Quantum Key Distribution over Quantum Repeaters with Encoding

Yumang Jing

University of Leeds

Faculty of Engineering and Physical Sciences

Doctor of Philosophy

June 2021

I declare that the research described in this thesis is original study, which I undertook at the University of Leeds during 2017 - 2021. This work has not previously been presented for an award at this, or any other, university. Except where stated, all of the work contained within this thesis represents the original contribution of the author.

Some parts of the materials in this thesis have been published in journals and/or made available online on the arXiv. The author of this thesis acknowledges the input of his collaborators, and has credited them appropriately throughout. A list of papers which overlap with this thesis are presented here.

• *Quantum key distribution over quantum repeaters with encoding: using error detection as an effective postselection tool*
Yumang Jing, Daniel Alsina and Mohsen Razavi. Published in Physical Review Applied **14**, 064037 (2020).

I have analyzed the system, obtained the simulation results and drafted the paper. D.A. contributed to the construction of the initial code. M.R. checked the validity of the results, provided feedback and improved the writing of the manuscript. The results of this work appear in Chapter 3.

• *Simple efficient decoders for quantum key distribution over quantum repeaters with encoding*
Yumang Jing and Mohsen Razavi. Published in Physical Review Applied **15**, 044027 (2021).

I have analyzed the system, obtained the simulation results and drafted the paper. M.R. checked the validity of the results, provided

feedback and improved the writing of the manuscript. The results of this work appear in Chapter 4.

• *Quantum repeaters with encoding on nitrogen-cacancy center platforms*
Yumang Jing and Mohsen Razavi. Submitted to Physical Review Applied arXiv:2105.14122.

I have analyzed the system, obtained the simulation results and drafted the paper. M.R. checked the validity of the results, provided feedback and improved the writing of the manuscript. The results of this work appear in Chapter 5.

A list of conference papers relevant to this thesis are presented here.

• Jing Y and Razavi M (August 2021) *Quantum key distribution over quantum repeaters with encoding*, QCrypt21 (Online), Amsterdam, Netherlands.

• Jing Y and Razavi M *Quantum repeaters with repetition codes using nitrogen-vacancy centers*, QCMC2020 (Postponed), Lisbon, Portugal.

• Jing Y and Razavi M (August 2019) *Quantum key distribution over quantum repeaters with repetition codes*, QCrypt19, Montreal, Canada.

• Jing Y and Razavi M (August 2018) *Resource analysis of future quantum repeater networks*, QCrypt18, Shanghai, China.

• Jing Y (May 2018) *Resource analysis of future quantum repeater networks*, 24th Young Atom Opticians Conference, Glasgow, UK.

Acknowledgements

First, I would like to greatly thank my supervisor, Professor Mohsen Razavi, for providing me the opportunity to conduct a PhD in Quantum Communications. I am very grateful for his guidance, patience and kindness during the last four years, without which, most of my PhD time would not have been pleasant.

Next, I would like to thank my colleagues, Ekaterina Orlova, Sima Bahrani, Guillermo Curras Lorenzo, Daniel Alsina and Masoud Ghalaii for accompanying me through this memorable journey. I would also like to thank our QCALL people for all the time we shared together, during every meet-up, conference and workshop. I am grateful for joining this project, which has exposed me to a large community and more possibilities.

Then, of course, I would like to thank my families for always being there as a strong backing. It is their presence that keeps giving me the courage to face this imperfect world.

Finally here come some irrelevant personal reflections: doing a PhD is a special experience but it is certainly not one of a kind. The end of this journey is a beginning of another. *Never long for the past, never fear the future.*

This work was supported by the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie Grant Agreement No. 675662 (QCALL) and partially by the UK EPSRC Grant No. EP/M013472/1.

Abstract

Quantum networks allow for the transmission of quantum information between physically separated quantum processors and can be used for both quantum communications and quantum computation applications. An enabling technology for future quantum networks is that of quantum repeaters (QRs). In this thesis, we study the performance of a quantum key distribution (QKD) system that is run over QRs with encoding. In such repeaters, quantum error correction techniques are used for entanglement distillation. We develop reliable and efficient tools, based on the linearity and transversality properties of the system, to obtain and study the shared states between two end users via such a repeater chain. We propose a post-selection technique which relies on the error-detection, rather than the error-correction, capability of the underlying code to sift out cases where an error has been detected. This simple but effective approach not only considerably improves the secret key rate and increases the resilience of the system to errors, but also simplifies the demonstration of such protocols in the near future.

In this thesis, we mainly implement our techniques for three- and five-qubit repetition codes by modeling different resources of error in crucial components of the system. By developing several scalable numerical and analytical techniques, we investigate in detail the resilience of the setup to those imperfections in gates, measurement modules, and the initialization of the setup, at any nesting levels we are interested in. Furthermore, we propose two alternative decoder structures for encoded repeaters that not only boost system performance but also make the implementation aspects easier by removing two-qubit gates from the QKD decoder. We compare this class of QRs against alternative fully probabilistic settings and benchmark the regimes of operation, where one class of repeater outperforms the other. We find that there are feasible regimes where encoded repeaters—based on simple three-qubit repetition codes—could offer practical advantages.

In order to get a view of how this type of QRs may behave in real life, among various promising candidates nowadays which enable deterministic entanglement swapping and distillation operations, here, we particularly investigate the suitability of platforms using nitrogen-vacancy (NV) centers in diamond as quantum memories. NV centers offer a two-qubit register, corresponding to their electron and nuclear spins, which makes it possible to perform deterministic two-qubit operations within one NV center. For QR applications, we however need to do joint operations on two separate NV centers. In this thesis, we study two NV-based repeater structures that enable such deterministic joint operations. One structure offers less consumption of classical communication, hence is more resilient to decoherence effects, whereas the other one relies on fewer numbers of physical resources and operations. We assess and compare their performance for the task of secret key generation under the influence of noise and decoherence with current and near-term experimental parameters. We quantify the regimes of operation, where one structure outperforms the other, and find the regions where encoded QRs offer practical advantages over their non-encoded counterparts.

Abbreviations

BSM	**B**ell-**S**tate **M**easurement
BS	**B**eam **S**plitter
BB84	**B**ennett-**B**rassard 19**84** (QKD Protocol)
BBM92	**B**ennett-**B**rassard-**M**ermin 19**92** (QKD protocol)
BDCZ	**B**riegel-**D**ür-**C**irac-**Z**oller (QR protocol)
CNOT	**C**ontrolled-**NOT**
CSS	**C**alderbank-**S**hor-**S**teane (Codes)
DLCZ	**D**uan-**L**ukin-**C**irac-**Z**oller (QR protocol)
ES	**E**ntanglement **S**wapping
ED	**E**ntanglement **D**istillation
EPR	**E**instein-**P**odolsky-**R**osen (States/Sources)
LOCC	**L**ocal **O**prations and **C**lassical **C**omunication
NV	**N**itrogen-**V**acancy centers
QKD	**Q**uantum **K**ey **D**istribution
QM	**Q**uantum **M**emory
QR	**Q**uantum **R**epeater
QEC	**Q**uantum **E**rror **C**orrection
QBER	**Q**uantum **B**it **E**rror **R**ate
TF	**T**win-**F**ield (QKD)

Contents

List of Figures

Chapter 1

Introduction

1.1 Quantum networks

The development of the quantum internet Kimble [2008], Wehner et al. [2018], will constitute a breakthrough in the backbone of future communications systems. If we can claim the Internet as the greatest invention of the 20th century, which has revolutionized our daily life, the stage of the 21st century will most likely belong to quantum devices, which will also intensively change our way of understanding the world.

Quantum networks, generally speaking, would allow the transmission of quantum information between any two separated quantum processors at any distances. They work in a fundamentally different way from classical network by exploiting the principles of quantum mechanics, and could eventually achieve results that are provably impossible on today's networks. Central to their power is the ability of encoding information on a superposition state. Instead of classical bits, which can only take values of 0 or 1, quantum bits, known as qubits, are able to represent the values 0 and 1 at the same time. It is this superposition ability that opens up the diversity of quantum world and facilitates functionalities that are out of reach by solely relying on classical physics.

Generally speaking, the applications of a quantum network can be broadly divided into two directions: quantum communication and quantum computation. At the current stage, they focus on different aspects of development of quantum technologies. Quantum communication is mainly focused on secure transmission

of information over long distances. This poses high requirements of the system on countering the transmission loss through the channels but is more tolerant regarding the processing ability of individual units. Simple quantum nodes capable of manipulating just a few qubits should be sufficient (at least for now). Whereas for quantum computation, it demands highly efficient and reliable operations of a large number of qubits, focusing more on dealing with the operational errors at local stations. Nonetheless, they both have to conquer the fragility of quantum systems since any disturbance may cause the collapse of a superposition state.

As promising as the theoretical works might be, the experimental challenges and technological requirements in making a quantum network a reality are very daunting. Thankfully, through the tremendous efforts being put in this field Awschalom et al. [2018], Northup & Blatt [2014], Pirandola et al. [2015], Reiserer & Rempe [2015], we may possibly see the realization of a small-scale quantum network, which just contains a few nodes within very short distances, in the next few years Wehner et al. [2018]. In this thesis, I focus around an enabling technology for future quantum networks known as quantum repeaters (QRs). I will study how they perform regarding quantum key distribution (QKD) application. In the following, I will present an overview of QRs and QKD firstly, which will offer an overall impression before getting into more details in the next chapter. At the end of this chapter, I will introduce research objectives and the scope of this thesis.

1.1.1 Quantum repeaters: Overview

QRs are important stepping stones for the establishment of quantum networks. The proposition of QRs aims at transmitting quantum data over very long distances. At first glimpse, it is mainly used for quantum communication purposes. Nevertheless, at the early stage of quantum computer age, it is very likely that we merely have a few available quantum computer devices that can be accessed via cloud services. A QR would be necessary then to enable connecting to such quantum servers.

However, the quality of quantum information degrades during transmission. In classical telecommunications, we often use relay nodes to receive, amplify,

and retransmit a signal. However, this approach introduces unavoidable noise in quantum world due to the rules of quantum mechanics. In order to solve this problem, the concept of QRs is proposed. The basic ideas behind and the building blocks that form it will be introduced and discussed in detail in the following chapter. Roughly speaking, QRs also root on the basis of dividing a whole long range link into shorter segments, managing the transmission regionally first and then extending it node-by-node to cover longer distances, while in a quantum fashion.

Since the first idea of QRs has been presented Briegel et al. [1998], various protocols have been formulated Azuma et al. [2015], Duan et al. [2001], Jiang et al. [2009], Muralidharan et al. [2014], Sangouard et al. [2011], while none of them has been established in the real world. There are different ways to categorize QR protocols Borregaard et al. [2019], Muralidharan et al. [2016], Razavi [2018] (I will look into a specific one in the next chapter), while in essence, it can be considered as if the entanglement has to be established or not. For protocols that require the establishment of entanglement, two-way classical signalling is always involved, partially or entirely, which would reduce the data exchange rate to a certain extent, but this kind of protocol is relatively easier to be achieved with the current and near-future technological progress. For protocols which do not rely on entanglement, redundancy encoding is indispensable Ewert et al. [2016], Munro et al. [2012], Muralidharan et al. [2014]. Such protocols only require one-way classical signaling and can therefore potentially be much faster, but would demand quantum processors with a large number of qubits, which may approach the hardness of building a quantum computer and is thus not within reach in the short term.

1.2 Quantum key distribution: Overview

Cryptography is a study and practice of techniques that facilitates the secure transmission of information in the presence of malicious adversaries. It is an indispensable tool that deeply rooted in our daily life, corresponds to the activities such as online transactions, digital signatures, email and instant messages. A

widely used class of cryptography schemes today, known as public-key cryptography or asymmetric cryptography, relies on the computational complexity to guarantee the security of the corresponding protocols Merkle [1980], Rivest et al. [1978]. It assumes that the eavesdropper only has access to limited computational powers, which would take a very long time in order to find the possible key to decipher our secrets. However, with the future development of quantum computers, such an assumption may no longer hold. What takes a few hundred years to be solved on a classical computer may only take a few minutes on a quantum one. Though reaching to that stage in quantum era may still sound like a far-off vision, tech giants such as Google are very optimistic about it, and aim at constructing the world first commercial quantum computer by 2030. Actually, with the so called "quantum supremacy" being claimed recently Arute et al. [2019], Boixo et al. [2018], we may not be that far away from such a reality.

In order to well prepare ourselves for such a coming day, the deployment of quantum cryptography Gisin et al. [2002], should not delay. Unlike classical cryptography, quantum cryptography relies on the law of quantum mechanics, which has been through the test of time. Its advantages lie in the fact that it is inherently impossible to copy any unknown information in quantum domain, known as the no-cloning theorem Dieks [1982], Wootters & Zurek [1982].

Quantum cryptography has many applications, among which the most known and mature technology is QKD. QKD enables information-theoretical security for key exchange problems. Combined with the one-time pad technique Bellovin [2011], it will offer unconditional security for information exchange even on a classical network (conditioned on that the two communicators, Alice and Bob, can authenticate each other). If any eavesdropper is trying to intercept the information of the key being established, they cannot avoid creating errors and leaving discrepancies that Alice and Bob can detect.

There are several ways to categorize the existing QKD protocols. For example, based on the encoding and detection techniques, most existing QKD protocols can be classified into two categories: discrete-variable (DV) QKD and continuous-variable (CV) QKD. The former one typically encodes data on the polarization, phase or time-bin degrees of freedom of the photon, and relies on single-photon detection to retrieve the information; whereas the latter one typically encodes

information in the quadratures of electromagnetic fields and relies on homodyne or heterodyne detection techniques Grosshans & Grangier [2002]. This classificaion is not within the discussion of this thesis, but we mention that we only focus on the DV one hereafter. Alternatively, based on the implementation techniques of the protocols, they can also be divided into prepare-and-measure QKD Bennett & Brassard [1984] or entanglement-based QKD Ekert [1991], which will be discussed in more detail in the next chapter. Briefly speaking, the former one works in the sense that the transmitter sends information to the receiver, who would then decode the data as required; whereas for the later one, both users will receive parts of the entangled states and perform corresponding measurements as required. These two protocols are essentially interlinked, while it might be easier sometimes to perform security analyses on the entanglement-based version.

While QKD is seemingly secure, its application faces the challenges of practicality Diamanti et al. [2016], Lo et al. [2014], Scarani et al. [2009]. This is mainly due to the inevitable transmission loss through the channel as well as imperfect sources and devices utilized for implementations. Any adversary can take advantage of those imperfections to intercept the data communicated, leading to a series of attacks and thus compromising the security of the protocol. Luckily, sustained efforts are being put in this field so that every time a possible attack arises, a new efficient QKD protocol would follow up to tackle it Diamanti et al. [2016], Scarani et al. [2009]. For instance, decoy-state protocol Lo et al. [2005b] was proposed in order to address the photon-number-splitting (PNS) attack arising from the imperfection of single-photon resources; measurement device independent (MDI) QKD Lo et al. [2012] and twin-field (TF) QKD Lucamarini et al. [2018] were proposed to cope with the detector side-channel attack (the latter one can even overcome the repeaterless bound).

1.3 Scope of this study and main contributions of the thesis

Within the above context, in this thesis, we focus on one specific type of QRs that applies redundancy encoding while is still entanglement-based. Such QRs

use quantum error correction techniques to compensate for noises in quantum operations. We look into the quality of the long-distance entanglement established by performing a simple QKD application on it. We are aiming at providing a complete and rigorous analysis of such a system and will explore its compatibility and performance on specific experimental platforms. We will model the system by considering various sources of error from its crucial components and will also take decoherence effect of quantum memories into account. Previous work on this subject often relies on various approximations, while in this thesis, we will try to remain as close as possible to the exact cases. We investigate the performance of such a system in the context of QKD and compare it with the case for some other types of QRs.

Main contributions of the thesis:

In Chapter 3, we develop our analytical approach based on the the linearity and transversality properties of the quantum circuits and employed codes to study the performance of the system for lower nesting level cases. We implement our technique for three-qubit repetition codes and investigate in detail the impact of different imperfections on the secret key generation rate of the QKD system. We study how one can use the information obtained during entanglement swapping and decoding stages to maximize the rate, which leads to an efficient post-selection technique based on quantum error detection, rather than quantum error correction features of the code to simplify its implementation. For benchmarking purpose, we also specify the maximum allowed error rates in different components of the setup below which positive key rates can be obtained. The results presented in Chapter 3 has been published on [PhysRevApplied.14.064037]; and made available on the arXiv [arXiv:2007.06376].

In Chapter 4, we extend our analysis for higher nesting level cases by developing several scalable numerical and analytical approximation techniques. We particularly consider QRs with encoding and compare them with probabilistic QRs. To that end, we propose two decoder structures for encoded repeaters that not only improve system performance but also make the implementation aspects

easier by removing two-qubit gates from the QKD decoder. We apply our techniques to three- and five-qubit repetition codes and obtain the normalized secret key generation rate per memory per second for encoded and probabilistic QRs. We quantify the regimes of operation, where one class of repeater outperforms the other, and find that there are feasible regimes of operation where encoded repeaters—based on simple three-qubit repetition codes—could offer practical advantages. The results presented in Chapter 4 has been published on [PhysRevApplied.15.044027]; and made available on the arXiv [arXiv:2012.13011].

In Chapter 5, we investigate the explicit implementation of such encoded QRs using nitrogen-vacancy (NV) centers in diamond as quantum memories. In particular, we study two NV-based repeater structures that enable deterministic joint operations between two NV centers. One structure offers less consumption of classical communication, hence is more resilient to decoherence effects, whereas the other one relies on fewer numbers of physical resources and operations. We assess and compare their performance for the task of secret key generation under the influence of noise and decoherence with current and near-term experimental parameters. We quantify the regimes of operation, where one structure outperforms the other, and find the regions where encoded QRs offer practical advantages over their non-encoded counterparts. The results drafted in Chapter 5 has been submitted to Physical Review Applied and made available on the arXiv [arXiv:2105,14122].

1.4 Thesis outline

Chapter 2 of this thesis gives a background of the basic idea behind QR structures and introduces one of their most important applications, i.e., QKD. This chapter briefly introduces the building blocks that constitute the system and discusses one of its classifications based on the implementation method utilized. One figure of merit used for QKD — the secret key rate — is also explained. In Chapter 3, we look into one specific type of QRs which uses quantum error correction for entanglement distillation. We propose a post-selection approach which relies on the error detection features of the code to boost the system performance. In Chapter 4, we extend our research in Chapter 3 to higher nesting level cases and

propose two alternative decoder structures which not only simplifies its demonstration, but also improves the secret key generation rate. In Chapter 5, we apply encoded QRs on NV center platform with decoherence effect being considered, and compare the system performance with their non-encoded counterparts. The thesis is summarized and looked forward in Chapter 6.

Chapter 2

Background

This chapter introduces the concept of a QR network and discusses the main building blocks and techniques used to implement it: entanglement distribution over elementary links, entanglement swapping, entanglement distillation and quantum error correction. I then discuss the classification of different QR protocols based on their implementation methods. In this thesis, I focus on a particular type of QR, in which entanglement distillation can be performed in a deterministic way using quantum error correction techniques. Finally, I review the main application considered in this thesis, i.e., QKD, and its figure-of-merit, the secret key generation rate.

2.1 Quantum repeaters

Quantum networks have the promise of enabling long-distance secure communication, large-scale quantum computation, and enhanced metrology through the distribution of entanglement across nodes Kimble [2008], Wehner et al. [2018]. Despite the continuous progress being made, the realization of such a network composed of many nodes and channels is still a far-off vision due to the inherent fragility of quantum systems; and this places challenging requirements on any possible practical platform. A key requirement for such networks is the ability to transfer quantum states in a reliable and efficient way among their nodes. This is where QRs become an instrumental platform for implementing future quantum networks.

The direct distribution of quantum states is limited by the transmission losses of the channel used [1]. For instance, the success probability of transmission a photon through a fibre-optic channel decays exponentially with distance. Even under certain optimistic assumptions for the technology evolution, the achievable distances are limited to a few hundred kilometers Boaron et al. [2018], Chen et al. [2020], Yin et al. [2016]. Unlike in classical communications, where amplifiers can be deployed to boost or regenerate the signals, here, this idea fails due to the fact that quantum states cannot be copied or amplified without any disturbance, known as the no-cloning theorem Dieks [1982], Park [1970], Wootters & Zurek [1982]. To tackle this problem, it has been proposed to use QR protocols.

QRs were initially proposed to enable entanglement distribution, in an efficient way, at long distances Briegel et al. [1998]. Using teleportation techniques Bennett et al. [1993], Boschi et al. [1998], Bouwmeester et al. [1997], Furusawa et al. [1998], one can then send quantum information across a quantum network once entangled states are shared between remote users. In its original form, the main idea behind such repeaters is to split the link into shorter *elementary* segments and first distribute and store entanglement over such links. One can then use entanglement swapping (ES) Zukowski et al. [1993] and, possibly, entanglement distillation (ED) at middle nodes Bennett et al. [1996], Deutsch et al. [1996] to establish high fidelity entanglement over long distances. The schematic of this basic idea is shown in Fig. 2.1. In principle, the key goal of a QR protocol is to try to change the scaling of entanglement distribution rate from exponential with distance to polynomial. For an optical fibre channel with a total distance L_{tot}, the chance that an entangled state is directly distributed is proportional to $\exp(-\alpha L_{\text{tot}})$, with α being a constant channel loss parameter. However, by dividing the overall link into 2^n segments, as shown in Fig. 2.1, and by adding quantum memories (QMs) in the middle nodes, we allow for the entanglement distribution over elementary links to succeed at different times, which effectively results in a rate scaling with $\exp(-\alpha L_0)$ now. For a fixed L_0, one can increase the entanglement distribution distance through increasing the nesting level n. It

[1] Similar to classical communications, the transmission channels typically considered in quantum communications are optical fibers and free-space. Throughout this thesis, I only discuss the transmission through optical fibers.

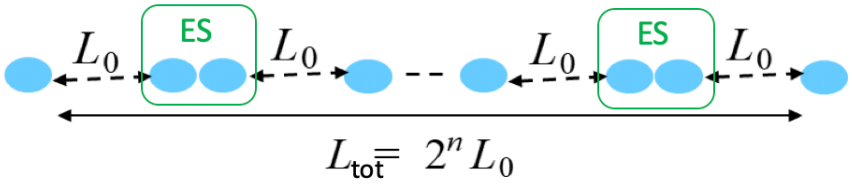

Figure 2.1: Schematic of generic QR protocols. The whole link with a total distance L_{tot} is divided into 2^n segments. Entanglement is first distributed and stored within those elementary links and is then extended over the entire link by performing ES operations at all middle nodes.

would then become important how efficiently we can perform ES operations, and how we can handle the errors that may result from them.

Note that an alternative way to use teleportation for quantum state transfer is to directly send quantum states across the channel by using strong error correction codes. I will discuss this advanced class of QRs, which do not rely on long quantum storage, later in Sec. 2.3.2. Before that, I discuss the key ingredients of conventional QRs in the following section.

2.2 Building blocks of quantum repeaters

Having provided the basic idea with regard to the framework of QRs, we now zoom into the corresponding building blocks and techniques for their implementation.

2.2.1 Entanglement distribution over elementary links

Entanglement is a form of correlation in quantum world, which does not have any classical counterpart. It is a phenomena in which the quantum states of composite systems cannot be described as a product of states of individual subsystems Horodecki et al. [2009]. The simplest example of entanglement is represented by the four maximally entangled two-qubit states, or Bell states Braunstein et al. [1992] : $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$, where

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \tag{2.1}$$

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{2.2}$$

Before getting down to QR business, we first discuss how to distribute entanglement over shorter segments.

Entanglement can be created through various types of particles Chen et al. [2006], Hald et al. [1999], Meekhof et al. [1996], Raimond et al. [2001]. However, the vast majority of quantum entanglement experiments to date use photons as entangled particles due to their easy manipulation and relatively sophisticated optical technologies. One of the most popular and efficient techniques for the generation of photonic entanglement is based on spontaneous parametric down-conversion (SPDC) Boyd [2020]. SPDC is a non-linear optical process, which splits one photon (the pump beam) into a pair of photons (the signal and idler beams), obeying the law of conservation of energy and momentum. Its type II down conversion results in entanglement of two photons whose polarizations are orthogonal.

Fig. 2.2(a) shows a possible structure for a QR using SPDC sources. Here, entangled photons are generated by SPDC sources located in the middle of each elementary link. Note that the position of the sources is not restricted to the exact middle position. One can of course create an entangled photon pair locally and then send one of the photons to the other node of elementary links. In order to perform ES between two neighbouring links, one must make sure that these entangled photons have reached their destinations. However, as mentioned before, photons may get lost in the channel. Such a probabilistic feature would require that the initially distributed entangled pair to be stored, until other elementary links are also entangled. Thus, QM modules are required in order to get a better rate scaling. The created photon pairs have to match the absorption profile of QMs Bussieres et al. [2013], Liu et al. [2021], Lvovsky et al. [2009], or frequency conversion among other things may be needed Fernandez-Gonzalvo et al. [2013], Fisher et al. [2016], Rančić et al. [2018], so that the moment they reach the QM sites, the state of the photon can be transferred to the QM. In addition, we also need a mechanism by which we can verify whether each loading attempt succeeds or not, that is, our entanglement distribution method must be *heralding* Barz

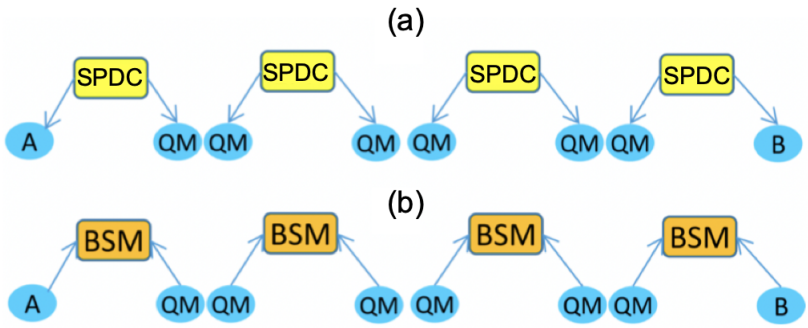

Figure 2.2: Entanglement distribution over elementary links by (a) direct distribution of entangled photons generated by SPDC, and (b) photon-interference at the middle position.

et al. [2010], Wagenknecht et al. [2010]. Implementing such a verification technique is, nonetheless, not always possible or at least not an easy job in practice.

Another way to distribute entanglement at a distance is based on establishment of memory-photon entanglement at each node first and a subsequent joint measurement of the photons transmitted to the middle of each link, as shown in Fig. 2.2(b). Such a joint measurement is known as a Bell-state measurement (BSM), which projects the input state into the entangled two-qubit bases formed by Eqs. (2.1-2.2). In this step, BSM typically employs linear optic elements, such as polarizing beam splitter, wave plates and photon detectors, to erase the *which-path* information of the photons and thus creates an entanglement between the two corresponding memory systems [1]. A successful BSM means that they have survived the path loss and thus can be seen as a heralding event of the successful distribution of entanglement over elementary links. This scheme was first proposed by Duan, Lukin, Cirac and Zoller, known as the DLCZ protocol Duan et al. [2001]. I will return to this protocol in Sec. 2.3.1.

There are other entanglement distribution techniques Cirac et al. [1997], Matsukevich et al. [2006], Munro et al. [2005], but, similar to the above mentioned schemes, they often require back-and-forth classical communication between senders

[1] We will introduce another implementation method of BSM in the following section.

and receivers in order to acknowledge the success of each attempt. For experimental platforms that enable fast local operations, the entanglement generation rate of a QR protocol is mainly limited by the time consumed for such signaling [1]. With a low successful probability for each attempt, the time it takes for a successful distribution of entangled states over all elementary links would be very considerable, which poses a high requirement on the coherence time of memory modules. One possible way to mitigate this problem is by applying multiplexed QMs Collins et al. [2007], Munro et al. [2010], Razavi et al. [2009]. The basic idea behind this is to compensate for low success rates by increasing the number of trials at each time, replacing single memory elements with memory banks. The memory banks can be constituted of many physical memory modules or they may deploy several degrees of freedom for a single memory module. However, even though such a technique is already feasible for certain platforms Li et al. [2020], Pu et al. [2017], Saglamyurek et al. [2011], Sinclair et al. [2014], Tang et al. [2015], Usmani et al. [2010], constructing it in a large scale while still keeping the fine control over individual accessibility, remains a challenge. In this thesis, I only consider applying it under certain cases just in order to have a clue that, to what extent, this technique can boost the system performance, without delving into much details.

2.2.2 Entanglement swapping

Once entanglement is heralded within each elementary link, one can think of connecting them in order to extend entanglement over longer distances. This process is implemented by using ES techniques Zukowski et al. [1993]. ES, enabled by a BSM, allows two formerly independent parties to be entangled without direct interaction between them. Consider two independently entangled links AB and CD, as shown in Fig. 2.3(a), A and D are far apart, while B and C are co-located. By performing the BSM on qubits B and C, we can generate

[1] It is worth pointing out that the classical and quantum communications are both subject to the same speed limit of light, either in optical fiber or free space. The failure of any attempt would lead to the repeat of both quantum distribution and classical confirmation, which takes time.

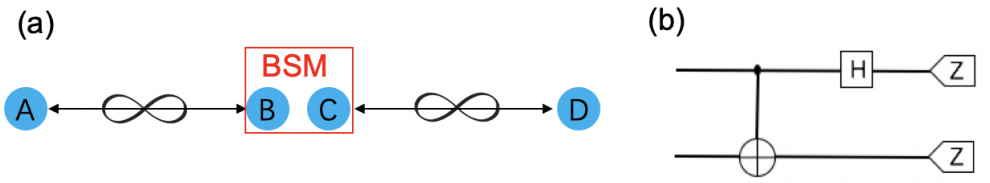

Figure 2.3: (a) Schematic of entanglement swapping. (b) Quantum circuit for gate-based Bell-state measurement, which is implemented through an entangling/disentangling operation on the pair of qubits followed by single qubit measurements.

entanglement between farther nodes A and D without them directly interacting with each other.

Besides what is mentioned in the above subsection where BSM can be performed through linear optics and photon detection, which is a probabilistic process subject to the successful arrival of photons, BSM can also be achieved through deterministic gate-based operations, which is a nonlinear process. Such a quantum circuit of ES uses controlled-NOT (CNOT) gates, Hadamard gates and measurement apparatus, as shown in Fig. 2.3(b). Solid-state based platforms such as trapped-ions Ballance et al. [2016], Gaebler et al. [2016] or color centers in diamond Taminiau et al. [2014], Zhang et al. [2014] allow for such deterministic operations, while some other platforms, such as atomic ensembles, would ask for ES to be performed optically in an inherently probabilistic manner Sangouard et al. [2011]. Based on how this step is operated, QRs can be classified into different types, to which I will return in Sec. 2.3.

The linear-optical realization of ES, without the help of ancillary photons, has a maximum success rate of 1/2 (when imperfections are considered, it is even less) Braunstein & Mann [1995], Calsamiglia & Lütkenhaus [2001]. Though deterministic gate-based Bell-state analyzers do not suffer from this limitation, they have their own drawback to address, particularly, the operational errors that may be added because of gate and measurement operations. Throughout this thesis, I mainly consider two types of such errors: bit-flip errors $|0\rangle \leftrightarrow |1\rangle$ and phase-flip errors $|0\rangle \leftrightarrow |0\rangle$, $|1\rangle \leftrightarrow -|1\rangle$, which correspond to Pauli X and Z

operators:

$$\begin{aligned} &\text{Pauli X} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ &\text{Pauli Z} \quad \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \end{aligned} \tag{2.3}$$

respectively. Even if perfect gates and measurements are considered, ES operations would still reduce the fidelity of the entangled state distributed. Each connection leads to an exponential decrease of the resulting fidelity, unless the two input states are also maximally entangled Dür et al. [1999]. Therefore, in practice, after multiple ES connections, the final long-distance entangled state distributed could be of very low quality that cannot be used for any applications. Luckily, there are two solutions to tackle this issue: entanglement distillation (ED) and quantum error correction (QEC), which both rely on using ancilla systems to compensate for the errors and noises in the channel. These two techniques will now be discussed more explicitly in the next subsections.

2.2.3 Entanglement distillation

ED is a procedure by which M pairs of non-ideal entangled states can be distilled or concentrated into $N < M$ entangled states of higher fidelity Bennett et al. [1996], Deutsch et al. [1996]. Before explain this scheme, we first clarify what *fidelity* is. In quantum mechanics, fidelity is a measure of the "closeness" of two quantum states. Consider two quantum states ρ_1 and ρ_2, the fidelity is defined as Jozsa [1994]

$$F(\rho_1, \rho_2) = \left(Tr(\sqrt{\sqrt{\rho_2}\rho_1\sqrt{\rho_2}}) \right)^2. \tag{2.4}$$

If $\rho_2 = |\phi\rangle\langle\phi|$ is a pure state, the fidelity is then reduced to

$$F(\rho, |\phi\rangle) = \langle\phi|\rho|\phi\rangle. \tag{2.5}$$

Throughout this thesis, unless specified, the fidelity is typically referred to the state we care about to the maximal two-qubit entangled states given by Eqs. (2.1-2.2). ED can be applied before and/or after ES operations. Roughly speaking, it

is implemented by constructing more than one entangled pairs in parallel fashion, applying local operations and measurements in both sides, followed by exchange of measurement outcomes using classical communication to decide whether it succeeds or not. Depending on different algorithms used, we may end up with different rate behaviours. Moreover, the input states for the distillation can be of the same quality or not, but generally, we would require the fidelity of the input states to be larger than 1/2 in order for distillation technique coming into force.

As described, conventional ED protocols always depend on two-way classical communication between the nodes to acknowledge the success or failure of any attempt. Even though all operations can be performed in a deterministicly gate-based way, it does not change their probabilistic and heralding features. One way to mitigate this is by applying QEC techniques, as I am about to discuss next.

2.2.4 Quantum error correction

Another solution utilized to cope with the loss and operational errors involved in the implementation of QR protocols is QEC. Similar to what classical error correction does, QEC is also based on the idea of redundant encoding. However, unlike what can be done in the classical world, there are two main hurdles that complicate this process in the quantum domain Devitt et al. [2013]: first, due to the no-cloning theorem of quantum mechanics, it is impossible to protect quantum data from errors by simply making enough copies of it Dieks [1982], Wootters & Zurek [1982]; second, direct measurement of the qubits to extract the error syndromes is not allowed since this will collapse or destroy any quantum superposition or entangled states Dirac [1981]. With that being the case, what QEC does is, typically, using a sequence of two-qubit gates to firstly couple ancilla qubits to the data block and then measuring those ancilla qubits in order to extract the error syndromes, based on which applying error-correction operations (typically bit-flip and/or phase-flip gates as given by Eq. (2.3)) on the original qubits accordingly. Thus the information can be possibly recovered or purified without any contamination of the data block.

QEC is a very wide field and is not limit to the domain of quantum communications. Many new codes, methodologies, techniques are being developed to

facilitate large-scale quantum algorithms (Arute et al. [2019], Wiebe et al. [2012]) and fault-tolerant quantum computation (Fowler et al. [2012], Shor [1996]). In this thesis, I only focus on one specific class, known as Calderbank-Shor-Steane (CSS) codes, named after their inventors. The main contributions of this thesis, however, is made from QRs based on an even simpler type, the repetition codes, which share the specific features owned by CSS codes but are much easier to be analyzed and implemented.

CSS codes are a special type of the more general class of stabilizer codes, which can be constructed from classical linear codes Nielsen & Chuang [2002]. The details of the code construction and error correction mechanisms are beyond the scope of this thesis. We emphasize that it is their *transversality* and *linearity* features that facilitate their use in the application of quantum communication. To be more specific, in order to process the encoded quantum information, all operations and measurements are also expected to be performed at the encoded level, which typically involves the mutual control over a large number of qubits. Luckily, the transversality property of CSS codes enables those processes to be done by directly applying the individual physical operators to each qubit in the code block, greatly reducing the complexity of operating on multi-qubit systems. Moreover, the encoding and decoding steps of CSS codes only require the application of Hadamard gates and CNOT gates, in each case with a number scaling linearly with the size of the code. Those advantages make their implementation aspects straightforward.

An important example of CSS codes is the 7-qubit Steane code Steane [1996], named after its inventor. The Steane code is defined as a $[[n, k, d]] = [[7, 1, 3]]$ quantum code, where $n = 7$ physical qubits are used to encode $k = 1$ logical qubit with a distance $d = 3$ that can correct up to $t = (d - 1)/2 = 1$ quantum error (for one quantum error we mean both a bit-flip error and a phase-flip error at the same time).

Larger codes are capable of correcting more errors, at the expense of requiring much more complicated and advanced multi-qubit quantum processors, which, despite the tremendous efforts being made, is still far off hands in practice. In this thesis, for most practical purpose, I will just focus on the simplest encoding structures, the repetition codes. The typical number of qubits used in our work

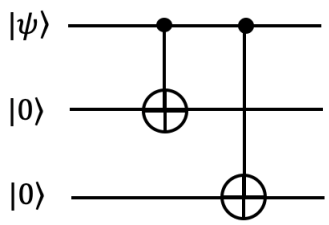

Figure 2.4: Quantum circuit for the 3-qubit repetition code.

is 3 or 5. We give a description of 3-qubit repetition code next and mention that the mechanism works similarly for the 5-qubit one.

The 3-qubit repetition code encodes a single logical qubit into three physical qubits, which can correct one bit-flip error [1] Braunstein [1996], Peres [1985]. The two logical qubits are given by

$$|0\rangle_L = |000\rangle, |1\rangle_L = |111\rangle, \tag{2.6}$$

such that an arbitrary single qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is mapped to,

$$(\alpha|0\rangle + \beta|1\rangle)|0\rangle|0\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle = |\psi\rangle_L. \tag{2.7}$$

This process is achieved by the quantum circuit depicted in Fig. 2.4. If the probability of a single physical qubit being flipped is $p_p = p$, that of a logical qubit would be $p_l = 3p^2 - 2p^3$, which corresponds to the situation where at least two physical qubits are flipped, with the majority rule being applied. So long as $p < 1/2$, the error probability after encoding is suppressed. Note that, strictly speaking, 3-qubit repetition code is not a full quantum code, since it cannot correct both bit- and phase- flip errors at the same time. However, the thorough analysis of its functionality regarding the implementation of QRs would still offer us a generic idea of how QRs with encoding would perform in the near future, which is at the heart of this thesis. Moreover, through our contribution that will be introduced in Chapter 4, we find that, for most practical purposes, the

[1] Note that 3-qubit repetition code can also correct first-order errors on all three qubits code, which in some error scenarios is a more realistic event. Please refer to Devitt et al. [2013] for detailed explanation.

simple 3-qubit repetition code might be the optimal choice for near-term QKD applications. Moreover, in any case, the full implementation of the simplest 3-qubit repetition code would certainly be the first attempt at building a QR with encoding.

It is also worth mentioning that 3-qubit repetition codes can be applied in the phase domain, where two logical qubits are given by

$$|0\rangle_L = |+++\rangle, |1\rangle_L = |---\rangle, \tag{2.8}$$

with $|\pm\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Such an encoding can correct up to one phase-flip error. It has the same characteristics as the code in Eq. (2.6). All operations required for error detection and correction are performed similarly just with additional Hadamard gates at appropriate points.

2.3 Categories of quantum repeaters

With the knowledge of essential building blocks being introduced in the last section, we are now more prepared to get on with the QR business. After being introduced in 1998, the development of QRs has theoretically gone through several stages, sometimes referred to as different QR generations Muralidharan et al. [2016]. Based on various implementation or error-suppression methods, there are different ways to classify them. In this section, we look at one way to categorize them based on the implementation techniques applied at ES modules.

2.3.1 Probabilistic quantum repeaters

Probabilistic QRs use photonic systems for both distribution and swapping of entanglement. In early implementations of QRs, it is expected that the initial entanglement distribution over elementary links Yu et al. [2020], as well as ES and ED operations to be achieved in this way. This can make the whole system too slow as many steps may need to be repeated upon a failure Razavi et al. [2009]. Such probabilistic QRs often require QMs with long coherence times, comparable to the transmission delay between the two end users Lo Piparo & Razavi [2013].

The pioneering work of this type is developed by Duan, Lukin, Cirac and Zoller in 2001 Duan et al. [2001], known as DLCZ, where they proposed atomic ensembles and linear optics to achieve the goal. More specifically, at entanglement generation step, the DLCZ protocol uses laser pulses to shine on atomic ensembles, to potentially drive a single Stokes photon correlated with atomic excited state. The photonic states from both ensembles are then transmitted to and combined at a middle 50/50 beam splitter (BS). The entanglement is generated between the two ensembles conditional on that a single photon detector clicks. If more than one photon or no photon is detected, the process fails and has to be repeated. Regarding the entanglement connection step, the atomic excitation stored in the two co-located ensembles should firstly be converted into anti-Stokes photons, followed by the same process and verification mechanism as in the entanglement generation step. It is due to the collective effects of the atomic ensemble, which enhances the coupling efficiency between the memory and the photons, that guarantees the feasibility of the scheme Liu et al. [2001], Lukin et al. [2000], Phillips et al. [2001], Yu et al. [2020]. After being introduced, various improvements over the DLCZ protocol have been proposed over years, with further details can be found in Sangouard et al. [2011].

One thing that is worth mentioning and also relevant to this thesis is the comparison between single-photon and two-photon detections for the implementation of entanglement generation. We mention that the specific implementation steps and the detailed working mechanisms behind those two methods depend on different experimental platforms and techniques utilized, which are beyond the scope of this thesis. Here, we only point out the generic contrasts between them. Each method has its own strength and weakness. The best choice of scheme depends on the specific physical situation and the application in mind.

Typically speaking, entanglement generation based on single-photon detection would ask for only one photon, which could have come from either of two distant nodes, to survive through the path loss and reach the middle interferometer. Such an interference leads to a success probability p_{succ} of each attempt as

$$p_{\text{succ}} \sim p_c \eta \eta_d, \tag{2.9}$$

where p_c is the coupling efficiency of a photon with the memory, η is the transmitivity of the channel over half of the elementary link $L_0/2$ and η_d is the photon detector efficiency. Single-photon detection typically corresponds to the so-called photon-number encoding technique, where the state is represented by the Fock states $|0\rangle$ and $|1\rangle$, denoting the absence and presence of the photon, respectively. Such an encoding is of limited use on its own though this scheme may offer a larger success probability and thus better scaling rate, compared to the two-photon detection cases. Firstly, it poses challenging requirement on the stabilization of the channel. Any phase fluctuation is disruptive, but inevitable in practice, especially for long distances. Secondly, by using such an encoding, it is literally not possible to get a perfect maximally entangled state if no post-selection technique is applied, even though perfect operations are assumed.

In contrast, for entanglement generation based on two-photon detection, where two photons, one coming from each node, are interfered at the middle stations, the established entangled state can be theoretically perfect. Such a scheme usually corresponds to encoding on polarisation or time-bin, and is of more practical use. However, this comes at a price of lower success probabilities, proportional to p_{succ}^2 now and thus a worse rate scaling.

Here, to conclude this subsection, we mention that, in the original DLCZ protocol, both entanglement generation and swapping are based on single-photon detection. But later, the created single-excitation entanglement is more used as a building block for more directly useful two-photon entanglement; details can be found in Sangouard et al. [2011]. I will return to this point in Chapter 5, where I discuss these two schemes on a solid-state platform, i.e., NV-center in diamond.

2.3.2 Deterministic quantum repeaters

Deterministic QRs is a type of QR where their ES operations are performed in a gate-based deterministic way Razavi [2018]. Some solid-state platforms such as trapped-ions or vacancy centers in diamond are promising candidates for such implementations. In fact, when QRs were first introduced in 1998, by Briegel, Dür, Cirac and Zoller, known as the BDCZ protocol Briegel et al. [1998], the BSMs were implemented through deterministic but erroneous gates. In their

work, the authors assumed that the initial entanglement distribution and storage had already taken place, and the goal was to connect a string of those imperfect EPR pairs into a single distant pair of high fidelity.

The deterministic ES operation is achieved through the circuit depicted in Fig. 2.3(b). Unlike probabilistic BSMs, deterministic BSMs are not possible with only linear optics Lütkenhaus et al. [1999]. It is typically achieved through a strongly coupled spin system with optical resonators, which does not require two-way classical communication to confirm its success. The immediate advantage is that the waiting time can be now reduced and the rate is thus increased. However, the quality of the resulting pair decreases exponentially with the number of connections, even though perfect operations are assumed. In order to solve this, in the BDCZ paper, the authors proposed a nested purification protocol, where unlike the distillation proposals given in Bennett et al. [1996], Deutsch et al. [1996], only used one auxiliary pair with constant fidelity at each purification step to distill the entanglement. This technique could be iterated and applied at higher nesting levels, thereby connecting and purifying correlations between more and more distant nodes whereas the resources grow only logarithmically with the distance. However, similar to Bennett et al. [1996], Deutsch et al. [1996], it also relied on local operations and classical communication (LOCC), which, in effect, had turned a deterministic repeater protocol to a probabilistic one. A remedy to this problem was proposed in Jiang et al. [2009], in which ED is effectively done by using QEC techniques. This operation can, in principle, be done deterministically, and, combined with deterministic ES operations, it can give a boost to the entanglement generation rate in a QR. I now discuss it with more detail in the following section.

2.4 Quantum repeaters with encoding

In this thesis, in the spirit of having an eye on near-future implementations, our focus will be on the transition from probabilistic QRs to deterministic QRs that use QEC techniques for their ED operations Jiang et al. [2009], Munro et al. [2010], Zwerger et al. [2014]. The detailed structure which we are working on will be described explicitly in the following chapters when we look at each

specific case. Here, briefly speaking, in such QRs, using a number of bipartite entangled states, we create a multi-qubit entangled codeword across elementary links. As we apply the ES operations, this codeword structure will then allow us to correct some of the operational errors that happen because of imperfections in the employed gates, and/or the noisy transmission channel [1]. The usage of deterministic ES and ED can greatly reduce the waiting time of the system, since one does not need to wait until the success of the previous step before moving to the next one. All deterministic operations can be performed simultaneously. However, this advantage, which lowers required coherence times of QMs, may come at the price of more demanding quantum processing requirements.

Memory-less quantum repeaters

By further improving the QEC and quantum processing capabilities, one can design QR systems that totally remove the necessities of entanglement distribution or the usage of QMs. In those advanced QR protocols Azuma et al. [2015], Fowler et al. [2010], Glaudell et al. [2016], Munro et al. [2012], Muralidharan et al. [2014, 2018], also known as the third generation of QRs, one can directly encode the message into a codeword state and send it hop-by-hop across the whole link. The schematic of such QRs is depicted in Fig. 2.5. The message qubit is encoded into a logical state which is resilient to loss and/or operational errors at the sender side, and then transmitted to the intermediate node, at which, the encoded state will firstly be decoded and retrieved if there are errors and losses (note that this process is mainly operated on ancilla systems without disrupting or revealing any encoded information, thus those nodes can be untrusted), followed by another encoding process and transmission to the next middle nodes, until it reaches the receiver side. Such a protocol saves lots of times since it does not need any two-way classical signaling to confirm the success or failure, but comes at the price of highly demanding quantum information processing abilities and asks for high-precision control over a larger number of qubits in practice. In

[1] In this thesis, I only focus on the combat of operational errors. For tackling of loss errors or both loss and operation errors, please refer to Gingrich et al. [2003], Zwerger et al. [2014] and the cited reference in the following subsection for more detail.

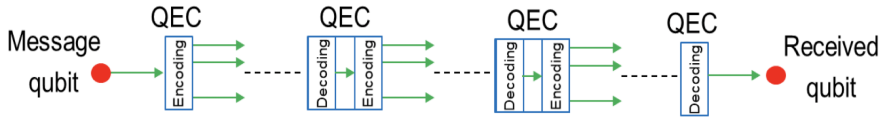

Figure 2.5: Schematic of the memory-less QR

fact, compared to the long-lived QM requirement for probabilistic QRs, this QR is even more challenging in terms of demonstration.

2.5 Quantum key distribution

With long-distance entanglement being established using QR protocols, one is able to perform many tasks such as secure communication Yin et al. [2020], clock synchronization Jozsa et al. [2000], quantum teleportation Pirandola et al. [2015], or simply use it as a building element for large-scale quantum internet Kimble [2008]. In this thesis, we limit ourselves to application of entanglement to QKD, which is perhaps the most mature quantum technology today.

QKD, the best-known application of quantum cryptography, provides a way of distributing and sharing secret keys based on quantum mechanics. Note that QKD does not necessarily rely on the establishment of entanglement. The basic principle behind QKD is the usage of non-orthogonal quantum states, which, due to the Heisenberg uncertainty principle, makes them impossible to be distinguished perfectly between each other without disturbing the system in a detectable way. The security of QKD does not rely on that the key never being intercepted, rather it relies upon detection of the eavesdropper, should they exist.

There are many different QKD protocols proposed over the past few decades: from BB84 Bennett & Brassard [1984, 2014], the first QKD protocol ever introduced in 1984, to memory-assisted QKD Bhaskar et al. [2020], Lo Piparo et al. [2017a,b], Panayi et al. [2014] and twin-field (TF) QKD Curty et al. [2019], Lucamarini et al. [2018], Zhong et al. [2019], the latest one being developed in 2018. Most of them fall into two categories: the prepare-and-measure protocols and the entanglement-based protocols. In this section, I will first briefly review the BB84 protocol, which is the first prepare-and-measure protocol and then describe its

entanglement-based counterpart, which is pertinent to this thesis. Finally I will discuss the main figure of merit used to quantify the performance of any QKD system.

2.5.1 Prepare-and-measure protocols

The concept of QKD was first introduced in the early 1970s, attributes to the work of Wiesner and Brassard Brassard & Crépeau [1996], but it was not until 1980s that it really began to shine, when Bennett and Brassard proposed the first ever QKD protocol, known as BB84 Bennett & Brassard [1984]. Its security is guaranteed by the impossibility of perfectly distinguishing between two non-orthogonal states, based on the Heisenberg uncertainty principle. The two complementary bases used for BB84 are typically the rectilinear basis (horizontal and vertical) and the diagonal basis (45° and 135°), where the key is encoded in the polarization photons. This protocol works in the following steps:

- **Raw key exchange:**
  (1) The sender, Alice, generates a long enough [1] random key string, and encodes each of them onto a polarised single photon with one of the two bases mentioned above.
  (2) She then sends the photons to the receiver, Bob, through the optical channel.
  (3) Bob randomly chooses one of the two bases for each photon he receives and then measures it.

- **Sifting:** Once there are a sufficient number of detections, Alice and Bob use a public but authenticated channel to communicate the measurement bases they choose. They keep the bits in which they have chosen the same basis and discard the others, after which, they end up with a sifted key.

- **Post-processing:** Alice and Bob apply error correction and privacy amplification techniques to reduce the discrepancy between their sifted keys and

[1] Long enough so that it can copy with the discarding of qubits for the following sifting and post-processing processes.

Alice's bits	0	0	1	1	0	1	0
Alice's sending basis	+	×	×	+	+	+	×
Photon polarization sent by Alice	→	↗	↖	↑	→	↑	↗
Bob's measuring basis	+	+	×	×	+	×	×
Photon polarization measured by Bob	→	Random	↖	Random	→	Random	↗
Public discussion							
Shared secret key	0		1		0		0

Table 2.1: An example of BB84 protocol.

the amount of information that might have leaked to the eavesdropper, Eve. This results in the final key shared between Alice and Bob.

An example of how BB84 works is sketched in Table 2.1. In order to check the presence of Eve, Alice and Bob have to estimate the discrepancy rate where they get discordant outcomes given the same choice of measurement basis, known as quantum bit error rate (QBER). This procedure may require making a part of the sifted key publicly available, which is then discarded and not used to create the key. This process offers the main parameters which will be used for secret key rate calculation. We mention that only photons that have successfully arrived will be measured. Photons that are lost or absorbed never arrive so are never considered for key generation. If the QBER is greater than a certain threshold (this threshold is typically $\sim 11\%$ Lütkenhaus [1999], but can be improved with more advanced post-processing techniques Pirandola et al. [2020]), the whole protocol will be aborted [1].

[1] In QBER estimation, we always consider the worst case scenario by assuming that all measured errors are down to eavesdroppers, even if some of them are not.

2.5.2 Entanglement-based protocols

Another main category of QKD protocols is based on entanglement, which is the focus of this thesis. The first entanglement-based protocol was proposed by Ekert in 1991, known as Ekert91 Ekert [1991]. This protocol consists of a source located between Alice and Bob, which emits pairs of entangled photons in the Bell state $|\psi^+\rangle_{AB}$, as given by Eq. (2.2). The photons then fly apart towards the two users where Alice and Bob randomly choose different measurement bases in their sets

$$\text{Alice} = \{0°, 45°, 90°\}, \quad \text{Bob} = \{45°, 90°, 135°\}, \tag{2.10}$$

respectively, for each photon they receive and measure it. They then publicly announce the bases they have chosen for each particular measurement and divide them into two groups: the first group for which they chose the same orientation and the second group for which they chose different ones. They discard the cases in which either or both of them failed to register a photon. Next, they use the outcomes of the second group, which need to be publicly announced, to test Bell inequality Bell [1964]. If Eve intercepts the entangled state, she would unavoidably demolish the quantum correlation and leave a footprint. Otherwise, if the absence of Eve can be proved, Alice and Bob are then able to extract the secret key based on the outcomes in their first group. The bit values 0 and 1 are assigned to different orientations following the rules shown in Table 2.1. Note that in this protocol, Alice and Bob do not need to trust the entanglement source and it can even be hold by Eve. Since the violation of the Bell inequality guarantees the existence of entanglement. Based on its monogamy property which states that two quantum systems that are maximally entangled cannot share any entanglement with a third party Coffman et al. [2000], Werner [1989a], the security of the protocol can be ensured.

Another important entanglement-based protocol, which is also the one used for this thesis in Chapters 3, 4 and 5, is BBM92, proposed by Bennett, Brassard and Mermin in 1992 Bennett et al. [1992]. It can be seen as an "entanglement version" of the original BB84 protocol in which they basically share the same sifting and post-processing steps. More explicitly, this protocol works in the following steps:

- **Raw key exchange:**
  (1) An entangled photon pair is generated between Alice and Bob and then flies apart towards them.
  (2) Alice and Bob randomly choose one of the two bases: the rectilinear one or the diagonal one, to measure the photon she/he received. The bit values 0 and 1 are assigned to corresponding polarizations following the rules as shown in Table 2.1.
  (3) This process is repeated many times until they have enough number of bits.

- **Sifting and post-processing:** These are operated similarly to BB84.

If the EPR sources, instead of located in between, is directly held by Alice. She can first measure one photon through the randomly chosen basis and then send the other, now with a known random polarization, to Bob. This would be equivalent to BB84 protocol. Since BBM92 does not require the test of Bell inequality, it should be more feasible than Ekert91 in terms of implementation. However, it is worth mentioning that Ekert91 is now expanded to the domain of device-independent QKD which is a type of protocol that is supposed to offer ultimate security, since it removes the characterisation requirements on the devices employed for implementation Vazirani & Vidick [2019]. This topic is beyond the scope of this thesis, and will not be expanded here.

Although BBM92 is entanglement-based, it does not rely on the violation of Bell inequality to guarantee the security of the scheme. In fact, its security analysis is similar to that of BB84, in which the existence of Eve can be detected by the calculation of the discrepancy rate.

2.5.3 Secret key rate

One important figure of merit for the performance of QKD is the secret key generation rate. In the entanglement-based QKD domain, this rate is given as a product of the amount of key, i.e., the quantity of bits, that can be extracted per entangled state, known as the secret fraction Scarani et al. [2009], and the entanglement generation rate. The secret fraction, which we denote as r throughout

this thesis, quantifies the quality of the entangled state distributed. The entanglement generation rate, as the name suggests, quantifies the rate of generating long-distance entanglement or more precisely, reflects the time required and the success probability for the implementation of repeater protocols.

The secret fraction is at the core of QKD as it is the quantity to which security analysis should give a bound. One of the earliest rate bounds for entanglement-based QKD system was proposed by Shor and Preskill in 2000 Shor & Preskill [2000]. In their security analysis, the secret fraction is lower bounded by

$$r = 1 - h(e_z) - h(e_x), \tag{2.11}$$

where $h(p) = -p \log_2 p - (1-p) \log_2 (1-p)$ is the binary Shannon entropy, and e_z and e_x are the QBER in, respectively, Z and X measurement bases. Briefly speaking, the term $h(e_z)$ quantifies the amount of bit-flip errors out of the sifted key, which is estimated at the error correction step of post-processing, and the term $h(e_x)$ quantifies the amount of information that is leaked to Eve, which is characterized at the privacy amplification step of post-processing Razavi [2018]. It should be pointed out that Eq. (2.11) only holds in the asymptotic limit of infinitely long sifted keys. A finite size case would affect the accuracy of parameter estimation, and a reduction in the secret fraction is expected Scarani et al. [2009]. However, in this thesis, we only stick to the ideal situation in order to avoid the complexity of finite-key analysis. Note that this bound is highly dependent on the specific QKD protocol in mind. In principle, one can always consider more advanced protocols in order to improve it.

The entanglement generation rate (or the raw key rate for prepare-and-measure protocols) depends on the specific QR protocol and is certainly limited by the details of the setup, such as transmitivity of the channel, efficiency of the detectors and coupling efficiency of photons to QMs. I will discuss this in more detail when we come to specific protocols in Chapters 3, 4 and 5.

Chapter 3

Quantum key distribution over quantum repeaters with encoding: Using error detection as an effective post-selection tool

3.1 Introduction

In this chapter, as specified in Sec. 2.4, we look at an interesting class of QRs, which rely on QEC for their ED Jiang et al. [2009], and examine how best such systems can be used for QKD applications. In principle, one can choose different code structures to implement such systems. Here, we choose the repetition codes to study and develop our methodology. They offer a simple structure, which can make their implementation easier, and still have relevance in systems where one type of error is more dominant than the other. For instance, if the memory decoherence is affected mainly by a dephasing process, the corresponding errors are modelled by the Pauli operator Z Panayi et al. [2014], hence a code structure resilient to this type of error could be useful. The repetition codes would also offer a good learning platform, for theoretical studies, to better understand how different components of the system can affect the final result, and to come up with relevant techniques for analysing more complicated code structures.

Our main contributions in this chapter:

In this chapter, we devise an analytical method to study the above QR setups. We, however, realise that, even for the seemingly simple case of repetition codes, the analysis can become cumbersome quite quickly. Previous work on this subject Bratzik et al. [2014], Jiang et al. [2009] often relied upon various approximations to analyse the system. In our work, we try to remain as close as we can to the exact results and only use approximations that are analytically justified and numerically verified. Our approach relies on the *linearity* of the quantum circuits, and the *transversality* of the code employed to manage the complexity of the analysis. This will enable us to obtain an accurate picture of the requirements of such systems in practice.

Using our methodology, we study the performance of QKD systems run over QRs with three-qubit repetition codes by accounting for various sources of error in the setup. We identify the terms that significantly impact the secret key generation rate, and then assess its dependence on relevant error parameters. In previous work on this subject Bratzik et al. [2014], the repeater chain is used to create a bipartite entangled state, which the two users will then employ to exchange a secret key. In our work, we allow the users to exploit the information obtained during the ES and decoding stages to divide the states that they obtain, and keys generated from them, into different groups. This not only improves the key rate and the resilience of the system to errors, but also allows us to identify states that contribute the most to the secret key rate. It turns out that in most cases the key contribution is from what we refer to as the *golden* states for which no error has been detected at either swapping or decoding stage. This will enable us to use an efficient post-selection technique that not only simplifies the analysis of the system, but also can reduce the complexity in any practical demonstration of the setup. We believe that our work can pave the way for similarly detailed analysis of other repeater protocols with more complex encoding. This will enable quantitative rate-versus-resource analysis for various protocols.

This chapter is organized as follows. In Sec. 3.2, we begin with a description of the repeater protocol in Ref. Jiang et al. [2009] and the error models we use to formulate the problem in hand. In Sec. 3.3, we discuss the linearization method

employed for our study and go over the exact analysis for nesting level one. We fully study the effect of different terms, components, and system imperfections before generalizing our results, in Sec. 3.4, to higher nesting levels. We present the dependence of the secret key generation rate for such QRs on different error parameters and find the corresponding thresholds for extracting a nonzero secret key rate at different nesting levels. Finally, we conclude this chapter in Sec. 3.5.

3.2 System Description

In this section, we first start with a detailed review of the QR scheme with encoding proposed by Jiang *et al.* Jiang et al. [2009] and the respective quantum circuits designed to implement it. Then, we introduce the error models considered in our analysis, followed by the problem statement and the key objectives of our study.

In this work, we mainly use the 3-qubit repetition code as an example to illustrate and develop our key ideas and techniques, where the logical qubits are encoded as

$$|\tilde{0}\rangle = |000\rangle \quad \text{and} \quad |\tilde{1}\rangle = |111\rangle, \tag{3.1}$$

where $|0\rangle$ and $|1\rangle$ represent the standard basis for a single qubit. This code can correct up to one bit-flip error (or may be small amplitude errors on all three qubits). Although it is not a strong error correction code, the thorough analysis of its performance with possible errors considered in its implementation will still offer us an indication of how this type of QRs performs.

3.2.1 Quantum repeater with 3-qubit repetition code

Here, we describe the ideal setting of the protocol proposed in Jiang et al. [2009] in the special case of 3-qubit repetition codes. In this protocol, depicted schematically in Fig. 3.1, we first generate encoded entangled states across *all* elementary links, which is a probabilistic process due to the heralding distribution of original Bell pairs; and then apply deterministic ES operations at intermediate nodes to both distill and swap entanglement across the chain.

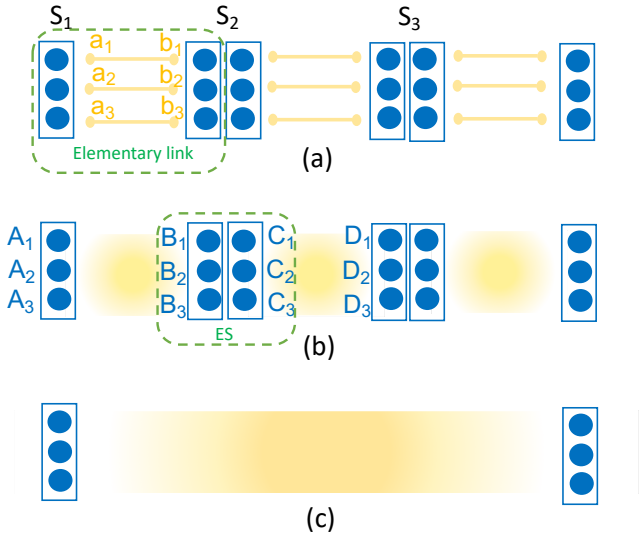

Figure 3.1: Schematic representation of quantum repeaters with encoding. (a) The codeword states are locally prepared at each memory bank (large blue circles) and original Bell pairs are distributed between neighboring nodes (small yellow circles connected by yellow lines); (b) Encoded Bell pairs are generated between neighbouring stations by performing remote CNOT gates; (c) The encoded ES operations are performed at each intermediate station simultaneously. This creates an encoded Bell pair between the two end users. Based on the measurement results at each middle node, the Pauli frame Knill [2005] of the final entangled state, which determines the establishment of a target encoded Bell state, can be adjusted.

The encoded entangled state of interest across an example elementary link A-B in Fig. 3.1 is in the form

$$|\tilde{\Phi}^{+}\rangle_{A,B} = \frac{1}{\sqrt{2}}(|\tilde{0}\rangle_A|\tilde{0}\rangle_B + |\tilde{1}\rangle_A|\tilde{1}\rangle_B), \tag{3.2}$$

where $|\tilde{i}\rangle_K \equiv |i\rangle_{K_1}|i\rangle_{K_2}|i\rangle_{K_3}$, for $i = 0, 1$ and $K = A, B$. In Fig. 3.1, the memory bank $K = \{K_1, K_2, K_3\}$ is shown by large (blue) circles. This multipartite entangled state is distributed between memory banks A and B in the following way:

Step 1 Initialize memory banks A and B in the codeword states $\frac{1}{\sqrt{2}}(|\tilde{0}\rangle_A + |\tilde{1}\rangle_A)$ and $|\tilde{0}\rangle_B$, respectively. The codeword state for node A can be achieved

by applying two (CNOT) gates, $\text{CNOT}_{A_1\to A_2}$ and $\text{CNOT}_{A_1\to A_3}$, on the state $\frac{1}{\sqrt{2}}(|0\rangle_{A_1}+|1\rangle_{A_1})|0\rangle_{A_2}|0\rangle_{A_3}$, where, in the notation $\text{CNOT}_{K\to J}$, K is the control qubit and J is the target qubit. We use the same notation for pairwise CNOT gates between qubits in two memory banks K and J. This ideally leads to the desired codeword state

$$\frac{1}{\sqrt{2}}(|000\rangle_A+|111\rangle_A)=\frac{1}{\sqrt{2}}(|\tilde{0}\rangle_A+|\tilde{1}\rangle_A). \tag{3.3}$$

The above state can, in principle, be obtained probabilistically as well, by repeating a preparation procedure until success. Given that the preparation is a local process, it can possibly be repeated at a sufficiently fast rate to ensure success in a reasonable time.

Step 2 In order to generate $|\tilde{\Phi}^+\rangle_{A,B}$, we share 3 bipartite maximally entangled states between the corresponding memories in memory banks a and b, shown by small yellow circles in Fig. 3.1(a), co-located, respectively, with memory banks A and B. These Bell states, shown by yellow lines in Fig. 3.1(a), can be distributed in advance, or in parallel with step 1. The implementation of this process and the quality of the generated entangled states depend on the specifics of the employed experimental platform. Normally, this step is mediated with photons, hence is often probabilistic and needs to be heralding.

Step 3 We use the distributed bipartite entangled states to implement three remote CNOT gates, see Fig. 3.2 and its caption for further detail, which are applied transversally, leading to the desired state for the elementary link:

$$\frac{1}{\sqrt{2}}(|\tilde{0}\rangle_A+|\tilde{1}\rangle_A)\otimes|\tilde{0}\rangle_B \overset{\text{CNOT}_{A\to B}}{\longrightarrow} |\tilde{\Phi}^+\rangle_{A,B}. \tag{3.4}$$

Once the encoded entangled states are distributed across all elementary links, the next step is to perform ES operations at all intermediate stations to extend the entanglement to the entire link. For instance, in Fig. 3.1(b), in order to establish multipartite entanglement between memory banks A and D, we perform an encoded Bell measurement on memory banks B and C. This, due to

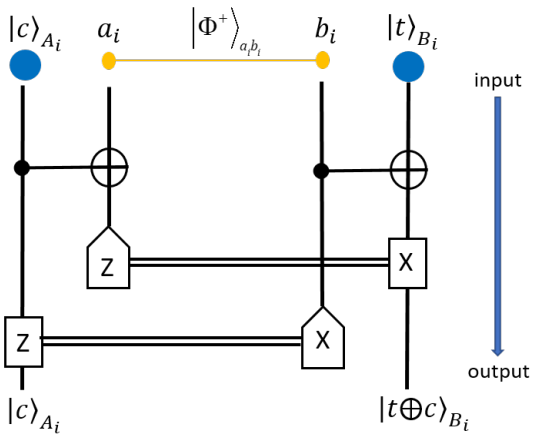

Figure 3.2: Circuit for remote CNOT gate Jiang et al. [2007] between a qubit c at node A_i, as control qubit, and a qubit t at node B_i, as the target qubit. Using the maximally entangled state shared between a_i and b_i nodes, and by applying two local CNOT gates on A_i-a_i and b_i-B_i pairs, we can effectively implement a remote CNOT gate on A_i-B_i. Note that this requires single-qubit measurements on a_i and b_i, classical communication, and local single-qubit rotation on A_i and B_i.

the *transversality* [1] of the employed code, is simply done by performing three individual BSMs on the corresponding pairs of physical qubits in B and C Jiang et al. [2009]. More specifically, such BSMs can be realized deterministically by applying $\text{CNOT}_{B_i \to C_i}$, followed by a projective X-measurement on qubit B_i and Z-measurement on qubit C_i, for $i = 1, 2, 3$. In the ideal case, right before the single-qubit measurements, the initial state of the two links would then undergo

[1] Roughly speaking, *transversality* is a property which ensures that a single error occurred anywhere in the encoded block causes at most one error per other block of the code. In essence, this property enables encoded gates to be constructed in a bitwise fashion and offers a general design principle for finding fault-tolerant circuits. For detailed explanation, please refer to Nielsen & Chuang [2002].

the following transformation Jiang et al. [2009]

$$\begin{aligned}
&|\tilde{\Phi}^+\rangle_{A,B} \otimes |\tilde{\Phi}^+\rangle_{C,D} \\
&= \frac{1}{2}(|\tilde{\Phi}^+\rangle_{A,D} \otimes |\tilde{\Phi}^+\rangle_{B,C} + |\tilde{\Phi}^-\rangle_{A,D} \otimes |\tilde{\Phi}^-\rangle_{B,C} \\
&\quad + |\tilde{\Psi}^+\rangle_{A,D} \otimes |\tilde{\Psi}^+\rangle_{B,C} + |\tilde{\Psi}^-\rangle_{A,D} \otimes |\tilde{\Psi}^-\rangle_{B,C}) \\
&\xrightarrow{\text{CNOT}_{B\to C}} \frac{1}{2}(|\tilde{\Phi}^+\rangle_{A,D} \otimes |\tilde{+}\rangle_B|\tilde{0}\rangle_C + |\tilde{\Phi}^-\rangle_{A,D} \otimes |\tilde{-}\rangle_B|\tilde{0}\rangle_C \\
&\quad + |\tilde{\Psi}^+\rangle_{A,D} \otimes |\tilde{+}\rangle_B|\tilde{1}\rangle_C + |\tilde{\Psi}^-\rangle_{A,D} \otimes |\tilde{-}\rangle_B|\tilde{1}\rangle_C),
\end{aligned} \tag{3.5}$$

where $|\tilde{\Phi}^\pm\rangle_{A,D} = \frac{1}{\sqrt{2}}(|\tilde{0}\rangle_A|\tilde{0}\rangle_D \pm |\tilde{1}\rangle_A|\tilde{1}\rangle_D)$, $|\tilde{\Psi}^\pm\rangle_{A,D} = \frac{1}{\sqrt{2}}(|\tilde{0}\rangle_A|\tilde{1}\rangle_D \pm |\tilde{1}\rangle_A|\tilde{0}\rangle_D)$ and

$$\begin{aligned}
|\tilde{\pm}\rangle_B &= \frac{1}{\sqrt{2}}(|\tilde{0}\rangle_B \pm |\tilde{1}\rangle_B) \\
&= \frac{1}{2}(|\pm\pm\pm\rangle_B + |\pm\mp\mp\rangle_B \\
&\quad + |\mp\pm\mp\rangle_B + |\mp\mp\pm\rangle_B),
\end{aligned} \tag{3.6}$$

with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ for a single qubit.

By measuring the states of B_i and C_i, $i = 1, 2, 3$, in, respectively, X and Z basis, we project the state of A and D in Eq. (3.5) into one of the encoded Bell states. This becomes possible because all terms in $|\tilde{+}\rangle$ ($|\tilde{-}\rangle$) have an odd (even) number of $|+\rangle$ states, and measuring $|\tilde{0}\rangle$ ($|\tilde{1}\rangle$) ideally results in three $|0\rangle$ ($|1\rangle$) states. In the non-ideal case, it is possible that, instead of three identical outputs, we get, for instance, two $|0\rangle$s and one $|1\rangle$. But, then, because of the employed error correction scheme, we can still identify which Bell state is the most likely outcome of the ES process. Note that, by accounting for the erroneous cases, there will be 64 different combinations of measurement outcomes, and each of them will uniquely lead to one type of encoded Bell pair. Even though the measurement outcomes at each middle station should be announced to Alice and Bob to determine the Pauli frame for the encoded Bell pair shared by them in the end, this scheme would not rely on any communication among middle stations, which reduces the time scaling from polynomial to polylogrithmic Muralidharan et al. [2016]. For applications, such as QKD, that can deal with Pauli frame adjustments at the post-measurement stage, this scheme also lowers the waiting time, and correspondingly the required coherence time for the memories.

After all ES operations, an encoded entanglement is ideally distributed between the two end users. In order to do QKD, or other possible applications, the final encoded entangled states can be decoded into a bipartite state. The decoding circuit employed in this work is simply the reverse process of the encoding procedure for three-qubit repetition codes Bratzik et al. [2014], as depicted in Fig. 3.3. Alice and Bob each apply this circuit to their three qubits in hand, and measure two of them. They flip the first qubit only if they measure $|1\rangle$ in the other two qubits.

The above repeater protocol implements an implicit entanglement distillation by using error correction techniques. This is partly done at the ES stage and is supplemented by the final error correction that happens at the decoding stage. But, for protocols such as QKD, which can cope with discarding data if needed, the other possibility is to use the information available at the ES stations to discount the end-to-end distributed state if an error has been detected at any intermediate stage. By doing so, we only keep the cases for which we are more confident that we have got the desired Bell state, and, effectively, distill the entanglement generated by the repeater chain. So long as the chance of error is low, this still offers a nearly deterministic solution for quantum repeaters.

In this work, we will examine how the above idea can improve the performance of QKD systems that run over such repeaters. It turns out that the secret key rate of such QKD systems is dominated by the post-measurement state corresponding to when no error has been detected at ES and decoding stages. Nevertheless, we still need to calculate the effect of errors on system performance. Detecting no errors by our error correction scheme does not guarantee the absence of errors. The decoded state is still affected by errors not detectable by our error correction scheme, some of which would correspond to higher order error terms that may not be properly accounted for if our analysis is not sufficiently accurate. In the following, we first summarise the error models used in our analysis. We then describe the problem in the context of previous research on this subject.

3.2.2 Error models

Three major imperfections are considered in our analysis:
(1) **Imperfections in initial Bell states:** The originally distributed Bell states,

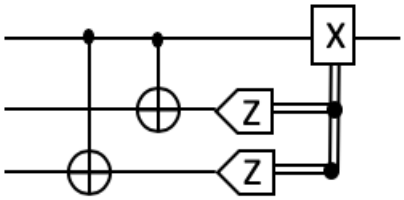

Figure 3.3: Quantum circuit for decoding 3-qubit repetition codes Bratzik et al. [2014]. Alice and Bob will both use the same circuit for decoding, in which they flip their first qubit if they measure $|1\rangle$ in all other qubits.

i.e., yellow links in Fig. 3.1(a), are not necessarily perfect. We model them as Werner states Werner [1989b] with fidelity F_0:

$$\rho^{\mathrm{W}} = F_0|\phi^+\rangle\langle\phi^+| + \frac{1-F_0}{3}(\mathbb{I}_4 - |\phi^+\rangle\langle\phi^+|), \tag{3.7}$$

where $|\phi^+\rangle$ is given by Eq. (2.1) and $\mathbb{I}_4$ is a 4×4 identity matrix.
(2) **Gate imperfections:** We employ the generic model for imperfect two-qubit operations introduced in Ref. Briegel et al. [1998]. The unitary operation $U_{i,j}$, acting on qubits i and j, is modelled by

$$\rho^{\mathrm{out}} = (1-\beta)U_{i,j}\rho^{\mathrm{in}}U_{i,j}^{\dagger} + \frac{\beta}{4}\mathrm{Tr}_{i,j}(\rho^{\mathrm{in}})\otimes\mathbb{I}_{i,j}, \tag{3.8}$$

where ρ^{in} (ρ^{out}) is the input (output) before (after) the two-qubit gate $U_{i,j}$, β is the gate error probability and $\mathbb{I}_{i,j}$ is the identity matrix for qubits i,j. The first term in Eq. (3.8) models the error-free component, whereas the identity operator in the second term, corresponding to the case of an error, fully and uniformly decoheres the state of qubits i and j. The main two-qubit gate used in this chapter is $\mathrm{CNOT}_{i\to j}$.
(3) **Measurement imperfections:** The projective measurements with errors to states $|0\rangle$ and $|1\rangle$ are, respectively, represented by

$$\begin{aligned} P_0 &= (1-\delta)|0\rangle\langle 0| + \delta|1\rangle\langle 1| \quad \text{and} \\ P_1 &= (1-\delta)|1\rangle\langle 1| + \delta|0\rangle\langle 0|, \end{aligned} \tag{3.9}$$

where δ is the measurement error probability. Similar measurement operators, $P_{\pm}$, are used for projective measurement in $|\pm\rangle$ basis.

In our analysis, we neglect other types of errors that may be present in a real setup. For instance, we assume all single-qubit unitary operations, i.e., bit-flip (X gate) or phase-flip (Z gate) rotations, are perfect. In the case of QKD as an application, this is justified as these operations can typically be implemented in the classical post-processing stage. In order to simplify the analysis, we also assume that quantum memories with sufficiently long coherence times are available. Considering that the waiting time for encoded QRs is comparatively low, we neglect the memory decoherence effects in this chapter. However, this effect will be discussed in more detail in Chapter 5, when we apply this QR structure to NV center platforms.

3.2.3 Problem Description

In this work, we study the performance of a QKD system that is run over an encoded QR setup with three-qubit repetition codes by accounting for errors in the setup as presented above. We consider an entanglement-based QKD setup that relies on BBM92 protocol Bennett et al. [1992]. We use an asymmetric implementation of the protocol where the two end users, Alice and Bob, choose the two measurement bases, i.e., Z and X bases, unevenly, in order to increase the basis-sift factor Lo et al. [2005a]. Our objective is to assess the dependence of the secret key generation rate in our QKD system on relevant error parameters. To this end, we first need to calculate the secret key generation rate per decoded state, ρ^{dec}, shared between Alice and Bob. In the asymptotic regime, this parameter, known as secret fraction Bratzik et al. [2014], is given by Shor & Preskill [2000]

$$r_{\infty}(\rho^{\text{dec}}) = \max\{0, 1 - h(e_z) - h(e_x)\}, \tag{3.10}$$

where $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary Shannon entropy, and

$$\begin{aligned} e_z &= \mathrm{Tr}(P_0^{\mathrm{Alice}} P_1^{\mathrm{Bob}} \rho^{\mathrm{dec}}) + \mathrm{Tr}(P_1^{\mathrm{Alice}} P_0^{\mathrm{Bob}} \rho^{\mathrm{dec}}) \\ &= (\delta^2 + (1-\delta)^2)(\langle\psi^+|\rho^{\mathrm{dec}}|\psi^+\rangle + \langle\psi^-|\rho^{\mathrm{dec}}|\psi^-\rangle) \\ &\quad + 2\delta(1-\delta)(\langle\phi^+|\rho^{\mathrm{dec}}|\phi^+\rangle + \langle\phi^-|\rho^{\mathrm{dec}}|\phi^-\rangle) \\ e_x &= \mathrm{Tr}(P_+^{\mathrm{Alice}} P_-^{\mathrm{Bob}} \rho^{\mathrm{dec}}) + \mathrm{Tr}(P_-^{\mathrm{Alice}} P_+^{\mathrm{Bob}} \rho^{\mathrm{dec}}) \\ &= (\delta^2 + (1-\delta)^2)(\langle\phi^-|\rho^{\mathrm{dec}}|\phi^-\rangle + \langle\psi^-|\rho^{\mathrm{dec}}|\psi^-\rangle) \\ &\quad + 2\delta(1-\delta)(\langle\phi^+|\rho^{\mathrm{dec}}|\phi^+\rangle + \langle\psi^+|\rho^{\mathrm{dec}}|\psi^+\rangle) \end{aligned} \tag{3.11}$$

are, respectively, the observed error rates in Z and X bases. $|\phi^{\pm}\rangle$ and $|\psi^{\pm}\rangle$ are the corresponding Bell states in the joint space of Alice and Bob, given by Eq. (2.1) and Eq. (2.2), respectively. Measurement operators are defined according to Eq. (3.9) with additional superscripts to specify the affected qubit.

In order to understand the effect of various system parameters on the final secret key rate, we simulate the above setting in the nominal mode of operation where no eavesdropper is present. In this case, ρ^{dec} will then be given by the shared state between Alice and Bob after decoding, from which we can calculate the error parameters e_z and e_x in the asymptotic regime, where an infinite number of entangled states are shared among users. Our problem would then reduce to specifying what ρ^{dec} is in a typical error-prone QR setting with encoding.

While at first glance this may look like a quite straightforward problem, in practice, we face some computational challenges. The obvious way to calculate the final entangled state is to obtain the encoded entangled state at each elementary link and then apply ES in a nested way. For a 3-qubit repetition code, the ES operation involves 12 qubits, so our operation is on a space with dimension 2^{12}. This may sound manageable, but certainly not scalable. The next simplest code, i.e., 5-qubit repetition code, requires operation on 20 qubits, or a space of dimension 2^{20}. It is easy to see how problem can get out of hand quite quickly. Proper analytical and numerical techniques are then needed to handle this problem.

Previous work on this subject Bratzik et al. [2014], Jiang et al. [2009] often rely on various approximations to solve the problem. The original work in Jiang et al. [2009] makes some assumptions on how the initial states are prepared, based on which they estimate how much error, to the first order, is expected in

each qubit. They then use their method to approximate the fidelity of the final state. While a good approach to prove the scaling improvement offered by their proposed scheme, it falls short of the accurate scheme that we need for key rate calculations. A follow-up paper by Bratzik *et al.* Bratzik et al. [2014] attempted to fill this gap by approximating the actual state that one would obtain for the decoded state of a 3-qubit repetition code by accounting for imperfections in the CNOT gates as well as the initial Bell states. They use several approximations to achieve this goal:

- They model the error in a cascade of operations by separating the ideal and the first-order error term in the output from the rest, where the rest is modelled by a generic identity operator at the output. The first-order error term is modelled by the identity operator for the involved qubits in the operation.
- They find a set of operations that will be corrected by the BSM operation, in addition to what may be corrected by the employed code. Based on this, they find a set of correctable states that will be mapped to the desired encoded Bell states. They use these states to crudely calculate the probability of obtaining the desired state after a number of ES operations, and assume that, in all other cases, the identity operator is obtained.

Based on the above assumptions, they would then conclude that the considered encoded QR cannot beat the original QR protocol in Briegel et al. [1998] in terms of the achievable key rate or the required gate error parameters.

In this work, we improve upon the approach taken in Bratzik et al. [2014] in several respects. First, we improve the accuracy of the calculations by accounting for errors in each gate individually rather than modelling the overall effect, for a cascade of gates, in a crude way. Our approach enables us to show that the encoded QRs are resilient to larger margins of error than previously thought. It is also easier to apply our method to other codes than the 3-qubit repetition code considered in Bratzik et al. [2014], as some of their steps are specific to this employed code. As such, extending their approach to other code structures is not necessarily straightforward. Here, we employ an analytical approach that relies on

the *linearity* of the quantum circuits and the *transversality* of the employed code. In principle, our approach can be applied to other code structures as long as they pose the *transversality* property. Finally, an important element of our key rate analysis is to use the information reported by the middle nodes of the repeater chain at its end nodes. This allows us to classify the decoded states, based on the measurement results at the ES and decoding stages, resulting in a considerable improvement of system performance. This also reduces the complexity of the corresponding key rate analysis. Overall, this work enables us to obtain a more accurate picture of the requirements of such systems in practice, and whether, any simplified version of them, can realistically be built with current technologies.

In the following sections, we will first use the simplest repeater setup, where only one swap operation is performed, to describe our methodology, and to justify certain simplifying assumptions that we make in neglecting the less dominant terms. Then, we will extend our results to higher nesting levels and obtain the secret key rate in our setup as a function of various system parameters. We will also compare our calculation results to the one show in Bratzik et al. [2014].

3.3 Methodology and Performance: Nesting level one

In this section, we look at the simplest repeater setup with only one middle node corresponding to nesting level one. The initial objective here is to find a scalable methodology by which the final entangled state shared by Alice and Bob can be calculated. We then find the secret fraction corresponding to different decoded states conditioned on the measurement results at the ES and decoding stages. This allows us to better understand how each term and each imperfection affect system performance. This guides us toward finding simple, but still tight, approximations that reduce the complexity of the problem in hand.

3.3.1 Linearization

Our first objective is to develop a methodology to calculate the joint state between memory banks A and D, ρ_{AD}, in Fig. 3.1(b), after one round of entanglement

swapping. We first explain this procedure when the initial codeword states in memory banks A–D are perfectly encoded as follows

$$\begin{aligned}\rho_A^{\text{in}} &= \frac{1}{2}(|000\rangle_A + |111\rangle_A)({}_A\langle 000| + {}_A\langle 111|) \\ &= \frac{1}{2}[(|0\rangle_A\langle 0|)^{\otimes 3} + (|0\rangle_A\langle 1|)^{\otimes 3} \\ &+ (|1\rangle_A\langle 0|)^{\otimes 3} + (|1\rangle_A\langle 1|)^{\otimes 3}], \\ \rho_B^{\text{in}} &= |000\rangle_B\langle 000| = (|0\rangle_B\langle 0|)^{\otimes 3},\end{aligned} \tag{3.12}$$

where $(|i\rangle_K\langle j|)^{\otimes 3} \equiv |i\rangle_{K_1}\langle j| \otimes |i\rangle_{K_2}\langle j| \otimes |i\rangle_{K_3}\langle j|$, for $i, j = 0, 1$. The initial state for C and D, ρ_C^{in} and ρ_D^{in}, are, respectively, similar to that of A and B. In this case, we can first find the joint state ρ_{AB} (ρ_{CD}) of memory banks A and B (C and D) after the remote CNOT operation, and then apply the ES operation. In this case, we have

$$\rho_{AB}^r = \frac{U_{AB}^r \text{Tr}_{ab}[M_{\text{RC}}^r \mathcal{E}_{\text{RC}}(\rho^{\text{in}})] U_{AB}^r}{\text{Tr}[M_{\text{RC}}^r \mathcal{E}_{\text{RC}}(\rho^{\text{in}})]}, \tag{3.13}$$

where Tr_{ab} is the partial trace over memory banks a and b, $\mathcal{E}_{\text{RC}}$ is the combination of all remote CNOT gate operations on Aa and bB memory banks, M_{RC}^r is the collective projective measurement operator at this step corresponding to the pattern of measurement results given by r, and U_{AB}^r is the corresponding Pauli frame correction in Fig. 3.2. In Eq. (3.13), the input state is given by

$$\rho^{\text{in}} = \rho_A^{\text{in}} \otimes \rho_B^{\text{in}} \otimes \rho_{ab}^{\text{W}}, \tag{3.14}$$

where $\rho_{ab}^{\text{W}} = \rho_{a_1b_1}^{\text{W}} \otimes \rho_{a_2b_2}^{\text{W}} \otimes \rho_{a_3b_3}^{\text{W}}$ as given by Eq. (3.7) for the subsystems specified by the subscripts. The quantum operation $\mathcal{E}_{\text{RC}}$ is also given by

$$\mathcal{E}_{\text{RC}} = \mathcal{E}_1 \otimes \mathcal{E}_2 \otimes \mathcal{E}_3, \tag{3.15}$$

with, for $i = 1, 2, 3$,

$$\mathcal{E}_i = \mathcal{E}_{A_ia_i} \otimes \mathcal{E}_{b_iB_i}, \tag{3.16}$$

where $\mathcal{E}_{KJ}$ is given by the transformation in Eq. (3.8) for the gate $\text{CNOT}_{K\to J}$.

As mentioned earlier the direct approach of calculating $\mathcal{E}_{\text{RC}}(\rho^{\text{in}})$ requires dealing with a space of dimension 2^{12} even for the simple 3-qubit repetition code

considered here. In order to simplify the process and reduce the time required for running the code, we use the linearity and transversality of operator $\mathcal{E}_{\rm RC}$ and its tensor product form in Eq. (3.15). To be more precise, using Eq. (3.12), we have

$$\mathcal{E}_{\rm RC}(\rho^{\rm in}) = \frac{1}{2}\sum_{j,k=0,1}\bigotimes_{i=1}^{3}\mathcal{E}_i(|j\rangle_{A_i}\langle k|\otimes|0\rangle_{B_i}\langle 0|\otimes\rho^{\rm W}_{a_ib_i}). \tag{3.17}$$

By the above trick, we reduce the computational complexity of the problem to effectively that of a 4 qubit system in each row comprising of qubits A_i, a_i, b_i, and B_i, for $i = 1, 2, 3$. For each component of the input state, we just need to calculate the output for one row, extend it to all rows by a simple tensor product, and then sum over all possible input components.

In order to calculate ρ^r_{AB} in Eq. (3.13), we also need to apply measurement operators. It turns out, however, that similar to a teleportation scheme, once unitary corrections, which are assumed error free here, are applied, the output state will not be a function of the measurement outcome. In fact, one can see in Fig. 3.2 that for any Bell state at a_ib_i input, the chance of having $|0\rangle$ and $|1\rangle$, at each input is identical. This probability does not change by the unitary operation of CNOT gates, or the identity operator in case of an error, hence right before Z and X-basis measurements on a_ib_i, all four possible outcomes are equally likely. Without loss of generality, we then drop the superscript r and calculate the output state for the particular r corresponding to $|0+\rangle_{a_ib_i}$, $i = 1, 2, 3$, for which no Pauli frame correction is needed. We can then apply relevant normalisation factors to Eq. (3.17) to find the joint state ρ_{AB} of memory banks A and B, and similarly C and D, after remote CNOT operation as follows:

$$\rho_{AB} = \frac{1}{2}\sum_{j,k=0,1}\bigotimes_{i=1}^{3}\rho^{jk}_{A_iB_i}, \tag{3.18}$$

where

$$\rho^{jk}_{A_iB_i} = 4{\rm Tr}_{a_ib_i}[P_0^{a_i}P_+^{b_i}\mathcal{E}_i(|j\rangle_{A_i}\langle k||0\rangle_{B_i}\langle 0|\rho^{\rm W}_{a_ib_i})]. \tag{3.19}$$

The next step is to model the ES stage, which can also be thought of certain gate operations, represented collectively by $\mathcal{E}_{\rm ES}$, followed by some single-qubit

measurements. In this case, the joint state of memory banks A and D, upon observing a measurement outcome m on B and C, is given by

$$\rho_{AD}^{m} = \frac{U_{AD}^{m}\mathrm{Tr}_{BC}[M_{BC}^{m}\mathcal{E}_{\mathrm{ES}}(\rho_{\mathrm{ES}}^{\mathrm{in}})]U_{AD}^{m}}{p_m}, \tag{3.20}$$

where $p_m = \mathrm{Tr}[M_{BC}^{m}\mathcal{E}(\rho_{\mathrm{ES}}^{\mathrm{in}})]$, M_{BC}^{m} is the collective projective measurement operator on memory banks B, in X basis, and C, in Z basis, corresponding to the measurement result m, U_{AD}^{m} is the corresponding Pauli frame correction, and the input state is given by

$$\rho_{\mathrm{ES}}^{\mathrm{in}} = \rho_{AB} \otimes \rho_{CD}, \tag{3.21}$$

with

$$\mathcal{E}_{\mathrm{ES}} = \bigotimes_{i=1}^{3} \mathcal{E}_{B_iC_i}. \tag{3.22}$$

Using the linear form of the input states as in Eq. (3.18), we then obtain

$$\mathcal{E}_{\mathrm{ES}}(\rho_{\mathrm{ES}}^{\mathrm{in}}) = \frac{1}{4}\sum_{j,k=0,1}\sum_{n,l=0,1}\bigotimes_{i=1}^{3}\mathcal{E}_{B_iC_i}(\rho_{A_iB_i}^{jk} \otimes \rho_{C_iD_i}^{nl}), \tag{3.23}$$

in which, again, the BSM operation is identical and separable in all rows, and only needs to be calculated once per row in our simulation code. Basically, by breaking the codeword in Eq. (3.12) into its individual terms, we have broken the entanglement that exists across different rows of Fig. 3.1(b) and can now deal with the state evolution in each row separately. The entanglement will be put together where in the end we add all corresponding terms before applying the decoding operation.

This whole process, including the imperfect measurement and decoding ones, has analytically been implemented in Mathematica to provide us with an exact description of ρ_{AD}^{m}, and its corresponding decoded states, for the first nesting level. The measurement part is straightforward as it also can be implemented horizontally along each row according to Eq. (3.9), by which B registers are measured in X basis and C memories are measured in Z basis. That is, in Eq. (3.20), we have

$$\mathrm{Tr}_{BC}[M_{BC}^{m}\mathcal{E}_{\mathrm{ES}}(\rho_{\mathrm{ES}}^{\mathrm{in}})] = \frac{1}{4}\sum_{j,k=0,1}\sum_{n,l=0,1}\bigotimes_{i=1}^{3}\rho_{A_iD_i}^{jknl}(m_i), \tag{3.24}$$

where

$$\rho^{jknl}_{A_iD_i}(m_i) = \mathrm{Tr}_{B_iC_i}[M^{m_i}_{B_iC_i}\mathcal{E}_{B_iC_i}(\rho^{jk}_{A_iB_i} \otimes \rho^{nl}_{C_iD_i})], \tag{3.25}$$

with $M^m_{BC} = \bigotimes_{i=1}^{3} M^{m_i}_{B_iC_i}$ and m_i representing the measurement outcome in row i. The decoding process has been implemented by modelling the CNOT gates in the decoding circuit of Fig. 3.3 according to Eq. (3.8). By referring to the whole decoding procedure by operator $\mathcal{E}_{\mathrm{dec}}$, we can obtain the final decoded state as follows

$$\rho^{\mathrm{dec}}_{m,d} = \frac{U^d_{A_1D_1}\mathrm{Tr}_{A_2A_3D_2D_3}[M^d_{\mathrm{dec}}\mathcal{E}_{\mathrm{dec}}(\rho^m_{AD})]U^d_{A_1D_1}}{p_{d|m}}, \tag{3.26}$$

where $p_{d|m} = \mathrm{Tr}[M^d_{\mathrm{dec}}\mathcal{E}_{\mathrm{dec}}(\rho^m_{AD})]$, M^d_{dec} is the corresponding measurement operator to outcome d at the decoder ends, and $U^d_{A_1D_1}$ is the corresponding correction operator.

Computationally speaking, in our method, we are mostly dealing with only 4-qubit systems. This considerably simplifies analytical calculations. There are, however, some exceptions to this. For the 3-qubit repetition code, the last step in Eq. (3.26) would involve dealing with a 6-qubit system, which is manageable. As the code grows in size, full implementation of the decoding circuit, which requires handling a multipartite entangled state in its input, would become more challenging. In that case, our scheme would still be helpful if we ignore the errors in the decoding circuit. Alternatively, one can think of simpler decoder structures that only rely on single-qubit measurements, which we will discuss in more detail in the next chapter. Imperfect encoding could also cause additional complexity in our technique. In the next subsections, we assess the importance of both encoding and decoding modelling in our analysis. But, before that, let us first explore which measurement outcomes would impact our secret key generation rate the most.

3.3.2 Good, bad, and golden states

The procedure described above can be used to find the decoded state, $\rho^{\mathrm{dec}}_{m,d}$, for any possible outcome m of the ES stage and d of the decoding stage. There are, however, 64 possible values for m and 16 for d, each of which could result in a

different decoded state, hence different secret key fraction for all those instances that we have got the same measurement outcomes.

To calculate the total secret fraction, we need to average over all possible outcomes as follows

$$r_{\infty}^{\text{total}} = \sum_{m,d} p_{m,d} r_{\infty}^{m,d}, \tag{3.27}$$

where

$$p_{m,d} = p_m p_{d|m} \tag{3.28}$$

is the probability of getting the measurement outcomes m and d and $r_{\infty}^{m,d} = r_{\infty}(\rho_{m,d}^{\text{dec}})$ is the secret fraction obtained from Eq. (3.10) and Eq. (3.11).

Note that in Eq. (3.27) we make full usage of the available measurement information, m and d, from earlier steps. This is expected to give us a higher key rate than the key rate that can be calculated from the state averaged over different ES and/or decoder outcomes. This is because of the convexity of the secret fraction formula in Eq. (3.10) as a function of e_x and e_z. Figure 3.4 confirms this assertion by comparing the secret fraction for the following four cases at $\delta = 0$ and $F_0 = 0.98$ versus β [1]: (i) when we use the full information in m and d as proposed in this work (solid line); (ii) when we assume the users have no knowledge of m, but know d, which can be locally obtained by each user (dash-dotted line). In this case, we first find the average ES state over all possible values of m, and then pass it to our decoder circuits; (iii) when the users have the information from the ES stage, but the decoder output d will only be used internally in the decoder to correct the shared state (dashed line). In this case, the total secret fraction is given by $\sum_m p_m r_{\infty}(\rho_m)$, where $\rho_m \equiv \sum_d p_{d|m} \rho_{m,d}^{\text{dec}}$; and (iv) when the users do not know of either m or d before doing QKD measurements (dotted line), i.e., when the decoded state is given by $\rho_{\text{avg}} = \sum_{m,d} p_{m,d} \rho_{m,d}^{\text{dec}}$. In this case, the whole repeater chain and decoders are seen as a black-box channel by the users. As can be seen, by accounting for all different outcomes separately, we can tolerate, respectively, roughly three and two times larger values of β, as compared to the cases where we use ρ_{avg} or ρ_m for secret key extraction. Even if we only use the information at the decoder units, which is at the same place

[1] For the definition of these three parameters, please refer to Eqs. (3.7-3.9), respectively.

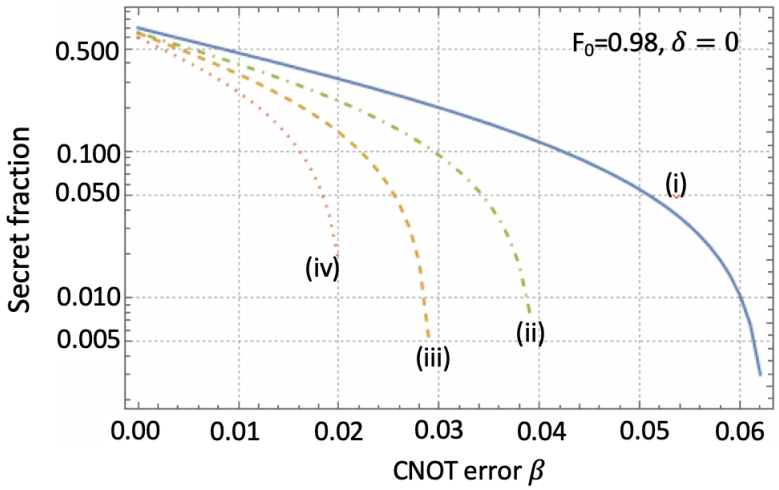

Figure 3.4: Secret fraction at $F_0 = 0.98$ and $\delta = 0$ for (i) when we fully use the knowledge of m and d, as given by Eq. (3.27) (solid blue curve), versus (ii) when only d is known to the users, but not m (dash-dotted green curve), or (iii) when only m is known to the users, but not d (dashed amber curve), or (iv) when none of m and d is used for key extraction (dotted red curve).

as the users' locations, we can obtain higher key rates than cases (iii) and (iv). This shows the importance of the internal information across the repeater chain and the user boxes in our QKD system. Note that a similar observation has been made for third generation quantum repeaters, and how accounting for syndrome information can boost system performance Namiki et al. [2016].

The key rate calculation in Eq. (3.27) can be cumbersome as many terms need to be considered. There are several ways by which we can group different terms in Eq. (3.27) together to reduce the required computation. First, note that, for QKD applications, the secret key analysis is independent of which Bell state is the target state as they are all the same up to local Pauli rotations. Furthermore, the Pauli frame adjustments needed after the BSMs consists of a series of single-qubit operations, which, in our analysis, are assumed perfect. Thus, in this work, we calculate the secret fraction for only $|\tilde{\Phi}\rangle_{A,D}$ as the ES measurement outcome, and use the same result for other encoded Bell states in Eq. (3.5). This reduces the number of relevant ES outcomes to 16 corresponding to the measurement

results $\{|++\rangle_B, |+-\rangle_B, |-+\rangle_B, |--\rangle_B\}$, at memory bank B, and $\{|000\rangle_C, |001\rangle_C, |010\rangle_C, |100\rangle_C\}$, at memory bank C. Further investigation shows that the four different outcomes at memory bank B do not affect the generated secret fraction as long as the measurement results at memory bank C are the same. We can then only limit ourselves to the specific measurement result $|++\rangle_B$, which further reduces the number of relevant ES outcomes to 4.

Based on the above discussion, we recognise two generic groups of output states, after the ES stage, which we refer to as *good* versus *bad* states. For $|\tilde{\Phi}\rangle_{A,D}$ as the ES measurement outcome, the good ES states correspond to the measurement outcome $|000\rangle_C$ where no bit flip has been detected at the ES stage, whereas the bad ES states correspond to the measurement outcomes $|001\rangle_C$, $|010\rangle_C$, or $|100\rangle_C$ in which we have detected a bit-flip error at the ES stage.

For both good and bad states, we still have 16 cases to consider for the decoder output. We refer to a decoded good state as a *golden* state if the two users detect no error at their decoder circuits. This corresponds to the measurement outcome $d_g = |00\rangle_{A_2A_3}|00\rangle_{D_2D_3}$. The probability of getting a golden state, and its corresponding total secret fraction is then given by

$$p_g = 16p_{m_g,d_g} \text{ and } r_\infty^g = p_g r_\infty^{m_g,d_g}, \tag{3.29}$$

where $m_g = |++\rangle_B|000\rangle_C$, and the factor 16 accounts for the four possible Bell states at the ES stage, and the four outcomes of the B register. Similarly, we have a group of good, but not golden, states, whose corresponding total probability of occurrence and secret fraction are given by

$$p_{gng} = 16\sum_{d\neq d_g} p_{m_g,d} \text{ and } r_\infty^{gng} = 16\sum_{d\neq d_g} p_{m_g,d} r_\infty^{m_g,d}. \tag{3.30}$$

Finally the corresponding probability and secret fraction to bad states are given by

$$p_b = 48\sum_{d} p_{m_b,d} \text{ and } r_\infty^{b} = 48\sum_{d} p_{m_b,d} r_\infty^{m_b,d}, \tag{3.31}$$

where $m_b = |++\rangle_B|100\rangle_C$, and the factor 48 covers three different locations of a single error in register C, each at 16 different cases of Bell state and B register outcomes as in golden states. The total secret fraction is then given by

$$r_\infty^{\text{total}} = r_\infty^g + r_\infty^{gng} + r_\infty^b. \tag{3.32}$$

One of the key results of this work is to show that, in most practical cases, the golden states are the main positive contributor to the key rate formula in Eq. (3.32), that is, $r_\infty^{\text{total}} \gtrapprox r_\infty^g$. This result allows us to considerably reduce the complexity of the problem in that, instead of accounting for all possible outcomes at different parts of the repeater chain, we only focus on a single class of states.

Here, we demonstrate how different kinds of states contribute to the key rate. Figure 3.5 shows the total secret fraction and its three main components in Eq. (3.32) for different parameter regimes, for the initial codeword states as in Eq. (3.12). We make several interesting observations from this figure, as summarized below:

- **Observation 1:** At $\delta = 0$, only golden states can generate positive key rates. This has been shown in Figs. 3.5(a)-(b). In Fig. 3.5(a), we have assumed that the initial Bell states are ideal and that there is no measurement error. We have then plotted the secret fraction versus the CNOT gate error parameter, β. It can be seen that, in this case, the golden state is the only contributor to the total secret fraction. It turns out that for all other states the phase error rate is at its worst possible value of 0.5 at which no secret key can be generated. We have a similar observation in Fig. 3.5(b), where, now, $\beta = 0$, and F_0 is a variable. In this case, our analysis indicates that most decoder outcomes simply never happen. But, even if they do, except for golden states, for all other terms $e_x = 0.5$. To see why this happens we can look back at the ideal state obtained after the ES operation in Eq. (3.5). In order to detect an error state such as $|++{+}{+}\rangle_B|100\rangle_C$ at the ES stage, we can either have an error corresponding to X_{C_1}, which results in $|\phi^+\rangle$ after decoding, or something like $Z_{B_1}X_{C_1}$, which results in $|\phi^-\rangle$. If we trace back these errors, using known circuits that convert an error after a CNOT gate to errors before it Bratzik et al. [2014], we can see that such errors, respectively, originate from $|\psi^+\rangle$ and $|\psi^-\rangle$ somewhere earlier in the circuit. In the case of imperfect Bell states, this is caused by the terms in the input Werner state in Eq. (3.7). The identity operator in the imperfect CNOT gate can similarly introduce such states in the circuit resulting in a similar behavior. In both cases, the weight of $|\psi^+\rangle$ and $|\psi^-\rangle$ is the same

at the input mixture, resulting in an equal mixture of $|\phi^+\rangle$ and $|\phi^-\rangle$ after decoding. At $\delta = 0$, according to Eq. (3.11), this results in $e_x = 0.5$.

- **Observation 2:** At $\delta \neq 0$, non-golden states can contribute to the total secret fraction but at comparatively much lower values. This can be seen from Figs. 3.5(c)-(d). In Fig. 3.5(c), we have fixed β and F_0 to their ideal values and have plotted the secret fraction for different values of δ. This is the first case in which r_∞^{gng} (dotted line) and r_∞^b (dash-dotted line) take nonzero values for some values of δ. The reason for this is that if we detect an error at the ES stage, for instance, by observing $|100\rangle_C$, because of measurement errors, the actual state in hand, according to Eq. (3.5), is most likely still the ideal state. Most cases for the decoder output are also similarly benign. The errors that may happen at the remote CNOT stage could equally result in bit or phase-flip errors, both with a probability scaling with δ. This allows us to have positive key rates for bad, as well as, good, but not golden, states. At low values of δ, however, the overall chance of obtaining such states is much lower than that of the golden states, which makes the total secret fraction still approximately the same as r_∞^g. Finally, in Fig. 3.5(d), we have verified this finding when β and δ are nonzero. We have chosen $\delta = 0.01$ as it gives a high rate for bad states in Fig. 3.5(c). We observe that the key rate for bad and good-but-not-golden states is nonzero for small value of β. This suggests that so long as the phase error rate is dominated by the measurement error we can get a positive key rate for non-golden states. But, once β increases to the level that the dominant source of phase error is what we discussed in Observation 1, then no secret keys can be extracted from such terms. At $\delta = 0.01$ the onset of dominance of CNOT errors is just before $\beta = 0.01$. At $\delta = 0.001$, we have verified that the golden state is the only contributor to the key rate for $\beta > 0.0046$. Given that in practice it is easier to have a low value for δ as compared to β, this observation suggests that for sufficiently small δ, the errors in the two-qubit gates would be the dominant factor in determining the final key rate. The latter can reliably be calculated from golden states in such cases.

- **Observation 3:** At cut-off point, the golden states are the main contributor to the key rate. Even though the non-golden states can contribute to a small extent to the key rate within some range of parameters, their contribution effectively ceases to zero by the time that we get to the cut-off point for our QKD system. This suggests that to find such maximum allowed error rates, one can reliably only calculate the key rate for the golden states.

- **Observation 4:** The measurement error δ has the lowest cut-off point ahead of β and $1 - F_0$. According to Fig. 3.5(c), at $\delta \approx 0.023$, the key rate drops to zero. This happens at $\beta \approx 0.07$, in Fig. 3.5(a), and $F_0 \approx 0.76$ in Fig. 3.5(b). This could simply be because of the number of measurement operations in the whole setup exceeding the number of CNOT gates. But, this also suggests that unless δ is sufficiently small, its effect cannot necessarily be neglected in a reliable analysis of the system.

Based on the above observations, in the remainder of this chapter, we only calculate r_∞^g. This is a tight lower bound on r_∞^{total}, in line with the common practice in calculating the key rate in QKD. More importantly, this suggests a practical distillation technique in such encoded repeaters, in which one can simply ignore the output if any error has been detected at the ES or decoding stage. This could substantially simplify the implementation of such systems in their early demonstrations. Under the assumption that r_∞^g closely follows r_∞^{total}, this distillation technique is more effective than relying on the error correction capabilities of the code. That is, in practical QKD settings, we may only need to use the error detection features of a code rather than its error correction power.

3.3.3 The effect of the encoding and decoding circuits on the secret fraction

In this section, we study how errors in encoding and decoding circuits would affect the achievable secret fraction. Thus far, we have only considered the perfectly encoded states as given by Eq. (3.12), which can be a reasonable assumption if one uses probabilistic techniques to initialize the memories. If, however, one uses CNOT gates to create such states deterministically, we should also account for

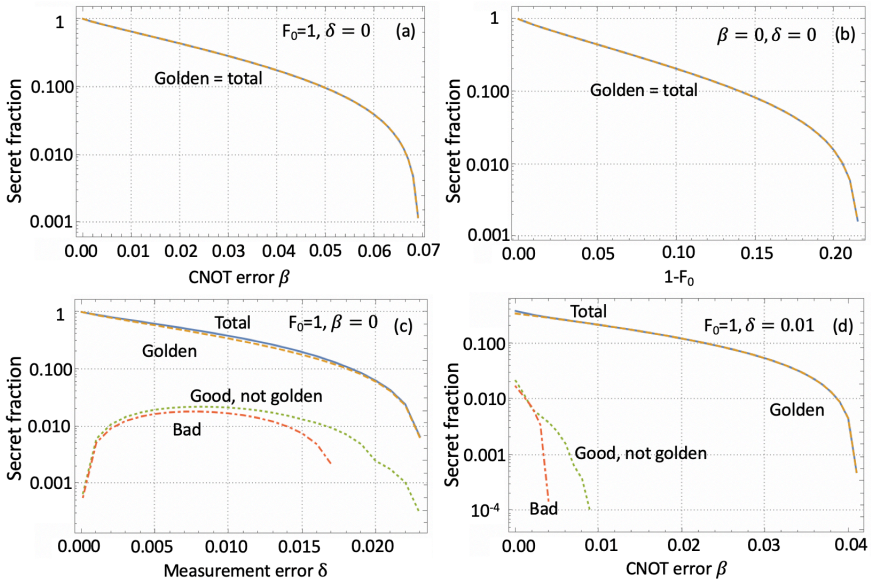

Figure 3.5: Secret fraction as a function of different error parameters at (a) $F_0 = 1$ and $\delta = 0$; (b) $\beta = 0$ and $\delta = 0$; (c) $F_0 = 1$ and $\beta = 0$; and (d) $F_0 = 1$ and $\delta = 0.01$. In all graphs, the top solid blue curve is for the total secret fraction, r_∞^{total}, followed by the dashed golden curve, r_∞^g, for golden states, the dotted green curve r_∞^{gng} for good, but not golden, states, and the dash-dotted red curve, r_∞^b, for bad states. In (a) and (b), the latter two terms are zero, so the dashed golden curve overlaps with the solid blue one.

errors in such gates. In this case, the initial codeword states for memory bank A, as an example, is given by Bratzik et al. [2014]

$$\rho_A^{\text{in}} = \rho_A^{\text{code}} + \rho_A^{\text{other}}, \tag{3.33}$$

where

$$\begin{aligned}\rho_A^{\text{code}} = &\frac{1}{2}[1 + \beta(\beta/2 - 5/4)](|000\rangle_A\langle 000| + |111\rangle_A\langle 111|) \\ &+ \frac{1}{2}(1-\beta)^2(|000\rangle_A\langle 111| + |111\rangle_A\langle 000|)\end{aligned} \tag{3.34}$$

and

$$\rho_A^{\text{other}} = \frac{\beta}{4}(3/2-\beta)(|101\rangle_A\langle 101| + |010\rangle_A\langle 010|) + \frac{\beta}{8}(|001\rangle_A\langle 001| + |100\rangle_A\langle 100|) + \frac{\beta}{8}(|110\rangle_A\langle 110| + |011\rangle_A\langle 011|). \quad (3.35)$$

The terms in Eq. (3.34) are effectively the encoded state in Eq. (3.12) although with modified weights to account for CNOT errors. Our linearization technique is easily applicable to these terms as they are still in the desired tensor product form of having the same input qubit in all rows. To apply our technique to the other terms in Eq. (3.35), we need to consider many more combinations of input states, which will increase the complexity of the simulation especially at higher nesting levels. Here, through the comparison of the secret fraction for different input states, we show that the coded part in Eq. (3.34) plays the major role in determining the secret fraction, based on which we can neglect the other terms. This will crucially simplify the code for further simulation. Note that the above states have been obtained by first applying $\mathcal{E}_{A_1A_2}$ and then $\mathcal{E}_{A_1A_3}$, as the two operators do not commute for nonzero values of β.

Figure 3.6 shows the secret fraction versus β at $F_0 = 0.98$ and $\delta = 0$ in several different cases. The top three curves (solid lines) give the secret fraction if we neglect all sources of error at the decoder stage, whereas the next batch of three curves (dashed lines) account for errors in the decoder circuit. In each batch, we consider three cases: (i) the encoding circuits are all perfect (top blue curves), that is, we assume $\beta = 0$ in these modules; (ii) The encoding process is modelled by the imperfect encoded state given in Eq. (3.33) (the bottom orange curves); and (iii) The encoding process is modelled by the state ρ_A^{code} in Eq. (3.34) (green curves in the middle of the circled batches). Two important observations can be made from this graph. First, it is clear that the imperfections in the decoder module is far more important than the encoder one. This is mainly because we have more chances to detect errors originated from the encoder than that of decoder. An error caused by encoding imperfections may be picked up at the entanglement swapping or decoding stage, and removed by our post-selection

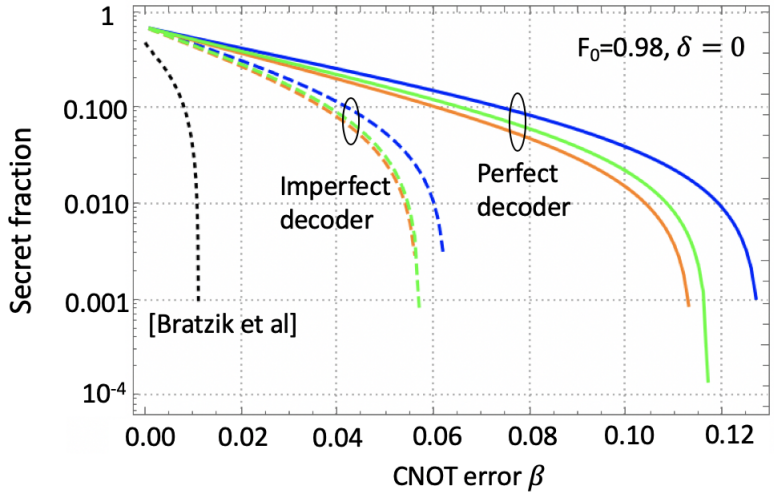

Figure 3.6: Secret fraction versus β at $F_0 = 0.98$ and $\delta = 0$. The solid lines correspond to error-free decoding circuits, and the dashed lines correspond to imperfect decoding circuits. The top blue curve in each batch corresponds to ideal encoding; the lower orange lines correspond to imperfect encoders as modelled by Eq. (3.33), and the middle green lines correspond to the coded part of the encoded state given by Eq. (3.34). In all cases the secret fraction is lower bounded by that of the golden states. The black dotted curve is the corresponding graph obtained in Bratzik et al. [2014] for the same parameter values for their model of imperfect encoders and decoders.

technique, whereas errors caused by decoder, if undetected, can directly affect the error rate. For a realistic analysis of the system, it will then be crucial to account for decoder errors, as we do in this chapter. The second point is that, especially in the case of imperfect decoders, which is of practical interest, the effect of ρ_A^{other} on the secret fraction is effectively negligible, as the curve obtained from ρ_A^{code} very closely follows that of the imperfect encoder modelled by the full state in Eq. (3.33). In the rest of this work, we will then only account for ρ_A^{code} when we model imperfections in the encoders. As mentioned earlier, this will substantially simplify our analysis as we only need to replace $\rho^{jk}_{A_iB_i}$ in Eq. (3.19) with $(C_{jk})^{1/3}\rho^{jk}_{A_iB_i}$, where $C_{00} = C_{11} = 1+\beta(\beta/2-5/4)$ and $C_{01} = C_{10} = (1-\beta)^2$.

In Fig. 3.6, we have also compared our results with Fig. 6 in Bratzik et al. [2014], which, for the same parameters, obtains the secret fraction for the same

system but without using the post-selection that we make on the basis of good/bad states, or decoder outputs. The corresponding curve in Bratzik et al. [2014] is shown by the dotted black line. The results clearly demonstrate how substantially one can improve the performance of QKD over encoded repeater setups by relying mainly on the error detection, rather than correction, features of the code. This could also change the main conclusion drawn in Bratzik et al. [2014] in that such repeaters can hardly outperform other classes of deterministic repeaters as the cut-off point for β has nearly improved by six folds from nearly 0.01 to about 0.06 when imperfections in both encoders and decoders are considered. Another distinction, between our work and that of Bratzik et al. [2014] is in the way errors have been modelled in each case. In Bratzik et al. [2014], errors are modelled collectively by an identity operator even if there is a cascade of operations. This is expected to overestimate the error in the system. In our work, we account for errors per individual gates, which gives us a more accurate picture of how errors propagate to the final state, and eventually affect the secret fraction. Based on the findings in Fig. 3.4 and Fig. 3.6, there is a two-fold improvement in the cut-off value of β because of such more accurate modelling and calculations.

In the following section, we use the results of this section to analyse the repeater chain at higher nesting levels. Based on the performance analysis for nesting level one, we will only consider the golden state contribution to the secret fraction. Unless otherwise mentioned, we fully account for imperfections in the decoder, but only use the coded components in Eq. (3.34) to model the encoder.

3.4 Extension to higher-nesting levels

The methodology developed in Section 3.3.1 can be extended to higher nesting levels in a recursive way. For instance, at nesting level $n = 2$, we can think of 8 memory banks named A to H, where we first apply our ES technique to BC and FG pairs and then DE. In this case, the output state of the ES stage, for measurement output $m_g = |+0\rangle$ at all corresponding ES measurements, can be written as follows:

$$\rho_{AH}^{m_g} = \rho_{\mathrm{ES}}^{(2)} / \mathrm{Tr}[\rho_{\mathrm{ES}}^{(2)}], \tag{3.36}$$

where

$$\rho_{\mathrm{ES}}^{(2)} = \frac{1}{16} \sum_{j_1,\ldots,j_8=0,1} \bigotimes_{i=1}^{3} \rho_{A_iH_i}^{j_1,\ldots,j_8}(m_g), \tag{3.37}$$

with

$$\rho_{A_iH_i}^{j_1,\ldots,j_8}(m_g) = \mathrm{Tr}_{D_iE_i}[M_{D_iE_i}^{m_g} \mathcal{E}_{D_iE_i}(\rho_{A_iD_i}^{j_1,\ldots,j_4}(m_g) \otimes \rho_{E_iH_i}^{j_5,\ldots,j_8}(m_g))]. \tag{3.38}$$

Here, $\rho_{A_iD_i}^{j_1,\ldots,j_4}(m_g)$ and $\rho_{E_iH_i}^{j_5,\ldots,j_8}(m_g)$ have already been calculated in Eq. (3.25). One can generalize this technique to higher nesting levels in a similar way to obtain the corresponding matrix $\rho_{\mathrm{ES}}^{(n)}$ for nesting level n. The corresponding golden state for the two end nodes A and A' is then given by

$$\rho_{AA'}^{(n)} = \rho_{\mathrm{dec}}^{(n)} / \mathrm{Tr}[\rho_{\mathrm{dec}}^{(n)}], \tag{3.39}$$

where

$$\rho_{\mathrm{dec}}^{(n)} = \frac{\mathrm{Tr}_{A_2A_3A_2'A_3'}[P_0^{A_2} P_0^{A_3} P_0^{A_2'} P_0^{A_3'} \mathcal{E}_{\mathrm{dec}}(\rho_{\mathrm{ES}}^{(n)})]}{\mathrm{Tr}[\rho_{\mathrm{ES}}^{(n)}]}. \tag{3.40}$$

The corresponding secret fraction can then be lower bounded by

$$r_{\infty}^{(n)} = 16^{2^n-1} \mathrm{Tr}[\rho_{\mathrm{ES}}^{(n)}] \mathrm{Tr}[\rho_{\mathrm{dec}}^{(n)}] r_{\infty}(\rho_{AA'}^{(n)}), \tag{3.41}$$

where the prefactors are, respectively, the number of golden states at nesting level n and the corresponding probability for each.

As an application of the analytical method we developed above, we look into the dependence of the secret fraction on various sources of errors in the setup. Figure 3.7 shows the secret fraction, for the first three nesting levels, as a function of β, δ, and $1 - F_0$, while, in each case, the other two parameters are assumed ideal. As expected, the secret fraction drops as we go to higher nesting levels as the number of gates and measurement operations exponentially grows with the nesting level. The resilience to error parameters would correspondingly go down, but, instead, we are covering exponentially longer distances, at higher nesting levels, if we assume the elementary link is of the same length in all cases. Given that by increasing the nesting level by one, we have over twice as many operations as before, a simple rule of thumb may suggest that the cut-off point

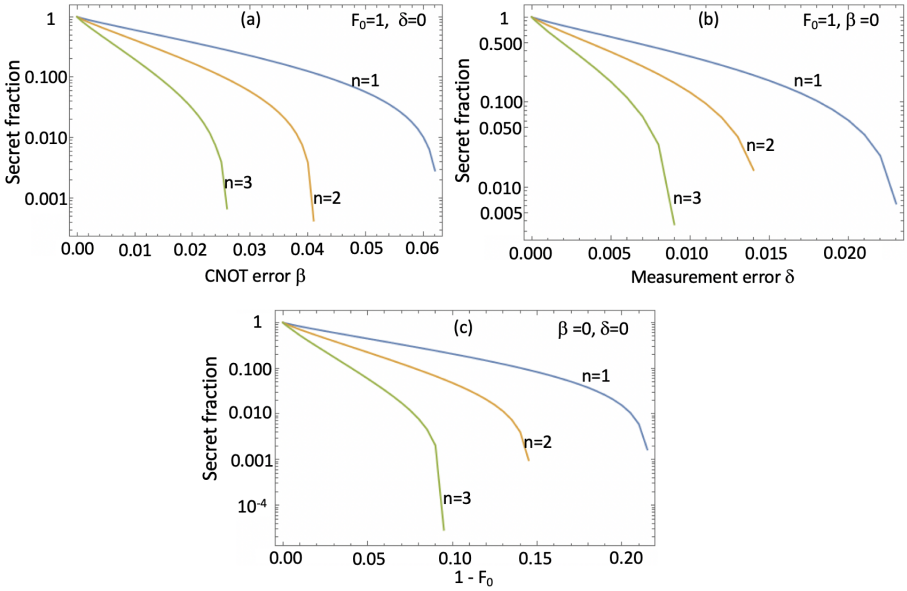

Figure 3.7: The secret fraction as a function of (a) gate error probability β, (b) measurement error probability δ, and (c) the error in the initial Bell states $1 - F_0$, at different nesting levels. In each case, the other two parameters have taken their ideal values.

for each source of error must be halved. Our more precise calculations suggest that the new cut-off points are slightly better than what is predicted by this rule of thumb, which could be because some errors cancel each other when one considers all possibilities, as we do in our analysis. For instance, at $n = 1, 2, 3$, the maximum allowed β is, respectively, 0.062, 0.041, and 0.026. As it was the case for $n = 1$, the secret fraction is most sensitive to δ and least sensitive to F_0. It is therefore crucial to have accurate single-qubit measurement operations in such QRs to make them useful for QKD purposes.

3.5 Conclusions and Discussion

In this chapter, we studied the performance of QKD systems run over a repeater setup that used three-qubit repetition codes for entanglement distillation. By modeling the error in all two-qubit gates and single-qubit measurements, we obtained an accurate picture of the requirements of such systems. It turned out

that such systems could considerably be more resilient to errors than previously thought. The system was most sensitive to measurement errors, but, provided that they were kept sufficiently low in the experimental setup, we showed that CNOT errors on the order of a few percents could be tolerated, which is feasible in practice already Ballance et al. [2016], Gaebler et al. [2016]. The QKD system could also handle imperfections in the initial Bell states aligned with what experimentally is achievable today Casabone et al. [2013], Dolde et al. [2014]. To handle the computational complexity associated with this many-qubit repeater setup, we devised an analytical technique for modelling the repeater chain, where, at the core of it, we only needed to deal with four qubits at a time. This enabled us to obtain the analytical form of the final entangled states shared between the two end users after several nesting levels. Moreover, our analysis enabled us to fully account for the information available to the end users, from entanglement swapping and decoding circuits, in their secret key distillation. By using this information, we showed three-fold increase in resilience to errors in CNOT gates as compared to when the repeater chain and decoders are treated as a black box. By looking at different sets of measurement outcomes, we then identified the key *golden* states that contributed the most to the final key rate. These golden states corresponded to the cases where no error had been detected at entanglement swapping and decoding stages. This observation resulted in a simple, but effective, post-selection tool for our QKD system that entirely relied on the error detection features of the code, rather than its error correction as when we treat the repeater chain as a black box. We also studied the impact of errors in the encoder and decoder circuits and showed that the latter is much more detrimental to the QKD system.

The analytical framework derived in this chapter can be improved and extended to consider more complex code structures and alternative decoders. One of the computational challenges that we have to deal with is the number of terms that needs to be calculated in the final state. In its exact form, we need to consider all combinations of input states to the elementary links, whose number grows exponentially with the nesting level. To manage the complexity, we need then to identify which input combinations have a major impact on the final key rate, and which ones could perhaps be neglected for a tight approximation. The

decoder setup could also pose computational challenges as in its current form, it takes a multi-qubit entangled state at its input and gives a bipartite state at its output. For large codes, it may be hard to computationally handle the large input. Alternative decoders may need to be designed to offer competitive performance especially if larger codes suffer more from errors in the system. Finally, this work mainly relied on finding the key rate once the repeater chain had generated an entangled state. In order to calculate the total key rate one should look at the timing of the protocol with respect to the initial entanglement distribution and how multiplexing is used in the system. All the above will be addressed in the next chapter.

Chapter 4

Simple efficient decoders for quantum key distribution over quantum repeaters with encoding

4.1 Introduction

In this chapter, we expand on the repeater-based QKD system studied in Chapter 3. The approach proposed previously, while accurate and effective for the first few nesting levels, will face computational problems at arbitrarily high nesting levels. The key reason for this is that the number of terms that need to be calculated will grow exponentially with the nesting level. At some point, as an approximation method, we need to drop the least significant terms and only keep those that majorly contribute to the key rate. In this chapter, we try to obtain a better understanding of such terms and devise analytical and numerical techniques that help us with reliable key rate calculations. This will then enable us to consider and analyze larger codes, e.g., five-qubit repetition codes, and compare them with simpler codes such as three-qubit repetition codes.

Another source of complexity in the analysis presented in Chapter 3 is the decoder module. The default decoder used in such settings is the one that reverses the entangling operation applied at the encoding stage Bratzik et al. [2014]. The decoder module is then often composed of a number of untangling CNOT gates between different pairs of input qubits, followed by syndrome measurement and

correction operations. Depending on the size of the employed code, the error analysis of the decoder part can become computationally complex. More importantly, the use of many erroneous CNOT gates has an adverse impact on the key rate as shown in 3.3.3. This is particularly the case because the decoder modules are the last components in the setup, therefore, errors occurred in this last stage may be harder to pick up.

Our main contributions in this chapter:

In this chapter, we offer a remedy for the above problems by introducing alternative decoder structures that only rely on single-qubit measurements. This not only simplifies the QKD setup but also, by removing the major source of error from the decoding circuits, results in better performance in many practical scenarios. Then, by developing several numerical and analytical methodologies, we allow for the key rate analysis being extend to larger codes (five-qubit repetition codes) and higher nesting levels (up to the 7th nesitng level). We account for various sources of error in the setup for each of the proposed decoders. We identify the terms that significantly impact the secret key generation rate, and then assess its dependence on relevant error parameters. Finally, we obtain the optimum structure for the QR setup at fixed distances, and the minimum requirements for the system to offer a positive key rate, or a rate, in bit per second per QM, larger than that of a probabilistic QR. We show that, in many practical regimes of operation, the simple three-qubit repetition code is our best choice.

This chapter is organized as follows. In Sec. 4.2, we describe the QKD setups of interest based on the repeater protocol of Ref. Jiang et al. [2009] with four different decoder structures. By considering relevant error models for different components of the system, in Sec. 4.3, we compare the secret key rate for different QKD decoders in the case of nesting level one for the QR setup. We then extend our results, in Sec. 4.4, to higher nesting levels by proposing several different approximation techniques. We study the dependence of the secret key generation rate on different error parameters and find the corresponding thresholds for extracting a nonzero secret key rate at different nesting levels. In Sec. 4.5, we consider the entanglement generation rate of the elementary links for probabilistic

and deterministic QRs, with and without multiplexing, and combine those results with the results of the previous section to obtain the total normalized secret key rates in bits per second. We also illustrate the parameter regions where one type of QR performs more efficiently than the other. Finally, we conclude this chapter in Sec. 4.6.

4.2 System Description

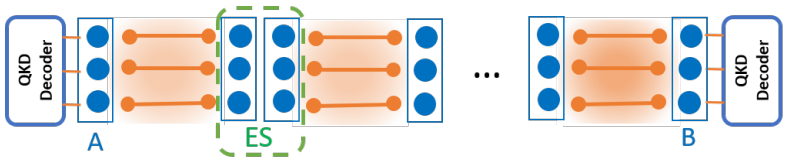

Figure 4.1: The schematic of the QKD setup on a repeater chain based on the three-qubit repetition code. The small circle pairs represent bipartite entangled state prepared in advance. Using remote CNOT gates, an encoded entangled state is generated across elementary links, and stored in memories represented by large circles. The encoded entanglement is then extended across the entire link by performing ES operations on the middle nodes. The two users will then apply decoding operation on this state to generate their raw key.

Figure 4.1 shows the schematic of the QKD system considered in this work. Here, we use a quantum repeater with encoding Jiang et al. [2009], Jing et al. [2020] to distribute entangled states in an encoded form across the two ends of the link. We then decode such states to share a raw key between the users, Alice and Bob, from which a secret key can be extracted using postprocessing techniques. Our objective is to assess the performance of the above QKD system in the nominal mode of operation where no eavesdropper is present. In such a case, it is crucial to consider errors that stem from imperfections in the system, three major sources of which we consider in this work as follows

(1) **Imperfections in initial Bell states:** The originally distributed Bell states in the QR setup are modeled as Werner states with fidelity F_0:

$$\rho^{\mathrm{W}} = F_0|\phi^+\rangle\langle\phi^+| + \frac{1-F_0}{3}(\mathbb{I}_4 - |\phi^+\rangle\langle\phi^+|), \tag{4.1}$$

where $|\phi^+\rangle$ is the target Bell state given by Eq. (2.1), and $\mathbb{I}_4$ is a 4×4 identity matrix.

(2) **Two-qubit gate imperfections:** The CNOT gate for a control qubit i and a target qubit j is modeled as Briegel et al. [1998]

$$\rho^{\mathrm{out}} = (1-\beta)U_{i,j}\rho^{\mathrm{in}}U_{i,j}^{\dagger} + \frac{\beta}{4}\mathrm{Tr}_{i,j}(\rho^{\mathrm{in}})\otimes\mathbb{I}_{i,j}, \tag{4.2}$$

where ρ^{in} (ρ^{out}) is the input (output) before (after) the CNOT gate, and $U_{i,j}$ represents the unitary operator corresponding to an ideal CNOT gate. The error in this two-qubit operation is modeled by a uniform depolarization of qubits i and j, represented by identity operator $\mathbb{I}_{i,j}$, with probability β.

(3) **Measurement imperfections:** The projective measurements to states $|0\rangle$ and $|1\rangle$ are, respectively, represented by

$$\begin{aligned} P_0 &= (1-\delta)|0\rangle\langle 0| + \delta|1\rangle\langle 1| \quad \text{and} \\ P_1 &= (1-\delta)|1\rangle\langle 1| + \delta|0\rangle\langle 0|, \end{aligned} \tag{4.3}$$

where δ is the measurement error probability. Similar measurement operators, $P_{\pm}$, are used for projective measurement in $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$ basis.

As in Chapter 3, here, we still assume all single-qubit operations are perfect and quantum memories with infinitely long coherence times are available.

In this chapter, we still mainly use the three-qubit repetition code as an example to illustrate our proposed techniques, where the logical qubits are given by Eq. (3.1). Some of our proposed techniques are, nevertheless, applicable to larger codes as well. Here, as an additional example, we also apply our analysis to the five-qubit repetition code, where the logical qubits are encoded as Braunstein [1996]

$$|\tilde{0}\rangle = |00000\rangle \quad \text{and} \quad |\tilde{1}\rangle = |11111\rangle. \tag{4.4}$$

This code can ideally correct up to two bit-flip errors, as compared to one in the three-qubit case. The comparison between the two codes allows us to learn how the interplay between noisy gates and stronger error-correction features affects the performance of the QKD system.

In the following, we briefly explain the repeater model and describe different decoding modules, used in Fig. 4.1, that we analyze and compare in this work.

4.2.1 Quantum repeater with repetition codes

Here, we briefly review the protocol proposed in Jiang et al. [2009] in the case of the three-qubit repetition code. The protocol with five-qubit repetition code is constructed in a similar way. For detailed description, please refer to the previous chapter.

The QR protocol operates in the following way. First, the codeword states, $\frac{1}{\sqrt{2}}(|\tilde{0}\rangle + |\tilde{1}\rangle)$ and $|\tilde{0}\rangle$, are locally prepared, respectively, at the left and right memory banks (large circles in Fig. 4.1), and Bell pairs are distributed between auxiliary memories (represented by small circles in Fig. 4.1) of all elementary links. Using these distributed Bell states, one can then implement remote CNOT gates, transversally, on main and auxiliary memories, after which, the encoded entangled states $\frac{1}{\sqrt{2}}(|\tilde{0}\rangle|\tilde{0}\rangle + |\tilde{1}\rangle|\tilde{1}\rangle)$ are ideally created across *all* elementary links. Next, we perform ES operations at all intermediate stations to extend the entanglement over the entire link. This, due to the transversality of the employed code, is simply done by performing three individual BSMs on the corresponding pairs of physical qubits. Finally, after all ES operations, an encoded entanglement is ideally distributed between the two end users. Depending on the application in mind, the final encoded entangled state can be decoded into a bipartite state as done in the previous chapter, or be used directly as we will introduce next. In all cases, some measurement information needs to be passed to the users to identify the relevant Pauli-frame rotation on the final state.

4.2.2 Decoder structures

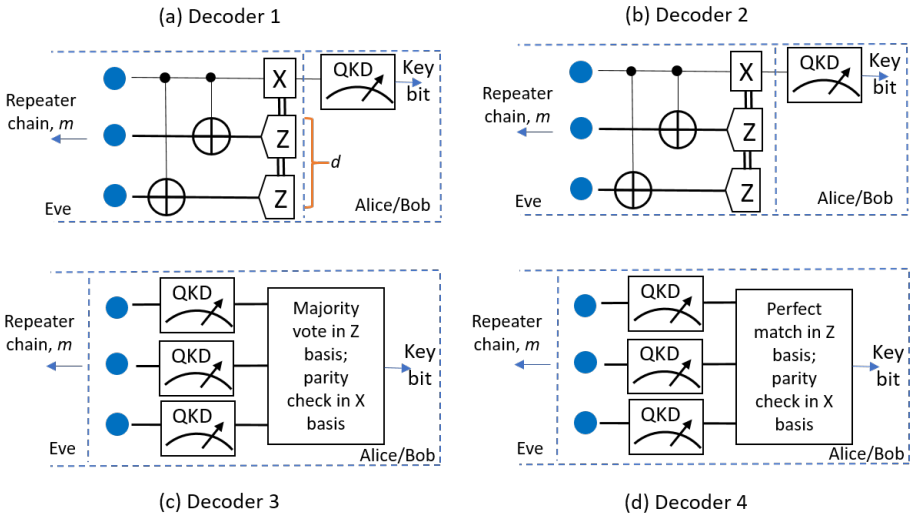

Figure 4.2: The schematic of different decoder structures considered in this paper: (a) the original decoder proposed in Chapter 3, where a decoding circuit is used to generate a qubit, on which a QKD measurement, either in Z or X basis, is performed. The decoding circuit would generate syndrome data d, which is used for state classification. (b) A modified version of the decoder proposed in Bratzik et al. [2014], which is very similar to (a) except that the decoder measurement outcome d is not used for classification. They still use the information in m in their key rate extraction. Note that, in both (a) and (b), Eve can control the decoder module, but has to pass some measurement data to users. (c) First alternative decoder, proposed in this work, where users directly measure the three qubits either all in Z basis or in X basis. They use majority (parity) rules, in Z (X) basis, to decode the key bit. (d) Our second alternative decoder, which is very similar to (c), except that in the Z basis a perfect match 111 (000) is mapped to bit 1 (0). In (c) and (d), we assume Alice and Bob have control over the final set of memories in their secure box.

Here, we consider four different decoder modules for the QR-QKD setup considered in this work. Figure 4.2 shows the schematic of these decoders. In the first two decoders, Alice and Bob use the biased version of the entanglement-based BBM92 protocol Bennett et al. [1992], Lo et al. [2005a] by applying QKD

measurements on a bipartite state obtained via a decoding circuit. This circuit can in principle belong to a third, untrusted, party, hence Alice and Bob do not need to characterize this device in decoders 1 and 2. Its operation is based on reversing the entangling operation applied at the encoding stage. This type of decoder may also find applications in non-QKD scenarios. Figure 4.2(a) shows the decoder setup used in Chapter 3, hereafter we refer to as decoder 1, in which, using CNOT gates, we first untangle the encoded entangled state, and then perform QKD measurements on the resulting bipartite state. In the previous chapter, it is shown that the measurement information obtained at the ES, m, and decoding, d, stages can be used to separate the type of entangled states shared by the users, and consequently obtain higher key rates overall. In decoder 1, we assume that the information in m and d is fully used to take advantage of this classification. The second decoder, decoder 2, is shown in Fig. 4.2(b), where, as in decoder 1, we also apply error-correction operation to the resulting bipartite state. This decoder does not, however, pass the information obtained at the decoder stage to the user ends, and, in that sense, treats the decoder setup as a black box. Both these decoders are studied in Chapter 3, where we show that, the particular case where no error is detected at decoding and ES stages is the major contributor to the key rate.

In this chapter, we try to account for specific requirements of the QKD system to possibly come up with simpler, and as turns out more efficient, decoders. There are several observations that lead us to these alternative structures. First, we note that, so long as QKD is concerned, the purpose of the decoder module is to perform measurements in two mutually unbiased bases. Secondly, physically speaking, the three quantum memories in the two end nodes of the repeater chain are practically held in the secure boxes of Alice and Bob. The corresponding error correction/detection operations can then be performed by the two legitimate users, and not necessarily a third party. Finally, at least in the case of repetition codes, error correction/detection, or part of it, can potentially be done as part of post-processing rather than quantum mechanically.

Putting together the above points, in this work, we propose two alternative decoders and compare their performance with that of decoders 1 and 2. In both decoders, Alice and Bob, instead of manipulating their three qubits by quantum

gates, directly measure them all in either X or Z basis. The two users choose their own basis independently, but randomly, according to the asymmetric QKD protocols Lo et al. [2005a]. They then use classical postprocessing to assign a certain bit to their raw key bit. In decoder 3, shown in Fig. 4.2(c), we use the majority rule, in Z basis, to replicate the error correction feature of the code against bit-flip errors. For instance, a measurement corresponding to $|101\rangle$ is mapped to bit 1. In that sense, decoder 3 can be thought of as a simplified version of decoder 2. In X basis, we map the measurement outcomes that have an odd number of $|+\rangle$ states to bit 0, and all other measurement outcomes to bit 1. The former (latter) corresponds to input states that result in $|+\rangle$ ($|-\rangle$) states in the output of an ideal decoder 2. In decoder 4, shown in Fig. 4.2(d), we additionally apply the postselection rule proposed in the previous chapter, where, in Z basis, only measurement outcomes corresponding to no errors, i.e., $|000\rangle$ or $|111\rangle$, is kept, and all other cases are discarded. In X basis, we use the same parity rule as in decoder 3. In both decoders 3 and 4, we use m to postselect only cases where no error has been detected at the ES stage.

As compared to decoders 1 and 2, our alternative decoders 3 and 4 do not need to deal with the errors in the decoder CNOT gates. This certainly reduces some sources of error in the decoder, which is a sensitive part in the whole setup. Our classical postprocessing is not, however, an exact replica of that of decoder 1 as we do not use the information available in d for classification. It will be interesting to see how the interplay between these two factors spans out, as we investigate in the next section.

4.3 Secret key analysis for nesting level one

In this section, we discuss the performance of the QKD system in Fig. 4.1 for different decoding structures of Fig. 4.2. As the first step, we investigate the dependence of the secret key generation rate in our QKD system on relevant error parameters in the case of one repeater node, i.e., the first nesting level. To this end, we first calculate the secret key generation rate per entangled state shared

between Alice and Bob. In the asymptotic regime for an efficient entanglement-based QKD protocol, this parameter, known as the secret fraction Bratzik et al. [2014], is lower bounded by Shor & Preskill [2000]

$$r_\infty(e_b, e_p) = \max\{0, 1 - h(e_b) - h(e_p)\}, \tag{4.5}$$

where $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the Shannon binary entropy function, and e_b and e_p are, respectively, the bit-flip and phase-flip error probability, or an upper bound of which, in the Z basis.

To calculate the secret fraction, in previous chapter, we develop a technique by which we analytically calculate the relevant density matrices with the above error parameters being included. Here, we use the same methodology to obtain the joint state, $\tilde{\rho}_m$, of the two memory banks held by Alice and Bob, upon observing the measurement outcome m at the ES stage, and the joint state $\rho_{m,d}$, after the decoding circuit in decoder 1, upon observing, in addition to m, the measurement outcome d at the decoding stage. The states $\tilde{\rho}_m$ and $\rho_{m,d}$ can, respectively, be obtained using Eqs. (3.20) and (3.26) in previous chapter, with the corresponding probability of occurrence denoted by p_m and $p_{m,d}$. In our calculations, we consider a partially imperfect encoder, as modelled by Eq. (3.34), where less significant cross terms are ignored. In the following, we obtain the secret fraction for each of the proposed decoders in the asymptotic regime, where an infinite number of entangled states have been shared. As mentioned before, we consider the normal mode of operation, where no eavesdropper is present, but we account for the device imperfections as modelled in Sec. 4.2.

4.3.1 Decoder 1

In this decoder, the users take full advantage of m and d to classify their entangled states as a function of these two parameters, and extract a secret key separately from each set. In this case, the total secret fraction is given by

$$r_\infty^{(1)} = \sum_{m,d} p_{m,d} r_\infty(e_b^{(1)}, e_p^{(1)}), \tag{4.6}$$

where

$$e_b^{(1)} = \mathrm{Tr}(P_0^{\mathrm{Alice}} P_1^{\mathrm{Bob}} \rho_{m,d}) + \mathrm{Tr}(P_1^{\mathrm{Alice}} P_0^{\mathrm{Bob}} \rho_{m,d}),$$
$$e_p^{(1)} = \mathrm{Tr}(P_+^{\mathrm{Alice}} P_-^{\mathrm{Bob}} \rho_{m,d}) + \mathrm{Tr}(P_-^{\mathrm{Alice}} P_+^{\mathrm{Bob}} \rho_{m,d}). \tag{4.7}$$

The measurement operators in Eq. (4.7) are defined according to Eq. (4.3) with additional superscripts to specify the user. Note that, in this case, the phase-error rate is effectively the same as the bit-flip error rate in the X basis.

4.3.2 Decoder 2

In the second decoder, the information in d is not used for classification, but only, internally, for error correction. For each m, the state on which QKD measurements are performed is then given by

$$\rho_m^{(2)} = \sum_d p_{d|m} \rho_{m,d}, \tag{4.8}$$

where $p_{d|m} = p_{m,d}/p_m$. The total secret fraction in this case is given by

$$r_\infty^{(2)} = \sum_m p_m r_\infty(e_b^{(2)}, e_p^{(2)}), \tag{4.9}$$

where

$$e_b^{(2)} = \mathrm{Tr}(P_0^{\mathrm{Alice}} P_1^{\mathrm{Bob}} \rho_m^{(2)}) + \mathrm{Tr}(P_1^{\mathrm{Alice}} P_0^{\mathrm{Bob}} \rho_m^{(2)}),$$
$$e_p^{(2)} = \mathrm{Tr}(P_+^{\mathrm{Alice}} P_-^{\mathrm{Bob}} \rho_m^{(2)}) + \mathrm{Tr}(P_-^{\mathrm{Alice}} P_+^{\mathrm{Bob}} \rho_m^{(2)}). \tag{4.10}$$

4.3.3 Decoder 3

Decoder 3 uses a direct measurement on the three qubits held by each user to specify the raw key. Before calculating the corresponding error parameters, it is then important to establish the security of this structure and how we can bound the bit error rate and the phase error rate in Z basis. This has been done in Appendix A, where we show that, in the ideal case, the measurement operators modelling decoder 3 are identical to that of decoder 2. We can then use a similar security proof to relate the phase error rate in the Z basis to the bit error rate in the X basis. In the imperfect implementation of either decoders, we end up

overestimating both parameters, which is still in line with the lower bound nature of Eq. (4.5). With this in mind, the total secret fraction for decoder 3 is given by

$$r_\infty^{(3)} = \sum_m p_m r_\infty(e_b^{(3)}, e_p^{(3)}), \tag{4.11}$$

where

$$\begin{aligned} e_b^{(3)} &= \mathrm{Tr}(\tilde{P}_0^{\mathrm{Alice}} \tilde{P}_1^{\mathrm{Bob}} \tilde{\rho}_m) + \mathrm{Tr}(\tilde{P}_1^{\mathrm{Alice}} \tilde{P}_0^{\mathrm{Bob}} \tilde{\rho}_m) \\ e_p^{(3)} &= \mathrm{Tr}(\tilde{P}_+^{\mathrm{Alice}} \tilde{P}_-^{\mathrm{Bob}} \tilde{\rho}_m) + \mathrm{Tr}(\tilde{P}_-^{\mathrm{Alice}} \tilde{P}_+^{\mathrm{Bob}} \tilde{\rho}_m) \end{aligned} \tag{4.12}$$

with

$$\begin{aligned} \tilde{P}_0 &= P_{000} + P_{100} + P_{010} + P_{001}, \\ \tilde{P}_1 &= P_{111} + P_{110} + P_{101} + P_{011}, \\ \tilde{P}_+ &= P_{+++} + P_{+--} + P_{-+-} + P_{--+}, \\ \tilde{P}_- &= P_{---} + P_{-++} + P_{+-+} + P_{++-} \end{aligned} \tag{4.13}$$

being, respectively, the corresponding measurement operators to bit 0 and 1 in Z basis and X basis, where $P_{ijk} = P_i \otimes P_j \otimes P_k$. Note that the majority rule is used in the Z basis.

4.3.4 Decoder 4

Decoder 4 is very similar to decoder 3 with an additional post-processing step in which, in the Z basis, we only accept the cases where either three 1s or three 0s have been obtained. This is inspired by the observation in the previous chapter that the output with no error in the decoding stage is the main contributor to the key rate. In this case, the bit error rate in the X basis is not necessarily an upper bound on the phase error rate for the post-selected data in the Z basis. But, we can consider the worst case scenario by assuming that all the errors that we observe in the X basis correspond to the post-selected part of the data in the Z basis. In this case, the total secret fraction for decoder 4 is lower bounded by

$$r_\infty^{(4)} = \sum_m p_{\mathrm{succ}} p_m r_\infty(e_b^{(4)}, e_p^{(4)}), \tag{4.14}$$

where

$$\begin{aligned} p_{\text{succ}} =& \text{Tr}(P_{000}^{\text{Alice}} P_{000}^{\text{Bob}} \tilde{\rho}_m) + \text{Tr}(P_{111}^{\text{Alice}} P_{111}^{\text{Bob}} \tilde{\rho}_m) \\ &+ \text{Tr}(P_{000}^{\text{Alice}} P_{111}^{\text{Bob}} \tilde{\rho}_m) + \text{Tr}(P_{111}^{\text{Alice}} P_{000}^{\text{Bob}} \tilde{\rho}_m) \end{aligned} \tag{4.15}$$

is the success probability for the post-selection step, i.e., detecting no error in the Z basis,

$$e_b^{(4)} = \frac{\text{Tr}(P_{000}^{\text{Alice}} P_{111}^{\text{Bob}} \tilde{\rho}_m) + \text{Tr}(P_{111}^{\text{Alice}} P_{000}^{\text{Bob}} \tilde{\rho}_m)}{p_{\text{succ}}}, \tag{4.16}$$

and

$$e_p^{(4)} = \min(\frac{e_p^{(3)}}{p_{\text{succ}}}, 0.5). \tag{4.17}$$

The final equation gives an upper bound on the phase error rate in the Z basis as explained above.

4.3.5 Comparison between different decoders

Now that we have all the ingredients to analyze all decoder settings, we can compare them in terms of their resilience to different error parameters. In Chapter 3, we have already established that, by properly using the information available in d, decoder 1 outperforms decoder 2; please see Fig. 3.4. Decoder 3, in the ideal case when there is no error in the decoder, should be identical to decoder 2, but, in the case of erroneous CNOT gates, it is expected that it outperforms decoder 2. It would not be trivial, however, if decoder 3 can outperform decoder 1 as well. Decoder 4 also, by postselecting in the Z basis, can reduce the bit-flip error rate, as compared to decoder 3, but its phase-error rate bound in Eq. (4.17) is not necessarily tight. We have to therefore investigate if decoder 4 can ever surpass decoder 3 in terms of performance. In this section, we try to answer these questions.

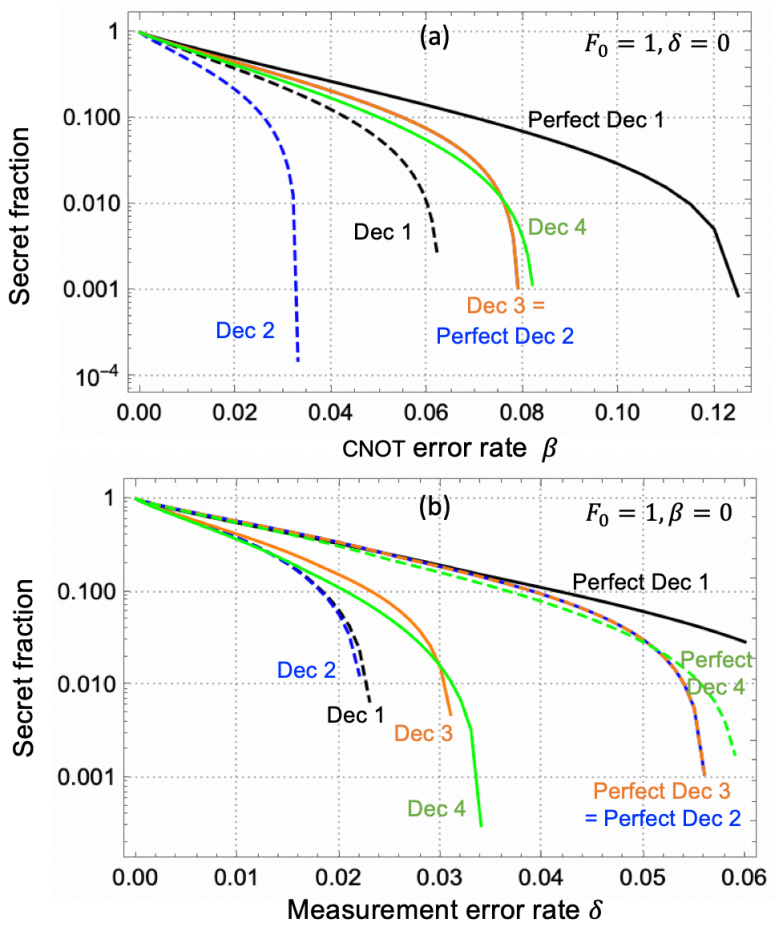

Figure 4.3: Secret fraction for different decoder (Dec) structures versus (a) gate error probability β at $F_0 = 1$ and $\delta = 0$, and (b) measurement error probability δ at $F_0 = 1$ and $\beta = 0$. In the curves corresponding to perfect decoders, all error parameters assume their ideal values just in the decoder module; the corresponding value in the rest of the system is as the graph shows.

Figures 4.3(a) and (b) show the performance of different decoders, respectively, as a function of gate error probability β, at $F_0 = 1$ and $\delta = 0$, and measurement error probability δ, at $F_0 = 1$ and $\beta = 0$. In both cases, we have also included several curves corresponding to perfect decoders as well. For instance, the perfect decoder in Fig. 4.3(a) uses perfect CNOT gates as well as ideal measurement modules in its decoder circuit, whereas in the rest of the system β can

take nonzero values. We make several interesting observations from these figures, which we summarize below:

- **Observation 1:** Decoders 3 (orange curves) and 4 (green curves) show better performance than decoders 1 (dashed black) and 2 (dashed blue), when the imperfections in the decoder circuit are considered. In Fig. 4.3(a), it is mainly the CNOT errors that make the difference. Without CNOT and measurement errors, even decoder 2 performs better than an imperfect decoder 1. This is an interesting result, which shows that the effect of CNOT errors in the decoder circuit can trump the benefits we may get from knowing the value of d in decoder 1. It then follows that decoder 3 is also better than imperfect decoder 1. At $\delta = 0$, this is because decoder 3 is identical to a perfect decoder 2 (see Appendix A). But, interestingly, this also holds even for nonzero values of δ as shown in Fig. 4.3(b). As a result, the maximum allowed value for β roughly moves from 0.03-0.06, for decoders 1 and 2, to 0.08, for decoders 3 and 4. A similar behavior is seen in Fig. 4.3(b), where maximum allowed value for δ roughly increases from 0.02 to 0.035.

- **Observation 2:** We notice that, the classification versus d could still play a role if all sources of error in the decoder could diminish. For instance in both figures, the curves corresponding to perfect decoder 1 offer the best performance. Also, it can be seen that, when there are no error parameters considered for decoders at all, decoders 2 and 3 perform similarly as expected by the results of Appendix A. That said, in practice, achieving this level of perfection may not be possible, hence, so far as QKD is concerned as an application, decoders 3 and 4 are the preferred option, which not only improve the performance, but are also easier to implement.

- **Observation 3:** In smaller error regions, decoder 3 performs slightly better than decoder 4, but eventually decoder 4, because of its postselection rule,

is more tolerant to errors [1]. The good thing is that decoder 4, in terms of hardware, is exactly the same as decoder 3, and the postselection rule can be applied by software in the postprocessing steps. It is therefore feasible that, for every regime of operation, we calculate both $r_\infty^{(3)}$ and $r_\infty^{(4)}$, and pick the higher rate. In this work, the secret fraction calculated for this setup hereafter is the maximum of these two parameters denoted by $r_\infty^{\text{opt}} = \max(r_\infty^{(3)}, r_\infty^{(4)})$.

- **Observation 4:** It is interesting that, in Fig. 4.3(b), where $\beta = 0$, decoder 3 still outperforms decoder 2 in the case of imperfect measurement modules. One may think that, given that both decoders rely on three single-qubit measurement operations, the secret fraction should be the same in both cases. Interestingly, this is not the case, and the reason for that is somehow because of the dependence of e_b parameters on the location of the error as we explain next. In decoder 2, to the first order approximation, $e_b^{(2)}$ is proportional to δ, corresponding to an error in the measurement on the top qubit. In decoder 3, however, we need to make at least two errors in order to have a bit flip, which means that, to the first-order approximation, $e_b^{(3)}$ is proportional to δ^2. This justifies why decoder 3 outperforms decoder 2 even if $\beta = 0$. More generally, in our calculations, we realize that the position where the bit-flip occurs affects the value of $e_b^{(3)}$ in an asymmetric way. It is important then that we consider all terms in Eq. (4.12) in calculating $e_b^{(3)}$. Note that the terms contributing to $e_p^{(3)}$ are mostly symmetric in terms of their subscripts as well as over Alice and Bob.

We finish this section by extending one of the key results of the last chapter, in using error detection as an effective postselection tool, to setups that use decoders 3 and 4. In Fig. 4.4, we have plotted r_∞^{opt} versus different error parameters,

[1] Decoder 4, in essence, slightly overestimates the errors in X basis. The crossing point between the performance of decoders 3 and 4 can be understood as a tradeoff between this overestimation of errors and the postselection rule. In smaller error regions, the error detection features have not come into effect so that the performance of decoder 4 is worse; whereas in larger error regions, by applying the postselection rule, most errors can be removed and thus the performance gets improved.

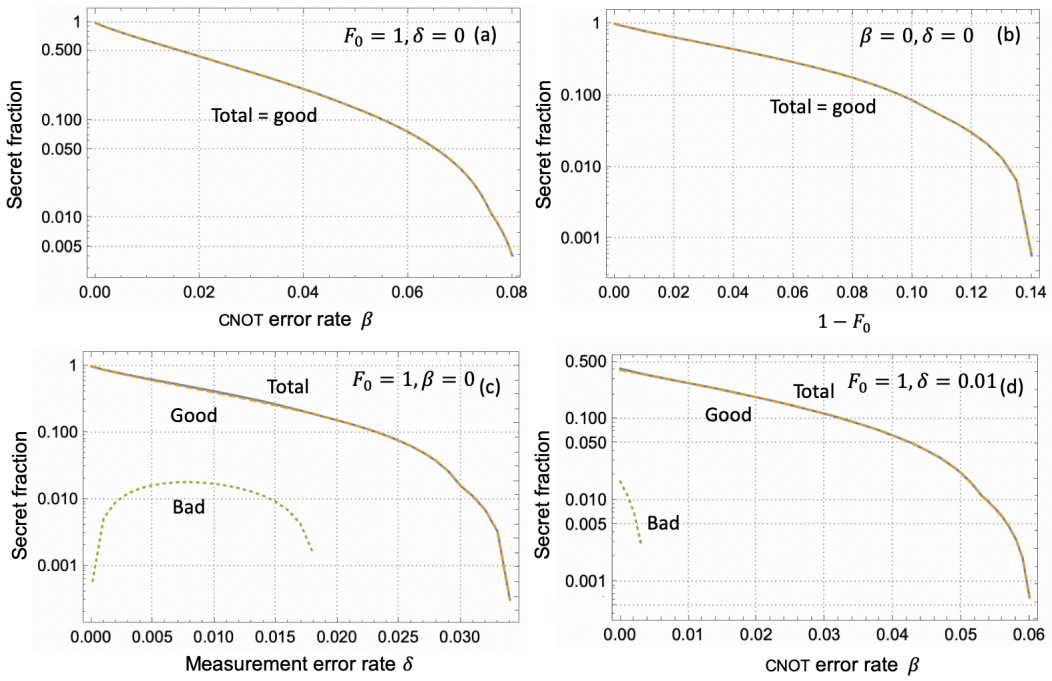

Figure 4.4: Secret fraction r_∞^{opt} versus (a) β, at $\delta = 1 - F_0 = 0$; (b) $1 - F_0$, at $\delta = \beta = 0$; (c) δ, at $\beta = 1 - F_0 = 0$; and (d) β, at $\delta = 0.01$ and $1 - F_0 = 0$. The curves labelled by good correspond to the output states where no error is detected at the ES stage, whereas the bad curves are for the output states where some errors are detected at the ES stage. The curves labeled by total are the weighted sum of good and bad terms as given by Eq. (4.11) and Eq. (4.14).

alongside the contributions from *good* states, corresponding to no error at the ES stage, and *bad* states, for which some error has been detected. We get very similar results to the previous chapter, where the total secret fraction is either equal to the contribution from good states, or almost equal to it. This observation allows us in the next section to only focus on the good states, when we calculate the rate at higher nesting levels.

4.4 Extension to higher-nesting levels

In order to estimate the secret key rate at higher nesting levels, we are going to use the same approach as proposed in the previous chapter, but we modify

it, using numerical and analytical approximations, so that we can manage its computational complexity. The key ingredient needed to calculate the key rate in the case of decoders 3 and 4 is the multipartite entangled state $\tilde{\rho}_m$. In this section, as explained before, we only account for the contribution from good states, and, as a representative, we only consider one particular good outcome among all that correspond to no error at the ES stage. We denote the corresponding output state to this outcome by $\tilde{\rho}_{\text{good}}$. Once $\tilde{\rho}_{\text{good}}$ is obtained, we can use Eq. (4.11) and Eq. (4.14) to obtain a tight lower bound on the secret fraction by ignoring the contribution from bad states. Our objective here is to get a realistic picture of what our encoded setup can achieve, and to what degree it is resilient to system errors. Exact lower bounds, which can securely be obtained in an experimental setup, are not then necessarily needed, and instead, we use tight estimates on such lower bounds to gain insight into system operation and its limitations.

In the previous chapter, we develop an analytical approach to find the joint multipartite state between Alice and Bob. In our proposed technique, we break down the initial state of the system to its core components, and apply possibly erroneous gate and measurement operations to each possible input combination separately. By using the traversality of the employed code, we then obtain $\tilde{\rho}_{\text{good}}$, while avoiding the computational complexity corresponding to large multi-qubit systems. Instead, we just need to deal with a four-qubit system at a time. The number of the input terms we need to consider, however, grows exponentially with the nesting level, and practically it is very difficult to use our previous approach in full for nesting levels greater than three. More precisely, the entangled state between memory banks A and B, held, respectively, by Alice and Bob, for nesting level n, is given by (ignoring normalization factors)

$$\tilde{\rho}^{(n)}_{\text{good}} = \sum_{\mathbf{j},\mathbf{k}} \bigotimes_{i=1}^{3} \rho^{\mathbf{j},\mathbf{k}}_{A_iB_i} \tag{4.18}$$

where $\mathbf{j} = [j_1, \ldots, j_{2^n}]$ and $\mathbf{k} = [k_1, \ldots, k_{2^n}]$ with each component taking a binary value. $\rho^{\mathbf{j},\mathbf{k}}_{A_iB_i}$ is the joint state of the ith memory in banks A and B if the initial state for the 2^{n+1} memories involved in the process is given by $\bigotimes_{l=1}^{2^n} \rho^{(l)}_{\text{init}}$, where $\rho^{(l)}_{\text{init}} = |j_l\rangle\langle k_l| \otimes |0\rangle\langle 0|$ is the initial state of elementary link l. In previous chapter, we use a recursive technique to write $\rho^{\mathbf{j},\mathbf{k}}_{A_iB_i}$, at nesting level n, in terms of $\rho^{\mathbf{j}'}_{A_iB_i}$

and $\rho^{\mathbf{k}'}_{A_iB_i}$, at nesting level $n-1$, with $\mathbf{j}' = [j_1, \ldots, j_{2^{n-1}}, k_1, \ldots, k_{2^{n-1}}]$ and $\mathbf{k}' = [j_{2^{n-1}+1}, \ldots, j_{2^n}, k_{2^{n-1}+1}, \ldots, k_{2^n}]$, going back to the starting point, where

$$\tilde{\rho}^{(0)}_{\text{good}} = \frac{1}{2} \sum_{j,k=0,1} \bigotimes_{i=1}^{3} \rho^{jk}_{A_iB_i} \tag{4.19}$$

can be calculated for each elementary link.

As can be seen in Eq. (4.18), the number of terms that need to be calculated for nesting level n is $2^{2^{n+1}}$. This is despite the fact that we already limit ourselves to a particular measurement outcome. For instance, at $n = 3$, the number of terms is $2^{16} = 65,536$, which means that our core 4-qubit calculations has to be run this many times in order to get all possible outputs. This may still sound manageable, but certainly not scalable especially if we are dealing with the analytical form of each term.

In this chapter, we develop several approximation techniques to handle the computational complexity in Eq. (4.18). By carefully analyzing each component, we find the terms that contribute negligibly to the secret fraction and can therefore be omitted. The principle behind our approximation techniques is to break the exponential growth trend and cut off the number of terms that has to be considered at each nesting level, thus improving the calculation speed dramatically. This has been achieved via analytical and numerical techniques as explained below. Using such techniques, we can also analyse larger codes in our setting, an example of which is given at the end of this section.

4.4.1 Analytical approximations

In this section, we investigate three approximation techniques. Figure 4.5 gives a comparison between these three techniques and that of exact results for $n = 1, 2, 3$ as a function of β. Our approximation method (i) is a crude one, in which, at each nesting level, we only keep four combination terms in which the initial state of all elementary links is assumed to be the same, i.e., j_l (k_l) is the same for all values of l and takes one of the possible values of 0 and 1. In other words, $\mathbf{j} = \mathbf{0}, \mathbf{1}$ and $\mathbf{k} = \mathbf{0}, \mathbf{1}$. The results, while not matching the exact curves, follows the trend very closely, at each nesting level, for small to moderate values of β. It suggests that,

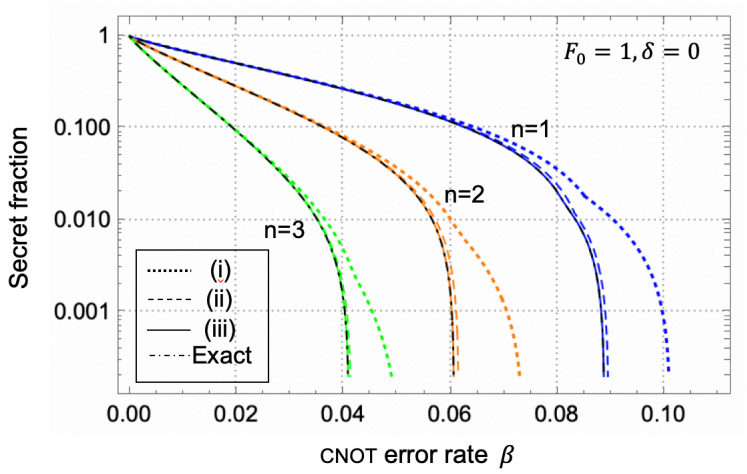

Figure 4.5: Secret fraction r_∞^{opt} versus gate error probability β for the first three nesting levels under three different approximation methods, with initial fidelity $F_0 = 1$ and measurement error probability $\delta = 0$.

in this region, the contribution from the four terms with identical input states at each elementary link is the major contributor to the key rate, and all other input combinations can somehow be neglected. Approximation (i), nevertheless, cannot correctly predict the maximum value of β at each nesting level, and only provides an upper bound on that. Our approximation techniques (ii) and (iii), respectively, correspond to the first-order and second-order approximations of the output state $\tilde{\rho}_{\text{good}}$, but with some nuances. The question is, as we deal, at lower nesting levels, with matrices corresponding to $\rho_{A_iB_i}^{\mathbf{j},\mathbf{k}}$, which of such matrices to keep at higher nesting levels, and which elements within each matrix needs to be accounted for. Note that each $\rho_{A_iB_i}^{\mathbf{j},\mathbf{k}}$ represents a two-qubit system, hence can be represented by a 4×4 matrix. In method (ii), starting from nesting level one, we keep all components $\rho_{A_iB_i}^{\mathbf{j},\mathbf{k}}$ for which their matrix representation has at least one element of order β, or lower. We also equate to zero all elements of such a matrix that are of the order of β^2 or higher. Please note that if an element has terms on the order of β or one, that element would be fully kept. We observe strange instability in our calculations, when β is moderately large, if we do not keep the whole element, including all higher order terms, in such cases. As a result of this purging, some combinations of $\mathbf{j}, \mathbf{k}$ do not contribute to either the

summation at the current level or as an input to next nesting levels. This makes the computation workload considerably lighter. Approximation method (iii) is very similar except that we keep matrices that have elements of order $\mathcal{O}(\beta^i)$, $i \leq 2$. In such a case, again, the full expression for the element is used even if some parts of it is of higher order than two.

As can be seen in Fig. 4.5, approximation methods (ii) and (iii) come very close to the exact results, with their difference to each other and the exact results becomes negligible at $n = 3$. It can then be concluded that either of them would be sufficient to give us a tight estimate of the key rate at high nesting levels. This could be because, in our scheme, we only use good states for generating secret key bits. The higher order error terms can result in a larger number of errors, which would be harder to remain unnoticed, in higher nesting levels, where quite a few measurements are performed at the ES stage. This would make the contribution from terms in higher orders of β less important. These analytical approximations give us some useful insight into which components contribute the most to the key rate [1]. With this in mind, in the next section, we introduce a numerical approximation technique, by which we can even consider higher nesting levels.

4.4.2 Numerical approximations

For arbitrarily high nesting levels, while the analytical approximation techniques discussed previously are still applicable, the simulation speed is still severely limited by the complexity of the analytical expressions after each ES operation. Numerical techniques will then be required to find the output state in such cases. Here, based on what we learned from our analytical techniques, we propose a numerical approximation method, which is both reliable and fast. In our method, starting from nesting level one, we use the following procedure

1. Calculate $\rho_{A_iB_i}^{\mathbf{j},\mathbf{k}}$ for all relevant combinations of $\mathbf{j}, \mathbf{k}$ that we have kept in the previous nesting level (i.e., all, at $n = 1$).

[1] We clarify that, based on our observation in Fig. 4.5, neglecting higher-order error terms gives a slightly optimistic prediction.

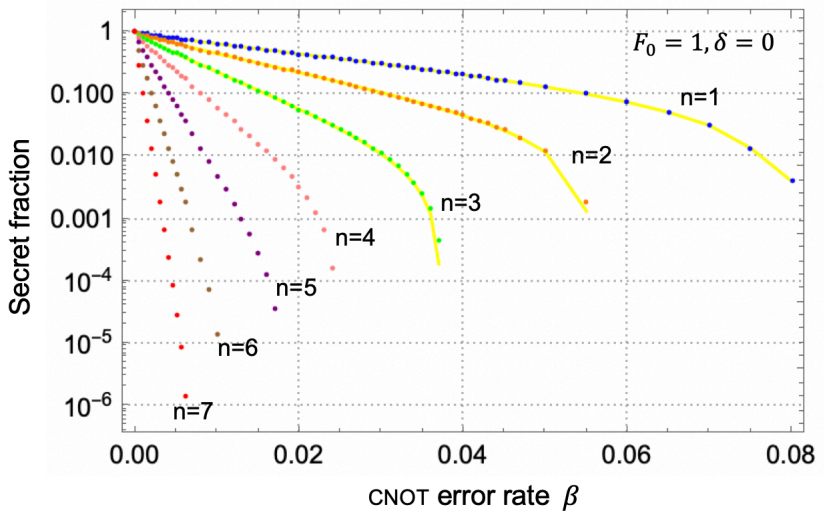

Figure 4.6: Secret fraction r_∞^{opt} for three-qubit repetition code, as a function of gate error probability β for different nesting levels, using our numerical approximation technique at $N_{\text{top}} = 20$, with initial fidelity $F_0 = 1$ and measurement error probability $\delta = 0$. Here, the errors in the encoding and decoding circuits are included. The exact simulation results for the first three nesting levels are shown (solid yellow lines) as comparison.

2. Each $\rho_{A_iB_i}^{\mathbf{j},\mathbf{k}}$ is represented by a 4×4 matrix. We collate all 16 elements for all states calculated in step 1, and sort them in the decreasing order based on their absolute values. We keep the top N_{top} elements, and equate the rest to zero.

3. We identify combinations $\mathbf{j}, \mathbf{k}$ whose corresponding matrices have at least one nonzero element after step 2. We keep these states, and ignore the rest.

4. Repeat the above steps for the next nesting level, until reaching the desired one.

In Fig. 4.6, we plot the secret fraction as a function of gate error probability β for up to seven nesting levels, using the above algorithm at $N_{\text{top}} = 20$, with initial fidelity $F_0 = 1$ and measurement error probability $\delta = 0$. We also present the exact simulation results (solid yellow lines) for the first three nesting levels. The value of $N_{\text{top}} = 20$ is chosen such that the results of our numerical approximation

match the exact calculation results with high accuracy. The results of the previous section regarding the higher order terms being negligible at high nesting levels give us some assurance that the numerical results remain accurate for $n > 3$ as well. We have included the results for up to seven nesting levels because, even for an elementary distance of 20 km, this already covers 10,000 km of distance for the repeater chain. This is the order of magnitude that we need for continental-scale quantum repeaters. We come back to this point in Sec. 4.5. An interesting observation in Fig. 4.6 is that, even at $n = 7$, the required threshold for β is on the order of 1%, which keeps the prospect of implementing such systems, at long distances, promising. For instance, QMs based on trapped ions or vacancy centers in diamond or silicon mostly meet the measurement and gate requirements for this setup, and can be used in early demonstrations Ballance et al. [2016], Erhard et al. [2019], Gaebler et al. [2016], Taminiau et al. [2014], Van der Sar et al. [2012], Zhang et al. [2014].

From Fig. 4.6, we can obtain the maximum gate error β that can be tolerated for extracting a non-zero secret key rate at different nesting levels. In Table II of Ref. Abruzzo et al. [2013], a similar analysis is performed for the original quantum repeater protocol Briegel et al. [1998], also known as the BDCZ protocol after its authors. Note that in Abruzzo et al. [2013], the authors use the gate quality $p_G = 1-\beta$ as a figure of merit. Compared with their results, we notice that the quantum repeater protocol in the present work is more tolerant to gate errors at nesting levels $n \geq 3$. At low nesting levels, the BDCZ quantum repeater may, however, work better, but considering that the memory decoherence is expected to hit harder the BDCZ protocol than the encoded repeater [1], it is likely that the latter can perform better at lower nesting levels as well, once we consider decoherence effects. This result can be taken as an improvement of the results obtained in Ref. Bratzik et al. [2014], where the authors conclude that the encoded QR is less tolerant against gate errors than the original QR. The change in conclusion could be mainly due to the more accurate modelling of gates and measurement modules, in our work, as well as the improvement that we get because of our classification

[1] This is because probabilistic ED operations are typically involved in the BDCZ protocol, which may take many rounds of classical information to confirm their success.

technique, i.e., separating the cases for which no error has been detected, at the ES stage, from the rest.

Table 4.1: The simulation time for calculating the secret key fraction for different methods: Exact analytical solution, analytical approximation method (iii) in Sec. 4.4.1, and the numerical approximation method at $N_{\text{top}} = 20$. Here we use three-qubit repetition codes with β as the variable, while the other two parameters are error-free. The time shown is the average time using a personal computer. The Numerical column represents the computation time per point.

Nesting level	Exact	Analytical (iii)	Numerical
$n = 1$	∼1.5 s	∼1.5 s	∼0.06 s
$n = 2$	∼3.1 s	∼2.7 s	∼0.12 s
$n = 3$	∼65.8 s	∼9.2 s	∼0.61 s
$n = 4$	>54852.2 s[1]	∼106.6 s	∼2.4 s
$n = 5$	N/A	N/A	∼5.3 s
$n = 6$	N/A	N/A	∼11.6 s
$n = 7$	N/A	N/A	∼31.4 s

[1] We stopped the simulation at this point without getting the final results.

Finally, it would be interesting to find out how computation time is improved using either of our analytical or numerical approximation techniques. Table 4.1 shows the time consumed in each technique, including the exact analytical approach, in order to obtain the secret key fraction, at different nesting levels, in a nominal setting corresponding to Figs. 4.5 and 4.6. That is, we use CNOT error rate, β, as a variable, and fix the initial fidelity at $F_0 = 1$ and measurement error probability at $\delta = 0$. The time shown may change if we change the parameter setting, and, in any case, they mainly represent the order of magnitude suitable for comparison, as the actual time may depend on the processor used and/or other conditions of the computing device. In our case, we have used a personal Mac machine, and we have run the simulations several times, under similar conditions, to get an average value for each point. Based on the numerical figures in Table. 4.1, we notice that, as expected, the computation time scales exponentially in almost all cases, but there is a huge difference in the slope of the growth in the

three cases, where for the exact analytical technique, even at $n = 4$, we could not find the final answer after spending over 15 hours, whereas for the analytical approximation approach, we obtain the answer in less than two minutes. This time was only around 2 s per point in the numerical approximation case. In the end, although at low nesting levels, the computation time is about the same for all schemes, the only solution that can practically be used to assess the performance in continental-scale scenarios, or for larger codes, is the numerical one. Note that the time figures shown in the numerical case are per calculated point. The total time needed would then need to be multiplied by the number of points we are interested in. But, this additional factor would only affect the total computation time linearly.

Now that we have sufficient tools to analyze our system, we can investigate the dependence of the key rate on another important design aspect, i.e., the employed code itself. So far, we have only dealt with the case of the three-qubit repetition code. This code is one of the simplest, and, therefore, weakest possible codes when it comes to error correction. One may wonder, if we use stronger codes, whether we get any improvement in system performance. We should bear in mind that larger codes require more gates for their encoding and decoding, and their additional error correction capabilities may be countered by the increase in the encoding errors. In the case of decoders 3 and 4, which we consider here, some key sources of error at the decoder are eliminated, but it would still be interesting to see how larger codes behave, as we investigate next.

The effect of the employed code

In this section, we find the secret fraction for a five-qubit repetition codes as described in Eq. (4.4). We will investigate if the ability of this code in correcting for up to two errors would be helpful for the QKD setup considered in this work. The setup and the protocol used is very similar to that of three-qubit code with certain obvious changes for the five-qubit case. For instance, the initial codeword state for node A, in Fig. 4.1, is now ideally given by $(|\tilde{0}\rangle_A + |\tilde{1}\rangle_A)/\sqrt{2}$, which can be achieved by applying four CNOT gates on the state $\frac{1}{\sqrt{2}}(|0\rangle_{A_1} + |1\rangle_{A_1})|0\rangle_{A_2}|0\rangle_{A_3}|0\rangle_{A_4}|0\rangle_{A_5}$, with A_i representing the individual memories in bank

A. Similar to what we have considered for the three-qubit repetition code, after accounting for errors in such gates, the codeword state for memory bank A is given by

$$\rho_A^{\text{in}} = \rho_A^{\text{code}} + \rho_A^{\text{other}}, \tag{4.20}$$

where

$$\begin{aligned}\rho_A^{\text{code}} =& \frac{1}{32}(16 - 44\beta + 49\beta^2 - 25\beta^3 + 5\beta^4)\times \\ & (|00000\rangle_A\langle 00000| + |11111\rangle_A\langle 11111|) \\ & + \frac{1}{2}(1-\beta)^4(|00000\rangle_A\langle 11111| + |11111\rangle_A\langle 00000|)\end{aligned} \tag{4.21}$$

contains the terms which are in the tensor product form of having the same input qubit in all rows. The state ρ_A^{other}, which contains many more combinations of input states, is lengthy and will not be given explicitly here. Based on the observation in Fig. 3.6 in chapter 3, where it is shown that ρ_A^{code} part plays the major role in determining the secret fraction, here we only consider Eq. (4.21) and neglect the other terms. This crucially simplifies the code for further simulation.

Figure 4.7 shows the secret fraction as a function of gate error β for QRs with five-(dashed lines) and three-qubit repetition codes (solid lines), at $F_0 = 1$ and $\delta = 0$, up to $n = 3$. We notice that, initially, the protocol with three-qubit repetition code generates more keys. This is expected as, at low values of β, there are not that many errors and the three-qubit code can detect them similarly to the five qubit code, without imposing additional encoding errors [1]. However, with the increase in β, the protocol with five-qubit repetition codes begins to show advantage over the three-qubit code since it can tolerate more errors. We have to wait and see if this possible advantage at higher error rates is of any practical relevance. We give an answer to this question in the following section.

[1] One may wonder if the performance of five-qubit code might be underestimated here due to the neglect of the other cross terms. We mention that this should not be the case based on the observation in Fig. 3.6, where the involvement of other cross terms deteriorates the performance rather than improves it. We would expect the similar performance also hold for five-qubit cases.

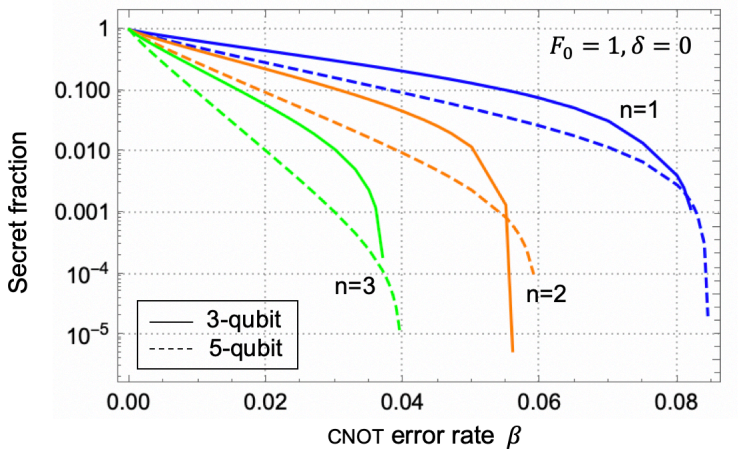

Figure 4.7: Secret fraction r_∞^{opt} of QRs encoded with three-qubit repetition code (solid lines) and five-qubit repetition code (dashed lines) for the first three nesting levels as a function of gate error probability β, with initial fidelity $F_0 = 1$ and measurement error probability $\delta = 0$. We have used our numerical approximation method at $N_{\text{top}} = 20$.

4.5 Secret key rate for the repeater chain

The most practical figure of merit for a QKD system is often represented by its total secret key generation rate, R, in bits per unit of time. Thus far, we have only focused on the secret fraction, which gives us the probability of generating a secret key once a multipartite entangled state is shared with the users. In order to obtain the total secret key generation rate, we need to multiply the secret fraction by the entanglement generation rate γ. In this section, we account for the latter factor, in two possible implementations of the setup in Fig. 4.1, as well as the corresponding fully probabilistic quantum repeater setups. This allows us then to specify the regions in which each setup could offer a better performance.

In all cases considered in this section, we assume that a DLCZ-like protocol Duan et al. [2001] is used to distribute entanglement over the elementary links. In this scheme, entangled memory-photon pairs are generated simultaneously at each elementary node, the photons are coupled into optical fibers and interfere in the middle of each segment. A successful BSM, which is classically communicated to the two end nodes of the elementary link, projects the corresponding

memory qubits into an entangled states. In our work, we assume that the success probability for each entangling attempt is given by Sangouard et al. [2009, 2011]

$$P_0 = \frac{1}{2} p^2 \eta_{\text{ch}}^2 \eta_d^2, \tag{4.22}$$

where p represents the probability of generating the initial memory-photon entanglement and the coupling efficiency of a photon into the optical fiber, η_d accounts for the detector efficiency and its corresponding coupling efficiency, and $\eta_{\text{ch}} = \exp\left[-\frac{L_0}{2L_{att}}\right]$ is the transmitivity of a photon through half of the elementary link with length L_0. L_{att} is the attenuation length of the channel, where for standard optical fibers is around 22 km. Also, ignoring the measurement time and the interaction time between memories and photons, each entangling attempt as above would take

$$T_0 = L_0/c, \tag{4.23}$$

which includes the initial transmission of the photon and the classical communication to verify the success, with $c = 2 \times 10^5$ km/s being the speed of light in fiber. With the successful probability for generating one Bell pair being P_0, the average waiting time for generating N Bell pairs is given by

$$< T >_N = T_0 Z_N(P_0) \tag{4.24}$$

where $Z_N(P_0)$ is the average number of trials required to distribute N Bell pairs given by Bernardes et al. [2011]

$$Z_N(P_0) = \sum_{k=1}^{N} \begin{pmatrix} N \\ k \end{pmatrix} \frac{(-1)^{k+1}}{1-(1-P_0)^k}. \tag{4.25}$$

Based on the above entanglement distribution protocol, we now consider several QR protocols based on error correction, with and without multiplexing, and probabilistic ES operations, and compare them together.

4.5.1 Encoded QR with no multiplexing

Here, we consider, the setup in Fig. 4.1, with minimal number of logical quantum memories, that is, $2q$ per memory bank for a q-qubit repetition code with $q = 3, 5$. The factor two accounts for the memories used for initial entanglement distribution (small circles) and those used for the remaining steps (large circles). The total number of memories, at nesting level n, in the setup is then given by $2^{n+2}q$. In this setting, whenever, at any intermediate node, the initial entanglement over its adjacent links are prepared, we can go ahead and perform the corresponding ES operation at that node. By this technique, on average it will take $Z_{N_{\rm det}}(P_0)$, for $N_{\rm det} = q \times 2^n$, until we have all elementary links entangled, and done the corresponding ES operations. The entanglement generation rate, i.e., the number of encoded entangled states shared per second is then given by

$$\gamma_{\rm det} = \frac{1}{< T >_{N_{\rm det}}}. \tag{4.26}$$

The subscript det refers to the deterministic QR considered in the present work. The normalized secret key generation rate is then given by

$$R_{\rm det} = \frac{r_\infty^{\rm opt} \times \gamma_{\rm det}}{2^{n+2}q}, \tag{4.27}$$

where $r_\infty^{\rm opt} = \max(r_\infty^{(3)}, r_\infty^{(4)})$.

Note that, in practice, each physical memory module may contain multiple logical qubits. For instance, for nitrogen vacancy centers in diamond, both electronic and nuclear spins can be used as a qubit. In such cases, the normalized rate in Eq. (4.27) can be modified to account for this factor.

4.5.2 Encoded QR with multiplexing

With the probability for successfully generating an entangled pair P_0 being small, a large number of attempts will be needed before one elementary link is ready for use. One could, however, do this entangling process in parallel across many pairs of memories. This multiplexing operation improves the rate and resilience to decoherence Collins et al. [2007], Razavi et al. [2009] at the price of requiring significantly more physical resources to minimize the required temporal resources.

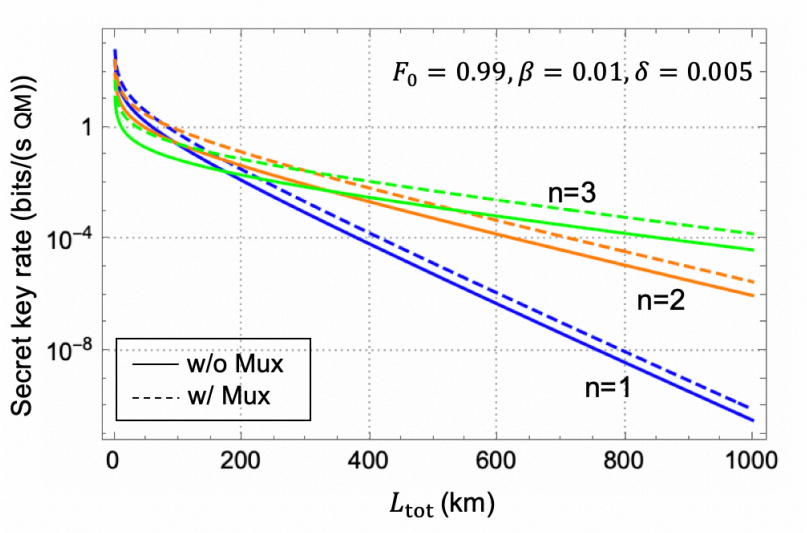

Figure 4.8: Normalized secret key rates for the encoded QRs with/without multiplexing for the first three nesting levels as a function of the total distance, with initial fidelity $F_0 = 0.99$, gate error probability $\beta = 0.01$ and measurement error probability $\delta = 0.005$. The secret key rate is calculated for the better of decoders 3 and 4 at $p = 0.5$, $\eta_d = 0.9$, and L_{att} =22 km using our numerical approximation technique at $N_{\text{top}} = 20$.

Here, we consider the case where there are a large number of memories N_m per station satisfying $N_m P_0 \gg 1$. Using this multiplexing technique, we can ensure that, after every attempted cycle of duration T_0, there are enough entangled pairs generated to immediately perform the QR swapping and QKD measurement operations. The entanglement generation rate, for this continuously running system, is given by

$$\gamma_{\text{det}}^{\text{Mux}} = \frac{N_m P_0}{q T_0}, \tag{4.28}$$

which leads to the normalized secret key generation rate as follows

$$R_{\text{det}}^{\text{Mux}} = \frac{r_\infty^{\text{opt}} \times \gamma_{\text{det}}^{\text{Mux}}}{4 N_m \times 2^n} = \frac{r_\infty^{\text{opt}} P_0}{2^{n+2} q T_0}. \tag{4.29}$$

In Fig. 4.8, we plot the normalized secret key rate for QRs with 3-qubit repetition code with and without multiplexing as a function of the total distance $L_{\text{tot}} =$

$2^n L_0$. We assume an initial fidelity $F_0 = 0.99$, gate error probability $\beta = 0.01$, and measurement error probability $\delta = 0.005$. As for other parameters, we have assumed $p = 0.5$, which is achievable for cavity-enhanced memories Riedel et al. [2017], and $\eta_d = 0.9$ Marsili et al. [2013]. For the chosen parameters, we can generate non-zero key rates up to the third nesting level. Note that according to Fig. 4.8, the optimum distance for elementary links is about 50 km. Since the memory coherence time and dark count rate of detectors are not taken into account in this analysis, we do not see the typical cut-off security distance beyond which secure key exchanges is not possible. It is expected that a coherence time on the order of $10T_0$ and $10 < T >_{N_{\text{det}}}$ are, respectively, needed for the proper operation of the system with and without multiplexing Lo Piparo & Razavi [2013]. We notice that, as expected, the multiplexing helps increase the secret key rate. The higher the nesting level, the more visible this increase is. But, even with multiplexing, the total rate achievable by the system is rather low. For instance, at a total distance of 800 km, we would need around 1000 quantum memories to obtain a total key rate on the order of bits per second. This is comparable with what one may achieve with probabilistic quantum repeaters. Next, we will consider this class of quantum repeaters for a more quantitative analysis.

4.5.3 Probabilistic quantum repeaters

The most feasible implementations of quantum repeaters rely on probabilistic operations for the initial entanglement distribution as well as further ES operation Yu et al. [2020]. Initially proposed by Duan, Lukin, Cirac and Zoller (DLCZ) Duan et al. [2001], it soon found various alternatives Amirloo et al. [2010], Sangouard et al. [2011]. Here, we use a generic model for this class of quantum repeaters to enable a fair comparison with encoded systems when it comes to QKD as an application. One key difference is in the fact that the implementation of probabilistic ES is not based on gate operations. Instead, a probabilistic photonic ES can be achieved by converting back the state of quantum memories to single photons and then do BSMs on the corresponding photons. We can therefore neglect all gate and measurement errors in probabilistic repeaters, and only consider imperfections in the initially distributed Bell states. The main drawback of such

a protocol is that probabilistic BSMs increase the waiting time and reduce the rate. The resilience to decoherence would also be lower, requiring coherence time on the order of $10 \times L_{\text{tot}}/c$, because of additional transmission delays, even if multiplexing is used Lo Piparo & Razavi [2013].

Based on above assumptions, in this work, the ES operation is modelled as follows. If, by nesting level n, the entangled states on ab and cd links is diagonal in the Bell basis and is given by $\rho_{ab} = \rho_{cd} = A_n|\phi^+\rangle\langle\phi^+| + B_n|\phi^-\rangle\langle\phi^-| + C_n|\psi^+\rangle\langle\psi^+| + D_n|\psi^-\rangle\langle\psi^-|$, the resulting state between a and d after a BSM on b and c can still be written in the Bell diagonal form with the following new coefficients Abruzzo et al. [2013]

$$\begin{aligned} A_{n+1} &= (A_n^2 + B_n^2 + C_n^2 + D_n^2), \\ B_{n+1} &= 2(A_n B_n + C_n D_n), \\ C_{n+1} &= 2(A_n C_n + B_n D_n), \\ D_{n+1} &= 2(A_n D_n + B_n C_n). \end{aligned} \tag{4.30}$$

The initial state of the elementary links in our analysis is given by Eq. (4.1). The successful probability for the ES operation is assumed to be

$$P_{\text{ES}} = \frac{1}{2} p_m^2 \eta_d^2, \tag{4.31}$$

where p_m is the reading and coupling efficiency of memories, which, for simplicity, here we assume $p_m = p$. The entanglement generation rate for such a protocol can be derived as Sangouard et al. [2011]

$$\gamma_{\text{prob}} = \frac{1}{< T >_{N_{\text{prob}}}} P_{\text{ES}}^n \tag{4.32}$$

for $N_{\text{prob}} = 2^n$. Here, we assume the ES success probability is the same for all nesting levels. The normalized secret key rate per memory is then given by

$$R_{\text{prob}} = \frac{r_\infty^{\text{prob}} P_{\text{click}} \gamma_{\text{prob}}}{2^{n+1}}, \tag{4.33}$$

where $P_{\text{click}} = \eta_d^2$ is the success probability for performing QKD measurements (twofold coincidence), and

$$r_\infty^{\text{prob}} = r_\infty(C_n + D_n, B_n + D_n) \tag{4.34}$$

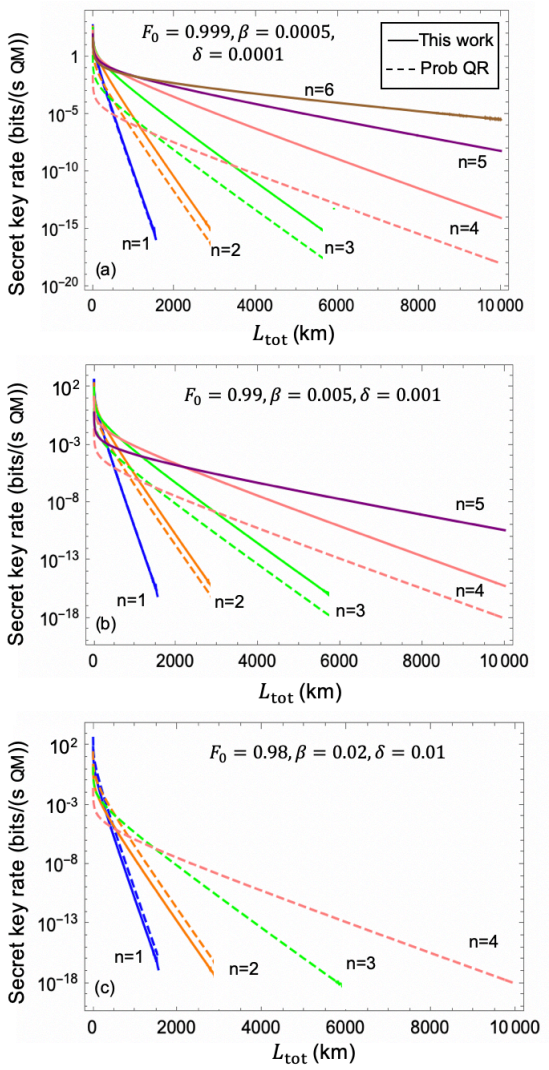

Figure 4.9: Normalized secret key rates for QRs with encoding (solid, three-qubit code) and probabilistic QRs (dashed) in the absence of multiplexing for up to six nesting levels as a function of the total distance, with different error parameters: (a) $F_0 = 0.999$, $\beta = 0.0005$ and $\delta = 0.0001$; (b) $F_0 = 0.99$, $\beta = 0.005$ and $\delta = 0.001$; (c)$F_0 = 0.98$, $\beta = 0.02$ and $\delta = 0.01$. Other parameters are as in Fig. 4.8. In the encoded repeater case, the secret key rate is calculated for the better of decoders 3 and 4 using our numerical approximation method at $N_{\text{top}} = 20$.

at nesting level n.

One can similarly find out the corresponding key rate equations in the case of multiplexed repeaters; see, for instance, Razavi et al. [2009]. The results are very similar to that of Fig. 4.8. For the sake of comparison that we are pursuing in this paper, we obtain similar results if we use encoded and probabilistic QRs both with, or without, multiplexing. Given that, for early demonstrations of quantum repeaters, quantum memories are quite precious, next we compare the two systems only in the case of no multiplexing for which fewer memories are needed.

4.5.4 Optimal QRs in different parameter regions

Figure 4.9 shows the secret key rate for encoded and probabilistic QRs for three sets of parameters. These three sets represent different degrees of reliability for our quantum gates and measurements. This mainly affects the encoded repeater case, and we notice that, in all three cases, the probabilistic QR (dashed lines) can only offer a key up to nesting level four, while the encoded QR (solid lines) can offer better rate-versus-distance scaling by using higher nesting levels. In Figs. 4.9(a) and (b), corresponding to low-error and moderately-low-error regimes, we notice that the QR with encoding offers higher key generation rates than the probabilistic one. This advantage increases with the nesting level to the point that, at $n = 4$, the QR with encoding improves the key rate by more than three orders of magnitude. In lower error regime with $F_0 = 0.999, \beta = 0.0005, \delta = 0.0001$, the encoded QR can generate secret keys up to $n = 6$ corresponding to 64 elementary links. If we multiply the number of QMs required at this nesting level by the normalized key rate, the total key rate is $\sim 10^{-2}$ bits per second at 10,000 km, which is comparable to what currently most advanced fiber-based QKD techniques can achieve at distances below 1000 km Chen et al. [2020], Currás-Lorenzo et al. [2021]. If the error parameters are increased by one order of magnitude, as in Fig. 4.9(b), secret key can only be extracted up to $n = 5$ for encoded QRs, and the generated key will be reduced by two orders of magnitude as compared to Fig. 4.9(a) at $n = 5$. In the higher error regime, shown in Fig. 4.9(c), the probabilistic QR shows better performance in most distances.

This is mainly because of the errors involved in the gates, which makes the use of error correction codes less effective. In Fig. 4.9(c), the QR with three-qubit encoding can only generate secret keys up to $n = 2$ with the specified error parameters. We conclude that the QR with encoding will only be useful when the error rates are moderately low.

The examples in Fig. 4.9 imply the existence of operation regions in which one or the other QR could offer a better performance. In Figs. 4.10(a) and (b), we have, respectively, specified these regions, at a fixed distance of 1000 km, for three-qubit and five-qubit repetition codes. The choice of 1000 km corresponds to possibly near-term implemetations of QR systems that outperform no-repeater systems. In both figures, we have highlighted which QR structure offers the higher key rate, if any, as a function of our three error parameters $1 - F_0$, β, and δ. We identify four regions in Figs. 4.10(a) and (b):

- Region 1: For low gate and measurement error probabilities, when initial fidelity of Bell states is high, the third nesting level of QRs with encoding dominates.
- Region 2: For the same region of gate and measurement error probabilities, when initial fidelity becomes worse, the second nesting level of QRs with encoding is more favourable.
- Region 3: For slightly higher gate and measurement error probabilities, the encoded QR loses its advantage, and probabilistic QRs are the best option.
- Region 4: For high error probabilities and low initial fidelity of the original entangled states, it is not possible to generate a secure key with either of QR protocols.

It is interesting to note that the region that the three-qubit code outperforms the probabilistic QR is larger than that of the five-qubit code. In fact, by the time that, according to Fig. 4.7, the five-qubit QR outperforms the three-qubit one, both encoded QR structures perform worse than the probabilistic repeater. This would suggest then it is likely that the best error correction codes for QKD purposes are the simplest ones, and it may not be necessary to overcomplicate

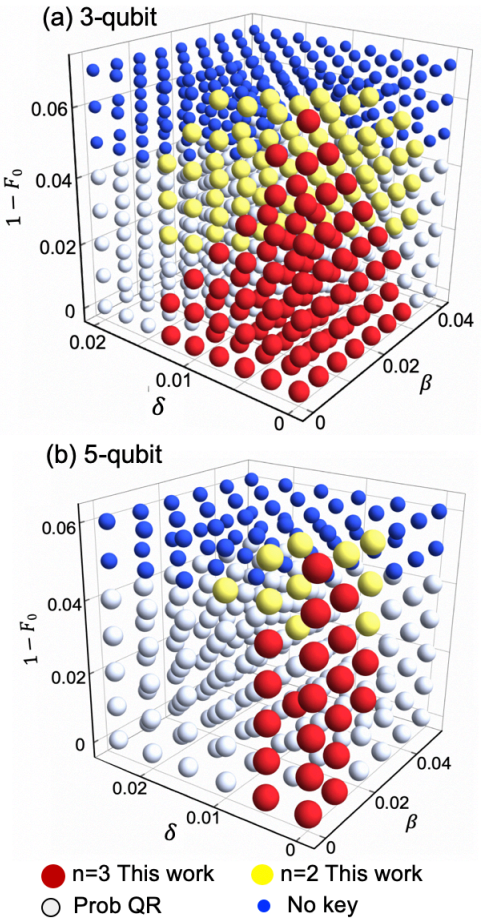

Figure 4.10: The region plots showing the distribution of the optimal QR protocol in a three-dimensional parameter space at $L_{\text{tot}} = 1000$km for (a) three-qubit repetition code and (b) five-qubit repetition code. Other parameters are as in Fig. 4.8. In the encoded repeater case, the secret key rate is calculated for the better of decoders 3 and 4 using our numerical approximation method at $N_{\text{top}} = 20$.

the system by employing larger codes. In fact, so long as QKD is concerned, the practical choices seem to be between a probabilistic structure for the quantum repeater versus the three-qubit code in the encoded structure. We mention that we do not consider all sources of imperfection in our analysis, and it may be ill judged to rule out the possibility of finding better codes. We should also note that, in our comparison, we have not considered the third generation of quantum repeaters, which rely on quantum error correction for handling both channel loss and gate errors. The requirements of such systems is much more stringent than the ones we considered here, and, at least, in the short term, our above conclusion may be the most relevant one for initial implementation of the system.

Another interesting observation in Fig. 4.10(a) is that the typical values required for $1 - F_0$, β, and δ, in order to offer an advantage over probabilistic repeaters, seems to be quite within a feasible range. For the key error parameter of β, up to 2% is acceptable, whereas for fidelity we are looking at lower ninety's, which both seem achievable with current technology. The measurement error can also be kept below 1%. All in all, our analysis suggests that extending the reach of trust-free terrestrial QKD links to 1000 km is within reach in the near future.

4.6 Conclusions

In this chapter, we benchmarked the performance of a QKD system that relied on QEC for ED against probabilistic QRs that do not necessarily use any additional distillation techniques. In order to improve system performance and simplify its implementation requirements, in the former case, we first proposed two decoding schemes that did not need any two-qubit gates. This reduced the decoding errors, as compared to conventional error-correction decoders, and increased the resilience of the system to common sources of error. In order to analyse the system, we also developed several numerical and analytical approximation techniques, and checked them against exact results in certain cases. This allowed us to study the performance of two codes from the family of repetition codes. We interestingly found that, for most practical purposes, the three-qubit system could offer the best performance so long as error parameters are around 1%. In higher error regimes, probabilistic QRs could already offer better rates, or secret

key exchange was not at all possible. Our results also shed light into how encoded QRs would compare with some other classes of QRs that relied on probabilistic ED techniques. We showed that for moderate to high nesting levels the encoded setup could tolerate more errors than the BDCZ protocol. We note that the extension of our decoding and approximation techniques are in principle possible to larger codes, but, in the case of QKD, this may not offer additional advantage. Based on our analysis, it seems feasible to employ current technologies for QMs to demonstrate this encoded class of repeaters.

Chapter 5

Quantum repeaters with encoding on nitrogen-vacancy center platforms

5.1 Introduction

In this chapter, we study the use of NV centers as a platform for QRs with encoding. This is partly driven by the successful implementation of deterministic two-qubit gates between electron and nuclear spins of a single NV center Jelezko et al. [2004], Taminiau et al. [2014], Waldherr et al. [2014]. Moreover, such memories are adopted for the first demonstration of a simple QR network between four cities in Netherlands Pompili et al. [2021], van Dam et al. [2017]. This offers a promising platform for the implementation of near-future encoded QR structures. Through the work of last two chapters, we learn that the simple three-qubit repetition code could be the best option for QKD applications over short to moderately long distances. In particular, we find that there are working regimes of operation where encoded QRs can outperform probabilistic QRs in Sec. 4.5. This means that for the type of networks that we are expecting to have in short term, it could be a rewarding exercise to implement encoded QRs despite their additional implementation challenges.

To get an accurate view of the requirements, versus gains, for NV-center based QRs with encoding, we need to consider realistic scenarios that such memories can

be used in. While, in Chapters 3 and 4, the performance of the QRs with three-qubit repetition codes is carefully studied in the presence of operational errors, such analyses are not directly applicable to the case of NV centers. Firstly, the work done previously assumes that a direct deterministic BSM on two separate QMs is readily available. This is not exactly the case for NV centers. While it is possible to use an entangled link between the electron spins of two NV centers to mediate a joint operation on them Vinay & Kok [2017], we should account for additional errors, or delays, that this may cause, and also different QR structures that we can then come up with based on this mediatory entangled link. Secondly, previous work ignores the impact of memory decoherence. Now that we have a chosen memory, which is short of ideal once it gets to coherence times, we should consider its effect on the performance to have a better assessment of system requirements.

Our main contributions in this chapter:

In this chapter, motivated by the ideas and structures in Vinay & Kok [2017] and Childress et al. [2006], we propose two structures for encoded QRs with NV centers. One structure has the advantage of requiring less consumption of classical communication, while the other one uses fewer resources. We will assess and compare their performance for generating secret key under the influence of erroneous operations and decoherence, using current or near-term experimental parameters. We compare the results with the simpler non-encoded structures where deterministic BSMs are employed but no ED operation is applied. Our results suggest that, while at short distances, the non-encoded schemes may offer the best performance, as we go to longer distances, it pays off to use structures that employ more encoded links. We also specify the gap between what we have experimentally available today versus the minimum required specifications for any of these systems to work.

This chapter is structured as follows. In Sec. 5.2, we begin with a description of the ideal implementation of encoded QRs motivated by Ref. Childress et al. [2005], Jiang et al. [2009] on NV-based platforms, and give the error models we use to formulate the problem in hand. In Sec. 5.3, we analyse the effect of

decoherence, as well as other system imperfections, on system performance, and calculate the secret key generation rates for such setups in Sec. 5.4. We compare our results with the case of QRs without encoding, and illustrate the parameter regions where one type of protocol outperforms the others. Finally, we conclude this chapter in Sec. 5.5.

5.2 System description

In this chapter, we study the implementation of QRs with encoding on NV center platforms. One of the key features of NV centers, which makes them a desirable option for QR setups, is their being a two-qubit register. This includes an electron spin acting as the optical interface with single photons, and a nuclear spin, due to neighboring carbon or nitrogen atoms to the vacancy, suitable for long-time quantum storage. Moreover, using microwave and radio frequency signals, within each NV center, two-qubit operations, e.g. controlled not (CNOT) and controlled phase gates, can be performed deterministically on these two qubits Everitt et al. [2014], Wei & Deng [2013]. Within each NV center, one can also map a quantum state from the electron to the nuclear spin, and vice versa Awschalom et al. [2018], Doherty et al. [2013], Dutt et al. [2007], Neumann et al. [2010]. All these tools come handy in dealing with operations that we need in the QR setup.

An additional requirement for an efficient QR setup is the ability to write and read single photons to and from a QM. By driving an NV center, embedded in a diamond crystal, with a laser field, we can drive many transitions that mostly involve vibrational mode phonons. Such transitions will not be useful for coherent operations as these vibrational modes often quickly die out within the crystal. Zero phonon line (ZPL) emissions are then effectively the key to generating entangled states with NV centers. Even at near zero Kelvin temperatures, however, such emission are typically only a small portion, around 3%, of all radiations from the NV center Barclay et al. [2011]. Accounting also for low collection efficiency from a bulk crystal, entanglement generation with NV centers has been extremely inefficient Epstein et al. [2005]. A remedy to both problems of ZPL emission rates and collection efficiency is to have a microcavity around the NV center Bogdanović et al. [2017], Hausmann et al. [2013], Nemoto et al. [2014], Ruf

et al. [2021]. There have been several efforts in this regard, which have improved the ZPL emission rates to 46% and have increased the collection efficiency by several factors Faraon et al. [2011], Le Sage et al. [2012], Riedel et al. [2017].

In this chapter, we assume cavity-based NV center platforms are available, and use known techniques with this technology to entangle light with NV centers and perform quantum operations and measurements on them. These tools are summarized in Sec. 5.2.1, based on which, we explain several QR protocols and structures, and then finish this section with our error models.

Throughout the paper, we denote electron (nuclear) spins with lower (upper) case letters, for instance, if $|0\rangle_a$ and $|1\rangle_a$ represent the basis vectors corresponding to, respectively, electron spin numbers $m_S = 0$ and $m_S = -1$, then $|0\rangle_A$ and $|1\rangle_A$ represent the basis vectors corresponding to, respectively, nuclear spin numbers $m_I = 0$ and $m_I = -1$ of the same NV center.

5.2.1 NV Center as a Toolbox

Here, we explain how specific features of NV centers can be used to implement the main components of encoded QRs.

Entanglement distribution

One of the key ingredients of QR protocols is to establish entangled states over elementary links. Suppose we want to share an entangled state $|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$ between nuclear spins A and B. We can then first share an entangled state between the corresponding electron spins a and b, and then map the state of a (b) to A (B). This mapping is performed by initialising the nuclear spins in $|00\rangle_{AB}$, performing CNOT gates within each NV center with the electron spin as the control qubit, and then measuring the electron spins in X basis.

There are several schemes for distributing entangled states between the electron spins of two remote NV centers. In most of them, the entanglement distribution involves generating a spin-photon entanglement at each end of the link and then swapping entanglement in the middle of the link Bernien et al. [2012], Hensen et al. [2015], Pfaff et al. [2014]. Depending on whether the spin-photon entanglement is in one optical mode (i.e., zero or one photon space), or two (e.g.,

the polarization, or time-bin, space), the BSM in the middle may rely on single-mode or two-mode interference. If the BSM is conclusive then the entanglement distribution task is heralded to be successful, otherwise it needs to be repeated until success. The schemes that rely on single-mode interference often require one photon to safely travel to the middle of the link, hence may have better rate scaling with distance for heralding success. However, in order to obtain a high fidelity entangled state, we should either keep the spin-photon entanglement generation rate very low (e.g., around 1%) Cabrillo et al. [1999], Humphreys et al. [2018], Pompili et al. [2021], Rozpędek et al. [2019] or rerun the procedure to distill the entangled state Barrett & Kok [2005], Bernien et al. [2013], Nemoto et al. [2014], Pfaff et al. [2014]. In both cases the effective success rate, in certain regimes of interest to this work, could then become comparable to the two-mode schemes, where the rate decays exponentially with the distance between nodes A and B. For instance, in our setup, where the optimum elementary link is around 10-20 km, the extra channel loss in the two-mode case is a small factor, although one has to also account for additional coupling or detector efficiencies. But, aside from the success rate of entanglement generation, another important factor is the amount of the initial noise, or loss in fidelity, that we can tolerate in our system. The two-mode schemes can, in principle, generate ideal entangled states, whereas, in the single-mode schemes, some errors, due to, e.g., generating one photon at each end, would be inevitable. In a real experiment, one has to factor in all these nuances, as well as practical restrictions on the system, to decide which entanglement distribution scheme may work best in their setting.

In order to encompass the essence of different entanglement distribution schemes available, here, we assume that a generic two-mode entanglement distribution scheme is used where, at each of nodes A and B, the polarization of a single photon is entangled with the electron spin of the NV center (see Lo Piparo et al. [2017a,b], for example). These photons are frequency converted [1], if needed, and will be coupled to an optical channel. Using linear optics and single-photon detectors, a partial BSM in the polarization basis is then performed on these two

[1] We clarify that, though in the specific analysis of this chapter, we do not directly include the frequency conversion rate, it can be embedded into the choice of coupling efficiency.

photons at the middle of the link. Once a successful BSM is heralded, this information will be sent back to nodes A and B, at which point, the state of electron spins is transferred and stored onto the corresponding nuclear spins. We model the generated entangled state as a Werner state as will be explained later in the next section. Note that any other entanglement distribution scheme can also be similarly analyzed using techniques and procedures provided in this work.

Encoded entanglement distribution

In this chapter, we again consider encoded QRs with three-qubit repetition codes as given by Eq. (3.1), which can correct up to one bit-flip error. Although this is not a strong error correction code, it has been shown in previous two chapters that so long as we rely on its error detection features it offers a reasonable performance at short and moderately long distances as compared to more complicated codes. We therefore analyse this particular code for our NV center platform.

The first step in an encoded QR is to ideally distribute encoded entangled states in the following form:

$$|\tilde{\Phi}^{+}\rangle_{\mathbf{AB}} = \frac{1}{\sqrt{2}}(|\tilde{0}\tilde{0}\rangle_{\mathbf{AB}} + |\tilde{1}\tilde{1}\rangle_{\mathbf{AB}}), \tag{5.1}$$

where here we consider two example memory banks $\mathbf{A} = (A_1, A_2, A_3)$ and $\mathbf{B} = (B_1, B_2, B_3)$ at the two ends of an elementary link. To this end, using the scheme described in the previous subsection, we first generate Bell pairs $|\Phi^{+}\rangle_{A_iB_i} = \frac{1}{\sqrt{2}}(|00\rangle_{A_iB_i} + |11\rangle_{A_iB_i})$, for $i = 1, 2, 3$. Once electron spins are available again in all NV centers of memory banks $\mathbf{a}$ and $\mathbf{b}$, we initialize them in the codeword states $\frac{1}{\sqrt{2}}(|\tilde{0}\rangle_{\mathbf{a}} + |\tilde{1}\rangle_{\mathbf{a}})$ and $|\tilde{0}\rangle_{\mathbf{b}}$. Finally, using transversal remote CNOT gates, shown in Fig. 5.1, we can generate the state in Eq. (5.1) Jiang et al. [2009]. The same procedure is applied to all elementary links.

Note that the remote CNOT circuit in Fig. 5.1 is slightly different from the one used in Fig. 3.3 in chapter 3. In the previous chapter, the remote CNOT circuit requires measurements on qubits that hold the initial Bell state, i.e., the nuclear spins in our NV-center setup. In NV centers, however, a nuclear spin is often measured by first mapping its state to an electron spin, using a CNOT gate, and then measuring the electron spin Neumann et al. [2008, 2010]. This is not,

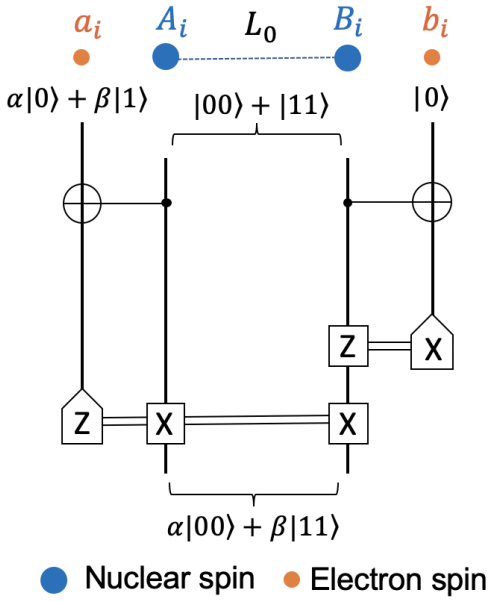

Figure 5.1: Quantum circuit for remote CNOT gate. Note that single-qubit measurements (trapezoidal boxes) are performed on electron spins. Here, $a_i - A_i$ represent the electron-nuclear spins in one NV center separated by a distance L_0 from the corresponding NV center at the other end of the elementary link.

however, possible in our case as this would ruin the initial state of the electron spins. We have therefore slightly changed the remote CNOT circuit such that the measurements are only done on electron spins with nuclear spins always in an entangled state.

Entanglement Swapping

Once encoded entangled states are distributed between the nuclear spins across all elementary links, the next step is to perform ES operations at all intermediate stations to extend the entanglement to the entire link. In the encoded repeater protocol, this can be done by performing BSMs, in a transversal way, on corresponding pairs of NV centers at each of the intermediate nodes. This operation would also allow us to pick up some of the errors that might have been accumulated by this stage, and help us distill the final entangled state. For instance,

in the 3-qubit repetition code considered here, the BSM is made of an X and a Z operator measurement, the results of which specify the type of encoded Bell state that will be shared between the remote nodes. Ideally, the results of the Z operator measurements must be 000 or 111. Because of the errors in the system, we may, however, get other combinations of 0 and 1, which correspond to detecting an error. The majority rule here can be used to specify the most likely post-BSM encoded Bell state. It turns out in previous chapter, however, that for QKD purposes, detecting the error, and using that information for post-selection, would provide us with an effective way to boost the key rate, and error correction, as envisaged in the original protocol Jiang et al. [2009], would not be needed.

For the above process, a direct joint measurement on the nuclear spins of two separate, although possibly co-located, NV centers may not be possible. To do a deterministic BSM on two separate nuclear spins, here, we distribute an additional Bell pair between the corresponding electron spins of the two NV centers. ES operations can then be performed by performing BSMs on the nuclear and electron spins within each NV center Vinay & Kok [2017]. This can be done by first applying a CNOT gate to nuclear and electron spins followed by relevant single-qubit measurements on each. Note that, in this procedure, we have to first measure the electron spin, and then map the nuclear spin state to the electron spin. The latter can be done by initialising the electron spin in an appropriate state and then performing a CNOT gate on the two spins with the nuclear spin as the control qubit. We can then measure the electron spin again, to effectively complete the measurement on the nuclear spin. A similar procedure can be used across the repeater chain. The measurement outcomes need to be notified to the end users to adjust the Pauli-frame on the final states, and/or for error correction or post-selection purposes.

Note that in the above procedure, the two NV centers do not necessarily need to be co-located, and, in principle, one can assume an arbitrary distance between the two memories. That would, however, change system resilience to memory decoherence. To study this, in the following, we define several protocols for different QR architectures and will analyse and compare them in the forthcoming sections.

5.2.2 Quantum repeater structures and protocols

In this section, based on whether we employ coding or not, and how deterministic BSMs are done, we define four protocols, as explained below.

Protocols for encoded repeaters

Here, we describe the ideal implementation of the protocol proposed in Ref. Jiang et al. [2009] with three-qubit repetition codes on NV center platforms. We consider two architectures, shown in Figs. 5.2 and 5.3, depending on whether the BSM is done on co-located NV centers or those apart by a distance L_0, corresponding to the length of an elementary link. In both structures, there are a total of 2^n elementary links, where n is the nesting level of the corresponding QR.

In what we refer to as protocol 1, we use the structure in Fig. 5.2, and carry out the following steps:

- Step 1: distribute encoded entanglement across all elementary links; see Sec. 5.2.1. As this requires multiple attempts to entangle all relevant pairs of NV centers, we stop this process, whether or not all relevant pairs are entangled, after a stoppage time T_1 and move to the next step.
- Step 2: perform BSMs at all intermediate nodes; see Sec. 5.2.1. We again stop this procedure, whether or not all relevant BSMs are completed, after a stoppage time T_2.
- Step 3: pass all measurement results to the two end users. If there are missing entangled pairs, or incomplete BSMs, then we discard the state generated in that round. We will account for the effect of such discarded states in our key rate analysis.

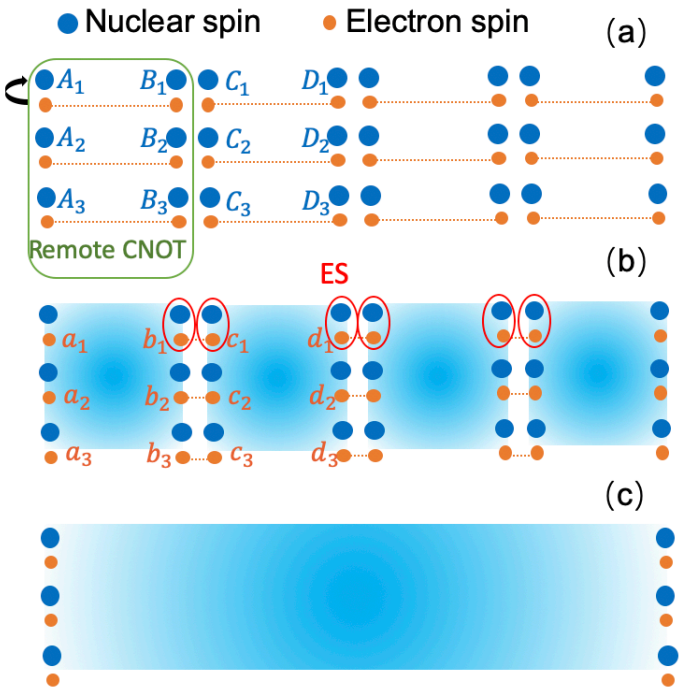

Figure 5.2: Schematic QR structure for protocol 1 with the following steps: (a) Distributing Bell pairs between electron spins (small orange circles) over all elementary links in a heralding way. Transferring and storing the entangled states to the corresponding nuclear spins (large blue circles), followed by remote CNOT gate. (b) Performing ES operation on nuclear spins at intermediate nodes by creating temporary Bell pairs between the corresponding electron spins, and then performing a BSM within each NV center. (c) The final encoded entangled state is created between the two end users. Based on the measurement results at each middle node, the Pauli frame of the final entangled state can be adjusted.

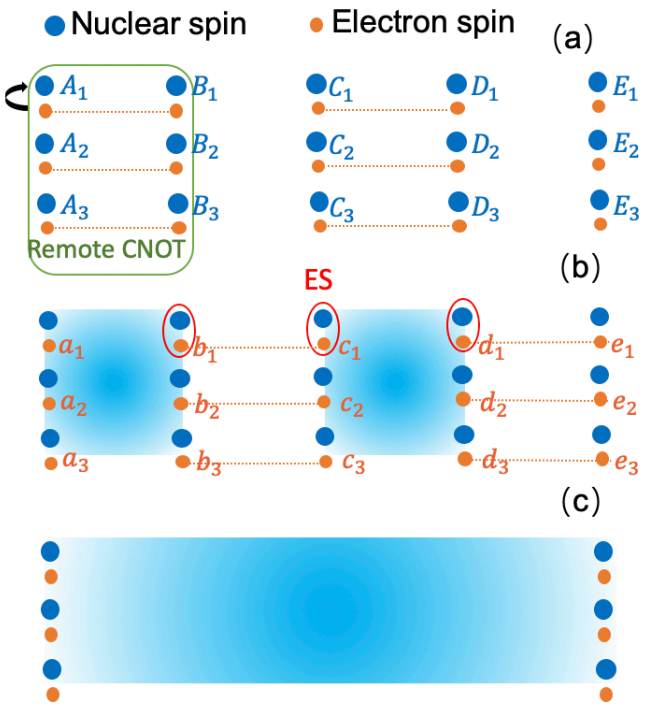

Figure 5.3: Schematic QR structure for protocol 2 with the following steps: (a) Generating encoded Bell pairs between nuclear spins in every other link; (b) Distributing Bell pairs between electron spins in all remaining links in order to facilitate BSM within each NV center at intermediate nodes. (c) The encoded entanglement is extended to end users. Based on the measurement outcomes gathered from middle stations, one can adjust the Pauli frame of the final entangled state.

In what we call protocol 2, motivated by Refs. Childress et al. [2005, 2006], we use the structure in Fig. 5.3, and carry out the following steps:

- Step 1: distribute encoded entanglement across every other elementary link; see Sec. 5.2.1. We stop this process after a stoppage time T_1 and move to the next step.
- Step 2: distribute uncoded entanglement across the electron spins of all remaining links; see Sec. 5.2.1. We stop this process after a stoppage time T_2 and move to the next step.

- Step 3: perform BSMs at all intermediate nodes, which now only contain single NV centers; see Sec.5.2.1.
- Step 4: pass all measurement results to the two end users. If there are missing entangled pairs, or incomplete BSMs, then we discard the state generated in that round.

Protocol 2 requires fewer NV centers and operations than protocol 1, and, in that sense, may offer some advantage. But, in the end, what matters is the overall performance, normalized by the total number of memories used, which we use for comparison between such protocols.

Protocols for uncoded repeaters

In order to better understand whether QRs with encoding will offer any advantages over their non-encoded versions, in this chapter, we also consider protocols 3 and 4, which are, respectively, the uncoded versions of protocols 1 and 2. For simplicity, we do not consider any distillations for protocols 3 and 4, as, without coding, that would turn them into probabilistic protocols. A comparison between encoded QRs and probabilistic ones is already available in chapter 4. In protocols 3 and 4, we just need to replace Step 1 with the following revised step:

- Step 1': distribute Bell pairs between nuclear spins in all, for protocol 3, or every other, for protocol 4, elementary links; see Sec. 5.2.1. We move to the next step after a stoppage time T_1.

The rest of the protocols is as in protocols 1 and 2, respectively.

5.2.3 Error models

In order to analyse the above QR setups, we consider three major sources of imperfections as follows.
(1) **Gate imperfections:** The CNOT gate for a control nuclear spin J and a target electron spin j, within an NV center, is modeled as Briegel et al. [1998]

$$\rho^{\text{out}} = (1-\beta)U_{J,j}\rho^{\text{in}}U_{J,j}^{\dagger} + \frac{\beta}{4}\text{Tr}_{J,j}(\rho^{\text{in}}) \otimes \mathbb{I}_{J,j}, \tag{5.2}$$

where ρ^{in} (ρ^{out}) is the input (output) before (after) the CNOT gate, and $U_{J,j}$ represents the unitary operator corresponding to an ideal CNOT gate. The error in this two-qubit operation is modeled by a uniform depolarization of qubits J and j, represented by identity operator $\mathbb{I}_{J,j}$, with probability β. We assume that a similar relationship as in Eq. (5.2) would also model a CNOT gate with the electron (nuclear) spin as the control (target) qubit. While not necessarily the case, for simplicity, we assume that the parameter β is the same in both cases. In NV centers, there are other common two-qubit gates, such as controlled phase gates, that may be used in practice. Using equivalent quantum circuits, however, such operations can often be modeled by a CNOT gate with possibly additional single-qubit rotations. In such cases, we assume parameter β captures the total error in the equivalent model. As in chapters 3 and 4, here, we assume all single-qubit operations are perfect.

(2) **Measurement errors:** The projective measurements to electron spin states $|0\rangle$ and $|1\rangle$ are, respectively, represented by

$$\begin{aligned} P_0 &= (1-\delta)|0\rangle\langle 0| + \delta|1\rangle\langle 1| \quad \text{and} \\ P_1 &= (1-\delta)|1\rangle\langle 1| + \delta|0\rangle\langle 0|, \end{aligned} \tag{5.3}$$

where δ is the measurement error probability. Similar measurement operators, $P_{\pm}$, are used for projective measurement in $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$ basis. The projective measurements of nuclear spins are modelled effectively in the same format but with error parameters $\beta/2+\delta$, since there should always be a mapping operation performed through a CNOT gate as described in Sec. 5.2.1.

(3) **Decoherence:** We model the decoherence effect in electron/nuclear spins by using a depolarizing channel. For a single qubit a (A), after a waiting time t_{w}, the initial state ρ will be mapped to

$$\begin{aligned} \mathcal{D}^{a}_{\text{depol}}(\rho) &= \lambda_2^{\text{e}}\rho + (1-\lambda_2^{\text{e}})(\mathbb{I}_2 - \rho), \\ \mathcal{D}^{A}_{\text{depol}}(\rho) &= \lambda_2^{\text{n}}\rho + (1-\lambda_2^{\text{n}})(\mathbb{I}_2 - \rho), \end{aligned} \tag{5.4}$$

where

$$\lambda_2^{\text{e/n}}(t_{\text{w}}) = \frac{1}{2} + \frac{e^{-\frac{t_{\text{w}}}{\tau_{\text{e/n}}}}}{2} \tag{5.5}$$

with $\tau_{\mathrm{e/n}}$ being the coherence time for electron/nuclear spins and $\mathbb{I}_d$ being a $d \times d$ identity matrix. The expression in Eq. (5.4) is a re-arranged form of the typical expression for a depolarizing channel, $p\rho + (1-p)\mathbb{I}_2/2$, with $p = \exp\Big\{(-t_{\mathrm{w}}/\tau_{\mathrm{e/n}})\Big\}$, in which $\lambda_2^{\mathrm{e/n}}$ represents the fidelity of the output state with respect to the input state, in the case of pure input states. As shown below, this formulation suits better the two special cases of interest we need to deal with in the setup under consideration.

The first case of interest is when we have a two-qubit system in an initial entangled state such as $|\Phi^+\rangle_{AB(ab)}$, for nuclear spins (electron spins). After a waiting time t_{w}, both spins decohere according to Eq. (5.4) resulting in $\mathcal{D}^{AB}_{\mathrm{depol}}(|\Phi^+\rangle_{AB}\langle\Phi^+|)$ as the output state for nuclear spins, where $\mathcal{D}^{AB}_{\mathrm{depol}} = \mathcal{D}^{A}_{\mathrm{depol}} \circ \mathcal{D}^{B}_{\mathrm{depol}}$, and similarly for electron spins. As shown in Appendix B, for $\rho = |\Phi^+\rangle_{AB(ab)}\langle\Phi^+|$, the output state can be written as

$$\begin{aligned} \mathcal{D}^{AB}_{\mathrm{depol}}(\rho) &= \lambda_4^{\mathrm{n}}\rho + (1-\lambda_4^{\mathrm{n}})(\mathbb{I}_4 - \rho)/3, \\ \mathcal{D}^{ab}_{\mathrm{depol}}(\rho) &= \lambda_4^{\mathrm{e}}\rho + (1-\lambda_4^{\mathrm{e}})(\mathbb{I}_4 - \rho)/3, \end{aligned} \tag{5.6}$$

where

$$\lambda_4^{\mathrm{e/n}}(t_{\mathrm{w}}) = \frac{1}{4}(3\lambda_2^{\mathrm{e/n}}(t_{\mathrm{w}}) - 1)^2 + \frac{3}{4}(1 - \lambda_2^{\mathrm{e/n}}(t_{\mathrm{w}}))^2 \tag{5.7}$$

is the fidelity of the output state with respect to the entangled input state. The same form as in Eq. (5.6) holds for any other Bell states, or any mixed state diagonal in Bell states, such as Werner states. For a general two-qubit state, Eq. (5.6) acts as a conservative approximation to decoherence effects given that it correctly specifies the fidelity of the output state, while maximizing the noise by using a maximally mixed state for all other off-diagonal terms. We use Eq. (5.6) to model decoherence across the elementary links as, in practical regions of interest, deviations from a Bell-diagonal state is reasonably small. Note that the off-diagonal terms ignored by our approximation often do not contribute to the QBER in QKD systems.

The second case of interest is when the initial state is of the form $|\tilde{\Phi}^+\rangle_{\mathbf{AB}}$, which is a six-qubit system, or a slight deviation from it. With similar calculations, we approximate the output state for an encoded entangled state ρ by

$$\mathcal{D}^{\mathbf{AB}}_{\mathrm{depol}}(\rho) = \lambda_{64}^{\mathrm{n}}\rho + (1-\lambda_{64}^{\mathrm{n}})(\mathbb{I}_{64} - \rho)/63, \tag{5.8}$$

where

$$\begin{aligned}\lambda_{64}^{\mathrm{e/n}}(t_{\mathrm{w}}) =& \frac{1}{64}[(3\lambda_2^{\mathrm{e/n}}(t_{\mathrm{w}})-1)^6 + 33(1-\lambda_2^{\mathrm{e/n}}(t_{\mathrm{w}}))^6 \\ &+ 15(3\lambda_2^{\mathrm{e/n}}(t_{\mathrm{w}})-1)^2(1-\lambda_2^{\mathrm{e/n}}(t_{\mathrm{w}}))^4 \\ &+ 15(3\lambda_2^{\mathrm{e/n}}(t_{\mathrm{w}})-1)^4(1-\lambda_2^{\mathrm{e/n}}(t_{\mathrm{w}}))^2] \end{aligned} \tag{5.9}$$

is the fidelity of the output state, with respect to the input state, if the initial state is the ideal encoded entangled state $|\tilde{\Phi}^+\rangle_{\mathbf{AB}}$. Similar to the two-qubit case, the above modeling of decoherence effectively treats all non-desired states as a maximally mixed state while correctly predicting the output fidelity; see Appendix B for more detail.

5.3 Error Analysis

In order to assess how well the NV-center based encoded QRs would operate, here, we obtain the final distributed state as a function of system parameters. In the case of measurement or gate errors, we have previously devised analytical and numerical techniques to accurately account for such issues and their impact on system performance. In this chapter, we additionally account for the effect of memory decoherence especially because, in terms of coherence time, the electron spins in the NV centers may impose some limitations on the achievable rates and distance.

Accounting for the decoherence effect, in an analytical way, in a system with many individual NV centers, where each decoheres on its own independently of others, is by no means an easy task. Here, we devise an approximation technique, in which, at each step of the way, we calculate the average waiting time for memories involved, and then assume all of them have decohered by the same average time. This should provide us with a reasonable approximation to what in practice can be achieved, which is what we are looking for here in the context of QKD as an application.

An expression that would come handy in our calculations is the average number of attempts that it takes for M independent Bernoulli experiments to all succeed after a total of W attempts. If the success probability for each attempt

is given by q, this average number of attempts is given by Praxmeyer [2013], Shchukin et al. [2019]

$$N(M,q,W) = \frac{1-(1-q^W)^M}{(1-q^{W+1})^M - q^M(1-q^W)^M} + \frac{(1-q^M)(W-\sum_{i=1}^{W-1}(1-q^i)^M)}{(1-q^{W+1})^M - q^M(1-q^W)^M}. \tag{5.10}$$

In the following, we calculate the relevant time parameters for each step of the proposed protocols and explain our methodology to obtain the QR final state as a function of system parameters.

5.3.1 Entanglement distribution

Here, we first obtain the entangled state distributed over an elementary link. This involves two steps: first, generating an entangled state between two electron spins, and, then, transferring that state to the corresponding nuclear spins. In both processes, we deviate from an ideal Bell pair because of gate errors and decoherence. We follow the two-photon protocol described in Sec. 5.2.1. For simplicity, we assume that the generated entangled state without any decoherence is the ideal Bell pair $|\Phi^+\rangle$. By the time that we hear about the success of entanglement distribution, this ideal state of electron spins has already decohered by the time it takes to transmit photons and learn about the success of the entanglement distribution protocol. In this chapter, we assume that, compared to the transmission time (which for our setup is typically on the order of tens of μs, or longer), the time it takes for any local operation is negligible. In that case, this waiting time, or, effectively, the repetition period for the entanglement distribution protocol is given by

$$T_0 = \frac{L_0}{c}, \tag{5.11}$$

where $L_0 = L_{\text{tot}}/2^n$ is the length of elementary links, with L_{tot} being the total distance between two end users and n is the nesting level. During this time, the desired target state $|\Phi^+\rangle$ decoheres in electron spins, according to Eq. (5.6), yielding

$$\rho_{\text{ee}} = F_0|\Phi^+\rangle\langle\Phi^+| + \frac{1-F_0}{3}(\mathbb{I}_4 - |\Phi^+\rangle\langle\Phi^+|), \tag{5.12}$$

which is a Werner state with

$$F_0 = \lambda_4^{\mathrm{e}}(T_0), \tag{5.13}$$

where λ_4^{e} is given by Eq. (5.7).

This state is then immediately transferred onto the corresponding nuclear spins. This is being done by applying one CNOT gate on each end, with electron spins as the control qubit and nuclear spins in an initial state $|0\rangle$, followed by X measurements on electron spins. This process has been analytically simulated, according to Eqs. (5.2) and (5.3), by the symbolic software Mathematica to give us the entangled state ρ_{nn} shared between two nuclear spins at distance L_0.

5.3.2 Encoded entanglement distribution

The next step in encoded protocols is to create encoded entanglement across certain elementary links. In principle, once the three Bell pairs required in each leg are established, we can proceed with the remote CNOT gate operation that distributes encoded entanglement across the corresponding link. In our proposed protocols, we, however, wait for a time T_1 before we proceed to the ES stage. This means that the nuclear spins in our system have decohered for an average time of $\overline{T}_1 = N(M, P_0(L_0), T_1/T_0)T_0$, with M being the total number of relevant Bell pairs, and

$$P_0(L_0) = \frac{1}{2}\eta_c^2\eta_t^2\eta_d^2 \tag{5.14}$$

being the success probability for each entangling attempt, where η_c accounts for the emission probability of a ZPL photon from the NV center, its collection and coupling efficiency into and out of the optical channel, and the efficiency of any required frequency conversion, η_d is the single-photon detector efficiency, and $\eta_t = \exp[-L_0/(2L_{\mathrm{att}})]$ is the transmissivity of a photon through half of the elementary link. In protocol 1, $M = 3 \times 2^n$, whereas in protocol 2, $M = 3 \times 2^{n-1}$. Similarly, in protocol 3, $M = 2^n$, and in protocol 4, $M = 2^{n-1}$.

Based on our average approach to accounting for decoherence across the repeater chain, here we assume all nuclear spins have decohered for a time $\overline{T}_1$ by the time we apply the remote CNOT gate operation for encoded repeaters. This

effect can be modelled by Eq. (5.6) at $\lambda_4^{\mathrm{n}}(\overline{T}_1)$, with input state $\rho = \rho_{\mathrm{nn}}$. We then model the operations in the remote CNOT circuit in Fig. 5.1, accounting for operation and measurement errors, to obtain ρ'_{nn} as the output state for this stage of the protocol. Note that, for remote CNOT operation, electron spins are initialized into the codeword states. This can be done, e.g., using techniques introduced in Bernardes & van Loock [2012], Cheng et al. [2013], Zheng et al. [2012]. Based on these techniques, in this chapter, we assume that the codeword states are created error-free and the time it takes to prepare them is embedded into T_1. This is because the remote CNOT operation can be done at each elementary link once the three required Bell states for that link are generated. That implies that, in terms of timing, the additional delay caused by the remote CNOT procedure, including the local preparation of the initial codeword states, would only matter for the elementary link that gets entangled the last. Given that T_1, in typical regimes of operation, is on the order of ms, and local operations are assumed to be much faster, we neglect this additional timing parameter. If this is not the case in a certain experiment, the parameter T_1 can be adjusted accordingly for rate calculations. In protocols 3 and 4, we follow the same procedure but we do not include the remote CNOT operation.

5.3.3 Entanglement swapping

Once encoded/uncoded entanglement is stored in the nuclear spins, additional electron-electron entanglement is established so that ES operations can be performed at intermediate stations. For protocols 2 and 4, this process is the same as what has been done for the distribution of original Bell pairs, whereas, in protocols 1 and 3, the Bell pairs are distributed only over a very short distance between two co-located electron spins. In the latter case, we assume that the corresponding electron-spin decoherence happens over a negligible time, whereas in the former the electron-electron state has the same form as ρ_{ee} in Eq. (5.12).

Once electron-electron entanglement is established, the corresponding ES operations between electron and nuclear spins are immediately performed. These ES operations could therefore be performed at different times for different memories. To estimate the decoherence during this step, and to follow the simple

	$\overline{T}_1$, P_{S1}	$\overline{T}_2$, P_{S2}
Protocol 1	$M = 3 \times 2^n$, $q = P_0(L_0)$	$M = 3 \times (2^n - 1)$, $q = P_0(0)$, T_s fixed
Protocol 2	$M = 3 \times 2^{n-1}$, x $q = P_0(L_0)$	$M = 3 \times 2^{n-1}$, $q = P_0(L_0)$, $T_s = T_0$
Protocol 3	$M = 2^n$, $q = P_0(L_0)$	$M = 2^n - 1$, $q = P_0(0)$, T_s fixed
Protocol 4	$M = 3 \times 2^{n-1}$, $q = P_0(L_0)$	$M = 2^{n-1}$, $q = P_0(L_0)$, $T_s = T_0$

Table 5.1: The relevant values of M, q, and T_s for calculating $\overline{T}_1$ and $\overline{T}_2$, as well as, P_{S1} and P_{S2}, for different protocols.

scheme we have adopted for decoherence analysis, we calculate the average time $\overline{T}_2(M, P_s) = T_s N(M, P_s, T_2/T_s)$, to do ES operations across the repeater chain, where T_s denotes the repetition period for the electron-electron entangling attempt, and P_s denotes its success probability. During this time, our state ρ'_{nn} would decohere. For protocol 1, the decoherence is modeled by Eq. (5.8) with λ^{n}_{64} calculated at $t_{\text{w}} = \overline{T}_2(3 \times (2^n - 1), P_0(0))$ and T_s being a small internal time constant. Note that while T_s in this case could be short, its product with N could result in a non-negligible amount of decoherence. For protocol 2, the decoherence is modeled by Eq. (5.8) with λ^{n}_{64} calculated at $t_{\text{w}} = \overline{T}_2(3 \times 2^{n-1}, P_0(L_0))$ and $T_s = T_0$. For protocol 3, the decoherence is modeled by Eq. (5.6) with λ^{n}_{4} calculated at $t_{\text{w}} = \overline{T}_2(2^n - 1, P_0(0))$ and T_s being a small internal time constant. Finally, for protocol 4, the decoherence is modeled by Eq. (5.6) with λ^{n}_{4} calculated at $t_{\text{w}} = \overline{T}_2(2^{n-1}, P_0(L_0))$ and $T_s = T_0$. Table 5.1 summarizes the choice of M and q for calculating $\overline{T}_1$ and $\overline{T}_2$ for different protocols.

Let us denote the resulting state after the above decoherence process as ρ''_{nn}. Using the error models in Sec. 5.2.3, and the techniques introduced in chapters 3 and 4, we can then calculate the final output state of the QR accounting for gate, measurement, and decoherence errors.

5.4 QKD Performance

It would be interesting to compare different QR structures and protocols in terms of their performance for a concrete application. Here, we choose QKD as our benchmarking tool. We use the decoder modules proposed in the last chapter, which only rely on single-qubit measurements, to generate a raw key bit. We also use the post-selection technique proposed in chapter 3, wherein only data points that no errors has been detected in the ES stage are used for key generation.

Here, we first calculate the secret key generation rate per entangled state between Alice and Bob for the BBM92 protocol Bennett et al. [1992]. In the asymptotic limit, and, for the efficient Lo et al. [2005a] entanglement-based QKD protocol, where one basis is used more often than the other, this parameter, known as the secret fraction Scarani et al. [2009], is given by

$$r_\infty = \text{Max}\{0, 1 - h(Q_z) - h(Q_x)\}, \tag{5.15}$$

where $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the Shannon binary entropy function and Q_i is the QBER in measurement basis i, i.e., the probability that Alice and Bob get discordant measurement outcomes in that basis. Here, the secret fraction is calculated for the better of two decoders proposed in chapter 4.

In order to obtain the total secret key generation rate, we need to multiply the secret fraction by the entanglement generation rate R. Due to our assumptions that the time for local operations and measurements is negligible, the overall timescale for the implementation of protocols is determined by the sum of T_1 and T_2. Thus, the rate to obtain a L_{tot}-distant entangled pair by dividing it into 2^n segments is expressed as

$$R = \frac{P_S}{T_1 + T_2}, \tag{5.16}$$

where $P_S = P_{S1}P_{S2}$ denotes the probability that, in step 1, all required elementary links are successfully entangled *and*, in step 2, all relevant BSMs are performed. The success probability for step 1 is given by $P_{S1} = (1-(1-q)^{T_1/T_0})^M$, and, in step 2, conditioned on success in step 1, by $P_{S2} = (1-(1-q)^{T_2/T_s})^M$, where, in each protocol, the corresponding values for q, M, and T_s are outlined in Table 5.1. In this chapter, we normalize secret key rate by the number of NV centers to assess

and compare the performance of proposed protocols. The normalized key rate is given by

$$
\begin{aligned}
R_{\mathrm{QKD}}^{\mathrm{P1}} &= \frac{R^{\mathrm{P1}} r_{\infty}^{\mathrm{P1}}}{6 \times 2^{n}}, \\
R_{\mathrm{QKD}}^{\mathrm{P2}} &= \frac{R^{\mathrm{P2}} r_{\infty}^{\mathrm{P2}}}{3 \times (2^{n}+1)}, \\
R_{\mathrm{QKD}}^{\mathrm{P3}} &= \frac{R^{\mathrm{P3}} r_{\infty}^{\mathrm{P3}}}{2^{n+1}}, \\
R_{\mathrm{QKD}}^{\mathrm{P4}} &= \frac{R^{\mathrm{P4}} r_{\infty}^{\mathrm{P4}}}{2^{n}+1},
\end{aligned}
\tag{5.17}
$$

for protocols 1 to 4, respectively, as specified by the superscripts.

Based on above expressions, we compare the secret key generation rate, in the nominal mode of operation where no eavesdropper is present, for protocols 1 to 4. Our objective is to estimate the relevant parameters in Eq. (5.17) to get some insight into how these protocols are expected to perform in practice.

The nominal parameter values used in our numerical results are as follows. We fix P_{S1} and P_{S2} to 0.99 each, from which T_1 and T_2 can be calculated for each protocol. We then calculate $\overline{T}_1$ and $\overline{T}_2$ to estimate the effect of decoherence on our system. To calculate $\overline{T}_1$ and $\overline{T}_2$, in our numerical results, we have used the following approximation to $N(M, P, W)$ in Eq. (5.10), which is sufficiently tight, for our purposes, when $W \gg 1$ Coopmans et al. [2021], Eisenberg [2008], Shchukin et al. [2019]:

$$
N(M, q) \approx \frac{1}{q}(\gamma + ln(M) + \frac{1}{2M}),
\tag{5.18}
$$

where $\gamma \approx 0.57721$ is the Euler-Mascheroni constant. For our set of parameters, $\overline{T}_1$ and $\overline{T}_2$, respectively, end up to be somewhere between 1/2 to 2/3 of T_1 and T_2. We set the coherence time of electron and nuclear spins as $\tau_{\mathrm{e}} = 10$ ms and $\tau_{\mathrm{n}} = 1$ s, respectively, which is achievable in practice Bar-Gill et al. [2013], Bernien et al. [2013], Maurer et al. [2012]. The above values mostly reflect the back action on nuclear spins, when electron spins are being manipulated, but recent work with this type of memory Abobeih et al. [2018], Bradley et al. [2019], Kalb et al. [2018], Pompili et al. [2021] has shown some progress with resolving this issue. We will therefore consider larger values of coherence time in our numerical results

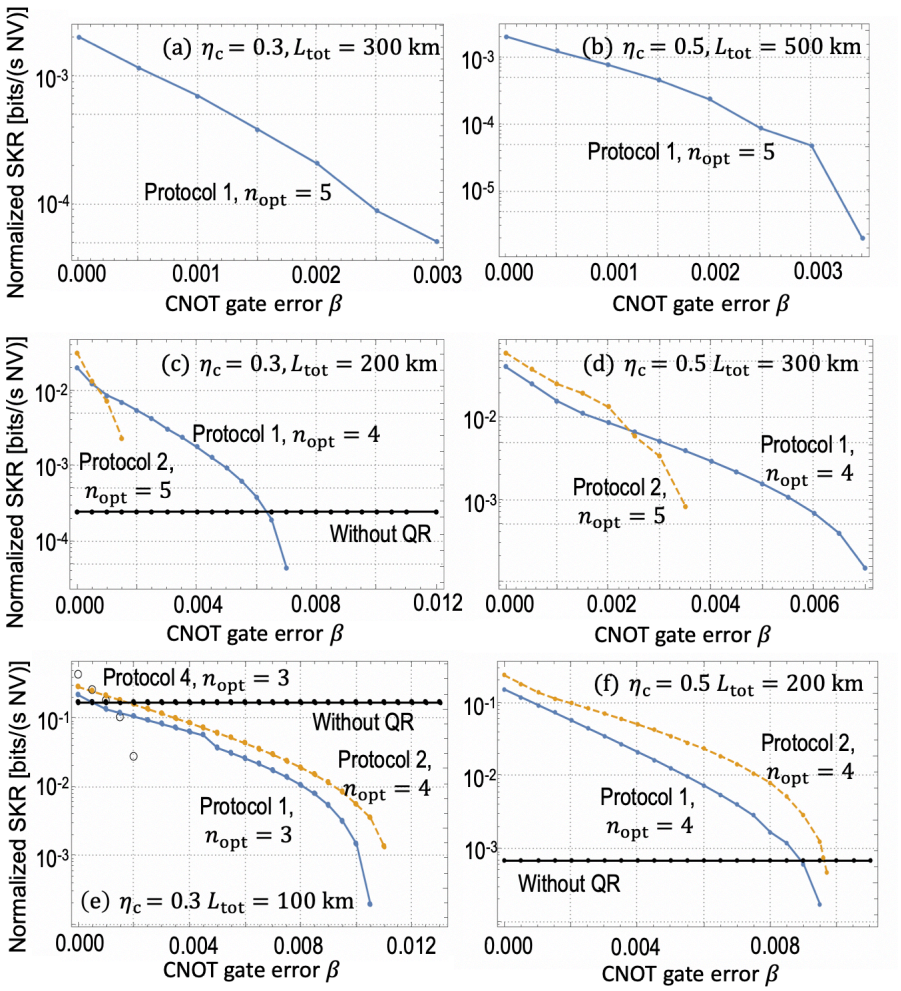

Figure 5.4: Comparison of normalized secret key rate as a function of gate error probability β at (a) $\eta_c = 0.3, L_{\text{tot}} = 300$ km, (b) $\eta_c = 0.5, L_{\text{tot}} = 500$ km, (c) $\eta_c = 0.3, L_{\text{tot}} = 200$ km, (d) $\eta_c = 0.5, L_{\text{tot}} = 300$ km, (e) $\eta_c = 0.3, L_{\text{tot}} = 100$ km, and (f) $\eta_c = 0.5, L_{\text{tot}} = 200$ km, for protocols 1–4. The result for repeaterless case without encoding is also calculated (black solid bound). The measurement error probability is set at $\delta = 10^{-4}$. The coherence time of electron spins and nuclear spins are $\tau_{\text{e}} = 10$ ms and $\tau_{\text{n}} = 1$ s, respectively. Note that for $L_{\text{tot}} > 200$ km, there is no key generated without using a repeater.

as well. The detector efficiency is set to $\eta_d = 0.9$, which can be achieved by using superconducting single-photon detectors Zhang et al. [2015], offering negligible dark counts in our case. The distribution time for next-to-each-other electron-electron entanglement is set to $T_s = 5$ μs, which is on the same order of magnitude as the timing of internal operations reported in Pompili et al. [2021]. We choose the optical fiber as our channel with the speed of light being $c = 2 \times 10^5$ km/s and $L_{\text{att}} = 22$ km.

Figure 5.4 illustrates the performance of different protocols for generating secret keys as a function of CNOT gate error probability β, at electron-spin measurement error probability $\delta = 10^{-4}$, in the presence of depolarizing noise. We have chosen two different values for the coupling efficiency, η_c, as well as four nominal distances of 100 km, 200 km, 300 km, and 500 km. Such distances are perhaps too short to have an immediate impact in practice, but they are relevant to early demonstrations of quantum networks as being pursued, e.g., in Netherlands Pompili et al. [2021]. For each value of β, we have found the optimum nesting level n, for each protocol, that maximizes the key rate in Eq. (5.17). Figures 5.4(a)-(f) show system performance at different combinations of such parameters. Note that, for some parameter regimes, some protocols have not been able to generate a positive key rate, and, therefore, are absent from the relevant graph. We make several interesting observations from this figure, as summarized below:

- **Observation 1:** Among different values chosen, in our simulation, for the total distance, Protocols 3 and 4 could only generate non-zero secret key rates at $L_{\text{tot}} = 100$ km. For the chosen measurement error probability and coherence time parameters, even if we improve the coupling efficiency to $\eta_c = 0.7$, there is still no key at $L_{\text{tot}} \geq 200$ km for these two protocols. This behavior is mainly because no distillation is considered in uncoded repeaters. But, given that conventional entanglement distillation techniques that do not rely on quantum error correction codes are probabilistic Bennett et al. [1996], Deutsch et al. [1996], it is not expected that they offer any improvement in key rate scaling. The reason for this is that whenever we need to do a probabilistic operation, we need to repeat that until success. This requires additional classical communication to herald the success or

failure of previous attempts, which results in additional delay and decoherence, both reducing the rate. Nevertheless, in the regions where uncoded QRs work (hollow circles in Fig. 5.4(e)), they offer, comparatively, high key rates at low values of β. Between protocols 3 and 4, we observe that the highest secret key rates are generated when we use protocol 4 at nesting level $n = 3$. This observation implies that, without any encoding, the QR protocols may only be able to cover short distances, due to their low tolerance of errors.

- **Observation 2:** Among the four protocols, protocol 1 has the highest computational overhead, but also the highest resilience to errors and decoherence. This is because of using encoded entanglement in all elementary links, as opposed to every other in protocol 2, or none in protocols 3 and 4. Because of this feature, in cases where decoherence or gate-error probability is high, this protocol is the only one surviving; see Figs. 5.4(a) and (b). But, if the decoherence is manageable, then protocol 2 starts offering better key rates for low values of β; see Figs. 5.4(c) and (d), although, at larger values of β, protocol 1 is still the only protocol offering non-zero key rates. When distance is low, or coupling efficiency is high, e.g., in Figs. 5.4(e) and (f), protocol 2 maintains its superiority over the entire region of β relevant to these two protocols. This seems to be because of the additional, but unnecessary, computational overhead in protocol 1, as compared to protocol 2. Another way to look at this trend is that protocol 2 uses fewer physical resources at the cost of having less protection against errors, due to its partial use of encoding, and having a longer cycle period, typically, over 1.5 times that of protocol 1. Both these issues make it more sensitive to decoherence. For instance, in Figs. 5.4 (a) and (d) (also, Figs. 5.4 (c) and (f)), where the total distance is fixed, at lower values of η_c, the decoherence time of the system will be longer and thus protocol 1 offers advantage (because it can detect cases of error that protocol 2 may miss). For higher values of η_c, the decoherence is not the major issue, thus the fewer number of erroneous operations and the less consumption of physical resources in protocol 2 make it the better choice.

- **Observation 3:** We notice that, for the optimum choice of nesting level, the inter-node distance varies roughly from 10-20 km, and it tends to be larger at longer total distances. This is somehow expected for this type of repeaters where the optimum distance is often on the order of L_{att}. This inter-node distance is more manageable than that of third generation QRs, for which nodes are only apart by a few kms Azuma et al. [2015], Borregaard et al. [2020], Ewert & van Loock [2017], Glaudell et al. [2016], Lee et al. [2019], Muralidharan et al. [2014], but it is more demanding than that of probabilistic QRs, where the inter-node distacne can be on the order of tens of kms Lo Piparo & Razavi [2013], Sangouard et al. [2011]. Also note that, at short distances, it may not make sense to use any repeater nodes at all, and one can directly distribute an entangled state between the far-end users. This case is shown by the horizontal black solid line in Fig. 5.4, and effectively represents the key rate at $n = 0$ for protocols 3 and 4, given by

$$R_0 = \frac{P_0(L_{\text{tot}}) \times r_{\infty}^{\text{P3}}}{2T_0}. \tag{5.19}$$

  Note that for $L_{\text{tot}} > 200$ km, there is no key generated without using a repeater.

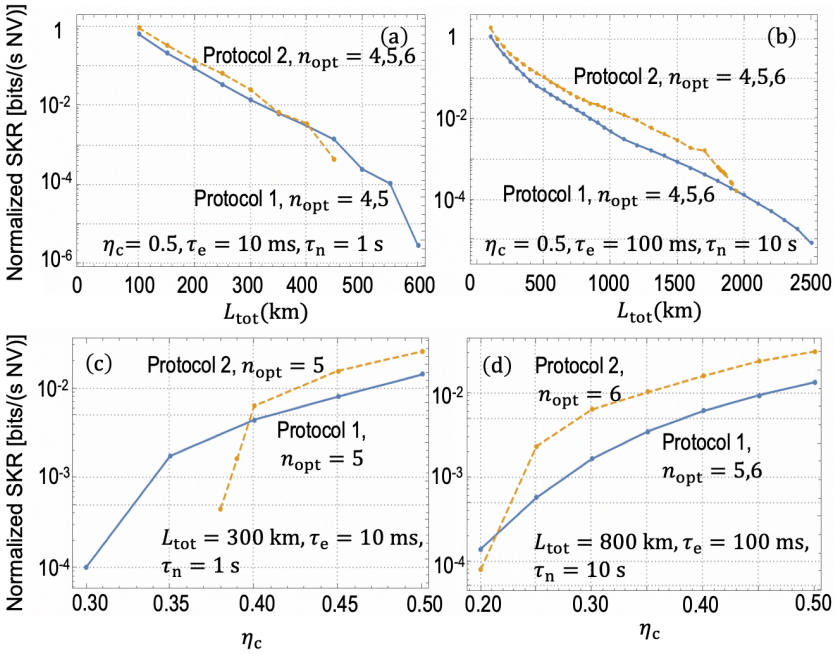

Figure 5.5: Comparison of normalized secret key rate as a function of total distance L_{tot} at (a) $\eta_c = 0.5$, $\tau_{\text{e}} = 10$ ms, $\tau_{\text{n}} = 1$ s, (b) $\eta_c = 0.5$, $\tau_{\text{e}} = 100$ ms, $\tau_{\text{n}} = 10$ s; and η_c at (c) $L_{\text{tot}} = 300$ km, $\tau_{\text{e}} = 10$ ms, $\tau_{\text{n}} = 1$ s, (d) $L_{\text{tot}} = 800$ km, $\tau_{\text{e}} = 100$ ms, $\tau_{\text{n}} = 10$ s; for protocols 1 and 2. The CNOT gate error probability and measurement error probability are $\beta = 10^{-3}$, $\delta = 10^{-4}$, respectively.

To further understand how protocols 1 and 2 compare to each other, in Fig. 5.5, we investigate the sensitivity of these protocols to the total distances L_{tot}, coupling efficiency η_c, and coherence times of nuclear, τ_{n}, and electron, τ_{e}, spins. Figures 5.5(a) and (b) show the normalized key rate versus total distance for two different sets of coherence times, where τ_{n} and τ_{e} in Fig. 5.5(b) are ten times that of Fig. 5.5(a). We observe that, in both figures, protocol 2 starts at a higher key rate than protocol 1, and this continues until a certain distance at which no secret keys can be generated via protocol 2, while protocol 1 can still offer positive key rates for another few hundreds of kilometers. For instance, for parameters of Fig. 5.5(b), protocol 1 can offer around 0.01 bit/s of key rate at 2000 km (once the number of memories used is accounted for), whereas protocol 2 offers zero key rate. Figures 5.5(c) and (d) compare the two protocols versus η_c. In Fig. 5.5(c),

for which coherence times are lower, there is again a crossing point beyond which protocol 2 outperforms protocol 1. In Fig. 5.5(d), in which coherene times are longer, protocol 2 maintains its superiority even at a longer distance of 800 km for $\eta_c > 0.22$. All those observations again confirm that, protocol 2 could be the better option if we are not in a noise-limited regime. When decoherence is high, or we need to reach longer distances, protocol 1 shows more resilience to errors and can reach longer distances, or work at lower coupling efficiencies. This trade-off needs to be considered when designing the optimal QR setting.

Based on our simulation results, we realize that the coherence time of nuclear spins is more crucial than that of electron spins. We observe that if we only improve the coherence time of electron spins, the QKD system performance is only boosted marginally. That being the case, in Fig. 5.6, we give the region plot highlighting the optimal QR structure that offers the highest key rate, at $\delta = 10^{-4}$, $\tau_{ec} = 10$ ms, $\tau_{nc} = 10$ s, in a three-dimensional parameter space. We first note that, even with the improved coherence time, the uncoded QR protocols, i.e., protocols 3 and 4 still only work at $L_{\text{tot}} = 100$ km, and protocol 4 offers the higher key rates compared to others at high efficiency and low gate error probability region. For longer distances and larger error probabilities, protocol 2 is most often the optimal. Here, we interestingly notice that, with the improved coherence time of the system and with three variables being considered, the region where protocol 1 outperforms protocol 2 becomes limited, which is also partially evidenced from Figs. 5.5(b) and (d). This leads to a practical conclusion that, for near-term implementations, the partially encoded QRs, which use fewer resources, might be the best option.

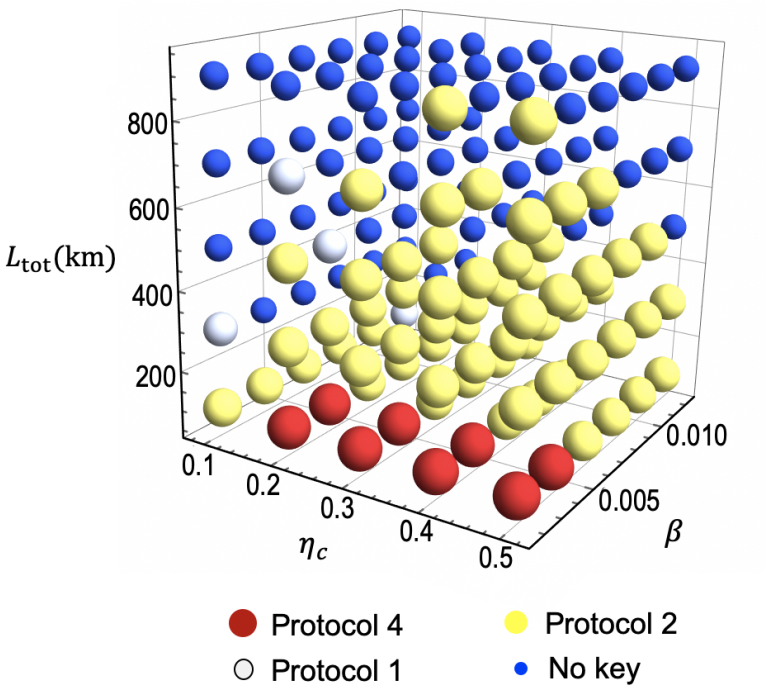

Figure 5.6: The region plot showing the distribution of the optimal QR protocol in a three-dimensional parameter space at $\delta = 10^{-4}$, $\tau_{\mathrm{e}} = 10$ ms, and $\tau_{\mathrm{n}} = 10$ s.

5.5 Conclusion

In this chapter, we analyse two quantum repeater protocols with three-qubit repetition codes on NV centers in diamond platforms, with operation errors and decoherence noise being considered. We benchmark such encoded repeaters against uncoded structures by using QKD as a concrete application. We find that, the uncoded QRs only work and possibly offer some advantage at short distances. For longer distances, QRs with encoding are the optimal choice. We notice that, typically, for intermediate distances or at high coupling efficiencies, the protocol that relies on only partially encoded entangled states, hence consuming fewer physical resources, is the best-performing scheme, while, at longer distances or lower efficiencies, the protocol that relies on encoded entanglement in all its elementary

links, and is thus more resilient to errors, is the optimal one. However, we interestingly find that, if the setup parameters are overall improved, the parameter region where the latter protocol shows some advantage becomes limited. This leads to a conjecture that, for the future implementation of encoded quantum repeaters, it seems that the partially encoded structures, rather than the fully encoded structure, are of more practical use.

Chapter 6

Summary and Future Work

6.1 Summary of results

In this thesis, we thoroughly analyzed the performance of QKD systems that run over QRs with encoding. We fully studied the effect of different components and system imperfections on the secret key generation rate of such systems. We summarize our main results as follows:

- In order to simulate the erroneous quantum circuits and get the analytical form of the final entangled state, we derived a hybrid analytical-numerical framework based on the linearization technique and the transversality of the code employed to handle the computational complexity of such analyses. Previous work on this subject often relied on various approximations to analyze the system. Here, we tried to remain as close as we can to the exact results and only used approximations that were analytically justified and numerically verified. Our techniques allowed us to only deal with four qubits at a time whatever the actual number of qubits in the whole system, which hugely improved the simulation speed.

- We found that, in the context of QKD, it is often more efficient to use the error detection, rather than the error correction, capability of the underlying code to sift out cases where an error has been detected. By doing so, we noticed that such systems could considerably be more resilient to errors

than previously thought. The system is most sensitive to measurement errors, but, provided that they are kept sufficiently low in the experimental setup, we showed that CNOT errors on the order of a few percents could be tolerated. The QKD system could also handle imperfections in the initial Bell states aligned with what experimentally is achievable today.

- A key enabler to improve the key rate is to classify the QKD data points into different groups based on the measurement results reported from ES and decoding stages. By using this information, we observed three-fold increase in resilience to errors in CNOT gates as compared to when the repeater chain and decoders were treated as a black box. We identified that the *golden* states that contributed the most to the final key rate correspond to the cases where no error has been detected at ES and decoding stages. This observation resulted in a simple, but effective, post-selection tool for the QKD system, which not only improved system performance but could also simplify the implementation of such systems in their early demonstrations.

- We noticed that, for such systems, the imperfections in the decoder modules are far more relevant and also more difficult to detect, than those in the encoder ones. In order to tackle this, we proposed two alternative decoder structures which only relied on single-qubit measurements. In contrast to conventional error-correction decoders, these decoding schemes did not need any two-qubit gates, which, therefore, offered lower decoding errors and increased the resilience of the system to common sources of error. The proposition of these decoders not only reduced the complexities of theoretical analysis for such systems, but also simplified the implementation aspects in many practical scenarios.

- In order to have a clue whether larger codes perform better, we applied our technique to QRs with five-qubit repetition codes. We noticed that, five-qubit codes only showed some advantages in high error region since it could tolerate more errors, but this advantage would be beaten by the deployment of probabilistic QRs, and thus might not be of any practical use. We found that, for most practical purposes at moderately long distances,

the three-qubit system could offer the best performance so long as error parameters were around 1%. Our analysis suggested that extending the reach of trust-free terrestrial QKD links to 1000 km is within reach in the near future.

- We investigated the explicit implementation of such encoded QR protocols on a practical platform enabled by NV centers in diamond. We studied two NV-based encoded repeater structures and their uncoded counterparts. One structure offered less consumption of classical communication, hence was more resilient to decoherence effects, whereas the other one relied on fewer physical resources and operations. We assessed and compared their performance for the task of secret key generation under the influence of noise and decoherence with current and near-term experimental parameters. We noticed that, the uncoded QRs only worked and possibly offered advantages at short distances. For longer distances, QRs with encoding were the better option. We realized that, typically, for intermediate distances or higher set-up efficiencies, protocol 2, the one which consumed less physical resources, was the best-performing scheme; whereas for longer distances or lower set-up efficiencies, protocol 1, the one which consumed less temporal resources and thus was less sensitive to decoherence, was the optimal. However, we interestingly noticed that, if the set-up parameters were overall improved, the parameter region where protocol 1 showed advantage became limited.

6.2 Future outlook

The framework developed in this thesis can be extended to more advanced CSS codes. Though we argued that larger codes might not of any practical use in moderately long distances in Chapter 4, this does not rule out the possibilities of finding better codes for arbitrary long distances. Moreover, since we did not include all possible sources of imperfections in our analysis in Chapter 4, such as decoherence of QMs, dark count rate of photon detectors, or non-ideal single-photon resources, it might be ill judged to just limit ourselves to simple codes for future possibilities. The next close step would be to look into the performance of

QRs with 7-qubit Steane code, which is a QEC code that can correct one bit-flip error as well as a phase-flip error at the same time. It would take more efforts to do such a simulation, but it is still doable and certainly worth trying.

During our calculation, we realized that, for QRs with encoding on solid-state platforms, where local operations can be performed fast and deterministically, the distribution time of initial Bell states is always the crucial limitation for secret key generation rate. This can be improved by applying the multiplexing techniques, as partially shown in Chapter 3. However, we have to mention that solid-state platforms, unlike atomic ensemble systems, are more constrained on the implementation of multiplexing schemes. This would ask us to investigate the possibility of cross-platform architectures that could benefit from both long-lived multimode QMs and deterministic fast local gate operations.

With various QR proposals, QEC codes, and experimental platforms being developed and applied nowadays, one major task that need to be addressed is to come up with a systematic and reliable figure of merit in order to quantify and compare the performance between different systems in a fair way. Such a criterion should also be able to guide us on finding a way to maximise the performance at the minimal cost for each specific case. On the other hand, so far, most of the research simply focus on the construction of a single repeater chain which only involves two end-users. However, with our ultimate ambitious goal, to establish a quantum internet world wide, in mind, proposals for 2D quantum network is being put on agenda. Such a network allows a large number of users to perform all kinds of different tasks at the same time, whereas the utilization ratio of different channels would certainly vary. For such cases, a practical and efficient optimal resource analysis would become more indispensable and critical. Designing codes for such 2D QRs would also be of interest as future work.

In addition, so far, we mainly considered to utilize the long-distance entanglement distributed for secret key generation applications. It would also be interesting to apply this framework to access the performance of non-QKD applications, such as quantum metrology, quantum teleportation, and even the test of fundamental quantum physics. Our analysis allows us to calculate the precise format, of the final distributed entanglement, analytically or numerically, with which the figure-of-merit parameters for those applications can be derived.

Appendix A

Equivalence of Decoders 2 and 3

In this Appendix, we prove that decoders 2 and 3, in the ideal case, are equivalent. That would then allow us to use the same security proof that we have for decoder 2, i.e., that of entanglement-based BBM92 protocol Bennett et al. [1992], to decoder 3 as well. In practice then, both decoders 2 and 3 implement the BBM92 protocol with erroneous decoders. Given that these errors result in overestimating bit-flip and phase-flip errors, we can still use the key rate formula in Eq. (4.5) to obtain a lower bound on the secret key rate.

In order to prove our conjecture, we effectively show that the measurement operators implemented, in the ideal case, by either decoders are identical. We first write down the perfect measurement operators for decoder 3 corresponding to measuring bit 0, or, equivalently, states $|0\rangle$ in Z and $|+\rangle$ in X bases, as follows

$$M_0^{(3)} = |000\rangle\langle 000| + |100\rangle\langle 100| + |010\rangle\langle 010| + |001\rangle\langle 001|, \tag{A.1}$$

$$\begin{aligned} M_+^{(3)} = {} & |++{+}\rangle\langle +++| + |+{-}{-}\rangle\langle +{-}{-}| \\ & + |-{+}{-}\rangle\langle -+-| + |-{-}{+}\rangle\langle --+|, \end{aligned} \tag{A.2}$$

respectively. The proof for bit 1 can similarly be done. In order to show that the effective measurement operators for decoder 2 are equivalent to Eq. (A.1) and Eq. (A.2), we break the circuit of decoder 2 into two parts (see Fig. 4.2(b)): the first step includes two CNOT operations and the second step contains the corresponding measurements of three qubits and the flip gate on the first qubit only if the outputs of the other two qubits are $|1\rangle$. We look at this process in a

backward way and the corresponding projectors right before the second part can be represented as

$$\begin{aligned} M_0^{\text{mid}} &= |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |111\rangle\langle 111|, \\ M_+^{\text{mid}} &= |+00\rangle\langle +00| + |+01\rangle\langle +01| \\ &\quad + |+10\rangle\langle +10| + |+11\rangle\langle +11|, \end{aligned} \tag{A.3}$$

which implies the fact that for QKD measurement in Z basis, the outputs of the second and the third qubits will affect the result of the first qubit, while for QKD measurement in X basis, the outputs of the other two qubits does not matter. If we now go back to the input stage of the decoder, where $\text{CNOT}_{1\to 2}$ and $\text{CNOT}_{1\to 3}$ are applied subsequently, Eq. (A.3) will be transformed to

$$\begin{aligned} M_0^{(2)} &= |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |100\rangle\langle 100|, \\ M_+^{(2)} &= (|000\rangle + |111\rangle)(\langle 000| + \langle 111|) \\ &\quad + (|001\rangle + |110\rangle)(\langle 001| + \langle 110|) \\ &\quad + (|010\rangle + |101\rangle)(\langle 010| + \langle 101|) \\ &\quad + (|011\rangle + |100\rangle)(\langle 011| + \langle 100|) \end{aligned} \tag{A.4}$$

Note that to calculate $M_+^{(2)}$, we represent the first qubit in $\{|0\rangle, |1\rangle\}$ basis before applying the corresponding CNOT gates. We can see that $M_0^{(2)} = M_0^{(3)}$ now. For $M_+^{(2)}$, after writing all three qubits in $\{|+\rangle, |-\rangle\}$ basis, we establish that $M_+^{(2)} = M_+^{(3)}$. The derivation steps are straightforward and are left out. This proves our conjecture.

Appendix B

Derivation of decoherence parameters

The decoherence model in Eq. (5.4) for a single qubit system, where $d = 2$ can be rewritten as

$$\begin{aligned}\mathcal{D}_{\text{depol}}(\rho) =&\lambda_2\rho + (1-\lambda_2)(\mathbb{I}_2 - \rho)\\ =&(2\lambda_2 - 1)\rho + (1-\lambda_2)\mathbb{I}_2\\ =&(2\lambda_2 - 1)\rho + (1-\lambda_2)\frac{\rho + X\rho X + Y\rho Y + Z\rho Z}{2}\\ =&\frac{3\lambda_2 - 1}{2}\rho + \frac{1-\lambda_2}{2}(X\rho X + Y\rho Y + Z\rho Z)\end{aligned} \tag{B.1}$$

where X, Y and Z are Pauli operations. For a two-qubit system, each qubit decoheres independently, which leads to

$$\begin{aligned}&\mathcal{D}^A_{\text{depol}} \circ \mathcal{D}^B_{\text{depol}}(\rho_{AB})\\ &= (\frac{3\lambda_2 - 1}{2})^2\rho_{AB} + \frac{(3\lambda_2 - 1)(1-\lambda_2)}{4}\\ &\times [(X_B, Y_B, Z_B)\rho_{AB}\begin{pmatrix} X_B \\ Y_B \\ Z_B \end{pmatrix} + (X_A, Y_A, Z_A)\rho_{AB}\begin{pmatrix} X_A \\ Y_A \\ Z_A \end{pmatrix}]\\ &+ (\frac{1-\lambda_2}{2})^2(X_B, Y_B, Z_B)(X_A, Y_A, Z_A)\rho_{AB}\begin{pmatrix} X_A \\ Y_A \\ Z_A \end{pmatrix}\begin{pmatrix} X_B \\ Y_B \\ Z_B \end{pmatrix}.\end{aligned} \tag{B.2}$$

If the state ρ_{AB} is a Bell diagonal state, we can verify that the output state obtained from (B.2) is equivalent to Eq. (5.6). Note that, in Eq. (B.2), a Bell state remains intact by the following operators: $\mathbb{I}_A\mathbb{I}_B, X_AX_B, Y_AY_B, Z_AZ_B$. Therefore, the fidelity of the output state with respect to the input Bell state is given by the sum of the corresponding coeffficients in (B.2) that

$$\lambda_4 = \frac{1}{4}(3\lambda_2 - 1)^2 - \frac{3}{4}(1-\lambda_2)^2, \tag{B.3}$$

which is the same as Eq. (5.7).

To obtain the decoherence effect on a six-qubit system, we have to apply the single qubit depolarizing model in Eq. (5.4) on each qubit independently, and calculate the tandem effect. This results in a lengthy expression for the output state, which we will not reproduce here. But, it can be verified that the operators that map the encoded Bell state $|\tilde{\Phi}^+\rangle_{\mathbf{AB}}$ to itself are given by: $\mathbb{I}^{\otimes 6}$, $X^{\otimes 6}$, $Y^{\otimes 6}$, $Z^{\otimes 6}$, $X^{\otimes 2}Y^{\otimes 4}$, $X^{\otimes 4}Y^{\otimes 2}$, $Z^{\otimes 4}\mathbb{I}^{\otimes 2}$ and $Z^{\otimes 2}\mathbb{I}^{\otimes 4}$. Again, one can calculate the corresponding fidelity for the output state by accounting for the coefficients of the relevant terms to obtain

$$\begin{aligned}\lambda_{64} =& \frac{1}{64}[(3\lambda_2 - 1)^6 + 33(1-\lambda_2)^6 \\ &+ 15(3\lambda_2 - 1)^2(1-\lambda_2))^4 \\ &+ 15(3\lambda_2 - 1)^4(1-\lambda_2)^2],\end{aligned} \tag{B.4}$$

which is equivalent to Eq. (5.9).

References

Abobeih, M.H., Cramer, J., Bakker, M.A., Kalb, N., Markham, M., Twitchen, D.J. & Taminiau, T.H. (2018). One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment. Nature communications, **9**, 1–8.

Abruzzo, S., Bratzik, S., Bernardes, N.K., Kampermann, H., van Loock, P. & Bruss, D. (2013). Quantum repeaters and quantum key distribution: Analysis of secret-key rates. Physical Review A, **87**, 052315.

Amirloo, J., Razavi, M. & Majedi, A.H. (2010). Quantum key distribution over probabilistic quantum repeaters. Phys. Rev. A, **82**, 032304.

Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., Biswas, R., Boixo, S., Brandao, F.G., Buell, D.A. et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature, **574**, 505–510.

Awschalom, D.D., Hanson, R., Wrachtrup, J. & Zhou, B.B. (2018). Quantum technologies with optically interfaced solid-state spins. Nature Photonics, **12**, 516.

Azuma, K., Tamaki, K. & Lo, H.K. (2015). All-photonic quantum repeaters. Nature communications, **6**, 1–7.

Ballance, C., Harty, T., Linke, N., Sepiol, M. & Lucas, D. (2016). High-fidelity quantum logic gates using trapped-ion hyperfine qubits. Physical review letters, **117**, 060504.

Bar-Gill, N., Pham, L.M., Jarmola, A., Budker, D. & Walsworth, R.L. (2013). Solid-state electronic spin coherence time approaching one second. Nature communications, **4**, 1–6.

Barclay, P.E., Fu, K.M.C., Santori, C., Faraon, A. & Beausoleil, R.G. (2011). Hybrid nanocavity resonant enhancement of color center emission in diamond. Physical Review X, **1**, 011007.

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

Barz, S., Cronenberg, G., Zeilinger, A. & Walther, P. (2010). Heralded generation of entangled photon pairs. Nature photonics, **4**, 553–556.

Bell, J.S. (1964). On the einstein podolsky rosen paradox. Physics Physique Fizika, **1**, 195.

Bellovin, S.M. (2011). Frank miller: Inventor of the one-time pad. Cryptologia, **35**, 203–222.

Bennett, C.H. & Brassard, G. (1984). Quantum cryptography: Public key distribution and con tos5. In Proceedings of the International Conference on Computers, Systems and Signal Processing, 175–179.

Bennett, C.H. & Brassard, G. (2014). Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci., **560**, 7–11.

Bennett, C.H., Brassard, G. & Mermin, N.D. (1992). Quantum cryptography without bellâ€™s theorem. Physical Review Letters, **68**, 557.

Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A. & Wootters, W.K. (1993). Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. Physical review letters, **70**, 1895.

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

Bernardes, N.K. & van Loock, P. (2012). Hybrid quantum repeater with encoding. Phys. Rev. A, **86**, 052301.

Bernardes, N.K., Praxmeyer, L. & van Loock, P. (2011). Rate analysis for a hybrid quantum repeater. Physical Review A, **83**, 012323.

Bernien, H., Childress, L., Robledo, L., Markham, M., Twitchen, D. & Hanson, R. (2012). Two-photon quantum interference from separate nitrogen vacancy centers in diamond. Physical Review Letters, **108**, 043604.

Bernien, H., Hensen, B., Pfaff, W., Koolstra, G., Blok, M.S., Robledo, L., Taminiau, T., Markham, M., Twitchen, D.J., Childress, L. et al. (2013). Heralded entanglement between solid-state qubits separated by three metres. Nature, **497**, 86–90.

Bhaskar, M.K., Riedinger, R., Machielse, B., Levonian, D.S., Nguyen, C.T., Knall, E.N., Park, H., Englund, D., Lončar, M., Sukachev, D.D. et al. (2020). Experimental demonstration of memory-enhanced quantum communication. Nature, 1–5.

Boaron, A., Boso, G., Rusca, D., Vulliez, C., Autebert, C., Caloz, M., Perrenoud, M., Gras, G., Bussières, F., Li, M.J. et al. (2018). Secure quantum key distribution over 421 km of optical fiber. Physical review letters, **121**, 190502.

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

Boixo, S., Isakov, S.V., Smelyanskiy, V.N., Babbush, R., Ding, N., Jiang, Z., Bremner, M.J., Martinis, J.M. & Neven, H. (2018). Characterizing quantum supremacy in near-term devices. Nature Physics, **14**, 595–600.

Borregaard, J., Sørensen, A.S. & Lodahl, P. (2019). Quantum networks with deterministic spin–photon interfaces. Advanced Quantum Technologies, **2**, 1800091.

Borregaard, J., Pichler, H., Schröder, T., Lukin, M.D., Lodahl, P. & Sørensen, A.S. (2020). One-way quantum repeater based on near-deterministic photon-emitter interfaces. Physical Review X, **10**, 021071.

Boschi, D., Branca, S., De Martini, F., Hardy, L. & Popescu, S. (1998). Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels. Physical Review Letters, **80**, 1121.

Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H. & Zeilinger, A. (1997). Experimental quantum teleportation. Nature, **390**, 575.

Boyd, R.W. (2020). Nonlinear optics. Academic press.

Bradley, C., Randall, J., Abobeih, M.H., Berrevoets, R., Degen, M., Bakker, M., Markham, M., Twitchen, D. & Taminiau, T.H. (2019). A ten-qubit solid-state spin register with quantum memory up to one minute. Physical Review X, **9**, 031045.

Brassard, G. & Crépeau, C. (1996). 25 years of quantum cryptography. ACM Sigact News, **27**, 13–24.

Bratzik, S., Kampermann, H. & Bruss, D. (2014). Secret key rates for an encoded quantum repeater. Physical Review A, **89**, 032335.

Braunstein, S.L. (1996). Quantum error correction of dephasing in 3 qubits. arXiv preprint quant-ph/9603024.

Braunstein, S.L. & Mann, A. (1995). Measurement of the bell operator and quantum teleportation. Physical Review A, **51**, R1727.

Braunstein, S.L., Mann, A. & Revzen, M. (1992). Maximal violation of bell inequalities for mixed states. Physical Review Letters, **68**, 3259.

Briegel, H.J., Dür, W., Cirac, J.I. & Zoller, P. (1998). Quantum repeaters: the role of imperfect local operations in quantum communication. Physical Review Letters, **81**, 5932.

Bussieres, F., Sangouard, N., Afzelius, M., De Riedmatten, H., Simon, C. & Tittel, W. (2013). Prospective applications of optical quantum memories. Journal of Modern Optics, **60**, 1519–1537.

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

Calsamiglia, J. & Lütkenhaus, N. (2001). Maximum efficiency of a linear-optical bell-state analyzer. Applied Physics B, **72**, 67–71.

Casabone, B., Stute, A., Friebe, K., Brandstätter, B., Schüppert, K., Blatt, R. & Northup, T. (2013). Heralded entanglement of two ions in an optical cavity. Physical Review Letters, **111**, 100505.

Chen, G., He, M.M., Li, J.Q. & Liang, J.Q. (2006). Entanglement between nuclear spin and field mode in gaas semiconductors. The European Physical Journal B-Condensed Matter and Complex Systems, **51**, 25–27.

Chen, J.P., Zhang, C., Liu, Y., Jiang, C., Zhang, W., Hu, X.L., Guan, J.Y., Yu, Z.W., Xu, H., Lin, J. et al. (2020). Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. Physical review letters, **124**, 070501.

Cheng, L.Y., Wang, H.F., Zhang, S. & Yeon, K.H. (2013). Quantum state engineering with nitrogen-vacancy centers coupled to low-q microresonator. Opt. Express, **21**, 5988–5997.

Childress, L., Taylor, J., Sørensen, A.S. & Lukin, M.D. (2005). Fault-tolerant quantum repeaters with minimal physical resources and implementations based on single-photon emitters. Physical Review A, **72**, 052330.

Childress, L., Taylor, J., Sørensen, A.S. & Lukin, M. (2006). Fault-tolerant quantum communication based on solid-state photon emitters. Physical Review Letters, **96**, 070504.

Cirac, J.I., Zoller, P., Kimble, H.J. & Mabuchi, H. (1997). Quantum state transfer and entanglement distribution among distant nodes in a quantum network. Physical Review Letters, **78**, 3221.

Coffman, V., Kundu, J. & Wootters, W.K. (2000). Distributed entanglement. Physical Review A, **61**, 052306.

Collins, O., Jenkins, S., Kuzmich, A. & Kennedy, T. (2007). Multiplexed memory-insensitive quantum repeaters. Physical review letters, **98**, 060502.

Coopmans, T., Brand, S. & Elkouss, D. (2021). Improved analytical bounds on delivery times of long-distance entanglement. arXiv preprint arXiv:2103.11454.

Currás-Lorenzo, G., Navarrete, Á., Azuma, K., Kato, G., Curty, M. & Razavi, M. (2021). Tight finite-key security for twin-field quantum key distribution. npj Quantum Information, **7**, 22.

Curty, M., Azuma, K. & Lo, H.K. (2019). Simple security proof of twin-field type quantum key distribution protocol. npj Quantum Information, **5**, 1–6.

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

Devitt, S.J., Munro, W.J. & Nemoto, K. (2013). Quantum error correction for beginners. Reports on Progress in Physics, **76**, 076001.

Diamanti, E., Lo, H.K., Qi, B. & Yuan, Z. (2016). Practical challenges in quantum key distribution. npj Quantum Information, **2**, 1–12.

Dieks, D. (1982). Communication by epr devices. Physics Letters A, **92**, 271–272.

Dirac, P.A.M. (1981). The principles of quantum mechanics. 27, Oxford university press.

Doherty, M.W., Manson, N.B., Delaney, P., Jelezko, F., Wrachtrup, J. & Hollenberg, L.C. (2013). The nitrogen-vacancy colour centre in diamond. Physics Reports, **528**, 1–45.

Dolde, F., Bergholm, V., Wang, Y., Jakobi, I., Naydenov, B., Pezzagna, S., Meijer, J., Jelezko, F., Neumann, P., Schulte-Herbrüggen, T. et al. (2014). High-fidelity spin entanglement using optimal control. Nature communications, **5**, 1–9.

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

Dür, W., Briegel, H.J., Cirac, J. & Zoller, P. (1999). Quantum repeaters based on entanglement purification. Physical Review A, **59**, 169.

Dutt, M.G., Childress, L., Jiang, L., Togan, E., Maze, J., Jelezko, F., Zibrov, A., Hemmer, P. & Lukin, M. (2007). Quantum register based on individual electronic and nuclear spin qubits in diamond. Science, **316**, 1312–1316.

Eisenberg, B. (2008). On the expectation of the maximum of iid geometric random variables. Statistics & Probability Letters, **78**, 135–143.

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

Epstein, R., Mendoza, F., Kato, Y. & Awschalom, D. (2005). Anisotropic interactions of a single spin and dark-spin spectroscopy in diamond. Nature physics, **1**, 94–98.

Erhard, A., Wallman, J.J., Postler, L., Meth, M., Stricker, R., Martinez, E.A., Schindler, P., Monz, T., Emerson, J. & Blatt, R. (2019). Characterizing large-scale quantum computers via cycle benchmarking. Nature Communications, **10**, 1–7.

Everitt, M.S., Devitt, S., Munro, W. & Nemoto, K. (2014). High-fidelity gate operations with the coupled nuclear and electron spins of a nitrogen-vacancy center in diamond. Physical Review A, **89**, 052317.

Ewert, F. & van Loock, P. (2017). Ultrafast fault-tolerant long-distance quantum communication with static linear optics. Physical Review A, **95**, 012327.

Ewert, F., Bergmann, M. & van Loock, P. (2016). Ultrafast long-distance quantum communication with static linear optics. Physical review letters, **117**, 210501.

Faraon, A., Barclay, P.E., Santori, C., Fu, K.M.C. & Beausoleil, R.G. (2011). Resonant enhancement of the zero-phonon emission from a colour centre in a diamond cavity. Nature Photonics, **5**, 301.

Fernandez-Gonzalvo, X., Corrielli, G., Albrecht, B., li Grimau, M., Cristiani, M. & de Riedmatten, H. (2013). Quantum frequency conversion of quantum memory compatible photons to telecommunication wavelengths. Optics express, **21**, 19473–19487.

Fisher, K.A., England, D.G., MacLean, J.P.W., Bustard, P.J., Resch, K.J. & Sussman, B.J. (2016). Frequency and bandwidth conversion of single photons in a room-temperature diamond quantum memory. Nature communications, **7**, 1–6.

Fowler, A.G., Wang, D.S., Hill, C.D., Ladd, T.D., Van Meter, R. & Hollenberg, L.C. (2010). Surface code quantum communication. Physical Review Letters, **104**, 180503.

Fowler, A.G., Mariantoni, M., Martinis, J.M. & Cleland, A.N. (2012). Surface codes: Towards practical large-scale quantum computation. Physical Review A, **86**, 032324.

Furusawa, A., Sørensen, J.L., Braunstein, S.L., Fuchs, C.A., Kimble, H.J. & Polzik, E.S. (1998). Unconditional quantum teleportation. science, **282**, 706–709.

Gaebler, J.P., Tan, T.R., Lin, Y., Wan, Y., Bowler, R., Keith, A.C., Glancy, S., Coakley, K., Knill, E., Leibfried, D. et al. (2016). High-fidelity universal gate set for be 9+ ion qubits. Physical Review Letters, **117**, 060505.

Gingrich, R.M., Kok, P., Lee, H., Vatan, F. & Dowling, J.P. (2003). All linear optical quantum memory based on quantum error correction. Physical review letters, **91**, 217901.

Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. (2002). Quantum cryptography. Reviews of modern physics, **74**, 145.

Glaudell, A.N., Waks, E. & Taylor, J.M. (2016). Serialized quantum error correction protocol for high-bandwidth quantum repeaters. New Journal of Physics, **18**, 093008.

Grosshans, F. & Grangier, P. (2002). Continuous variable quantum cryptography using coherent states. Physical review letters, **88**, 057902.

Hald, J., Sørensen, J., Schori, C. & Polzik, E. (1999). Spin squeezed atoms: a macroscopic entangled ensemble created by light. Physical review letters, **83**, 1319.

Hausmann, B.J.M., Shields, B.J., Quan, Q., Chu, Y., de Leon, N.P., Evans, R., Burek, M.J., Zibrov, A.S., Markham, M., Twitchen, D. et al. (2013). Coupling of nv centers to photonic crystal nanobeams in diamond. Nano letters, **13**, 5791–5796.

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

Horodecki, R., Horodecki, P., Horodecki, M. & Horodecki, K. (2009). Quantum entanglement. Reviews of modern physics, **81**, 865.

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

Jelezko, F., Gaebel, T., Popa, I., Domhan, M., Gruber, A. & Wrachtrup, J. (2004). Observation of coherent oscillation of a single nuclear spin and realization of a two-qubit conditional quantum gate. Physical Review Letters, **93**, 130501.

Jiang, L., Taylor, J.M., Sørensen, A.S. & Lukin, M.D. (2007). Distributed quantum computation based on small quantum registers. Physical Review A, **76**, 062323.

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

Jing, Y., Alsina, D. & Razavi, M. (2020). Quantum key distribution over quantum repeaters with encoding: Using error detection as an effective postselection tool. Physical Review Applied, **14**, 064037.

Jozsa, R. (1994). Fidelity for mixed quantum states. Journal of modern optics, **41**, 2315–2323.

Jozsa, R., Abrams, D.S., Dowling, J.P. & Williams, C.P. (2000). Quantum clock synchronization based on shared prior entanglement. Physical Review Letters, **85**, 2010.

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

Kimble, H.J. (2008). The quantum internet. Nature, **453**, 1023–1030.

Knill, E. (2005). Quantum computing with realistically noisy devices. Nature, **434**, 39–44.

Le Sage, D., Pham, L.M., Bar-Gill, N., Belthangady, C., Lukin, M.D., Yacoby, A. & Walsworth, R.L. (2012). Efficient photon detection from color centers in a diamond optical waveguide. Physical Review B, **85**, 121202.

Lee, S.W., Ralph, T.C. & Jeong, H. (2019). Fundamental building block for all-optical scalable quantum networks. Physical Review A, **100**, 052303.

Li, C., Jiang, N., Wu, Y.K., Chang, W., Pu, Y.F., Zhang, S. & Duan, L.M. (2020). Quantum communication between multiplexed atomic quantum memories. Physical Review Letters, **124**, 240504.

Liu, C., Dutton, Z., Behroozi, C.H. & Hau, L.V. (2001). Observation of coherent optical information storage in an atomic medium using halted light pulses. Nature, **409**, 490–493.

Liu, X., Hu, J., Li, Z.F., Li, X., Li, P.Y., Liang, P.J., Zhou, Z.Q., Li, C.F. & Guo, G.C. (2021). Heralded entanglement distribution between two absorptive quantum memories. Nature, **594**, 41–45.

Lo, H.K., Chau, H.F. & Ardehali, M. (2005a). Efficient quantum key distribution scheme and a proof of its unconditional security. Journal of Cryptology, **18**, 133–165.

Lo, H.K., Ma, X. & Chen, K. (2005b). Decoy state quantum key distribution. Physical review letters, **94**, 230504.

Lo, H.K., Curty, M. & Qi, B. (2012). Measurement-device-independent quantum key distribution. Physical review letters, **108**, 130503.

Lo, H.K., Curty, M. & Tamaki, K. (2014). Secure quantum key distribution. Nature Photonics, **8**, 595–604.

Lo Piparo, N. & Razavi, M. (2013). Long-distance quantum key distribution with imperfect devices. Physical Review A, **88**, 012332.

Lo Piparo, N., Razavi, M. & Munro, W.J. (2017a). Measurement-device-independent quantum key distribution with nitrogen vacancy centers in diamond. Physical Review A, **95**, 022338.

Lo Piparo, N., Razavi, M. & Munro, W.J. (2017b). Memory-assisted quantum key distribution with a single nitrogen-vacancy center. Physical Review A, **96**, 052313.

Lucamarini, M., Yuan, Z.L., Dynes, J.F. & Shields, A.J. (2018). Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. Nature, **557**, 400–403.

Lukin, M., Yelin, S. & Fleischhauer, M. (2000). Entanglement of atomic ensembles by trapping correlated photon states. Physical Review Letters, **84**, 4232.

Lütkenhaus, N. (1999). Estimates for practical quantum cryptography. Physical Review A, **59**, 3301.

Lütkenhaus, N., Calsamiglia, J. & Suominen, K.A. (1999). Bell measurements for teleportation. Physical Review A, **59**, 3295.

Lvovsky, A.I., Sanders, B.C. & Tittel, W. (2009). Optical quantum memory. Nature photonics, **3**, 706–714.

Marsili, F., Verma, V.B., Stern, J.A., Harrington, S., Lita, A.E., Gerrits, T., Vayshenker, I., Baek, B., Shaw, M.D., Mirin, R.P. et al. (2013). Detecting single infrared photons with 93% system efficiency. Nature Photonics, **7**, 210–214.

Matsukevich, D., Chaneliere, T., Jenkins, S., Lan, S.Y., Kennedy, T. & Kuzmich, A. (2006). Entanglement of remote atomic qubits. Physical review letters, **96**, 030405.

Maurer, P.C., Kucsko, G., Latta, C., Jiang, L., Yao, N.Y., Bennett, S.D., Pastawski, F., Hunger, D., Chisholm, N., Markham, M. et al. (2012). Room-temperature quantum bit memory exceeding one second. Science, **336**, 1283–1286.

Meekhof, D., Monroe, C., King, B., Itano, W. & Wineland, D. (1996). Generation of nonclassical motional states of a trapped atom [phys. rev. lett. 76, 1796 (1996)]. Physical Review Letters, **77**, 2346.

Merkle, R.C. (1980). Protocols for public key cryptosystems. In 1980 IEEE Symposium on Security and Privacy, 122–122, IEEE.

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

Munro, W.J., Nemoto, K. & Spiller, T.P. (2005). Weak nonlinearities: a new route to optical quantum computation. New Journal of Physics, **7**, 137.

Munro, W.J., Stephens, A.M., Devitt, S.J., Harrison, K.A. & Nemoto, K. (2012). Quantum communication without the necessity of quantum memories. Nature Photonics, **6**, 777.

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

Muralidharan, S., Li, L., Kim, J., Lütkenhaus, N., Lukin, M.D. & Jiang, L. (2016). Optimal architectures for long distance quantum communication. Scientific reports, **6**, 20463.

Muralidharan, S., Zou, C.L., Li, L. & Jiang, L. (2018). One-way quantum repeaters with quantum reed-solomon codes. Physical Review A, **97**, 052316.

Namiki, R., Jiang, L., Kim, J. & Lütkenhaus, N. (2016). Role of syndrome information on a one-way quantum repeater using teleportation-based error correction. Physical Review A, **94**, 052304.

Nemoto, K., Trupke, M., Devitt, S.J., Stephens, A.M., Scharfenberger, B., Buczak, K., Nöbauer, T., Everitt, M.S., Schmiedmayer, J. & Munro, W.J. (2014). Photonic architecture for scalable quantum information processing in diamond. Physical Review X, **4**, 031022.

Neumann, P., Mizuochi, N., Rempp, F., Hemmer, P., Watanabe, H., Yamasaki, S., Jacques, V., Gaebel, T., Jelezko, F. & Wrachtrup, J. (2008). Multipartite entanglement among single spins in diamond. science, **320**, 1326–1329.

Neumann, P., Beck, J., Steiner, M., Rempp, F., Fedder, H., Hemmer, P.R., Wrachtrup, J. & Jelezko, F. (2010). Single-shot readout of a single nuclear spin. Science, **329**, 542–544.

Nielsen, M.A. & Chuang, I. (2002). Quantum computation and quantum information.

Northup, T. & Blatt, R. (2014). Quantum information transfer using photons. Nature photonics, **8**, 356–363.

Panayi, C., Razavi, M., Ma, X. & Lütkenhaus, N. (2014). Memory-assisted measurement-device-independent quantum key distribution. New Journal of Physics, **16**, 043005.

Park, J.L. (1970). The concept of transition in quantum mechanics. Foundations of Physics, **1**, 23–33.

Peres, A. (1985). Reversible logic and quantum computers. Physical review A, **32**, 3266.

Pfaff, W., Hensen, B., Bernien, H., van Dam, S.B., Blok, M.S., Taminiau, T.H., Tiggelman, M.J., Schouten, R.N., Markham, M., Twitchen, D.J. et al. (2014). Unconditional quantum teleportation between distant solid-state quantum bits. Science, **345**, 532–535.

Phillips, D.F., Fleischhauer, A., Mair, A., Walsworth, R.L. & Lukin, M.D. (2001). Storage of light in atomic vapor. Physical review letters, **86**, 783.

Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A. & Braunstein, S.L. (2015). Advances in quantum teleportation. Nature photonics, **9**, 641–652.

Pirandola, S., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C. et al. (2020). Advances in quantum cryptography. Advances in Optics and Photonics, **12**, 1012–1236.

Pompili, M., Hermans, S.L., Baier, S., Beukers, H.K., Humphreys, P.C., Schouten, R.N., Vermeulen, R.F., Tiggelman, M.J., dos Santos Martins, L., Dirkse, B. et al. (2021). Realization of a multinode quantum network of remote solid-state qubits. Science, **372**, 259–264.

Praxmeyer, L. (2013). Reposition time in probabilistic imperfect memories. arXiv preprint arXiv:1309.3407.

Pu, Y., Jiang, N., Chang, W., Yang, H., Li, C. & Duan, L. (2017). Experimental realization of a multiplexed quantum memory with 225 individually accessible memory cells. Nature communications, **8**, 1–6.

Raimond, J.M., Brune, M. & Haroche, S. (2001). Manipulating quantum entanglement with atoms and photons in a cavity. Reviews of Modern Physics, **73**, 565.

Rančić, M., Hedges, M.P., Ahlefeldt, R.L. & Sellars, M.J. (2018). Coherence time of over a second in a telecom-compatible quantum memory storage material. Nature Physics, **14**, 50–54.

Razavi, M. (2018). An introduction to quantum communication networks: Or, how shall we communicate in the quantum era? Morgan & Claypool Publishers.

Razavi, M., Piani, M. & Lütkenhaus, N. (2009). Quantum repeaters with imperfect memories: Cost and scalability. Physical Review A, **80**, 032301.

Reiserer, A. & Rempe, G. (2015). Cavity-based quantum networks with single atoms and optical photons. Reviews of Modern Physics, **87**, 1379.

Riedel, D., Söllner, I., Shields, B.J., Starosielec, S., Appel, P., Neu, E., Maletinsky, P. & Warburton, R.J. (2017). Deterministic enhancement of coherent photon generation from a nitrogen-vacancy center in ultrapure diamond. Physical Review X, **7**, 031040.

Rivest, R.L., Shamir, A. & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, **21**, 120–126.

Rozpędek, F., Yehia, R., Goodenough, K., Ruf, M., Humphreys, P.C., Hanson, R., Wehner, S. & Elkouss, D. (2019). Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission. Physical Review A, **99**, 052330.

Ruf, M., Weaver, M.J., van Dam, S.B. & Hanson, R. (2021). Resonant excitation and purcell enhancement of coherent nitrogen-vacancy centers coupled to a fabry-perot microcavity. Physical Review Applied, **15**, 024049.

Saglamyurek, E., Sinclair, N., Jin, J., Slater, J.A., Oblak, D., Bussieres, F., George, M., Ricken, R., Sohler, W. & Tittel, W. (2011). Broadband waveguide quantum memory for entangled photons. Nature, **469**, 512–515.

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

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

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N. & Peev, M. (2009). The security of practical quantum key distribution. Reviews of modern physics, **81**, 1301.

Shchukin, E., Schmidt, F. & van Loock, P. (2019). Waiting time in quantum repeaters with probabilistic entanglement swapping. Physical Review A, **100**, 032322.

Shor, P.W. (1996). Fault-tolerant quantum computation. In Proceedings of 37th Conference on Foundations of Computer Science, 56–65, IEEE.

Shor, P.W. & Preskill, J. (2000). Simple proof of security of the bb84 quantum key distribution protocol. Phys. Rev. Lett., **85**, 441–444.

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

Steane, A. (1996). Multiple-particle interference and quantum error correction. Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, **452**, 2551–2577.

Taminiau, T.H., Cramer, J., van der Sar, T., Dobrovitski, V.V. & Hanson, R. (2014). Universal control and error correction in multi-qubit spin registers in diamond. Nature nanotechnology, **9**, 171.

Tang, J.S., Zhou, Z.Q., Wang, Y.T., Li, Y.L., Liu, X., Hua, Y.L., Zou, Y., Wang, S., He, D.Y., Chen, G. et al. (2015). Storage of multiple single-photon pulses emitted from a quantum dot in a solid-state quantum memory. Nature communications, **6**, 1–7.

Usmani, I., Afzelius, M., De Riedmatten, H. & Gisin, N. (2010). Mapping multiple photonic qubits into and out of one solid-state atomic ensemble. Nature Communications, **1**, 1–7.

van Dam, S.B., Humphreys, P.C., Rozpędek, F., Wehner, S. & Hanson, R. (2017). Multiplexed entanglement generation over quantum networks using multi-qubit nodes. Quantum Science and Technology, **2**, 034002.

Van der Sar, T., Wang, Z., Blok, M., Bernien, H., Taminiau, T., Toyli, D., Lidar, D., Awschalom, D., Hanson, R. & Dobrovitski, V. (2012). Decoherence-protected quantum gates for a hybrid solid-state spin register. Nature, **484**, 82–86.

Vazirani, U. & Vidick, T. (2019). Fully device independent quantum key distribution. Communications of the ACM, **62**, 133–133.

Vinay, S.E. & Kok, P. (2017). Practical repeaters for ultralong-distance quantum communication. Phys. Rev. A, **95**, 052336.

Wagenknecht, C., Li, C.M., Reingruber, A., Bao, X.H., Goebel, A., Chen, Y.A., Zhang, Q., Chen, K. & Pan, J.W. (2010). Experimental demonstration of a heralded entanglement source. Nature Photonics, **4**, 549–552.

Waldherr, G., Wang, Y., Zaiser, S., Jamali, M., Schulte-Herbrüggen, T., Abe, H., Ohshima, T., Isoya, J., Du, J., Neumann, P. et al. (2014). Quantum error correction in a solid-state hybrid spin register. Nature, **506**, 204–207.

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

Wei, H.R. & Deng, F.G. (2013). Compact quantum gates on electron-spin qubits assisted by diamond nitrogen-vacancy centers inside cavities. Physical Review A, **88**, 042323.

Werner, R.F. (1989a). An application of bell's inequalities to a quantum state extension problem. Letters in Mathematical Physics, **17**, 359–363.

Werner, R.F. (1989b). Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. Physical Review A, **40**, 4277.

Wiebe, N., Braun, D. & Lloyd, S. (2012). Quantum algorithm for data fitting. Physical review letters, **109**, 050505.

Wootters, W.K. & Zurek, W.H. (1982). A single quantum cannot be cloned. Nature, **299**, 802–803.

Yin, H.L., Chen, T.Y., Yu, Z.W., Liu, H., You, L.X., Zhou, Y.H., Chen, S.J., Mao, Y., Huang, M.Q., Zhang, W.J. et al. (2016). Measurement-device-independent quantum key distribution over a 404 km optical fiber. Physical review letters, **117**, 190501.

Yin, J., Li, Y.H., Liao, S.K., Yang, M., Cao, Y., Zhang, L., Ren, J.G., Cai, W.Q., Liu, W.Y., Li, S.L. et al. (2020). Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature, **582**, 501–505.

Yu, Y., Ma, F., Luo, X.Y., Jing, B., Sun, P.F., Fang, R.Z., Yang, C.W., Liu, H., Zheng, M.Y., Xie, X.P. et al. (2020). Entanglement of two quantum memories via fibres over dozens of kilometres. Nature, **578**, 240–245.

Zhang, J., Souza, A.M., Brandao, F.D. & Suter, D. (2014). Protected quantum computing: interleaving gate operations with dynamical decoupling sequences. Physical Review Letters, **112**, 050502.

Zhang, J., Itzler, M.A., Zbinden, H. & Pan, J.W. (2015). Advances in ingaas/inp single-photon detector systems for quantum communication. Light: Science & Applications, **4**, e286–e286.

Zheng, A., Li, J., Yu, R., Lü, X.Y. & Wu, Y. (2012). Generation of greenberger-horne-zeilinger state of distant diamond nitrogen-vacancy centers via nanocavity input-output process. Opt. Express, **20**, 16902–16912.

Zhong, X., Hu, J., Curty, M., Qian, L. & Lo, H.K. (2019). Proof-of-principle experimental demonstration of twin-field type quantum key distribution. Physical Review Letters, **123**, 100506.

Zukowski, M., Zeilinger, A., Horne, M.A. & Ekert, A.K. (1993). "event-ready-detectors"bell experiment via entanglement swapping. Physical Review Letters, **71**, 4287–4290.

Zwerger, M., Briegel, H. & Dür, W. (2014). Hybrid architecture for encoded measurement-based quantum computation. Scientific Reports, **4**, 1–5.