncertainty that is due to Bob's lack of information (LOI) versus uncertainty that is intrinsic or unavoidable. To help clarify these notions, we remark that a classical theory admits no intrinsic uncertainty. Classical here refers to commuting measurements that are jointly diagonal in one predefined basis. If Alice employed such measurements in the aforementioned guessing game, then the only way for her to prevent Bob from winning the game would be for her to add noise to her measurement outcomes, i.e., implement noisy measurements. Yet, we would classify Bob's uncertainty in this case as LOI uncertainty, as he simply lacks the information about the noise Alice adds. Hence, the arising uncertainty is clearly not an intrinsic feature of the measurements.

Notice that preparing the register R in the maximally mixed state $\rho_R = \mathbb{I}/2$ injects classical randomness into the protocol. It is unclear whether or not this randomness is ultimately responsible for the uncertainty principle, and this is a question we aim to answer. We emphasise that the scenario we consider differs from other variants of the uncertainty principle which derive bounds involving the purity or entropy of ρ_B [5, 9–22].

Interestingly we find that in the special case where Bob's system is a qubit ($d = 2$), there is no intrinsic uncertainty but all the uncertainty is due to LOI. That is, if Bob has complete knowledge about the preparation of R (i.e., R is in a pure state), then his uncertainty vanishes. In contrast, for all dimensions $d > 2$, we find that there is always some intrinsic uncertainty. That is, even with the full knowledge about the preparation of R, Bob cannot win the guessing game with unit probability. Before we discuss these results in detail, let us outline the physical setup.

8.2. PHYSICAL SETUP

8.2.1. DEGREES OF IGNORANCE

In this section we describe the generalised guessing game shown in Fig. 8.1. Here, Alice prepares a register system R in some state ρ_R. Meanwhile Bob prepares system B in state ρ_B and sends it to Alice. Alice measures B in a basis determined by the state of R. Then she passes R to Bob, and he tries to guess her measurement outcome, possibly using the information stored in R. We are interested in understanding how much of Bob's uncertainty (i.e., his inability to win this game) is due to LOI and how much corresponds to intrinsic (or unavoidable) uncertainty.

To better understand this, let us examine what Bob does and does not have access to in Fig. 8.1. Since ρ_R is generally a mixed state, it can be purified by considering an additional system, P. Even though Bob is given access to R, we emphasise that he does not have access to P in our guessing game. Hence, we can think of P as representing Bob's LOI.

For example, consider the case when $\rho_R = \mathbb{I}/2$ is maximally mixed, which corresponds to the case where the measurement choice is a classical coin flip (i.e., the typical uncertainty game considered in the literature [5]). The purification is a maximally

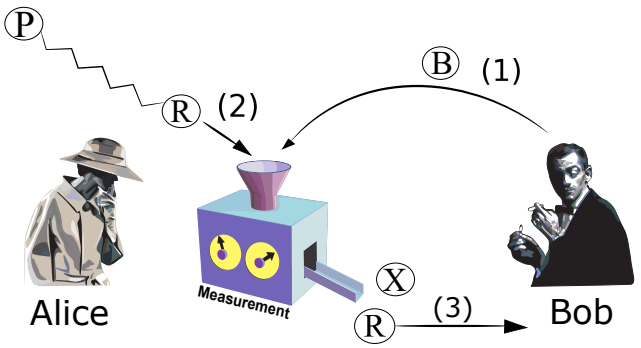

Figure 8.1: Uncertainty guessing game. The game runs as follows: (1) First, Bob prepares system B in a state ρ_B and sends it to Alice. We show in Appendix 8.6.1 that Bob's best strategy is to prepare a pure state $\rho_B = |\phi\rangle\langle\phi|_B$. (2) Second, Alice measures B in a basis determined by the state of register R. (3) Finally, Alice obtains the classical outcome X and sends R to Bob. Bob can then measure R in order to help him guess X. Note that R may be initially prepared in a mixed state ρ_R, and Bob does not have access to the purifying system of ρ_R, denoted as P in the figure. Hence, P embodies Bob's lack of information in this game.

entangled state such as

$$|\xi_{RP}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_R|0\rangle_P + |1\rangle_R|1\rangle_P\right). \tag{8.3}$$

At the other extreme is the case where ρ_R is pure, i.e.,

$$|\xi_{RP}\rangle = |\xi_R\rangle \otimes |\xi_P\rangle \tag{8.4}$$

is a product state. We will take $|\xi_R\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, i.e., we choose an equal superposition in correspondence with the idea that both measurements were previously chosen with equal probability. Intuitively, when the initial state is maximally entangled, then Bob will later suffer from a maximum LOI about P. However, in the case where the two systems are uncorrelated, Bob does not need P at all. In other words, there is no LOI on his part, because R is pure.

There are many ways to interpolate between these two extremes in terms of a measure of correlation between R and P. Here, we choose one that is intuitive when we think about "how much" of P Bob is actually lacking. Concretely, we imagine that apart from the classical coin C (which is a part of R), R and P are actually comprised of many environmental subsystems $E_1, \ldots, E_n$, and we quantify Bob's LOI by the number of the environment systems that are part of P instead of part of R. Specifically, we take

$$|\xi_{RP}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_C \otimes \bigotimes_{i=1}^{n}|\alpha\rangle_{E_i} + |1\rangle_C \otimes \bigotimes_{i=1}^{n}|\beta\rangle_{E_i}\right), \tag{8.5}$$

where $RP = CE_1 \ldots E_n$. The environments E_j's are two-dimensional registers and $\left|\langle\alpha|\beta\rangle\right| = 1-\epsilon$, with $\epsilon > 0$ and $\epsilon \ll 1$ so that each individual E_j holds very little information

about the state of the coin C. However, we see that $\langle\alpha|\beta\rangle^n \to 0$ as $n \to \infty$. We thus see that for $n \to \infty$ and $R = C$, $P = E_1 \dots E_n$, we approach the extreme case of R being essentially classical, and $|\xi_{RP}\rangle$ being maximally entangled. This idea of approximating the notion of a classical register by "copying" information into a large number of environmental systems E_j is due to Zurek [23].

We can now interpolate between the two extremes by letting $R = CE_1 \dots E_j$ and $P = E_{j+1} \dots E_n$. We have that

$$\rho_R = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + \gamma^*|0\rangle\langle 1| + \gamma|1\rangle\langle 0|)\,, \tag{8.6}$$

where

$$|0\rangle_R := |0\rangle_C \otimes \bigotimes_{i=1}^{j} |\alpha\rangle_{E_i}\,, \tag{8.7}$$

$$|1\rangle_R := |1\rangle_C \otimes \bigotimes_{i=1}^{j} |\beta\rangle_{E_i}\,, \tag{8.8}$$

$$\gamma = \langle\alpha|\beta\rangle^{n-j}\,. \tag{8.9}$$

We see that $|\gamma|$ increases monotonically with j, the number of environmental subsystems contained in R, and hence the number of subsystems to which Bob is given access later on. The extreme cases $\gamma = 0$ and $\gamma = 1$ correspond respectively to $j = 0$ and $j = n$ (again note that the number of environment subsystems is very large so that we always consider the limit $n \to \infty$). In Appendix 8.6.1 we show that for the uncertainty game it is only the modulus of γ that matters. Therefore, we will only consider the case of real and positive γ, i.e. $\gamma \in [0,1]$.

8.2.2. UNCERTAINTY GAME

Let us now revisit our uncertainty guessing game (see Fig. 8.1 and Fig. 8.2) with a more detailed description. First, Bob prepares system B in a state ρ_B and sends it to Alice. Second, Alice measures B and obtains the classical outcome X, with the measurement basis determined by the state of register R given by:

$$\rho_R = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + \gamma|0\rangle\langle 1| + \gamma|1\rangle\langle 0|)\,. \tag{8.10}$$

Specifically, as depicted in Fig. 8.2, states $|0\rangle$ and $|1\rangle$ on R are, respectively, associated with measuring in the standard basis and Fourier basis on B (we have chosen maximally incompatible bases to maximise the "inherent" uncertainty). Next, Alice sends Bob the register R. Finally Bob measures R to help him produce a guess for X. This defines a two-parameter family of uncertainty games which depend on: $d \in \{2,3,\dots\}$, the number of possible outcomes (which fixes the dimension of the quantum state ρ_B supplied by Bob and the dimension of the Fourier transform in Fig. 8.2) and $\gamma \in [0,1]$, describing the amount of information about R that is held in P, or equivalently the amount of coherence in R.

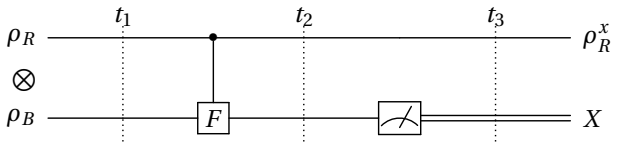

Figure 8.2: Quantum circuit of the uncertainty game. At time t_1, Alice's register R and Bob's system B are uncorrelated. We will assume that Alice measures in the standard basis and one additional basis depending on the state of register R. To allow for maximum intrinsic uncertainty, we take the other basis to be maximally incompatible. Here, we choose it to be the Fourier basis. Hence the two measurements correspond to measuring in two mutually unbiased bases. If B is a qubit, then this means that Alice measures in the standard and Hadamard basis, which are the two bases used in BB84 quantum key distribution. This basis choice is performed by Alice applying a controlled unitary between the two registers, leading to a correlated state at time t_2. Alice then measures B to obtain the measurement outcome X. If the register R is classical, then the two operations together correspond to performing a random measurement. If the register R contains some non-zero coherence, then those operations describe a procedure which could be understood as a "measurement in a superposition of two bases". After time t_3, Alice sends R to Bob. At this stage, $\rho_{RX} = \sum_x p_x \rho_R^x \otimes |x\rangle\langle x|_X$ is a qc-state. Bob can then make a measurement in order to distinguish the states ρ_R^x, i.e., to help him guess X. Note that Bob knows which states ρ_R^x he wants to distinguish since he knows the form of the initial state $|\xi_{RP}\rangle$ and the measurements Alice can perform.

8.3. METHODS

Here we provide a high level overview of the methods used to obtain the results presented in the next section. For complete analysis we refer the reader to the appendices.

After Alice has performed her measurement, at time t_3 in Fig. 8.2 the resulting qc-state between the register R and the outcome register X is:

$$\rho_{RX}(\gamma, d, \rho_B) = \sum_x \tilde{\rho}_R^x(\gamma, d, \rho_B) \otimes |x\rangle\langle x|_X \,, \tag{8.11}$$

where $\tilde{\rho}_R^x(\gamma, d, \rho_B) = p_x(d, \rho_B)\rho_R^x(\gamma, d, \rho_B)$ is the subnormalised post-measurement state of the register R corresponding to the outcome $X = x$. In terms of Bob's input state ρ_B, this state has the form:

$$\tilde{\rho}_R^x(\gamma, d, \rho_B) = \frac{1}{2}\begin{pmatrix} \langle x|\rho_B|x\rangle & \gamma\langle x|\rho_B F^\dagger|x\rangle \\ \gamma\langle x|F\rho_B|x\rangle & \langle x|F\rho_B F^\dagger|x\rangle \end{pmatrix}, \tag{8.12}$$

as derived in Appendix 8.6.1. Since Bob later gains access to register R, we see that in order to guess the resulting outcome $X = x$, Bob should try to determine which quantum state $\rho_R^x(\gamma, d, \rho_B)$ he has received. Hence, his guessing problem becomes equivalent to the problem of distinguishing quantum states $\{\rho_R^x(\gamma, d, \rho_B)\}$ occurring with probabilities $\{p_x(d, \rho_B)\}$.

The probability of Bob correctly discriminating those states with the optimal strategy, i.e., with the optimal measurement on R (described by POVM elements $\{M_x\}$), is given by [24]:

$$p_{\text{guess}}(\gamma, d, \rho_B) = \max_{\{M_x\}} \sum_{x=0}^{d-1} p_x(d, \rho_B) \operatorname{Tr}[M_x \rho_R^x(\gamma, d, \rho_B)] \,. \tag{8.13}$$

In Appendix 8.6.1 we show that to achieve $p^{\max}_{\text{guess}}(\gamma, d)$, the guessing probability optimised over input states ρ_B, it is sufficient to consider only pure input states $\rho_B = |\phi\rangle\langle\phi|_B$. Hence, the maximum value of $p_{\text{guess}}(\gamma, d, \rho_B)$ for a given γ and d is the result of optimising the guessing probability over all input states $|\phi\rangle_B$ of Bob (for convenience we will often omit the subscript "B" from $|\phi\rangle_B$). That is,

$$p^{\max}_{\text{guess}}(\gamma, d) = \max_{|\phi\rangle} p_{\text{guess}}(\gamma, d, |\phi\rangle)\,. \tag{8.14}$$

Solving this optimisation problem is not an easy task. Note that the function which we want to optimise over all the POVM elements $\{M_x\}$ in Eq. (8.13) is linear in those operators. Hence, for a specific input state $|\phi\rangle_B$ the optimisation can be performed using techniques of semi-definite programming. However, the above optimisation problem in Eq. (8.14) involves optimisation both over POVM elements and input states $|\phi\rangle_B$. Clearly, $\tilde{\rho}^x_R(\gamma, d, |\phi\rangle_B)$ is quadratic in $|\phi\rangle_B$. Note that this problem can be made linear in the input state by again considering optimisation over all mixed states ρ_B, i.e. our problem is then linear in ρ_B. However, the full problem of optimising over both $\{M_x\}$ and ρ_B:

$$p^{\max}_{\text{guess}}(\gamma, d) = \max_{\rho_B} \max_{\{M_x\}} \sum_{x=0}^{d-1} p_x(d, \rho_B)\,\text{Tr}[M_x \rho^x_R(\gamma, d, \rho_B)] \tag{8.15}$$

turns out not to be jointly concave in both of those variables and so cannot be solved using techniques of convex optimisation.

8.3.1. TWO-DIMENSIONAL GAME

Nevertheless, we can solve this problem analytically for $d = 2$. For this case, we derived our result (stated below in Theorem 8.4.1) by noting that the problem of optimising over the POVM elements in Eq. (8.13) (for fixed states $\{\rho^x_R\}$ occuring with fixed probabilities $\{p_x\}$) has been solved analytically by Helstrom [25]:

$$p_{\text{guess}}(\gamma, d = 2, \rho_B) = \frac{1}{2}\left(1 + \left\|\tilde{\rho}^0_R(\gamma, \rho_B) - \tilde{\rho}^1_R(\gamma, \rho_B)\right\|_1\right), \tag{8.16}$$

where $\|\cdot\|_1$ denotes the trace norm and we have omitted the $d = 2$ argument in $\tilde{\rho}^0_R$ and $\tilde{\rho}^1_R$. In this way we obtain an expression for $p_{\text{guess}}(\gamma, d = 2, \rho_B)$ which we then analytically optimise over the input states ρ_B for every value of $\gamma \in [0, 1]$ to obtain $p^{\max}_{\text{guess}}(\gamma, d = 2)$ (see Appendix 8.6.2). For completeness, we still optimise over all qubit states ρ_B, not only the pure ones. This allows us to find all the qubit input states that achieve $p^{\max}_{\text{guess}}(\gamma, d = 2)$.

8.3.2. HIGHER-DIMENSIONAL GAMES

For $d > 2$ we cannot calculate $p^{\max}_{\text{guess}}(\gamma, d > 2)$ analytically, since there exists no known analytical expression for the probability of correctly distinguishing more than two quantum states. However, we can find $p_{\text{guess}}(\gamma, d, |\phi\rangle)$ for an arbitrary state $|\phi\rangle$ using techniques from semi-definite programming. We obtain numerical lower bounds for $p^{\max}_{\text{guess}}(\gamma, d)$, shown in Fig. 8.3, by solving a semi-definite programme for $p_{\text{guess}}(\gamma, d, |\phi\rangle)$ and numerically searching for local maxima of $p_{\text{guess}}(\gamma, d, |\phi\rangle)$ with respect to the input state $|\phi\rangle$ using the Nelder-Mead algorithm. We repeat the search multiple times with a randomly generated initial state in each run, that is drawn uniformly from unit vectors on $\mathbb{C}^d$.

8.4. RESULTS

In Section 8.1 we discussed that classical uncertainty arises solely from LOI. Here we show that even in the quantum case, uncertainty can in part be understood as a LOI that Bob has - namely a lack of quantum information about the register P. For the case of $d = 2$ and BB84 measurements as they are used in quantum key distribution (QKD), this effect is indeed dramatic. We find (see Theorem 8.4.1 below) that there is no more uncertainty at all in the case where R is pure and P is uncorrelated, meaning that Bob does not suffer from any LOI.

First, we consider the typical uncertainty game where R is a classical coin, i.e., R and P are maximally entangled ($\gamma = 0$). In this case the maximum value of the guessing probability (for completeness derived in Appendix 8.6.3) is given by:

$$p_{\text{guess}}^{\max}(\gamma = 0, d) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right). \tag{8.17}$$

The states ρ_B that achieve the guessing probability of Eq. (8.17) are the pure states

$$|\phi_{jl}\rangle := c(|j\rangle + \omega^{jl} F^\dagger |l\rangle), \tag{8.18}$$

where $c = \sqrt{\sqrt{d}/(2\sqrt{d}+2)}$ is the normalisation constant, F denotes a quantum Fourier transform defined in Appendix 8.6.1, ω is the d-th root of unity and j and l are integer indices that lie in the range $\{0, 1, \ldots, d-1\}$ so that the pure states $|j\rangle$ and $|l\rangle$ denote the corresponding eigenstates of the standard basis. The states defined in Eq. (8.18) are the states where the dominant classical outcome for the measurement is j in the standard basis and l in the Fourier basis.

Now we consider the more general case where R may have some coherence. For $d = 2$ we have found the analytical solution for all $\gamma \in [0, 1]$. In this case the guessing probability is equal to the probability of successfully distinguishing the two possible post-measurement states of the basis register, namely ρ_R^0 and ρ_R^1 corresponding to outcomes 0 and 1 respectively (see Fig. 8.2).

Theorem 8.4.1. *The maximum guessing probability for a two-dimensional game ($d = 2$), optimised over all input states ρ_B is given by:*

$$p_{\text{guess}}^{\max}(\gamma, d = 2) = \frac{1}{2}\left(1 + \frac{\sqrt{2 + 2\gamma^2}}{2}\right). \tag{8.19}$$

In particular, for $\gamma = 1$ one achieves perfect guessing, that is $p_{\text{guess}}^{\max}(\gamma = 1, d = 2) = 1$.

It is also possible to express this guessing probability in terms of the purity of the basis register:

$$p_{\text{guess}}^{\max}(\gamma, d = 2) = \frac{1}{2}\left(1 + \sqrt{\text{Tr}[\rho_R^2]}\right). \tag{8.20}$$

For all $\gamma \in [0, 1]$, this guessing probability can be achieved by one of two orthogonal input states of Bob, $|\phi_{01}\rangle = c(|0\rangle + |-\rangle)$ and $|\phi_{10}\rangle = c(|1\rangle + |+\rangle)$, which are mapped by the Hadamard transformation onto each other. (For $\gamma = 0$ this guessing probability can of course also be achieved by $|\phi_{00}\rangle$ and $|\phi_{11}\rangle$, as then Eq. (8.19) reduces to Eq. (8.17).

For $\gamma = 1$ the optimal input states form a continuous one-parameter family, see Appendix 8.6.2.)

From Eq. (8.19) we see that Bob can achieve perfect guessing probability for the case when R is uncorrelated from P (and so P holds no information about R and there is no LOI about the measurement process on Bob's side). This is connected to the fact, that for $\gamma = 1$ and a suitable choice of input state ρ_B, the joint state ρ_{RB} becomes maximally entangled at time t_2 just before Alice's measurement in Fig. 8.2 (see Appendix 8.6.4 below for discussion of this connection). The above results for $d = 2$ are derived in Appendix 8.6.2.

Now it is interesting to ask what happens to the measurement uncertainty in the game with more than two measurement outcomes in higher dimension. It is intuitive that the dramatic effect we see for $d = 2$ should be less prominent here. After all, Bob is trying to guess measurement outcomes that can take on d values, while R and P each remain two-dimensional and can hence only contain limited information about the outcomes. We first make this intuition precise in the following theorem.

Theorem 8.4.2. *For d-dimensional games with any $d > 2$ it is not possible to achieve perfect guessing, i.e.,*

$$p^{\max}_{\text{guess}}(\gamma, d > 2) < 1\,, \qquad \forall\ \gamma \in [0,1]\,. \tag{8.21}$$

Crucially, however, coherence in register R *always* facilitates guessing.

Theorem 8.4.3. *For d-dimensional games with d being arbitrary, the maximum guessing probability when R has any non-zero amount of coherence is always strictly greater than the case of maximally mixed R. That is, for all $\gamma' > 0$*

$$p^{\max}_{\text{guess}}(\gamma = \gamma', d) > p^{\max}_{\text{guess}}(\gamma = 0, d)\,, \qquad \forall\ d \geq 2\,. \tag{8.22}$$

Moreover, we show that for a subclass of the input states that are optimal for $\gamma = 0$, the guessing probability monotonically increases with γ. Specific values of $p^{\max}_{\text{guess}}(\gamma, d)$ are lower bounded numerically. Those results are depicted in Fig. 8.3.

8.5. DISCUSSION

We have shown that quantum preparation uncertainty is not always inherent to the measurement process but on the contrary it depends on the amount of information that one has about this process. In particular, for $d = 2$, if Bob has all the information about the measurement process, then he can perfectly predict the measurement outcome. In the cryptographic protocols that use BB84 states, ρ_R is a maximally mixed state. Hence, from the perspective of cryptographic security, this shows that it is important for the purification of ρ_R to remain inaccessible to the adversary. In particular, the more of the purification P becomes incorporated into R, the larger the guessing probability becomes and so the more the security of our cryptographic protocols becomes compromised. Passive encoding schemes [26], which generate the QKD signal states by performing a measurement on a quantum register (analogous to our R), would especially need to consider this issue.

On the other hand, we found that there is always some unavoidable uncertainty for guessing games in higher dimensions, $d > 2$. This result is somewhat intuitive when one

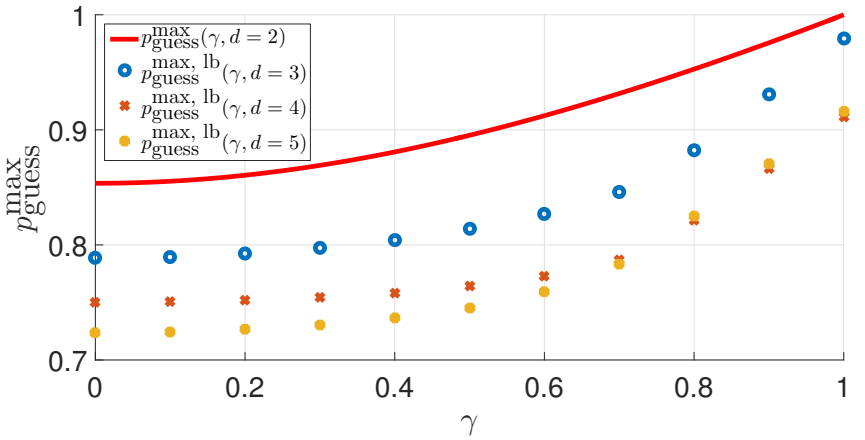

Figure 8.3: The optimal guessing probabilities $p_{\text{guess}}^{\max}(\gamma, d)$ as a function of γ for different d. The solid line corresponds to the analytical solution $p_{\text{guess}}^{\max}(\gamma, d=2)$ for a two-dimensional game. The remaining data corresponds to the numerical lower bounds $p_{\text{guess}}^{\max,\,\text{lb}}(\gamma, d)$ for $d = 3, 4, 5$. For $\gamma = 0$ the numerical values coincide with the analytical solution $p_{\text{guess}}^{\max}(\gamma = 0, d) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right)$. The crossing of the dotted lines corresponding to $d = 4$ and $d = 5$ is discussed in Section 8.5.

considers that our guessing game allows for two measurements, and hence system R is only two-dimensional. The intuition behind this unavoidable uncertainty is that the state ρ_R, in which the information about the measurement outcome becomes encoded, is always a qubit, while the number of outcomes is d. Hence, even if Bob inputs a state that results in entanglement between the two systems, this entanglement lives in a two-dimensional subspace of the d-dimensional space $\mathcal{H}_B$. Therefore, the joint state cannot be maximally entangled and since the Fourier transformation applied to elements of the standard basis generates a basis that is unbiased to it, the correlations before the measurement of Alice do not align with the standard basis in which the measurement is performed. This fact can also be seen by noting that perfect guessing could only occur if only two of the resulting outcomes had non-zero probability and if those outcomes produced orthogonal post-measurement states of the register R. It turns out that all those conditions cannot be met simultaneously.

The crossing of the dotted lines corresponding to $d = 4$ and $d = 5$ in Fig. 8.3 is an interesting phenomenon. We have investigated it extensively using multiple methods and numerical solvers on which we now elaborate. As mentioned in Section 8.3 the problem of optimisation over both input states and measurements is in general very hard because the optimisation problem that we face is not convex. That is we can have no guarantee that the solution that we find is the global maximum. Therefore the numerical results are just the lower bounds on the $p_{\text{guess}}^{\max}$, as they represent achievable values of $p_{\text{guess}}^{\max}$ that have been found. Nevertheless we have used multiple methods to look for these optimal bounds. Apart from the method described in Section 8.3.2 (where part of the data was checked by rerunning the programme with multiple numerical solvers), we have tried imposing a net over the statespace and solving the semi-definite programme

	Schmidt coefficients	
$d=3$	0.8122	0.5834
$d=4$	0.8314	0.5556
$d=5$	0.7415	0.6709

Table 8.1: Schmidt coefficients of the joint state on RB at time t_2 for the input states that achieve $p_{\text{guess}}^{\text{max, lb}}(\gamma=1,d)$.

over the measurements for each of those states. Then the procedure was repeated with a denser net in the region where the highest guessing probability has been found. This step of "zooming-in" has then been repeated multiple times. Finally we have also used the "Penlab" solver, which can also provide achievability bounds for non-linear problems. Application of those other methods however resulted in much worse bounds and so they shed no light on the nature of the crossing in Fig. 8.3.

Nevertheless, despite the fact that we only find achievable bounds, we believe that the crossing seen in Fig. 8.3 could in principle arise even for the exact solution. We note that while asymptotically we expect $p_{\text{guess}}^{\text{max}}(\gamma,d)$ to tend to 0.5 as d tends to infinity, it is possible for $p_{\text{guess}}^{\text{max}}(\gamma,d)$ to be larger for $d=5$ than for $d=4$ above some threshold $\gamma=\gamma_0$. As we mentioned earlier, the optimal guessing probability depends on the optimal correlations between two-dimensional register R and d-dimensional register B. The resulting state is asymmetric and so it is possible that certain favourable correlations are possible for $d=5$, while not possible for $d=4$. The complexity of the problem can be seen by looking at the Schmidt coefficients of the joint state of registers R and B at time t_2 in Fig. 8.2. For $d=2$ and $\gamma=1$ the optimal input states are precisely the ones that lead to a maximally entangled state between those two registers at time t_2. One might intuitively guess that also for $d>2$ forming maximally entangled states within the two-dimensional subspace of B will lead to the optimal guessing probability for $\gamma=1$. This turns out not be sufficient: we checked specific states that lead to maximal entanglement in dimensions $d=3,4,5$ and their performance is suboptimal. At the same time, all the optimal input states found numerically that achieve $p_{\text{guess}}^{\text{max, lb}}(\gamma=1,d)$ for $d=3,4,5$ lead to unbalanced Schmidt coefficients. While we have found multiple states that achieve $p_{\text{guess}}^{\text{max, lb}}(\gamma=1,d)$ for each of $d=3,4,5$, all of them lead to exactly the same Schmidt coefficients of the joint state, which we list in Table 8.1. This fact, together with the irregularity of our numerical curves, reveals the complexity of the geometry of this problem.

In future work, it would be very natural to consider games with more than two measurements. It would be interesting to investigate whether a higher dimensional register R could then encode more information about the measurement outcome. Specifically, for the scenario with d mutually unbiased measurements (if they exist) and d possible outcomes, it is reasonable to ask whether one can again achieve perfect guessing (e.g., due to the possibility of creating maximal entanglement between R and B).

Another natural extension of our game would be to provide Bob with access to a quantum memory [5]. In such a scenario an interesting task would be to investigate

the effect of the trade-off between Bob's amount of accessible information about the measurement process and the quality of entanglement between B and Bob's quantum memory.

Finally, we would like to emphasise that while the described guessing game seems to be only an abstract tool that we use to investigate the connection between quantum preparation uncertainty and lack of information, the game described in Fig. 8.1 could in fact be implemented experimentally, e.g., using a Mach-Zehnder interferometer for single photons. For simplicity consider the case $d = 2$, although the following discussion can be extended to $d > 2$ by considering an interferometer with more than two paths. Suppose that system R is the photon's polarisation, while B is the photon's spatial degree of freedom (the path that it takes in the interferometer). Allowing Bob to have access to the first variable beam splitter of the interferometer allows him to prepare an arbitrary pure qubit state ρ_B inside the interferometer (Bob is allowed to freely choose the reflectance and the relative phase of the beam splitter). The controlled Fourier transform in Fig. 8.2 is implemented by making the second beam splitter of the interferometer a so-called quantum balanced beam splitter [7]. That is, the photon's polarisation controls whether or not the balanced (50/50) beam splitter appears in the photon's path. Hence, this beam splitter can be effectively in a superposition of being absent and present, if one chooses the polarisation to be in a superposition. This would be a so-called quantum control experiment [8]. Let us note that such a quantum beam splitter has been implemented experimentally [27–29]. The winning condition of the game for Bob is correctly guessing which one of the two photon detectors clicked, after being able to measure the polarisation state of the photon behind the quantum beam splitter.

8.6. APPENDIX

8.6.1. THE UNCERTAINTY GAME: DEFINITIONS AND BASIC DERIVATIONS

TIME EVOLUTION OF THE QUANTUM CIRCUIT

Following the quantum circuit of the uncertainty game in Fig. 8.2 (in the main article), we derive the explicit form of the density matrices that Bob needs to distinguish in order to win the game. There are different classes of games depending on the parameter d corresponding to the dimension of the Fourier transform or equivalently, the number of possible outcomes of Alice. Bob prepares a state ρ_B of dimension d and sends it to Alice in register B. She holds another register R in a state $\rho_R(\gamma) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1| + \gamma^*|0\rangle\langle 1| + \gamma|1\rangle\langle 0|)$, where $\gamma \in \mathbb{C}$ and $|\gamma| \leq 1$. This γ determines how coherent the register is. Specifically, in the later part of this appendix we show that we can restrict γ to be real and $\gamma \in [0,1]$. Hence at the beginning (time t_1) the total state of the entire system is:

$$\rho_{RB}(\gamma, \rho_B) = \rho_R(\gamma) \otimes \rho_B = \frac{1}{2}(|0\rangle\langle 0|_R + |1\rangle\langle 1|_R + \gamma^*|0\rangle\langle 1|_R + \gamma|1\rangle\langle 0|_R) \otimes \rho_B \,. \tag{8.23}$$

The state $\rho_R(\gamma)$ determines the measurement basis in the following way: $|0\rangle$ corresponds to the measurement in the standard basis and $|1\rangle$ to the measurement in the Fourier basis (which is represented by applying the Fourier transformation to Bob's state and then measuring in the standard basis). Hence, the choice of the measurement basis can

be represented by the controlled Fourier transform:

$$U = |0\rangle\langle 0|_R \otimes \mathbb{I}_B + |1\rangle\langle 1|_R \otimes F_B \,. \tag{8.24}$$

We adopt the following convention for the Fourier transform: $F|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{jk} |k\rangle$ with $\omega = \exp\left(\frac{2\pi i}{d}\right)$ being the d-th root of unity. After Alice applies the above unitary, the state at time t_2 is:

$$\rho'_{RB}(\gamma, d, \rho_B) = U\rho_{RB}(\gamma, \rho_B)U^\dagger = U(\rho_R(\gamma) \otimes \rho_B)U^\dagger \tag{8.25}$$

$$= \frac{1}{2}(|0\rangle\langle 0|_R \otimes \rho_B + \gamma^* |0\rangle\langle 1|_R \otimes \rho_B F_B^\dagger + \gamma |1\rangle\langle 0|_R F_B \rho_B + |1\rangle\langle 1|_R \otimes F_B \rho_B F_B^\dagger) \,. \tag{8.26}$$

Then Alice performs her measurement and the outcome is stored in the output register X. The total state after the measurement at time t_3 is:

$$\rho_{RX}(\gamma, d, \rho_B) = \sum_x \mathrm{Tr}_B[(\mathbb{I}_R \otimes |x\rangle\langle x|_B)\rho'_{RB}(\gamma, d, \rho_B)] \otimes |x\rangle\langle x|_X \,. \tag{8.27}$$

Hence, we see that the subnormalised post-measurement states of the basis register corresponding to Alice's measurement outcome x are:

$$\begin{aligned} \tilde{\rho}_R^x(\gamma, d, \rho_B) = p_x(d, \rho_B)\rho_R^x(\gamma, d, \rho_B) &= \mathrm{Tr}_B[(\mathbb{I}_R \otimes |x\rangle\langle x|_B)\,\rho'_{RB}] \\ &= \frac{1}{2}\begin{pmatrix} \langle x|\rho_B|x\rangle & \gamma^*\langle x|\rho_B F^\dagger|x\rangle \\ \gamma\langle x|F\rho_B|x\rangle & \langle x|F\rho_B F^\dagger|x\rangle \mathbb{I} \end{pmatrix}, \end{aligned} \tag{8.28}$$

where $p_x(d, \rho_B) = \mathrm{Tr}[\tilde{\rho}_R^x(\gamma, d, \rho_B)]$ is the probability that Alice observes outcome $x \in \{0, 1, ..., d-1\}$. Note that p_x does not depend on γ, which only appears in the off-diagonal elements of $\tilde{\rho}_R^x$. These subnormalised $\tilde{\rho}_R^x$'s are the states to which Bob has access and so his ability to predict Alice's measurement outcome $|x\rangle$ is determined by how well he can distinguish the quantum states $\{\rho_R^x\}$ occurring with probabilities $\{p_x\}$.

8

SIMPLIFYING LEMMAS

In the second part of this appendix we prove two lemmas, which allow us to restrict the coherence parameter γ to real and positive numbers and the input state ρ_B to pure states.

Lemma 8.6.1. *In our problem, we can describe all the possible qualitatively different games just with $\gamma \in [0, 1]$. That is, all games corresponding to $\gamma \in \mathbb{C}, |\gamma| \leq 1$ are equivalent to some game with $\gamma \in [0, 1]$.*

Proof. Let $\gamma = |\gamma| e^{i\theta}$. Then:

$$\tilde{\rho}_R^x(\gamma, d, \rho_B) = \frac{1}{2}\begin{pmatrix} \langle x|\rho_B|x\rangle & |\gamma| e^{-i\theta}\langle x|\rho_B F^\dagger|x\rangle \\ |\gamma| e^{i\theta}\langle x|F\rho_B|x\rangle & \langle x|F\rho_B F^\dagger|x\rangle \end{pmatrix}, \tag{8.29}$$

Let $V(\theta)$ denote the rotation matrix in the xy plane of the Bloch sphere by angle θ. That is:

$$V(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}. \tag{8.30}$$

Then it can be easily verified that:

$$\tilde{\rho}_R^x(\gamma,d,\rho_B) = V(\theta)\tilde{\rho}_R^x(|\gamma|,d,\rho_B)V^\dagger(\theta)\,, \tag{8.31}$$

where $|\gamma| \in [0,1]$. Hence all the output states $\tilde{\rho}_R^x(\gamma,d)$ up to a unitary rotation $V(\theta)$ are the same as the corresponding states $\tilde{\rho}_R^x(|\gamma|,d)$. Clearly, rotating all the output states of register R by a fixed angle θ does not affect their distinguishability. Hence, it is sufficient to consider real and positive $\gamma \in [0,1]$. □

The probability of successfully discriminating states $\rho_R^x(\gamma,d,\rho_B)$, optimised over all measurements is [24]:

$$p_{\text{guess}}(\gamma,d,\rho_B) = \max_{\{M_x\}} \sum_{x=0}^{d-1} p_x(d,\rho_B)\,\text{Tr}[M_x\rho_R^x(\gamma,d,\rho_B)] = \max_{\{M_x\}} \sum_{x=0}^{d-1} \text{Tr}[M_x\tilde{\rho}_R^x(\gamma,d,\rho_B)]\,, \tag{8.32}$$

where $\{M_x\}$ is a POVM. Here, by p_{guess} we denote the guessing probability optimised over all POVM's but for a specific input state ρ_B, while later we will use $p_{\text{guess}}^{\max}$ to denote the guessing probability p_{guess} optimised over all inputs states of Bob. Both p_{guess} and $p_{\text{guess}}^{\max}$ are calculated for a specific game parameterised by $d \geq 2$ and for a specific $\gamma \in [0,1]$. Hence, we have $p_{\text{guess}}^{\max}(\gamma,d) = \max_{\rho_B} p_{\text{guess}}(\gamma,d,\rho_B)$.

Lemma 8.6.2. *To achieve $p_{\text{guess}}^{\max}$ it is sufficient for Bob to consider pure input states.*

Proof. Firstly, let us consider the case when not only does Bob hold no quantum memory, but he also does not have any classical memory. Consider then a scenario in which Bob sends Alice a mixed state $\rho_B = \sum_i q_i|\phi_i\rangle\langle\phi_i|$, where he is given freedom to choose the probabilities $\{q_i\}$. Then using Eq. (8.12):

$$\begin{aligned}\tilde{\rho}_R^x(\gamma,d,\rho_B) &= \sum_i q_i \frac{1}{2}\begin{pmatrix} |\langle x|\phi_i\rangle|^2 & \gamma\langle x|\phi_i\rangle\langle\phi_i|F^\dagger|x\rangle \\ \gamma\langle\phi_i|x\rangle\langle x|F|\phi_i\rangle & |\langle x|F|\phi_i\rangle|^2 \end{pmatrix} \\ &= \sum_i q_i \tilde{\rho}_{R,i}^x(\gamma,d,|\phi_i\rangle)\,,\end{aligned} \tag{8.33}$$

where $\tilde{\rho}_R^x(\gamma,d,|\phi_i\rangle)$ denotes a post-measurement register state $\tilde{\rho}_R^x(\gamma,d,\rho_B)$ corresponding to Bob inputting a pure state $\rho_B = |\phi_i\rangle\langle\phi_i|$. In this case the guessing probability from Eq. (8.32) becomes:

$$\begin{aligned}p_{\text{guess}}(\gamma,d,\rho_B) &= \max_{\{M_x\}} \sum_{x=0}^{d-1} \text{Tr}\left[M_x \sum_i q_i \tilde{\rho}_R^x(\gamma,d,|\phi_i\rangle)\right] \leq \sum_i q_i \max_{\{M_x\}} \sum_{x=0}^{d-1} \text{Tr}[M_x\tilde{\rho}_R^x(\gamma,d,|\phi_i\rangle)] \\ &= \sum_i q_i\, p_{\text{guess}}(\gamma,d,|\phi_i\rangle) \leq \max_i p_{\text{guess}}(\gamma,d,|\phi_i\rangle) = p_{\text{guess}}(\gamma,d,|\phi_m\rangle)\,,\end{aligned} \tag{8.34}$$

where $p_{\text{guess}}(\gamma,d,|\phi_i\rangle) = \max_{\{M_x\}} \sum_{x=0}^{d-1} \text{Tr}[M_x\tilde{\rho}_R^x(\gamma,d,|\phi_i\rangle)]$ and by index m we denote the largest of all $p_{\text{guess}}(\gamma,d,|\phi_i\rangle)$ over all i's. Hence it is optimal for Bob to prepare a state $\rho_B = \sum_i q_i|\phi_i\rangle\langle\phi_i| = |\phi_m\rangle\langle\phi_m|$ (so that $q_i = \delta_{i,m}$), such that $|\phi_m\rangle \in \{|\phi_i\rangle\}$ and $p_{\text{guess}}(\gamma,d,|\phi_m\rangle) = \max_i p_{\text{guess}}(\gamma,d,|\phi_i\rangle)$.

Now, if we allow Bob to have classical memory, he could then prepare a mixed state ρ_B which is classically correlated to this memory. Then for each of the states ρ_B^i, corresponding to the state of the classical memory $|i\rangle_M$, we need to solve a separate optimisation problem given by Eq. (8.32). Hence, if Bob prepares a state:

$$\rho_{BM} = \sum_i s_i \rho_B^i \otimes |i\rangle\langle i|_M \tag{8.35}$$

according to the probability distribution $\{s_i\}$, then the guessing probability will be a weighted average of the individual guessing probabilities corresponding to each of the states ρ_B^i, namely:

$$p_{\text{guess}}(\gamma, d, \rho_B) = \sum_i s_i \, p_{\text{guess}}(\gamma, d, \rho_B^i) \leq p_{\text{guess}}(\gamma, d, \rho_B^k), \tag{8.36}$$

where ρ_B^k is the input state that gives the highest guessing probability out of all the states $\{\rho_B^i\}$. Hence, classical memory does not allow us to achieve guessing probability higher than individual ρ_B^k, for which (as we have just seen) the guessing probability is upper bounded by its value corresponding to the optimal pure state $|\phi_m\rangle$ in the decomposition $\rho_B^k = \sum_i q_i |\phi_i\rangle\langle\phi_i|$. □

Hence we will restrict our attention to scenarios in which Bob prepares a pure state $|\phi\rangle_B$. In this case the post-measurement states of the basis register are:

$$\tilde{\rho}_R^x(\gamma, d, |\phi\rangle_B) = \frac{1}{2}\begin{pmatrix} \left|\langle x|\phi\rangle\right|^2 & \gamma\langle x|\phi\rangle\langle\phi|F^\dagger|x\rangle \\ \gamma\langle x|F|\phi\rangle\langle\phi|x|\rangle & \left|\langle x|F|\phi\rangle\right|^2 \end{pmatrix}. \tag{8.37}$$

8.6.2. GUESSING PROBABILITY FOR TWO-DIMENSIONAL GAME ($d = 2$)

In this appendix we prove Theorem 8.4.1. That is, we derive the analytical formula for the maximum guessing probability as a function of $\gamma \in [0, 1]$, for a game with two-dimensional Fourier transform (Hadamard transform) in our circuit and two possible outcomes. In this game the state ρ_B that Bob prepares is a qubit. The two possible outcomes for Alice are: 0 and 1. We firstly restate this theorem below.

Theorem 8.4.1. *The maximum guessing probability for a two-dimensional game ($d = 2$), optimised over all input states ρ_B is given by:*

$$p_{\text{guess}}^{\max}(\gamma, d = 2) = \frac{1}{2}\left(1 + \frac{\sqrt{2 + 2\gamma^2}}{2}\right). \tag{8.38}$$

In particular, for $\gamma = 1$ one achieves perfect guessing, that is $p_{\text{guess}}^{\max}(\gamma = 1, d = 2) = 1$.

Proof. The guessing probability is determined by how well Bob can distinguish states $\tilde{\rho}_R^0$ and $\tilde{\rho}_R^1$ defined in Eq. (8.37) (for convenience we will omit writing out explicitly the dependence on γ and d). The problem of distinguishing two states has been solved by Helstrom [25] and the guessing probability is:

$$p_{\text{guess}} = \frac{1}{2}(1 + \|G\|_1), \tag{8.39}$$

where $G = \tilde{\rho}_R^0 - \tilde{\rho}_R^1 = p_0\rho_R^0 - p_1\rho_R^1$ and $\|\cdot\|_1$ denotes the trace-norm of the matrix. Firstly we note that for $d = 2$, $F = F^\dagger = H$. Secondly, since ρ_B is a qubit, it is convenient to use the Bloch sphere representation:

$$\rho_B = \frac{1}{2}\left(\mathbb{I} + \sum_i c_i\sigma_i\right), \tag{8.40}$$

with $c_x^2 + c_y^2 + c_z^2 \leq 1$. Although we have already shown in Appendix 8.6.1 that the optimal guessing probability $p_{\text{guess}}^{\max}$ will be achieved for a pure input state ρ_B, here we are interested in all the qubit states that achieve this maximum guessing probability (under the assumption of Bob having no classical memory; if Bob had access to some classical memory, then any mixture of such optimal states correlated with this memory would also be an optimal state). Hence, in this appendix we again assume ρ_B to be an arbitrary (possibly mixed) qubit state. Plugging the Bloch sphere representation of ρ_B into Eq. (8.12), we can first calculate $\tilde{\rho}_R^0$ and $\tilde{\rho}_R^1$ and then G:

$$G = \frac{1}{2}\begin{pmatrix} c_z & \frac{\gamma(1-i\cdot c_y)}{\sqrt{2}} \\ \frac{\gamma(1+i\cdot c_y)}{\sqrt{2}} & c_x \end{pmatrix}. \tag{8.41}$$

The eigenvalues of G are:

$$\lambda = \frac{(c_x + c_z) \pm \sqrt{(c_x - c_z)^2 + \gamma^2(1 + c_y^2)}}{4}. \tag{8.42}$$

Now, let us consider two cases:

(a) $\lambda_1 \cdot \lambda_2 \geq 0$.

Then $\|G\|_1^{\text{a}} = |\lambda_1| + |\lambda_2| = |c_x + c_z|/2$ (the superscript "a" labels the case $\lambda_1 \cdot \lambda_2 \geq 0$). We are interested in the maximum possible value of $\|G\|_1^{\text{a}}$ for a given γ. Hence we want to maximise the expression $|c_x + c_z|$ subject to the constraint $c_x^2 + c_y^2 + c_z^2 \leq 1$. Clearly, this gives us $|c_x + c_z| \leq \sqrt{2}$. and so $\|G\|_1^{\text{a, max}} \leq \frac{\sqrt{2}}{2}$. In particular, this bound is tight for $c_y = 0$ and $c_x = c_z = \pm\frac{1}{\sqrt{2}}$ (those states clearly satisfy the condition $\lambda_1 \cdot \lambda_2 \geq 0$). Hence, $\|G\|_1^{\text{a, max}} = \frac{\sqrt{2}}{2}$.

(b) $\lambda_1 \cdot \lambda_2 < 0$.

Then:

$$\lambda_1 = \frac{(c_x + c_z) + \sqrt{(c_x - c_z)^2 + 2\gamma^2(1 + c_y^2)}}{4} > 0 \tag{8.43}$$

$$\lambda_2 = \frac{(c_x + c_z) - \sqrt{(c_x - c_z)^2 + 2\gamma^2(1 + c_y^2)}}{4} < 0. \tag{8.44}$$

Hence in this case:

$$\|G\|_1^{\text{b}} = \lambda_1 - \lambda_2 = \frac{\sqrt{(c_x - c_z)^2 + 2\gamma^2(1 + c_y^2)}}{2}. \tag{8.45}$$

Now we need to optimise this expression subject to the constraint $c_x^2+c_y^2+c_z^2 \leq 1$. Let us use a substitution $a = \frac{c_x - c_z}{\sqrt{2}}$ $b = \frac{c_x + c_z}{\sqrt{2}}$. Then the constraint becomes: $a^2 + c_y^2 + b^2 \leq 1$ and the norm of G is:

$$\|G\|_1^{\mathrm{b}} = \frac{\sqrt{2a^2 + 2\gamma^2(1+c_y^2)}}{2}. \tag{8.46}$$

Clearly, since the term c_y^2 is scaled by the positive factor $2\gamma^2 \leq 2$, while a^2 is scaled by a factor of exactly 2, optimising this expression corresponds to setting a^2 to its maximum possible value which is 1 (so that $c_x = -c_z = \pm\frac{1}{\sqrt{2}}$). Then $c_y = b = 0$ (one can easily verify that those values satisfy the condition of (b) $\lambda_1 \cdot \lambda_2 < 0$, for all $\gamma \in [0,1]$). This gives:

$$\|G\|_1^{\mathrm{b,\,max}} = \frac{\sqrt{2+2\gamma^2}}{2}, \tag{8.47}$$

Clearly $\|G\|_1^{\mathrm{b,\,max}} \geq \|G\|_1^{\mathrm{a,\,max}}$ for all $\gamma \in [0,1]$ (the equality relation holds only for $\gamma = 0$). Hence:

$$\|G\|_1^{\max} = \frac{\sqrt{2+2\gamma^2}}{2}, \tag{8.48}$$

Using $\|G\|_1^{\max}$, for every γ we can now calculate the maximum value of the guessing probability:

$$p_{\mathrm{guess}}^{\max}(\gamma, d=2) = \frac{1}{2}(1 + \|G\|_1^{\max}) = \frac{1}{2}\left(1 + \frac{\sqrt{2+2\gamma^2}}{2}\right). \tag{8.49}$$

We see also that for a fully coherent register with $\gamma = 1$, we obtain $p_{\mathrm{guess}}^{\max} = 1$. □

In order to find the optimal states we need to consider 3 separate cases depending on the value of γ.

- $\gamma = 0$. In this case $\|G\|_1^{\max} = \frac{\sqrt{2}}{2}$. This value occurs for two classes of states. One of them satisfies $a^2 = 1$ and $b = c_y = 0$ which gives two solutions: $c_x = -c_z = \pm\frac{1}{\sqrt{2}}$. Hence we obtain two states: $(c_x, c_y, c_z) = \left(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}\right)$ and $(c_x, c_y, c_z) = \left(-\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$. The other class can be seen by noticing that $\|G\|_1^{\max} = \frac{\sqrt{2}}{2} = \|G\|_1^{\mathrm{a,\,max}}$ and so it can also be obtained from the case (a) for two states that achieve this value: $(c_x, c_y, c_z) = \left(\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$ and $(c_x, c_y, c_z) = \left(-\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}\right)$.

- $\gamma \in (0,1)$. Here we only have the class $a^2 = 1$ and $b = c_y = 0$, that is the states: $(c_x, c_y, c_z) = \left(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}\right)$ and $(c_x, c_y, c_z) = \left(-\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$.

- $\gamma = 1$. Now $\|G\|_1^{\mathrm{b}} = \frac{\sqrt{2a^2+2(1+c_y^2)}}{2}$, and so this expression subject to the Bloch sphere normalisation is maximised by the pure states satisfying $a^2 + c_y^2 = 1$ and $b = 0$. These are all pure states with $c_z = -c_x$ and $c_y = \pm\sqrt{1-2c_x^2}$. We can use angular parametrisation of those coefficients, in which case we can write this entire family of states as $(c_x, c_y, c_z) = \left(\sin(\theta), \pm\sqrt{\cos(2\theta)}, -\sin(\theta)\right)$ for all $\theta \in [-\frac{\pi}{4}, \frac{\pi}{4}]$. Geometrically, these states correspond to all pure states on the Bloch sphere that lie in the

plane perpendicular to the Hadamard rotation axis and Hadamard transformation rotates them by π rad to their orthogonal complement.

From Eq. (8.49) we see that the lowest value of $p^{\max}_{\text{guess}}$ occurs for $\gamma = 0$ and it is $p^{\max}_{\text{guess}} = \frac{1}{2}\left(1+\frac{1}{\sqrt{2}}\right)$. As the basis register state is becoming more pure by letting γ grow, the $p^{\max}_{\text{guess}}$ grows, until $p^{\max}_{\text{guess}} = 1$ for $\gamma = 1$. We can also rephrase the guessing probability in terms of the purity of the basis register:

$$\text{Tr}[\rho_R^2] = \frac{1}{4}\text{Tr}\left[\begin{pmatrix}1 & \gamma\\ \gamma & 1\end{pmatrix}\begin{pmatrix}1 & \gamma\\ \gamma & 1\end{pmatrix}\right] = \frac{1}{4}\text{Tr}\left[\begin{pmatrix}1+\gamma^2 & 2\gamma\\ 2\gamma & 1+\gamma^2\end{pmatrix}\right] = \frac{1+\gamma^2}{2}. \tag{8.50}$$

Hence:

$$p^{\max}_{\text{guess}}(\gamma, d=2) = \frac{1}{2}\left(1+\sqrt{\text{Tr}[\rho_R^2]}\right). \tag{8.51}$$

8.6.3. GUESSING PROBABILITY FOR THE D-DIMENSIONAL GAME

We have already seen that in two dimensions utilising entanglement allows for guessing with probability equal to 1. In higher dimensions however, we show that this is not possible. This fact is expressed in Theorem 8.4.2 in the main text. We restate and prove this theorem below.

Theorem 8.4.2. *For d-dimensional games with any $d > 2$ it is not possible to achieve perfect guessing, i.e.,*

$$p^{\max}_{\text{guess}}(\gamma, d > 2) < 1, \qquad \forall\, \gamma. \tag{8.52}$$

Proof. We construct a proof by contradiction. Let us assume that there exists $d > 2$ and $\gamma \in [0,1]$, such that $p^{\max}_{\text{guess}}(\gamma, d) = 1$. Since the states $\tilde{\rho}^x_R(\gamma, d, |\phi\rangle)$ are two-dimensional, it is only possible to perfectly distinguish at most 2 such states (if they are orthogonal). Hence, that means that to achieve $p^{\max}_{\text{guess}}(\gamma, d) = 1$ it is required that at least $d-2$ output states ρ^x_R occur with probability zero. Hence, $\tilde{\rho}^x_R \neq 0$ for at most two values of x. Let us denote those two values of $x \in \{0, 1, ..., d-1\}$ for which it is possible that $\tilde{\rho}^x_R \neq 0$ by x_0 and x_1. We assume that those values are distinct so that $x_0 \neq x_1$. Specifically, let us assume that $\tilde{\rho}^{x_0}_R \neq 0$, while $\tilde{\rho}^{x_1}_R$ may or may not be equal to zero. Then let us define $\mathscr{P} = \{0, 1, ..., d-1\} \setminus \{x_0, x_1\}$. Therefore we require that $\tilde{\rho}^x_R = 0$ for all $x \in \mathscr{P}$. Thus we obtain the following two requirements:

1) $\langle x|\phi\rangle = 0$ for all $x \in \mathscr{P}$,

2) $\langle x|F|\phi\rangle = 0$ for all $x \in \mathscr{P}$.

The requirement 1) implies that the physical input state of Bob must be of the form:

$$|\phi\rangle = \alpha_0|x_0\rangle + \alpha_1|x_1\rangle, \tag{8.53}$$

with

$$|\alpha_0|^2 + |\alpha_1|^2 = 1. \tag{8.54}$$

In this framework, the scenario in which only $\tilde{\rho}_R^{x_0} \neq 0$ would require $\alpha_1 = 0$. Now, note that:

$$F^\dagger|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{-jk}|k\rangle\,, \tag{8.55}$$

where $\omega = \exp\left(\frac{2\pi i}{d}\right)$ and so:

$$\langle\phi|F^\dagger|x\rangle = \frac{1}{\sqrt{d}}(\alpha_0^*\omega^{-xx_0} + \alpha_1^*\omega^{-xx_1})\,. \tag{8.56}$$

Then 2) implies that:

$$\alpha_0^* + \alpha_1^*\omega^{x(x_0-x_1)} = 0\,, \qquad \forall x \in \mathscr{P}\,. \tag{8.57}$$

Eq. (8.57) together with Eq. (8.54) require that α_0 and α_1 are of the form:

$$\alpha_0 = \frac{1}{\sqrt{2}} e^{i\theta_0}\,, \tag{8.58}$$

$$\alpha_1 = \frac{1}{\sqrt{2}} e^{i\theta_1}\,. \tag{8.59}$$

The above requirement shows that α_1 cannot be zero, which in turn means that the scenario in which only $\tilde{\rho}_R^{x_0} \neq 0$ is not possible. Plugging the above forms of α's into Eq. (8.57) and using the fact that ω is the d-th root of unity, we obtain the following requirement:

$$\theta_0 \equiv \theta_1 + \pi + 2\pi\left[\frac{x}{d}(x_1 - x_0)\right] (\mathrm{mod}\ 2\pi)\,, \qquad \forall x \in \mathscr{P}\,. \tag{8.60}$$

Note that for $d = 3$, this expression can be easily satisfied since in this case $|\mathscr{P}| = 1$, so e.g. $\theta_0 = \theta_1 + \pi + 2\pi\left[\frac{x_{\mathscr{P}}}{d}(x_1 - x_0)\right]$, where $x_{\mathscr{P}} \in \mathscr{P}$ satisfies Eq. (8.60). Hence the case $d = 3$ needs to be analysed separately. For $d > 3$ this equation can be satisfied if and only if:

$$\frac{x_1 - x_0}{d} \in \mathbb{Z}\,, \tag{8.61}$$

where $\mathbb{Z}$ denotes the set of integers. However, $x_0, x_1 \in \{0, d-1\}$ and $x_0 \neq x_1$. Therefore this equation cannot be satisfied. Hence, for $d > 3$, it is not possible to have $p_{\mathrm{guess}}(\gamma, d) = 1$. Now, let us consider the case $d = 3$. Eq. (8.53) and Eq. (8.58)-(8.60) imply that

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|x_1\rangle - \omega^{x_{\mathscr{P}}(x_1-x_0)}|x_0\rangle\right)\,, \tag{8.62}$$

where we fix the global phase by setting $\theta_1 = 0$. Since $x_{\mathscr{P}}, x_0, x_1$ must be all different, there are 6 possible states $|\phi\rangle$ corresponding to the above expression. Let $|\psi_{kl}\rangle = \frac{1}{\sqrt{2}}\left(|l\rangle - \omega^{x_{\mathscr{P}}(l-k)}|k\rangle\right)$. Then note that for every value of $x_{\mathscr{P}}$, the state $|\phi\rangle = |\psi_{kl}\rangle$ with $x_0 = k, x_1 = l$ and the state $|\phi\rangle = |\psi_{lk}\rangle$ with $x_0 = l, x_1 = k$ up to the global phase correspond to exactly the same state, since:

$$|\psi_{kl}\rangle = \frac{1}{\sqrt{2}}\left(|l\rangle - \omega^{x_{\mathscr{P}}(l-k)}|k\rangle\right) = -\omega^{x_{\mathscr{P}}(l-k)}\frac{1}{\sqrt{2}}\left(-\omega^{x_{\mathscr{P}}(k-l)}|l\rangle + |k\rangle\right) = -\omega^{x_{\mathscr{P}}(l-k)}|\psi_{lk}\rangle\,. \tag{8.63}$$

Hence, we need only to consider 3 separate cases:

- For $x_{\mathscr{P}} = 0, x_0 = 1, x_1 = 2$, that is when $\tilde{\rho}_R^0 = 0$, we have:

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|2\rangle - |1\rangle\right). \tag{8.64}$$

Then:

$$F|\phi\rangle = i\frac{1}{\sqrt{2}}\left(|2\rangle - |1\rangle\right) = i|\phi\rangle. \tag{8.65}$$

This means that if we define a matrix

$$\rho_c(\gamma) = \frac{1}{2}\begin{pmatrix} 1 & -i\gamma \\ i\gamma & 1 \end{pmatrix}, \tag{8.66}$$

then $\tilde{\rho}_R^0 = 0, \tilde{\rho}_R^1 = \left|\langle 1|\phi\rangle\right|^2 \rho_c(\gamma), \tilde{\rho}_R^2 = \left|\langle 2|\phi\rangle\right|^2 \rho_c(\gamma)$. Hence, $\tilde{\rho}_R^1 = \tilde{\rho}_R^2 = \frac{1}{2}\rho_c(\gamma)$ and so we see that $\tilde{\rho}_R^1$ and $\tilde{\rho}_R^2$ correspond to the same state $\rho_c(\gamma)$ occurring with probability 0.5. This means that guessing probability in this case is 0.5 for all $\gamma \in [0,1]$.

- For $x_{\mathscr{P}} = 1, x_0 = 2, x_1 = 0$ with $\tilde{\rho}_R^1 = 0$ the input state is:

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - \omega^{-2}|2\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle - \omega|2\rangle\right). \tag{8.67}$$

Then:

$$F|\phi\rangle = \frac{1}{\sqrt{6}}(1-\omega)\left(|0\rangle - \omega^2|2\rangle\right). \tag{8.68}$$

Hence,

$$\tilde{\rho}_R^0 = \frac{1}{4}\begin{pmatrix} 1 & \gamma\frac{1}{\sqrt{3}}(1-\omega^*) \\ \gamma\frac{1}{\sqrt{3}}(1-\omega) & 1 \end{pmatrix}, \tag{8.69}$$

$$\tilde{\rho}_R^1 = 0, \tag{8.70}$$

$$\tilde{\rho}_R^2 = \frac{1}{4}\begin{pmatrix} 1 & \gamma\frac{1}{\sqrt{3}}(1-\omega^*)\omega^* \\ \gamma\frac{1}{\sqrt{3}}(1-\omega)\omega & 1 \end{pmatrix}. \tag{8.71}$$

One can now show that $\mathrm{Tr}[\tilde{\rho}_R^0\tilde{\rho}_R^2] \neq 0$ for all $\gamma \in [0,1]$. Hence those states are not orthogonal and perfect guessing is not possible.

- For $x_{\mathscr{P}} = 2, x_0 = 0, x_1 = 1$, with $\tilde{\rho}_R^1 = 0$ the input state is:

$$|\phi\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle - \omega^2|0\rangle\right). \tag{8.72}$$

Then:

$$F|\phi\rangle = \frac{1}{\sqrt{6}}\left((1-\omega^2)|0\rangle + \sqrt{3}i|1\rangle\right). \tag{8.73}$$

Hence,

$$\tilde{\rho}_R^0 = \frac{1}{4}\begin{pmatrix} 1 & \gamma\frac{1}{\sqrt{3}}(1-\omega^*) \\ \gamma\frac{1}{\sqrt{3}}(1-\omega) & 1 \end{pmatrix}, \tag{8.74}$$

$$\tilde{\rho}_R^1 = \frac{1}{2}\rho_c(\gamma), \tag{8.75}$$

$$\tilde{\rho}_R^2 = 0. \tag{8.76}$$

Again $\mathrm{Tr}[\tilde{\rho}_R^0 \tilde{\rho}_R^1] \neq 0$ for all $\gamma \in [0,1]$. Hence also in this case perfect guessing is not possible.

We have shown that perfect guessing in $d = 3$ case is not possible either. Therefore we conclude that for all $d > 2$ and for all $\gamma \in [0,1]$, $p_{\text{guess}}^{\max}(\gamma, d) < 1$. □

The case $\gamma = 0$ is a special case and can be solved analytically for all $d \geq 2$.

Proposition 1. *For $\gamma = 0$ the maximal guessing probability is:*

$$p_{\text{guess}}^{\max}(\gamma = 0, d) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right), \tag{8.77}$$

and under assumption of Bob having no classical memory, it is achieved if and only if Bob's input state ρ_B belongs to the following family of pure states:

$$|\phi_{jl}\rangle = c\left(|j\rangle + \omega^{jl} F^\dagger |l\rangle\right), \tag{8.78}$$

where $\omega = \exp\left(\frac{2\pi i}{d}\right)$, $j, l \in \{0, 1, ..., d-1\}$ and $c = \sqrt{\frac{\sqrt{d}}{2\sqrt{d}+2}}$.

Proof. If one measures in the standard basis, the guessing probability for a fixed input state ρ_B is:

$$p_{\text{guess}}^{\text{standard}}(d, \rho_B) = \max_l \mathrm{Tr}[|l\rangle\langle l|\rho_B]. \tag{8.79}$$

If one measures in the Fourier basis:

$$p_{\text{guess}}^{\text{Fourier}}(d, \rho_B) = \max_l \mathrm{Tr}[|l\rangle\langle l|F\rho_B F^\dagger] = \max_l \mathrm{Tr}[F^\dagger|l\rangle\langle l|F\rho_B]. \tag{8.80}$$

Since each measurement occurs with probability 50% and in the classical game the register R only tells Bob which measurement basis was used, the guessing probability optimised over all input states of Bob is:

$$\begin{aligned} p_{\text{guess}}^{\max}(\gamma = 0, d) &= \frac{1}{2}\max_{\rho_B}(p_{\text{guess}}^{\text{standard}}(d, \rho_B) + p_{\text{guess}}^{\text{Fourier}}(d, \rho_B)) \\ &= \frac{1}{2}\max_{\rho_B}\max_{j,l}\mathrm{Tr}[(|j\rangle\langle j| + F^\dagger|l\rangle\langle l|F)\rho_B] \\ &= \frac{1}{2}\max_{j,l}\left\| |j\rangle\langle j| + F^\dagger|l\rangle\langle l|F \right\|_\infty, \end{aligned} \tag{8.81}$$

where $\|\cdot\|_\infty$ denotes the infinity norm. The matrix whose infinity norm we need to find is a rank-2 matrix. Let $p_{\text{guess}} = \frac{1}{2}\|M\|_\infty$ and $M = |\alpha\rangle\langle\alpha| + |\beta\rangle\langle\beta|$ be a rank-2 matrix. The largest eigenvalue of such a matrix is $\|M\|_\infty = \lambda_{\max} = 1 + \left|\langle\alpha|\beta\rangle\right|$. In our case: $|\alpha\rangle = |j\rangle$ and $|\beta\rangle = F^\dagger|l\rangle$. This means that $\|M\|_\infty = 1 + \frac{1}{\sqrt{d}}$ and so:

$$p_{\text{guess}}^{\max}(\gamma = 0, d) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right). \tag{8.82}$$

The eigenstate corresponding to this eigenvalue $\lambda_{\max}$ is:

$$|\phi_{jl}\rangle = c\left(|j\rangle + \omega^{jl} F^\dagger |l\rangle\right). \tag{8.83}$$

Hence only the states of this form will give us the maximum guessing probability. □

We will now show that for a subclass of the states of this form Bob will be guessing always either j or l, for all $\gamma \in [0,1]$ and all $d \geq 2$, since those 2 outcomes have much higher probabilities of occurrence $p_j(d,|\phi_{jl}\rangle)$ and $p_l(d,|\phi_{jl}\rangle)$ than all other outcomes (i.e. we will show that for input state $|\phi_{jl}\rangle = c\left(|j\rangle + \omega^{jl}F^\dagger|l\rangle\right)$ such that $j \neq l$ the optimal strategy aims at distinguishing only the two states $\tilde{\rho}_R^j(\gamma,d,|\phi_{jl}\rangle)$ and $\tilde{\rho}_R^l(\gamma,d,|\phi_{jl}\rangle)$).

Lemma 8.6.3. *For all $d \geq 2$, for all $\gamma \in [0,1]$ and for all states $|\phi_{jl}\rangle = c\left(|j\rangle + \omega^{jl}F^\dagger|l\rangle\right)$, such that $j,l \in \{0,1,...,d-1\}$ and $j \neq l$, the optimal guessing probability can be achieved by Bob if his measurement on the state of register R is a POVM with only two occurring outcomes, that is the matrix elements of this POVM are: $M_j \neq 0$, $M_l \neq 0, M_k = 0$, for all $k \in \mathscr{P}$, where $\mathscr{P} = \{0,1,...,d-1\} \setminus \{j,l\}$.*

Proof. The case $d = 2$ is trivial, since then there are only two output states.

Now considering the general case, let $\lambda_{\min}(\gamma,d,|\phi_{jl}\rangle)$ denote the guessing probability corresponding to this restricted POVM. The "min" subscript indicates that this guessing probability is a lower bound on $p_{\text{guess}}(\gamma,d,|\phi_{jl}\rangle)$, the guessing probability optimised over all POVMs. That is: $\lambda_{\min}(\gamma,d,|\phi_{jl}\rangle) \leq p_{\text{guess}}(\gamma,d,|\phi_{jl}\rangle)$. We then have:

$$\lambda_{\min}(\gamma,d,|\phi_{jl}\rangle) = \max_{M_j,M_l} \text{Tr}[M_j\tilde{\rho}_R^j(\gamma,d,|\phi_{jl}\rangle)] + \text{Tr}[M_l\tilde{\rho}_R^l(\gamma,d,|\phi_{jl}\rangle)], \tag{8.84}$$

Effectively this is again the problem of distinguishing 2 states solved by Helstrom [25], the only difference is that this time $p_j(d,|\phi_{jl}\rangle) + p_l(d,|\phi_{jl}\rangle) \leq 1$. Hence

$$\lambda_{\min}(\gamma,d,|\phi_{jl}\rangle) = \frac{1}{2}\left[\left\|G(\gamma,d,|\phi_{jl}\rangle)\right\|_1 + p_j(d,|\phi_{jl}\rangle) + p_l(d,|\phi_{jl}\rangle)\right], \tag{8.85}$$

where $G(\gamma,d,|\phi_{jl}\rangle) = \tilde{\rho}_R^j(\gamma,d,|\phi_{jl}\rangle) - \tilde{\rho}_R^l(\gamma,d,|\phi_{jl}\rangle)$. Now we will show that this bound is tight, i.e. we will show that the above $\lambda_{\min}(\gamma,d,|\phi_{jl}\rangle)$ is in fact also an upper bound on $p_{\text{guess}}(\gamma,d,|\phi_{jl}\rangle)$. For this purpose let us consider the dual program [24] in which we consider all matrices

$$\begin{aligned} Q(\gamma,d,|\phi_{jl}\rangle) \in \mathscr{Z}, \text{ where } \mathscr{Z} = \Big\{ & Q \in \mathbb{C}^{2\times 2} : Q = Q^\dagger \wedge \forall k \in \{0,1,...,d-1\}, \\ & Q(\gamma,d,|\phi_{jl}\rangle) \geq \tilde{\rho}_R^k(\gamma,d,|\phi_{jl}\rangle)\Big\}. \end{aligned} \tag{8.86}$$

Then for each $Q \in \mathscr{Z}$ we define $\lambda_{\max}^Q(\gamma,d,|\phi_{jl}\rangle) = \text{Tr}[Q(\gamma,d,|\phi_{jl}\rangle)]$. From this it follows that $p_{\text{guess}}(\gamma,d,|\phi_{jl}\rangle) \leq \lambda_{\max}^Q(\gamma,d,|\phi_{jl}\rangle)$ for all $Q \in \mathscr{Z}$ [24] and so $\lambda_{\max}^Q(\gamma,d,|\phi_{jl}\rangle)$ is an upper bound on $p_{\text{guess}}(\gamma,d,|\phi_{jl}\rangle)$. For simplicity, we will now omit writing explicitly the dependence on γ, d and $|\phi\rangle$. Consider a hermitian matrix:

$$Q' = \frac{1}{2}(\tilde{\rho}_R^j + \tilde{\rho}_R^l + |G|). \tag{8.87}$$

Then:

$$\text{Tr}[Q'] = \frac{1}{2}(p_j + p_l + \|G\|_1) = \lambda_{\min}. \tag{8.88}$$

Now, if Q' satisfies $Q' \geq \tilde{\rho}_R^k, \forall k$, then $Q' \in \mathscr{Z}$ and so $\text{Tr}[Q'] = \lambda_{\max}^{Q'}$. And since then $\text{Tr}[Q'] = \lambda_{\min} = \lambda_{\max}^{Q'}$, this means that $\text{Tr}[Q'] = p_{\text{guess}}$. Hence, we will now prove that $\forall d \geq 3, \gamma \in [0,1]$ we have $Q' \in \mathscr{Z}$.

Consider

$$Q' - \tilde{\rho}_R^j = \frac{1}{2}(-\tilde{\rho}_R^j + \tilde{\rho}_R^l + |G|) = \frac{1}{2}(-G + |G|)\,. \tag{8.89}$$

Note that $|G| \geq G$ and so $Q' - \tilde{\rho}_R^j \geq 0$. Hence $Q' \geq \tilde{\rho}_R^j$. Analogously

$$Q' - \tilde{\rho}_R^l = \frac{1}{2}(\tilde{\rho}_R^j - \tilde{\rho}_R^l + |G|) = \frac{1}{2}(G + |G|)\,. \tag{8.90}$$

Clearly: $|G| \geq -G$ and so $Q' - \tilde{\rho}_R^l \geq 0$. Hence $Q' \geq \tilde{\rho}_R^l$.

Now we need to prove that $Q' \geq \tilde{\rho}_R^k, \forall k \in \mathscr{P}$ and for all $\gamma \in [0,1], d \geq 3$. In order to do that, we need to explicitly calculate all the output states of the register R. Those states are:

$$\tilde{\rho}_R^j(\gamma, d, |\phi_{jl}\rangle) = \frac{1}{2}\begin{pmatrix} A^2 & \gamma AB\omega^{-j^2} \\ \gamma AB\omega^{j^2} & B^2 \end{pmatrix}, \tag{8.91}$$

$$\tilde{\rho}_R^l(\gamma, d, |\phi_{jl}\rangle) = \frac{1}{2}\begin{pmatrix} B^2 & \gamma AB\omega^{-l^2} \\ \gamma AB\omega^{l^2} & A^2 \end{pmatrix}, \tag{8.92}$$

$$\tilde{\rho}_R^k(\gamma, d, |\phi_{jl}\rangle) = \frac{B^2}{2}\begin{pmatrix} 1 & \gamma\omega^{jl-jk-kl} \\ \gamma\omega^{jk+kl-jl} & 1 \end{pmatrix}, \tag{8.93}$$

where $A = c\left(1 + \frac{1}{\sqrt{d}}\right), B = \frac{c}{\sqrt{d}}, k \in \mathscr{P}$. Then $Q' - \tilde{\rho}_R^k = \frac{1}{2}(\tilde{\rho}_R^j + \tilde{\rho}_R^l - 2\tilde{\rho}_R^k + |G|)$. Consider the operator:

$$\begin{aligned} D &= \tilde{\rho}_R^j + \tilde{\rho}_R^l - 2\tilde{\rho}_R^k \\ &= \frac{1}{2}\begin{pmatrix} A^2 - B^2 & \gamma B\left(A\omega^{-j^2} + A\omega^{-l^2} - 2B\omega^{jl-jk-kl}\right) \\ \gamma B\left(A\omega^{j^2} + A\omega^{l^2} - 2B\omega^{jk+kl-jl}\right) & A^2 - B^2 \end{pmatrix}. \end{aligned} \tag{8.94}$$

We will now show that for all $k \in \mathscr{P}$ we have $D \geq 0$. Note that for 2×2 matrices, $D \geq 0$ if and only if $\mathrm{Tr}[D] \geq 0$ and $\mathrm{Det}(D) \geq 0$. Firstly, we see that $\mathrm{Tr}[D] = A^2 - B^2 \geq 0, \forall d \geq 3$. Secondly, the determinant of D is:

$$\begin{aligned} \mathrm{Det}(D) = \frac{1}{4}\Bigg[&(A^2 - B^2)^2 - \gamma^2 B^2\left(2A^2 + 4B^2 + 2A^2\cos\left(\frac{2\pi(j^2 - l^2)}{d}\right)\right. \\ &\left.-4AB\cos\left(\frac{2\pi(j^2 - jk - kl + jl)}{d}\right) - 4AB\cos\left(\frac{2\pi(l^2 - jk - kl + jl)}{d}\right)\right)\Bigg]. \end{aligned} \tag{8.95}$$

Now we want to show that $\mathrm{Det}(D) \geq 0$ for all $j, l \in \{0, 1, ..., d-1\}, k \in \mathscr{P}, \gamma \in [0,1], d \geq 3$. From the above expression we see that $\mathrm{Det}(D)$ is monotonic in $\gamma \in [0,1]$. Clearly for $\gamma = 0, \mathrm{Det}(D) = \frac{1}{4}(A^2 - B^2)^2 \geq 0$. For $\gamma = 1$, we have:

$$\begin{aligned} \mathrm{Det}(D) = \frac{1}{4}\Bigg[&A^4 - 3B^4 - 4A^2B^2 - 2A^2B^2\cos\left(\frac{2\pi(j^2 - l^2)}{d}\right) \\ &+4AB^3\cos\left(\frac{2\pi(j^2 - jk - kl + jl)}{d}\right) + 4AB^3\cos\left(\frac{2\pi(l^2 - jk - kl + jl)}{d}\right)\Bigg]. \end{aligned} \tag{8.96}$$

Note that $A = B(1+\sqrt{d})$. Thus we see that:

$$\begin{aligned}\mathrm{Det}(D) &= \frac{B^4}{4}\left[(1+\sqrt{d})^4 - 3 - 4(1+\sqrt{d})^2 - 2(1+\sqrt{d})^2\cos\left(\frac{2\pi(j^2-l^2)}{d}\right)\right.\\ &\left.+4(1+\sqrt{d})\cos\left(\frac{2\pi(j^2-jk-kl+jl)}{d}\right)+4(1+\sqrt{d})\cos\left(\frac{2\pi(l^2-jk-kl+jl)}{d}\right)\right]\\ &\geq \frac{B^4}{4}\left[(1+\sqrt{d})^4 - 3 - 4(1+\sqrt{d})^2 - 2(1+\sqrt{d})^2 - 4(1+\sqrt{d}) - 4(1+\sqrt{d})\right]\\ &= \frac{B^4}{4}\left(d^2+4d\sqrt{d}-16\sqrt{d}-16\right).\end{aligned} \tag{8.97}$$

Let

$$y(d) = \left(d^2+4d\sqrt{d}-16\sqrt{d}-16\right), \tag{8.98}$$

then $\mathrm{Det}(D) \geq \frac{B(d)^4}{4}y(d)$. Clearly $B(d) \geq 0, \forall\, d \geq 3$ and $y(d) \geq 0, \forall\, d \geq 4$. Hence $\mathrm{Det}(D) \geq 0, \forall\, d \geq 4$. For $d = 3$ we use the exact expression from the first part of Eq. (8.97) and we find that for all the cases $j \neq l$, $\forall\, k \in \mathscr{P}$, $\mathrm{Det}(D) \geq 0$. Hence $\mathrm{Det}(D) \geq 0, \forall\, d \geq 3$. Since both $\mathrm{Det}(D) \geq 0$ and $\mathrm{Tr}[D] \geq 0$, $D \geq 0$ and so $Q' \geq \tilde{\rho}_R^k, \forall\, k \in \{0,1,...,d-1\}$ and for all $\gamma \in [0,1], d \geq 3$. Therefore $Q' \in \mathscr{Z}$ and

$$\mathrm{Tr}[Q'] = \lambda_{\max}^{Q}(\gamma, d, |\phi_{jl}\rangle) = \lambda_{\min}(\gamma, d, |\phi_{jl}\rangle) = p_{\mathrm{guess}}(\gamma, d, |\phi_{jl}\rangle). \tag{8.99}$$

□

Now, knowing that the strategy of distinguishing only the two most probable outcomes for the input state $|\phi_{jl}\rangle = c\left(|j\rangle + \omega^{jl}F^\dagger|l\rangle\right)$, such that $j \neq l$ is actually an optimal strategy for those states, we can calculate the guessing probability for these states for all $d \geq 2$ and for all $\gamma \in [0,1]$:

$$\begin{aligned}p_{\mathrm{guess}}(\gamma, d, |\phi_{jl}\rangle) &= \frac{1}{2}(p_j + p_l + \|G\|_1)\\ &= \frac{1}{4(d+\sqrt{d})}\left(2+2\sqrt{d}+d\right.\\ &\left.+\sqrt{d(2+\sqrt{d})^2+2\gamma^2(1+\sqrt{d})^2\left(1-\cos\left(\frac{2\pi(j^2-l^2)}{d}\right)\right)}\right).\end{aligned} \tag{8.100}$$

Clearly for $\gamma = 0$ the above expression reduces to Eq. (8.82). That is $p_{\mathrm{guess}}(\gamma = 0, d, |\phi_{jl}\rangle) = p_{\mathrm{guess}}^{\max}(\gamma = 0, d)$, since the states for which we have evaluated $p_{\mathrm{guess}}(\gamma, d)$ above are the optimal states for $\gamma = 0$. Note that $A^2 = p_{\mathrm{guess}}^{\max}(\gamma = 0, d)$ and so it is easy to see that for $\gamma = 0$ the optimal measurement is:

$$M_j = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad M_l = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \qquad M_k = 0, \qquad \forall\, k \in \mathscr{P}. \tag{8.101}$$

We can also see that for the game with $d = 2$, the two cases $j = 0, l = 1$ and $j = 1, l = 0$ correspond to the two optimal states for all $\gamma \in [0,1]$. Hence, for these cases the above equation reduces to Eq. (8.49).

Lemma 8.6.4. *There exist states for which* $p_{\text{guess}}(\gamma_1, d, |\phi\rangle) > p_{\text{guess}}(\gamma_2, d, |\phi\rangle) > p^{\max}_{\text{guess}}(\gamma = 0, d)$*, for* $\gamma_1 > \gamma_2 > 0, \forall\, d \geq 2$.

Proof. Consider all input states of the form $|\phi_{jl}\rangle = c\left(|j\rangle + \omega^{jl} F^{\dagger}|l\rangle\right)$ such that $\frac{j^2-l^2}{d} \notin \mathbb{Z}$ and $\forall\, d \geq 2$. Then firstly, $j \neq l$ and so the guessing probability corresponding to those states is given by Eq. (8.100) and secondly the coefficient in front of γ^2 is positive. Hence in these cases $p_{\text{guess}}(\gamma, d, |\phi_{jl}\rangle)$ is monotonically increasing in $\gamma \in [0,1], \forall\, d \geq 2$. Hence, $\forall\, d \geq 2$, for all input states $|\phi_{jl}\rangle = c\left(|j\rangle + \omega^{jl} F^{\dagger}|l\rangle\right)$ such that $\frac{j^2-l^2}{d} \notin \mathbb{Z}$ we have $p_{\text{guess}}(\gamma_1, d, |\phi_{jl}\rangle) > p_{\text{guess}}(\gamma_2, d, |\phi_{jl}\rangle) > p^{\max}_{\text{guess}}(\gamma = 0, d)$, for $\gamma_1 > \gamma_2 > 0$.

□

Theorem 8.4.3 follows directly from the above lemma by noting that $p^{\max}_{\text{guess}}(\gamma, d) \geq p_{\text{guess}}(\gamma, d, |\phi\rangle)$, for all $\gamma \in [0,1]$, $d \geq 2$ and for all states $|\phi\rangle$.

One can also see that for the input states $|\phi_{jl}\rangle = c\left(|j\rangle + \omega^{jl} F^{\dagger}|l\rangle\right)$ with $j \neq l$ but with $\frac{j^2-l^2}{d} \in \mathbb{Z}$, Eq. (8.100) reduces to $p_{\text{guess}}(\gamma, d, |\phi_{jl}\rangle) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right) = p^{\max}_{\text{guess}}(\gamma = 0, d)$. That is for those states $p_{\text{guess}}(\gamma, d, |\phi_{jl}\rangle)$ stays constant in γ for all d.

8.6.4. COHERENCE AND QUANTUM CORRELATIONS

To give a deeper insight into the relation between the guessing probability and the coherence γ, we also look at the correlations between the registers B, R and P (the initial purification of R), at times t_1, t_2 and t_3 in Fig. 8.2 (in the main article). Specifically, we focus on the two-dimensional game with optimal input states. We then quantify the arising correlations using min-entropy and the results are depicted in Fig. 8.4. It needs to be noted that independently of the dimension of our game, Bob's requirements for perfect guessing are perfect classical correlations between R and X, the classical register denoting the measurement outcome after Alice has performed her measurement on the system B at time t_3 in Fig. 8.2. However, classical correlations are basis dependent and effectively the measurement of Alice involves two mutually unbiased bases. Hence it is impossible to have perfect guessing with just classically correlating the two systems before the measurement. From the perspective of the quantum circuit in Fig. 8.2, those perfect classical correlations that arise after the conditional Fourier transform will never be perfectly aligned with the measurement basis of Alice (standard basis). As a result, even if the system is classically perfectly correlated before the measurement, the correlations are no longer maximal after the measurement on B. For two-dimensional game, this can be seen in Fig. 8.4 where for $\gamma = 0$, $H_{\min}(B|R) = 0$, but $H_{\min}(X|R) > 0$. The advantage for Bob coming from the quantum coherence in register R and the resulting quantum correlations is that for maximal entanglement (which is possible if $d = 2$), independently of the basis in which the system B has been measured, the outcomes of that measurement are maximally correlated with the state of the register R. Hence, if the two systems become maximally entangled ($H_{\min}(B|R) = -1$ for $\gamma = 1$), then the post-measurement state becomes classically maximally correlated ($H_{\min}(X|R) = 0$) enabling perfect guessing.

8.6.5. CONDITIONAL MIN-ENTROPIES FOR THE TWO-DIMENSIONAL GAME

The controlled Fourier transform in the circuit in Fig. 8.2 (in the main article) results in (quantum) correlations between the two systems B and R. These correlations are

exploited by Bob in order to guess the measurement outcome on the state ρ_B. However, this measurement has a destructive effect on these correlations. Here we quantify this destructive effect of the measurement using min-entropy. The conditional min-entropy will be calculated using the definition presented in [30]. Firstly let us define a correlation measure:

$$q_{\text{corr}}(B|R) = d \max_{\mathscr{E}} F\left((\mathscr{E}_R \otimes \mathbb{I}_B)(\rho_{RB}), |\Psi\rangle\langle\Psi|_{RB}\right)^2, \tag{8.102}$$

where F is fidelity defined using the trace norm as $F(\rho,\sigma) = ||\sqrt{\rho}\sqrt{\sigma}||_1$ (when one of the states is pure, that is when $\sigma = |\Psi\rangle\langle\Psi|$, the fidelity reduces to $F(\rho,\sigma) = \sqrt{\langle\Psi|\rho|\Psi\rangle}$), d is the dimension of subsystem B, $\mathscr{E}$ is a local operation described by a trace-preserving completely positive map and $|\Psi\rangle$ is a maximally entangled state (note that $q_{\text{corr}}(B|R)$ is independent of which maximally entangled state we use, since all such states are the same up to a unitary rotation on one of the qudits; this rotation can always be compensated on ρ_{RB} by the corresponding rotation on system R as part of the local operation $\mathscr{E}$). Then one can calculate the conditional min-entropy of a quantum-quantum (qq) state as $H_{\min}(B|R) = -\log(q_{\text{corr}}(B|R))$. Note that for classical-quantum (cq) states, $q_{\text{corr}}(X|R)$ becomes the guessing probability $p_{\text{guess}}(X|R)$ (here X denotes the classical subsystem) [30].

We are interested in the relation between the min-entropy $H_{\min}(B|R)$ of a qq-state (the min-entropy of the input state ρ_B before Alice's measurement, given access to R) and the min-entropy $H_{\min}(X|R)$ of the cq-state after the measurement has been performed (the min-entropy of the classical outcome X after Alice's measurement, given access to ρ_R). For that purpose we will investigate the tightness of the inequality derived in [15]:

$$H_{\min}(X|R) \leq H_{\min}(B|R) + \log(d), \tag{8.103}$$

where d is the dimension of the outcome space. This inequality tells us that for two-dimensional states, the increase of the conditional min-entropy due to the measurement cannot exceed 1.

For $d = 2$ we will now calculate both of those entropies explicitly starting with $H_{\min}(B|R)$. In our calculation let us pick one of the two states which give us the maximum guessing probability for all values of γ, namely $|\phi_{10}\rangle$ which in the Bloch sphere representation can be expressed as $(c_x, c_y, c_z) = \left(\frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}\right)$ [one can analogously show that the other state $|\phi_{01}\rangle$ or equivalently $(c_x, c_y, c_z) = \left(-\frac{1}{\sqrt{2}}, 0, \frac{1}{\sqrt{2}}\right)$ will give exactly the same $H_{\min}(B|R)$]. For this input state, the overall state $\rho'_{RB}(\gamma, d = 2, |\phi\rangle)$ before the measurement at time t_2 in Fig. 8.2 is:

$$\begin{aligned}\rho'_{RB}(\gamma, d = 2, |\phi\rangle) = \frac{1}{4}\Bigg(&|0\rangle\langle 0|_R \otimes (\mathbb{I} + \frac{1}{\sqrt{2}}(\sigma_x - \sigma_z)) + \gamma[|0\rangle\langle 1|_R \otimes (H_B + \frac{1}{\sqrt{2}}(\sigma_x - \sigma_z)H_B) \\ &+ |1\rangle\langle 0|_R \otimes (H_B + \frac{1}{\sqrt{2}}H_B(\sigma_x - \sigma_z))] + |1\rangle\langle 1|_R \otimes (\mathbb{I} + \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x))\Bigg).\end{aligned} \tag{8.104}$$

We can now diagonalise this state so that we obtain:

$$\rho'_{RB}(\gamma, d = 2, |\phi\rangle) = \frac{1+\gamma}{2}|\psi_1\rangle\langle\psi_1| + \frac{1-\gamma}{2}|\psi_2\rangle\langle\psi_2|, \tag{8.105}$$

where the eigenstates written in their Schmidt bases are:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0'\rangle_R|1\rangle_B + |1'\rangle_R|0\rangle_B)\,, \tag{8.106}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0''\rangle_R|1\rangle_B + |1''\rangle_R|0\rangle_B)\,. \tag{8.107}$$

The Schmidt bases: $\{|0'\rangle, |1'\rangle\}$ and $\{|0''\rangle, |1''\rangle\}$ are given by:

$$|0'\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2-\sqrt{2}}}|0\rangle - \frac{1}{\sqrt{2+\sqrt{2}}}|1\rangle\right), \tag{8.108}$$

$$|1'\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2+\sqrt{2}}}|0\rangle + \frac{1}{\sqrt{2-\sqrt{2}}}|1\rangle\right), \tag{8.109}$$

$$|0''\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2-\sqrt{2}}}|0\rangle + \frac{1}{\sqrt{2+\sqrt{2}}}|1\rangle\right), \tag{8.110}$$

$$|1''\rangle = \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2+\sqrt{2}}}|0\rangle - \frac{1}{\sqrt{2-\sqrt{2}}}|1\rangle\right). \tag{8.111}$$

The states $|\psi_1\rangle$ and $|\psi_2\rangle$ are mutually orthogonal maximally entangled states. To calculate $H_{\min}(B|R)$ we use the formulation of the min-entropy in terms of the semi-definite programmes, as expressed in [30]. The primal, as stated before, is $H_{\min}(B|R) = -\log(q_{\text{corr}}(B|R))$ where $q_{\text{corr}}(B|R)$ is given in Eq. (8.102). The dual problem is:

$$H_{\min}(B|R) = -\log \min_{\substack{\sigma_R \geq 0 \\ \sigma_R \otimes \mathbb{I}_B \geq \rho_{RB}}} \text{Tr}(\sigma_R)\,. \tag{8.112}$$

For the primal programme, let us consider a local transformation $\mathscr{E}$ acting on subsystem R which performs a rotation such that the state will now be diagonal in the basis that includes $|\Psi\rangle_{RB}$, with maximal probability in this mixture corresponding to the state $|\Psi\rangle_{RB}$. This feasible solution gives:

$$\max_{\mathscr{E}} F\left((\mathscr{E}\otimes\mathbb{I}_B)(\rho'_{RB}), |\Psi\rangle\langle\Psi|_{RB}\right) \geq \sqrt{\frac{1+\gamma}{2}}\,. \tag{8.113}$$

Hence:

$$q_{\text{corr}}(B|R) \geq 1+\gamma\,, \tag{8.114}$$

and so:

$$H_{\min}(B|R) = -\log q_{\text{corr}}(B|R) \leq -\log(1+\gamma)\,. \tag{8.115}$$

Similarly, for the dual programme, let us consider a matrix $\sigma_R = \left(\frac{1+\gamma}{2}\right)\mathbb{I}_R \geq 0$. Then $\sigma_R \otimes \mathbb{I}_B = \left(\frac{1+\gamma}{2}\right)\mathbb{I}_{4\times 4}$. Clearly $\sigma_R \otimes \mathbb{I}_B \geq \rho'_{RB}$, so that we obtain:

$$H_{\min}(B|R) \geq -\log \text{Tr}[\sigma_R] = -\log(1+\gamma)\,. \tag{8.116}$$

Combining the results from the primal and dual programmes allows us to conclude that $H_{\min}(B|R) = -\log(1+\gamma)$ for all $\gamma \in [0,1]$.

The min-entropy after the measurement is related to the guessing probability as $H_{\min}(X|R) = -\log p_{\text{guess}}(X|R)$ and so it is:

$$H_{\min}(X|R) = -\log\left(\frac{1}{2}\left(\frac{\sqrt{2+2\gamma^2}}{2}+1\right)\right) = 1-\log\left(\frac{\sqrt{2+2\gamma^2}}{2}+1\right). \tag{8.117}$$

Hence:

$$H_{\min}(X|R) - H_{\min}(B|R) = 1-\log\left(\frac{\sqrt{2+2\gamma^2}+2}{2(1+\gamma)}\right). \tag{8.118}$$

We then see that $H_{\min}(X|R) - H_{\min}(B|R)$ monotonically increases with $\gamma \in [0,1]$ until it reaches the value of one for $\gamma = 1$. Hence the inequality (8.103) is tight for $\gamma = 1$ which corresponds to the greatest possible increase of the conditional min-entropy during the measurement performed on a qubit (see Fig. 8.4).

We also compute the min-entropy $H_{\min}(P|R)$ to get some insight into the correlations between basis register R and its purification P as a function of γ. For that purpose, let us redefine the way we label the states of registers R and P with respect to the labelling and notation used in Eqs. (8.5) to (8.9). Specifically, let $|\alpha\rangle, |\beta\rangle$ be now the two states of the entire register P (joint states of all the environmental subsystems E_i that are in P) corresponding to the states $|0\rangle, |1\rangle$ of the register R respectively. The real parameter $\gamma \in [0,1]$, that quantifies the amount of information that P holds about R, satisfies now:

$$\langle\alpha|\beta\rangle = \gamma, \tag{8.119}$$

so that the joint state of registers R and P can be written as:

$$|\xi(\gamma)\rangle_{RP} = \frac{1}{\sqrt{2}}(|0\rangle_R|\alpha\rangle_P + |1\rangle_R|\beta\rangle_P). \tag{8.120}$$

Note that the state $|\xi(\gamma)\rangle_{RP}$ defined in Eq. (8.120) is pure. Then $H_{\min}(P|R) = -\log(\text{Tr}[\sqrt{\rho_R}])^2$ $= -\log(\text{Tr}[\sqrt{\rho_P}])^2$. Note that $\text{Tr}[\sqrt{\rho_R}] = \text{Tr}[\sqrt{\rho_P}]$ is the sum of the Schmidt coefficients of the state $|\xi(\gamma)\rangle_{RP}$. The eigenvalues of $\rho_R(\gamma)$ defined in Eq. (8.6) (with real and positive γ) are $\lambda_1 = \frac{1+\gamma}{2}$ and $\lambda_2 = \frac{1-\gamma}{2}$. Hence:

$$H_{\min}(P|R) = -\log\left(\sqrt{\frac{1+\gamma}{2}} + \sqrt{\frac{1-\gamma}{2}}\right)^2 = -\log(1+\sqrt{1-\gamma^2}). \tag{8.121}$$

Similarly we calculate $H_{\min}(P|R)$ after the conditional Fourier transform in Fig. 8.2 has been applied, to quantify the effect of this operation on the correlations between R and P. Firstly we need to calculate ρ_{RP} at time t_2. That is, again following the circuit in Fig. 8.2 but now including the purification P, the initial state at time t_1 is $|\Phi(\gamma,d,|\phi\rangle)\rangle_{RPB} = |\xi(\gamma)\rangle_{RP} \otimes |\phi\rangle_B$. Then the state at time t_2 is $|\Phi'(\gamma,d,|\phi\rangle)\rangle_{RPB} = U|\Phi(\gamma,d,|\phi\rangle)\rangle_{RPB}$, where U is given by:

$$U = |0\rangle\langle 0|_R \otimes \mathbb{I}_P \otimes \mathbb{I}_B + |1\rangle\langle 1|_R \otimes \mathbb{I}_P \otimes F_B. \tag{8.122}$$

8

Hence:

$$|\Phi'(\gamma,d,|\phi\rangle)\rangle_{RPB} = \frac{1}{\sqrt{2}}(|0\rangle_R|\alpha\rangle_P|\phi\rangle_B + |1\rangle_R|\beta\rangle_P F_B|\phi\rangle_B)\,, \tag{8.123}$$

We can now trace out B.

$$\begin{aligned}\rho'_{RP}(\gamma,d,|\phi\rangle) = \frac{1}{2}\Big(&|0\rangle\langle 0|_R\otimes|\alpha\rangle\langle\alpha|_P + \langle\phi|F^\dagger|\phi\rangle|0\rangle\langle 1|_R\otimes|\alpha\rangle\langle\beta|_P \\ &+ \langle\phi|F|\phi\rangle|1\rangle\langle 0|_R\otimes|\beta\rangle\langle\alpha|_P + |1\rangle\langle 1|_R\otimes|\beta\rangle\langle\beta|_P\Big)\,.\end{aligned} \tag{8.124}$$

Now let us consider the two-dimensional game again with $|\phi\rangle_B$ being one of the two states that achieve $p^{\max}_{\text{guess}}(\gamma,d=2)$ for all $\gamma\in[0,1]$ (these are the states $|\phi\rangle=|\phi_{10}\rangle$ and $|\phi\rangle=|\phi_{01}\rangle$). Then $\langle\phi|F|\phi\rangle=0$, so the state on R and P at t_2 is:

$$\rho_{RP}(\gamma,d=2,|\phi\rangle) = \frac{1}{2}\left(|0\rangle\langle 0|_R\otimes|\alpha\rangle\langle\alpha|_P + |1\rangle\langle 1|_R\otimes|\beta\rangle\langle\beta|_P\right). \tag{8.125}$$

To calculate $H_{\min}(P|R)$ we again use the formulation of min-entropy in terms of the semi-definite programmes [30]. For the dual programme in Eq. (8.112), note that ρ_{RP} has eigenvalues $\{\frac{1}{2},\frac{1}{2},0,0\}$. Hence $\sigma_R=\dfrac{\mathbb{I}_R}{2}$ clearly satisfies the constraints, as then $\sigma_R\otimes\mathbb{I}_P=\dfrac{\mathbb{I}_{4\times4}}{2}$ and so $\sigma_R\geq 0$ and $\sigma_R\otimes\mathbb{I}_P\geq\rho_{RP}$. The corresponding solution is $H_{\min}(P|R)\geq 0$. Similarly, in Eq. (8.102), let us consider $\mathscr{E}$ to be a quantum channel acting on R with Krauss operators $\{M_i\}$, where $M_0=|\alpha\rangle\langle 0|$ and $M_0=|\beta\rangle\langle 1|$. Then:

$$\rho'_{RP} = (\mathscr{E}\otimes\mathbb{I}_P)(\rho_{RP}) = \frac{1}{2}\left(|\alpha\rangle\langle\alpha|_R\otimes|\alpha\rangle\langle\alpha|_P + |\beta\rangle\langle\beta|_R\otimes|\beta\rangle\langle\beta|_P\right). \tag{8.126}$$

Since $\langle\alpha|\beta\rangle=\gamma$, we have $\langle\alpha^\perp|\beta\rangle=e^{i\phi}\sqrt{1-\gamma^2}$ for some phase ϕ, where $\langle\alpha|\alpha^\perp\rangle=0$. Now, let $|\Psi\rangle_{RP}$ be a maximally entangled state of the form $|\Psi\rangle_{RP}=\frac{1}{\sqrt{2}}(|\alpha\rangle_R|\alpha\rangle_P+e^{2i\phi}|\alpha^\perp\rangle_R|\alpha^\perp\rangle_P)$. Therefore:

$$\begin{aligned}q_{\text{corr}}(P|R) &= 2F\left(\rho'_{RP},|\Psi\rangle\langle\Psi|_{RP}\right)^2\\ &= \frac{1}{2}\left(\langle\alpha|_R\langle\alpha|_P + e^{-2i\phi}\langle\alpha^\perp|_R\langle\alpha^\perp|_P\right)(|\alpha\rangle\langle\alpha|_R\otimes|\alpha\rangle\langle\alpha|_P\\ &+|\beta\rangle\langle\beta|_R\otimes|\beta\rangle\langle\beta|_P)\left(|\alpha\rangle_R|\alpha\rangle_P + e^{2i\phi}|\alpha^\perp\rangle_R|\alpha^\perp\rangle_P\right)\\ &= \frac{1}{2}\left(1+\left|\langle\alpha|\beta\rangle\right|^4+\left|\langle\alpha^\perp|\beta\rangle\right|^4+e^{2i\phi}(\langle\alpha|\beta\rangle)^2(\langle\beta|\alpha^\perp\rangle)^2+e^{-2i\phi}(\langle\beta|\alpha\rangle)^2(\langle\alpha^\perp|\beta\rangle)^2\right)\\ &= \frac{1}{2}\left(1+\gamma^4+\left(1-\gamma^2\right)^2+2\gamma^2\left(1-\gamma^2\right)\right)\\ &= 1\,.\end{aligned} \tag{8.127}$$

Hence the corresponding solution is $H_{\min}(P|R)\leq 0$. Therefore combining the results from the primal and dual programmes we conclude that $H_{\min}(P|R)=0$ for all $\gamma\in[0,1]$.

REFERENCES

[1] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing,* International Conference on Computer System and Signal Processing, IEEE (1984).

[2] W. Heisenberg, *Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik,* Zeitschrift für Physik **43**, 172 (1927).

[3] E. H. Kennard, *Zur Quantenmechanik einfacher Bewegungstypen,* Zeitschrift fur Physik **44**, 326 (1927).

[4] H. P. Robertson, *The uncertainty principle,* Physical Review **34**, 163 (1929).

[5] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, *The uncertainty principle in the presence of quantum memory,* Nature Physics **6** (2010), 10.1038/nphys1734.

[6] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, *Entropic uncertainty relations and their applications,* Reviews of Modern Physics **89**, 015002 (2017).

[7] R. Ionicioiu and D. R. Terno, *Proposal for a quantum delayed-choice experiment,* Physical Review Letters **107**, 230406 (2011).

[8] L. C. Céleri, R. M. Gomes, R. Ionicioiu, T. Jennewein, R. B. Mann, and D. R. Terno, *Quantum control in foundational experiments,* Foundations of Physics **44**, 576 (2014).

[9] J. Sánchez-Ruiz, *Improved bounds in the entropic uncertainty and certainty relations for complementary observables,* Physics Letters A **201**, 125 (1995).

[10] M. Berta, P. J. Coles, and S. Wehner, *Entanglement-assisted guessing of complementary measurement outcomes,* Physical Review A **90**, 062127 (2014).

[11] M. J. W. Hall, *Information exclusion principle for complementary observables,* Physical Review Letters **74**, 3307 (1995).

[12] M. Christandl and A. Winter, *Uncertainty, monogamy, and locking of quantum correlations,* IEEE Transactions on Information Theory **51**, 3159 (2005).

[13] J. M. Renes and J.-C. Boileau, *Conjectured strong complementary information tradeoff,* Physical Review Letters **103**, 020402 (2009).

[14] F. Dupuis, O. Fawzi, and S. Wehner, *Entanglement sampling and applications,* IEEE Transactions on Information Theory **61**, 1093 (2015).

[15] M. Berta, O. Fawzi, and S. Wehner, *Quantum to classical randomness extractors,* IEEE Transactions on Information Theory **60**, 1168 (2014).

[16] S. Liu, L.-Z. Mu, and H. Fan, *Entropic uncertainty relations for multiple measurements,* Physical Review A **91**, 042133 (2015).

[17] P. J. Coles, R. Colbeck, L. Yu, and M. Zwolak, *Uncertainty relations from simple entropic properties,* Physical Review Letters **108**, 210405 (2012).

[18] R. L. Frank and E. H. Lieb, *Extended quantum conditional entropy and quantum uncertainty inequalities,* Communications in Mathematical Physics **323**, 487 (2013).

[19] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, *Position-momentum uncertainty relations in the presence of quantum memory,* Journal of Mathematical Physics **55**, 122205 (2014).

[20] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, *Information-theoretic treatment of tripartite systems and quantum channels,* Physical Review A **83**, 062338 (2011).

[21] S. L. Luo, *Quantum versus classical uncertainty,* Theoretical and Mathematical Physics **143**, 681 (2005).

[22] K. Korzekwa, M. Lostaglio, D. Jennings, and T. Rudolph, *Quantum and classical entropic uncertainty relations,* Physical Review A **89**, 042122 (2014).

[23] W. H. Zurek, *Decoherence, einselection, and the quantum origins of the classical,* Reviews of Modern Physics **75**, 715 (2003).

[24] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).

[25] C. W. Helstrom, *Quantum detection and estimation theory* (Academic Press New York, 1976).

[26] M. Curty, X. Ma, H.-K. Lo, and N. Lütkenhaus, *Passive sources for the Bennett-Brassard 1984 quantum-key-distribution protocol with practical signals,* Physical Review A **82**, 052325 (2010).

[27] J.-S. Tang, Y.-L. Li, C.-F. Li, and G.-C. Guo, *Revisiting Bohr's principle of complementarity with a quantum device,* Physical Review A **88**, 014103 (2013).

[28] F. Kaiser, T. Coudreau, P. Milman, D. B. Ostrowsky, and S. Tanzilli, *Entanglement-enabled delayed-choice experiment,* Science **338**, 637 (2012).

[29] A. Peruzzo, P. Shadbolt, N. Brunner, S. Popescu, and J. L. O'Brien, *A quantum delayed-choice experiment,* Science **338**, 634 (2012).

[30] R. Konig, R. Renner, and C. Schaffner, *The operational meaning of min- and max-entropy,* IEEE Transactions on Information Theory **55**, 4337 (2009).

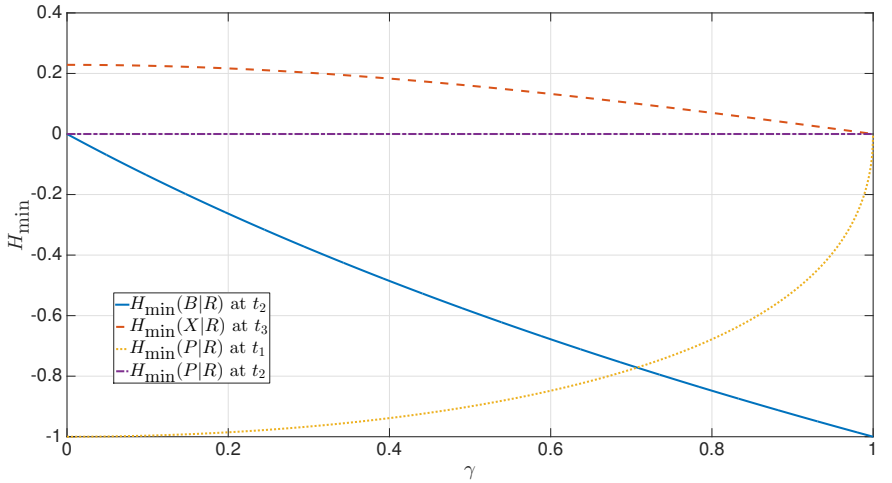

Figure 8.4: Conditional min-entropies as a function of γ for the two-dimensional game ($d = 2$) with Bob's input state $|\phi_{01}\rangle = c(|0\rangle + |-\rangle)$ or $|\phi_{10}\rangle = c(|1\rangle + |+\rangle)$. The blue solid line corresponds to the $H_{\min}(B|R)$ at time t_2 in Fig. 8.2. The red dashed line shows $H_{\min}(X|R)$ at time t_3 after Alice's measurement, where the state is averaged over all the outcomes, as Bob does not have access to the measurement result. The yellow dotted line corresponds to $H_{\min}(P|R)$ at time t_1 and hence shows the initial quantum correlations between R and its purification P. The correlations between those systems at time t_2 are illustrated by the purple dash-dotted flat line $H_{\min}(P|R) = 0$. By comparing the blue solid and red dashed lines, one can see that for $\gamma = 1$ the increase of the conditional entropy between $H_{\min}(B|R)$ and $H_{\min}(X|R)$ due to the measurement on B is the greatest possible, that is, it is equal to 1. The reason is that the measurement is the most destructive in this case, as it destroys all the quantum correlations of a maximally entangled state. On the other end of the spectrum, if $\gamma = 0$, there are no quantum correlations between B and R present and so the measurement has a relatively small influence on the system. It only affects the classical correlations, which are not aligned with the standard basis in which the measurement performed by Alice takes place (the final measurement in the circuit in Fig. 8.2). Hence, in this case the increase of conditional entropy is small. Comparing the yellow dotted and blue solid lines we see that decreasing the amount of entanglement between P and R results in the increase in the amount of entanglement between B and R that can be generated using the controlled Fourier transform. Finally, from the flat purple dash-dotted line we see that independently of the coherence of R and its initial correlations with P, the correlations between those two systems at time t_2 can be only classical. All the above entropies are derived in Appendix 8.6.5.

9

CONCLUSION

9.1. SUMMARY OF RESULTS

We summarize the main results of this thesis as follows:

- We have established that current quantum technologies already possess the capabilities for demonstrating efficient generation of long-distance entanglement and a proof of principle quantum repeater. In particular we have verified these statements for NV-centre platform where we have observed that the necessary property of such experimental setups is the optical interface of the memories with high photon extraction efficiency. It is expected that the demonstration of these parameters can be achieved by embedding the quantum memory system within an optical cavity to enhance the emission into the desired zero phonon line and into the preferential directional mode.

- We have examined the performance of multiplexed entanglement generation using quantum memories with a single-optical interface and multiplexed memory qubits. We have found that for the NV centre platform the gate time of transferring the quantum state between the communication qubit and the memory qubit plays a crucial role in making such multiplexing possible. For currently achievable times of such a swap gate which still allows for maintaining high coherence of the memory qubits for hundreds of subsequent entanglement generation attempts, using more than one such multiplexed memory will no longer provide any benefit. This shows that the ability to perform fast local gates at the memory nodes will play a crucial role in future quantum repeater networks based on such multiplexing schemes.

- We have established two crucial methods for quantum repeater networks that allow for counteracting the effect of noise in the system. The first one is the cut-off on the storage time which enables overcoming the problem of decoherence in the quantum memories at the expense of reducing the yield of the protocol. We find that optimising over this cut-off can not only significantly boost the performance of the studied repeater schemes but for large distances it is even necessary in order to be able to demonstrate a non-zero performance. Moreover, from the implementation perspective, the application of the optimal cut-off corresponds only to adjusting the settings of the devices and hence is much easier to implement than the previously suggested method of optimising the position of the repeater for specific sequential protocols. Secondly, we have shown that for QKD the secret-key rate achievable with our repeater schemes can be significantly enhanced by introducing two-way classical post-processing instead of typically considered one-way error correction. Such a two-way advantage distillation scheme is known to be very efficient in the high-noise regime, which is the regime in which realistic proof of principle repeater schemes operate. In fact we show that for some more complex schemes such advantage distillation is necessary in order to be able to generate any non-zero amount of key. Again, implementation of such a two-way post-processing does not carry any additional cost with respect to the one-way error correction as the entire procedure is implemented in a fully classical part of the protocol.

- We have proposed a general framework for investigating the trade-off between fidelity and probability of success in entanglement distillation and we have provided methods to improve existing distillation schemes. Using this framework, we have demonstrated that specific well-known realistic entanglement distillation schemes that operate on two copies of a two-qubit state and involve only one round of local operations and classical communication are in fact optimal over all LOCC protocols. To be more precise, we observe that they offer the optimal trade-off between the output fidelity and probability of success. This shows that in order to obtain better trade-off between those two figures of merit, it is necessary in those cases to aim for implementation of protocols that can jointly operate on more than two-copies of the input state.

- We have examined the origin of uncertainty in the quantum guessing games modelling specific types of attacks of an eavesdropper in QKD. We have found that a significant part, and in certain cases even all, of the resulting uncertainty is related to the lack of knowledge about the choice of the measured observable. If the eavesdropper could gain access to the quantum information about this choice, they would be able to guess the measurement outcomes with significantly higher probability and even with full certainty for the specific cases, without being detectable in any way. In this way we have demonstrated that it is vital for such quantum information to remain inaccessible to Eve. From a broader perspective we have shown that certain entropic formulations of the preparation aspect of the quantum uncertainty principle do not quantify exclusively the intrinsic quantum uncertainty but also include a classical component related to a lack of information.

9.2. FUTURE OUTLOOK

9.2.1. REMOTE ENTANGLEMENT GENERATION AND FIRST GENERATION QUANTUM REPEATERS WITH OTHER PHYSICAL PLATFORMS

In this thesis we have looked at specific remote entanglement generation and proof of principle repeater schemes and their implementation based on the NV-centre platform. However, the multiplexed remote entanglement generation schemes that we propose in Chapter 4 and the SiSQuaRe repeater scheme could also be applied to other platforms where local nodes consist of multiple qubits with a single optical interface accessible at any given moment.

An example of such a platform could consist of multiple ions confined to a single trap [1]. In the corresponding implementation of the SiSQuaRe repeater scheme or the multiplexed remote entanglement generation, one could consider multiple such ions coupled to an optical cavity [2, 3]. Since we want to be able to independently operate on each of the memories and make use of their photonic interface, similarly to the NV based implementation, the memory-photon entanglement generation procedure would need to be conducted in a sequential way. This can be done either by hiding/unhiding the spectator ions during the memory-photon entanglement generation [4] or by combining different atomic isotopes of different resonant frequencies in one trap [5, 6]. For the implementation of the second method it is natural to consider one isotope as a communication qubit with an optical interface and the other memories of different species

as memory qubits as was implemented in [7]. Moreover, this platform also offers a functionality of performing deterministic gates between the ions in a single trap, allowing us to implement a deterministic local Bell measurement and a swap gate between the ions. Hence, we see that effectively the qualitative capabilities of such a trapped ion based system fit exactly within the general requirements of the SiSQuRe scheme and the framework of multiplexed remote entanglement generation analysed in Chapter 4. A significant advantage of this platform is that the interaction between the two ions can be switched on and off on demand, hence completely eliminating the effect of decoherence during storage due to subsequent entanglement generation attempts, which seems to be the dominant source of noise in the NV based implementation.

On the other hand, quantum dots encapsulated in optical cavities seem to be another promising candidate for the implementation of the single-photon scheme for QKD [8, 9]. While their coherence properties are rather limited, the single-photon scheme does not require any quantum storage at all. In fact, as we have discussed in Appendix 7.8.9 in Chapter 7, it is possible to run a prepare-and-measure version of this scheme where Alice and Bob are only required to prepare the desired superposition of the presence and absence of a photon. It has been demonstrated in [10] that quantum dots can indeed act as efficient sources of such single-rail encoded photonic qubits.

In Chapter 4 we have discussed multiplexed remote entanglement generation for experimental platforms utilising a single communication qubit acting as an optical interface and multiple memory qubits used for storage. Although in that chapter we have performed an explicit analysis for the NV platform, we have already noted that other platforms such as trapped ions would also be suitable. However, we have already observed that the duration of the swap gate between the communication and the memory qubit in realistic scenarios provides a dominant limitation to the usability of those additional quantum memories in such multiplexing schemes. In principle this problem could be mitigated by coupling the communication and the memory qubits more strongly in order to achieve faster gates and at the same time mitigating the resulting decoherence on the memory by e.g. utilising encodings based on decoherence protected subspaces of multiple such memories [11, 12]. Nevertheless, the number of multiplexed quantum memories that will allow for deterministic transfer of the quantum state from a single communication qubit realistically will not exceed more than a few storage qubits.

A much more unconstrained approach to multiplexing seems to be possible with quantum memories based on atomic ensembles [13]. These platforms enable implementations of a multimode quantum memory. Multiplexing in multiple degrees of freedom, such as temporal [14, 15], spectral [16] or spatial [17], has already been demonstrated in such ensemble based systems. Moreover, combination of all those multiplexing strategies in a single setup has also been demonstrated [18]. Combining such different degrees of freedom could offer a highly multiplexed quantum memory with large number of parallel storage modes enabling efficient remote entanglement generation. A significant limitation of remote entanglement generation schemes using atomic ensemble based memories in comparison to the schemes based on NV-centres or individual ions is that many of them require use of sources of entangled photons. These sources at the moment have very low efficiency and non-negligible probability of multi-photon emission events introducing significant amount of noise [19, 20].

Nevertheless, access to a large number of modes reaching orders of $10^5 - 10^6$ together with photon number resolving detectors [21, 22] or application of near-deterministic sources of entangled photons, which could be achieved using e.g. quantum dots as single-photon sources [23], could overcome this problem. However, such repeater schemes suffer significantly from the necessity of implementing entanglement swapping in a probabilistic way using optical Bell state measurement and the efficiency of such a measurement is fundamentally restricted to 50% [24]. While adding additional photons as ancillary resources can increase that probability [25–27], the required number of such resources does not make this method a realistic scheme for achieving a near deterministic performance. Hence, investigating cross platform architectures that could benefit from both multimode quantum memories and from the functionality of deterministic multi-qubit gates could provide a feasible solution to the above discussed problems. In particular, possible techniques of overcoming the limitations of the linear-optics based Bell-measurement would involve transferring quantum states from the multimode quantum memories to either NV-centres or trapped ions/atoms where a deterministic entanglement swapping operation could be performed. Another ambitious method would be to use a deterministic Bell-state analyser [28]. Such cross-platform integration techniques could allow for designing more efficient repeater schemes benefiting from the advantages of all those physical systems at the same time.

9.2.2. ENTANGLEMENT DISTILLATION

In Chapter 5 we have developed a framework and methods for evaluating the trade-off between fidelity and probability of success in entanglement distillation. We have also applied this framework to examine the optimality of some existing distillation schemes, mostly for the case when two input copies of a two-qubit state are distilled to such a single copy.

It would be now interesting to investigate such trade-offs for the protocols that distil from three to one copy using MX operations. One could then compare the performance of such protocols to the upper bounds obtained using our numerical package. A simple distillation protocol that makes use of such three copies has been analysed in [29].

In the larger context, the general framework for deriving distillation protocols that operate on a larger number of copies of two-qubit states and consider operations that effectively permute Bell states was proposed in [30]. In [31], on the other hand, the authors take a more "bottom-up" approach and construct optimised entanglement distillation circuits from optimal subcircuits when operating on Bell-diagonal states.

For particular experimentally relevant scenarios one might want to follow more specific techniques. It would be particularly very useful to investigate generalisations of the EPL scheme to a higher number of copies of a two-qubit state such that effectively all of them are correlated in phase, analogously to the state in Eq. (5.46) in Chapter 5 for two copies. One way of performing such a generalisation could possibly be achieved by considering techniques based on hashing.

9.2.3. HIGHER GENERATION QUANTUM REPEATERS

We have already discussed in Section 3.2.3 in Chapter 3 the so-called third generation of quantum repeaters where the requirement on the coherence time of quantum memo-

ries becomes significantly reduced to just the local processing time. However, most of the proposed codes such as parity codes require the ability to perform high-quality operations on a very large number of memories at the same time [32, 33]. The possible solution would be to remove the requirement on any quantum memories completely, as has been proposed in [34, 35] where the only quantum systems used are large photonic claster states. Effectively, the quantum memories are then simulated using the large photonic tree code encodings that protect the logical qubits against photon loss during transmission and allow for loss-tolerant measurements on them. Generation of such states in a near deterministic fashion is in principle feasible using e.g. quantum dots in cavities as proposed in [36], however the needed sizes of such cluster states place very high requirements on the number of such single photon sources that would need to be used in a practical scenario.

Another possible third generation repeater could make use of the so-called bosonic codes, where the quantum state is encoded in a subspace of a harmonic oscillator, specifically in the Fock space of a photonic mode [37–39]. Multiple classes of such codes have been proposed with superconducting circuits being the most promising platform for generating such bosonic codes. However, this platform operates in the microwave domain so an efficient way of converting photons from microwave to optical domain would be necessary in order to be able to use such generated encoded states for quantum communication applications [40].

9.2.4. 2-D QUANTUM NETWORK

While a large number of proposals exist for an efficient repeater chain, not much investigation has been devoted to more complex networks which involve more than two end-node parties. However, a practical quantum internet should allow a large number of parties to perform various communication tasks across such a network at the same time and often involving more than two parties in each of those individual tasks. In such scenarios new questions arise that do not have a corresponding counterpart in a simple repeater chain case. One of such issues is the fact that certain centrally localised nodes and links will be in general used much more frequently than the end links connecting individual users to the network. This asymmetry suggests the possibility that the optimal repeater architecture might make simultaneous use of multiple physical platforms, e.g. faster remote entanglement generation schemes might need to be utilised between the central nodes even at the expense of lower quality of the generated entanglement while the links connecting the end users could make use of other platforms for which higher quality entanglement is produced possibly at a much slower rate. In general, optimising both the network topology and the network architecture connecting a fixed number of users is a very challenging task.

Another important question in such a 2-D network relates to routing quantum entanglement [41]. If the network offers a possibility of using multiple paths to generate entanglement between two or more users, it is a big challenge to find an optimal way of generating entanglement across those paths and connecting it in such a way as to allow for efficient use of all the connections for multiple user pairs (or higher number of users performing a joint task) at the same time. This question becomes even more challenging, when one considers the fact that most of the nodes in the network will in general

only have access to a very limited amount of knowledge regarding the existing entanglement connections across the network at any given moment. This is because updating all the nodes about the status of the network takes time and the required amount of communication could become overwhelming, even for the corresponding classical network.

REFERENCES

[1] C. Monroe and J. Kim, *Scaling the ion trap quantum processor,* Science **339**, 1164 (2013).

[2] M. Steiner, H. M. Meyer, C. Deutsch, J. Reichel, and M. Köhl, *Single ion coupled to an optical fiber cavity,* Physical Review Letters **110**, 043003 (2013).

[3] T. Northup and R. Blatt, *Quantum information transfer using photons,* Nature Photonics **8**, 356 (2014).

[4] B. Casabone, A. Stute, K. Friebe, B. Brandstätter, K. Schüppert, R. Blatt, and T. Northup, *Heralded entanglement of two ions in an optical cavity,* Physical Review Letters **111**, 100505 (2013).

[5] C. Ballance, V. Schäfer, J. P. Home, D. Szwer, S. C. Webster, D. Allcock, N. M. Linke, T. Harty, D. A. Craik, D. N. Stacey, *et al.*, *Hybrid quantum logic and a test of bell's inequality using two different atomic isotopes,* Nature **528**, 384 (2015).

[6] T. R. Tan, J. P. Gaebler, Y. Lin, Y. Wan, R. Bowler, D. Leibfried, and D. J. Wineland, *Multi-element logic gates for trapped-ion qubits,* Nature **528**, 380 (2015).

[7] I. Inlek, C. Crocker, M. Lichtman, K. Sosnova, and C. Monroe, *Multispecies trapped-ion node for quantum networking,* Physical Review Letters **118**, 250502 (2017).

[8] A. Delteil, Z. Sun, W. B. Gao, E. Togan, and S. Faelt, *Generation of heralded entanglement between distant hole spins,* Nature Physics **12**, 218 (2016).

[9] R. Stockill, M. Stanley, L. Huthmacher, E. Clarke, M. Hugues, A. Miller, C. Matthiesen, C. Le Gall, and M. Atatüre, *Phase-tuned entangled state generation between distant spin qubits,* Physical Review Letters **119**, 010503 (2017).

[10] J. Loredo, C. Antón, B. Reznychenko, P. Hilaire, A. Harouri, C. Millet, H. Ollivier, N. Somaschi, L. De Santis, A. Lemaître, *et al.*, *Generation of non-classical light in a photon-number superposition,* arXiv preprint arXiv:1810.05170 (2018).

[11] A. Reiserer, N. Kalb, M. S. Blok, K. J. van Bemmelen, T. H. Taminiau, R. Hanson, D. J. Twitchen, and M. Markham, *Robust quantum-network memory using decoherence-protected subspaces of nuclear spins,* Physical Review X **6**, 021040 (2016).

[12] N. Kalb, P. Humphreys, J. Slim, and R. Hanson, *Dephasing mechanisms of diamond-based nuclear-spin memories for quantum networks,* Physical Review A **97**, 062330 (2018).

[13] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, *Quantum repeaters based on atomic ensembles and linear optics,* Reviews of Modern Physics **83**, 33 (2011).

[14] M. Bonarota, J. Le Gouët, and T. Chaneliere, *Highly multimode storage in a crystal,* New Journal of Physics **13**, 013013 (2011).

[15] J.-S. Tang, Z.-Q. Zhou, Y.-T. Wang, Y.-L. Li, X. Liu, Y.-L. Hua, Y. Zou, S. Wang, D.-Y. He, G. Chen, *et al., Storage of multiple single-photon pulses emitted from a quantum dot in a solid-state quantum memory,* Nature Communications **6**, 8652 (2015).

[16] N. Sinclair, E. Saglamyurek, H. Mallahzadeh, J. A. Slater, M. George, R. Ricken, M. P. Hedges, D. Oblak, C. Simon, W. Sohler, *et al., Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control,* Physical Review Letters **113**, 053603 (2014).

[17] S.-Y. Lan, A. Radnaev, O. Collins, D. Matsukevich, T. Kennedy, and A. Kuzmich, *A multiplexed quantum memory,* Optics Express **17**, 13639 (2009).

[18] T.-S. Yang, Z.-Q. Zhou, Y.-L. Hua, X. Liu, Z.-F. Li, P.-Y. Li, Y. Ma, C. Liu, P.-J. Liang, X. Li, *et al., Multiplexed storage and real-time manipulation based on a multiple degree-of-freedom quantum memory,* Nature Communications **9**, 3407 (2018).

[19] C. Clausen, F. Bussieres, A. Tiranov, H. Herrmann, C. Silberhorn, W. Sohler, M. Afzelius, and N. Gisin, *A source of polarization-entangled photon pairs interfacing quantum memories with telecom photons,* New Journal of Physics **16**, 093058 (2014).

[20] J. C. Loredo, N. A. Zakaria, N. Somaschi, C. Anton, L. de Santis, V. Giesz, T. Grange, M. A. Broome, O. Gazzano, G. Coppola, I. Sagnes, A. Lemaitre, A. Auffeves, P. Senellart, M. P. Almeida, and A. G. White, *Scalable performance in solid-state single-photon sources,* Optica **3**, 433 (2016).

[21] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, *Rate-loss analysis of an efficient quantum repeater architecture,* Physical Review A **92**, 022357 (2015).

[22] H. Krovi, S. Guha, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, *Practical quantum repeaters with parametric down-conversion sources,* Applied Physics B **122**, 52 (2016).

[23] A. Dousse, J. Suffczyński, A. Beveratos, O. Krebs, A. Lemaître, I. Sagnes, J. Bloch, P. Voisin, and P. Senellart, *Ultrabright source of entangled photon pairs,* Nature **466**, 217 (2010).

[24] J. Calsamiglia and N. Lütkenhaus, *Maximum efficiency of a linear-optical bell-state analyzer,* Applied Physics B **72**, 67 (2001).

[25] W. P. Grice, *Arbitrarily complete bell-state measurement using only linear optical elements,* Physical Review A **84**, 042331 (2011).

[26] F. Ewert and P. van Loock, *3/4-efficient bell measurement with passive linear optics and unentangled ancillae,* Physical Review Letters **113**, 140403 (2014).

[27] S.-W. Lee, K. Park, T. C. Ralph, and H. Jeong, *Nearly deterministic bell measurement for multiphoton qubits and its application to quantum information processing,* Physical Review Letters **114**, 113603 (2015).

[28] J. Borregaard, A. Sørensen, and P. Lodahl, *Quantum networks with deterministic spin-photon interfaces,* arXiv preprint arXiv:1811.08242 (2018).

[29] K. Fujii and K. Yamamoto, *Entanglement purification with double selection,* Physical Review A **80**, 042308 (2009).

[30] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, *Local permutations of products of Bell states and entanglement distillation,* Physical Review A **67**, 022310 (2003).

[31] S. Krastanov, V. V. Albert, and L. Jiang, *Optimized Entanglement Purification,* Quantum **3**, 123 (2019).

[32] W. Munro, A. Stephens, S. Devitt, K. Harrison, and K. Nemoto, *Quantum communication without the necessity of quantum memories,* Nature Photonics **6**, 777 (2012).

[33] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, *Ultrafast and fault-tolerant quantum communication across long distances,* Physical Review Letters **112**, 250501 (2014).

[34] K. Azuma, K. Tamaki, and H.-K. Lo, *All-photonic quantum repeaters,* Nature Communications **6**, 6787 (2015).

[35] M. Pant, H. Krovi, D. Englund, and S. Guha, *Rate-distance tradeoff and resource costs for all-optical quantum repeaters,* Physical Review A **95**, 012304 (2017).

[36] A. Russo, E. Barnes, and S. E. Economou, *Photonic graph state generation from quantum dots and color centers for quantum communications,* Physical Review B **98**, 085303 (2018).

[37] D. Gottesman, A. Kitaev, and J. Preskill, *Encoding a qubit in an oscillator,* Physical Review A **64**, 012310 (2001).

[38] M. H. Michael, M. Silveri, R. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. M. Girvin, *New class of quantum error-correcting codes for a bosonic mode,* Physical Review X **6**, 031006 (2016).

[39] V. V. Albert, K. Noh, K. Duivenvoorden, D. J. Young, R. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. Girvin, *et al.*, *Performance and structure of single-mode bosonic codes,* Physical Review A **97**, 032346 (2018).

[40] M. Zhang, C.-L. Zou, and L. Jiang, *Quantum transduction with adaptive control,* Physical review letters **120**, 020502 (2018).

[41] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha, *Routing entanglement in the quantum internet,* npj Quantum Information **5**, 25 (2019).

ACKNOWLEDGEMENTS

QuTech has been a very stimulating research environment. It has been a great experience to be involved in so many projects and discussions with fellow quantum researchers and friends relating to various topics ranging from theoretical and experimental aspects of quantum communication to more philosophical themes such as interpretations of quantum mechanics.

Firstly, I would like to greatly thank my supervisor Stephanie for providing me an opportunity to conduct a PhD in Quantum Information Theory. I am very thankful for your guidance and the effort you have put in my development. Your supervision over the last four years has enabled me to grow as a scientist and acquire numerous scientific skills that I am sure will play a crucial role in my future scientific endeavours. I am also very grateful for your efforts to introduce me to the Quantum Information community, giving me the opportunity to attend a large number of conferences and summer schools all over the world.

Dzięki Ci Jędrek za Twoja stałą pomoc i mądre porady, szczególnie w chwilach zwątpienia i na początku doktoratu. Jestem Ci bardzo wdzięczny za Twoją cierpliwość, zrozumienie i poczucie humoru. Fajnie było rozmawiać o nauce, życiu i wyglądzie gęsi. Gdybyś tylko nie przykręcał tak bardzo ogrzewania to już w ogóle byłoby super.

Kenneth, heel erg bedankt voor onze samenwerk. Ik kan nog onthouden hoe voor vier jaren wij samen een project over de onuitsprekelijke informatie gedaan hebben. Het hat mij heel veel plezier gegeven, samen de realistische (en ook de onrealistische) parameter regimes voor de kwantum repeaters te onderzoeken. Het was ook heel leuk dat ik met jou mijn Nederlands oefenen kon (ik geloof dat het niet te veel fouten in deze paragraf zijn).

David, thanks a lot for your great support, the numerous discussions and for passing me the vast knowledge about QKD and other aspects of quantum communication. I also very much enjoyed our joint karaoke, and I am again very sorry for the unexplored influence of quantum gravity on classical computers.

Corsin and Nelly, it was great to share with you the first half of my PhD experience in Delft and listen to your stories about Singapore (fortunately I had a chance to verify some of them during the QCMC conference there). I would also like to thank other members of the group from my early times in Delft with whom I very much enjoyed working, TA-ing and discussing common artistic interests: Eddie, Marius and Willem.

It was also a great experience to see myself as a supervisor. Thomas, Roeland, Christopher, Guus, David and Julian, thanks for your trust in my hopefully not too chaotic attempt to help and guide you in your projects. Thomas, thank you also very much for teaching me so much about Julia and Roeland for explaining me the basics of NetSquid, including how to schedule a ping and listen to a pong. David, Julian and Guus, it was a lot of fun to prepare for a Blueprint Hackathon in Lisbon and to partially rediscover

NetSquid after forgetting everything that Roeland had explained to me one year earlier. Guus, I wish you good luck at the beginning of your PhD!

Mark, unsere häufige Diskussionen auf Deutsch (die normalerweise mit der Äußerung "Oh, hi Mark!" begonnen haben) waren für mich eine Quelle von vielen Inspirationen. Matt, mam nadzieję, że będziemy miło wspominać nasze przygody w Portugalii. I am also very thankful to Antal, Axel, Bas, Ben, Carlo, Constantijn, Gláucia, Hans, Kaushik, Jérémy, Jonas, Lennart, Leon, Liangzhong, Raja, Sebastiaan, Sébastian, Stefan, Thinh, Tim, Valentina, Victoria and Wojtek for supporting me so much, both academically and personally over the last years. Victoria, dzięki wielkie także za wielokrotną pomoc w zakresie graficznym.

Ronald, it was a great pleasure to collaborate with your group so much and be a witness to so many breakthrough experiments. I am looking forward to the experimental demonstration of a quantum repeater in the NV platform (despite the fact that there is still no agreement in the community what a quantum repeater is :)). Norbert and Andreas thank you for introducing me to the physics of NV devices. Norbert, in reply to the request in the acknowledgements in your thesis, indeed we should go punting in Cambridge again, but I will first need to practice in advance so that we don't keep turning around like last time. Suzanne and Peter, it was a great experience to multiplex NVs with you. Thank you so much for the great discussions, and not only those ones about NV physics and quantum communication in general, but also those more humorous ones which culminated with brewing three cups of tea from a single tea bag (Peter, I know that it really pushed you out of your comfort zone). Max, thank you so much for joining our second repeater project as an NV cavity expert!

I would also like to thank all my collaborators and coauthors. Additionally to my collaborators that I have mentioned here already, I would also like to thank Andrew, Arian, Dario, Julio, Matteo, Mohsen, Patrick, Przemek, Rob and Tracy. I have learnt a lot from you during our work together. Tracy, I am also very thankful for hosting me in Innsbruck for our repeater discussions. My PhD experience has also been so enjoyable because of many friends at QuTech and Physics from many different scientific fields. Thank you Albert, Doru, Gustavo, James, João, Josh, Marijn, Rafał, Sebastian, Sophie and Xiang.

Francesco, our dinner discussions gave me a little glimpse of insight into the physics of superconducting qubits and a bigger one into the understanding which dishes cannot be combined together. I've been very much enjoying sharing our attic flat over the last one and a half years. Kenneth, Guus, Max, Dario and Josh thanks a lot for proof reading various sections of this thesis! Thank you Chantal, Joanna, Jolijn, Judith, Marja and Yuki for all your help throughout these years with all the administrative matters.

I am very grateful to Natalia Korolkova and Frieder König for helping me discover quantum information and quantum optics and for guiding me and my interest in these fields during my undergraduate years at St Andrews. Your support during my two internships in your group and especially during my last year in St Andrews has been of immense value to me. Dima, thank you so much for designing the amazing cover of this thesis. Moreover, as you see, although it's already seven years since our work together, your pictures of Alice, Bob and Eve have been very much alive over the last years, many of which you can actually find across the chapters of this book. Thank you very much both for your academic and your graphical support! From my time in Scotland, I would

also like to thank Thomas Neukirch for his valuable academic guidance during my last year in St Andrews.

I would also like to thank many friends from outside my academic environment. Over these last years it was a lot of fun to practice Scottish Country Dancing all over Europe. I would like to thank all my Scottish dancing friends in the Netherlands, Scotland and in Germany. Margaret, thank you for introducing me to the dancing community in the Netherlands, Elmer, for all the dancing adventures in the Netherlands and Germany, and Ute for giving me the opportunity to join the German Team. Martin, your creativity and spontaneity was a source of many great adventures. Though I was able to visit only one of your exhibitions, your approach to the notions of space and time both in your work with clay and in our discussions has really made me step outside of the box. And thank you so much for writing so cool and unconventional displays. Turning me into a dancing priest in a dance competition will for sure stay for long in my memory. I would also like to thank Batman and Robin for protecting Gotham City against evil, despite all the challenges. Yannis and Esther, thank you for all the great food, relaxing discussions and the possibility of organising my defence party at your place. Elitza, thank you so much for your strong friendship and support and all the travel adventures together. Lisa, thank you for your help in dislodging many fixed and limiting ideas and Tony, thank you very much for not being helpful in any way at all :)

Na koniec dziękuję bardzo rodzicom, siostrze oraz całej rodzinie za to, że cały czas mnie mocno wspieraliście. To bardzo miło z Waszej strony :).

CURRICULUM VITÆ

Filip Damian ROZPĘDEK

11-12-1990 Born in Warsaw, Poland.

EDUCATION

2006–2009 High School
XXXIII LO im. Mikołaja Kopernika, Warsaw, Poland

2009–2014 Master in Mathematics and Theoretical Physics, MPhys
University of St Andrews, Scotland, UK

2011–2012 Exchange year abroad
Queen's University, Ontario, Canada

2015-2019 PhD in Quantum Information Theory
Delft University of Technology, The Netherlands
Thesis: Building blocks of quantum repeater networks
Promotor: Prof. dr. S. Wehner

ACADEMIC RESEARCH INTERNSHIPS

2012 Summer Internship in Quantum Optics
University of St Andrews, Scotland, UK
Research project on free-space quantum communication
Supervisors: Dr. D. Vasylyev and Dr. N. Korolkova

2013 Summer Internship in Solar Physics
Montana State University, Montana, US
Research project on chromospheric evaporation
Supervisor: S. Brannon

LIST OF PUBLICATIONS

7. A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, **F. Rozpędek**, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. de Oliveira Filho, R. Hanson, S. Wehner, *A Link Layer Protocol for Quantum Networks*, arXiv preprint arXiv: 1903.09778 (2019).

6. **F. Rozpędek** [*], R. Yehia [*], K. Goodenough [*], M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner and D. Elkouss, *Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission*, Phys. Rev. A **99**, 052330 (2019).

5. **F. Rozpędek** [*], T. Schiet [*], L. P. Thinh, D. Elkouss, A. C. Doherty and S. Wehner, *Optimizing practical entanglement distillation*, Phys. Rev. A **97**, 062333 (2018).

4. **F. Rozpędek** [*], K. Goodenough [*], J. Ribeiro, N. Kalb, V. Caprara Vivoli, A. Reiserer, R. Hanson, S. Wehner and D. Elkouss, *Parameter regimes for a single sequential quantum repeater*, Quantum Sci. Technol. **3**, 034002 (2018).

3. S. B. van Dam [*], P. C. Humphreys [*], **F. Rozpędek** [*], S. Wehner and R. Hanson, *Multiplexed entanglement generation over quantum networks using multi-qubit nodes*, Quantum Sci. Technol. **2**, 034002 (2017).

2. **F. Rozpędek**, J. Kaniewski, P. J. Coles and S. Wehner, *Quantum preparation uncertainty and lack of information*, New J. Phys. **19**, 023038 (2017).

1. D. Vasylyev, **F. Rozpędek** and N. Korolkova, *Reconciliation witness and reliability of a quantum atmospheric channel*, Phys. Scr. **2013**, 014061 (2013).

[*]These authors contributed equally.