Influence of coherence time drift on the secret key rate

By

Emlyn Arturo Stephens

Master of Science
in Applied Physics

Supervisor:	Prof. Stephanie Wehner
Daily Supervisor:	M.Sc. Guus Avis
Thesis committee:	Prof. David Elkouss
	Prof. Miriam Blaauboer
Year:	2021 - 2022

Abstract

Quantum communication provides a plethora of new possibilities compared to the realm of classical communication. Since the channels used are noisy, losses are unavoidable, and quantum repeaters are needed to transmit a signal over longer distances to overcome these exponential losses. To increase the performance of these repeaters, cutoff times can be introduced. These cutoffs limit the amount of time a qubit can be stored in the quantum memory. Based on previous work done by Avis et al., this work analyzes how a variation in the initial coherence time, called a drift in coherence time, affects the optimal cutoff, the optimal secret key rate, and the loss in secret key rate. The main conclusions are that the greater the coherence time, the less the need for accurate cutoff times. This is due to losses in the secret key rate being inherently smaller at larger coherence times. Furthermore, the loss in secret key rate can be approximated using the derivations found in this thesis. Suggestions for further work is introduced; implementing these is beyond this thesis's scope.

Acknowledgements

First and foremost, I want to thank my supervisor, Prof. Stephanie Wehner, for giving me the possibility to work in such an incredible and cutting-edge environment. Also, I want to thank my daily supervisor Guus Avis. You helped me tremendously throughout this project with your intelligent input and constructive comments. Together with Guus, the Blueprint team was an incredible team to experience the wonders of the quantum world with. Thanks, David, Francisco, and Hana, for making me feel welcomed whenever we had the chance to meet in person (and online). A big thank you to Tim Coopmans for fruitful discussions at the beginning of my project. Thank you, Helena, not only for helping with the planning but also in general for your kindness and support. Finally, I want to express my gratitude towards Prof. Elkouss and Prof. Blaauboer for accepting not only the invitation to join the thesis committee but also for taking the time to read this thesis.

I do not know how to thank all the people who have helped me throughout this pandemic. Thank you, Fio, for being by my side and supporting me whenever I needed it. Thank you, Zheng and Zuhra, for reading through this thesis, and thank you, Jasmin and Luke, for reading through it again. Thank you, Janice, for being a partner in crime in the Blueprint team. Thank you to all the friends who helped me smile - Habib, Leo, Aitor, Aschraf, Hiresh, Pim, Dona, Ahmad, Mido, and other people I forgot to mention. And finally, the biggest thank you to my family - Mum and Dad for always believing and supporting me and Bryn and Gwyneth for making me smile even in the most difficult of times.

Contents

Chapter 1

Introduction

Almost forty years have passed since Feynman's paper about simulating quantum physics by using - *quantum physics* [1], and much has happened since then. Methods of breaking RSA using *Shor's Algorithm* were introduced [2], the quantum mechanical analogon to Shannons Information Theory [3], the birth of *Quantum Information Theory*, and the development of a protocol that makes it impossible for an attacker to eavesdrop - the *BB84 protocol* [4].

Parallel to this was the rapid expansion and adaption of a technology no one could have anticipated being as globally impacting as it was, socially as well as economically - the *Internet* [5]. Connecting many entities (nodes) with each other over vast distances relies on amplifying signals on midpoints. The quantum mechanical counterpart, the *Quantum Internet*, aims to facilitate quantum communication between any two parties - achieving things classically impossible such as secure quantum cloud computation [6, 7]. Contrary to the classical internet, copying quantum information for amplification is prohibited due to the no-cloning theorem [8]. To circumvent the no-cloning theorem, the *quantum repeater* was proposed [9]. Albeit no physical realization has been achieved, a first step into this direction has been reached by implementing the first entanglement-based three-node network in 2021 at QuTech [10]. Even though entanglement swapping was accomplished, this node did not improve transmission compared to direct transmission.

Outline: This thesis is structured as follows:

Background:

- In Chapter 2, we introduce the formalism used throughout this thesis. We introduce the quantum mechanics needed, the BB84 protocol with a focus on the secret key rate. We present simplified models of quantum memories as well as explain the notion of a *cutoff time* and how it can improve the quality of a quantum state.
- Chapter 3 shows the model used to calculate the secret key rate for a single quantum repeater. The equations to calculate this secret key rate are presented.

New Research:

- Chapter 4 shows what is meant when discussing a *drift in coherence time*. To illustrate this, we plot the secret key rate for different values of the coherence time. Next, the optimal cutoff times are found numerically with respect to the coherence time. These optimal cutoff times are used to calculate the improvement of using a secret key rate with a cutoff time compared to the secret key rate without a cutoff time. Further, we formally introduce the condition when the secret key rate is maximized with respect to a specific cutoff time. Using this, we present a first-order approximation to the optimal cutoff time as a function of the coherence time and analyze the sensitivity of the cutoff time with respect to changes in the coherence time.

- Chapter 5 combines the previous chapters to introduce the notion of *loss in secret key rate*. We explain what is meant by the loss and approximate it to second order in the coherence time. We finalize this chapter by investigating the validity of this approach.

- Concluding with Chapter 6, we summarize the results and propose possible further improvements and research.

Part I
Background

Chapter 2

Theory

This chapter serves as a foundation on the theoretical background needed to understand the research presented. Section 2.1 introduces the general quantum-mechanical formalism required as well the notion of entanglement and applications thereof. The no-cloning theorem is presented as well as quantum channels with a focus on the depolarizing channel. Section 2.2 introduces quantum communication focusing on the BB84 protocol and the secret key rate. Section 2.3 shows the problems associated with a *quantum repeater*, what the building blocks are, and an explanation of what is meant when referring to a *cutoff time*.

2.1 Quantum mechanics

2.1.1 Quantum mechanics formalism

Definition 2.1.1 (Qubit)**.** A qubit describes the simplest quantum system, which is an element of the complex two-dimensional Hilbert space, $|\psi\rangle \in \mathcal{H} \cong \mathbb{C}^2$.

A qubit is the quantum mechanical analog to the classical bit, usually denoted as "0" or "1" [11]. This qubit can be written in Dirac notation as a complex linear combination of the basis states $|k\rangle$ as,

$$|\psi\rangle = \sum_{k\in\mathbb{Z}_2} c_k \, |k\rangle \, , \tag{2.1}$$

where the coefficients $c_k \in \mathbb{C}$ obey the normalization $|c_0| + |c_1| = 1$.

Definition 2.1.2 (Product state & Entanglement)**.** A pure state $|\Psi\rangle \in \mathcal{H}_{\mathcal{AB}} = \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ of the composite system is separable if it can be written as a tensor product of subsystems i.e.,

$$|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle \, , \quad \text{with } \; |\psi\rangle \in \mathcal{H}_{\mathcal{A}} \text{ and } \; |\phi\rangle \in \mathcal{H}_{\mathcal{B}}. \tag{2.2}$$

If this is not the case, it is *entangled.*

Entanglement is an essential resource in quantum information theory and the building block for important applications - one of those applications being the quantum repeater. The simplest example of entanglement, namely maximally entangled states, are the Bell states. These can be written as

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \qquad \left|\Phi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \tag{2.3a}$$

$$\left|\Psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \qquad \left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right). \tag{2.3b}$$

An important application of quantum entanglement is *quantum teleportation.* Two parties, Alice and Bob, share an entangled pair $|\Phi\rangle_{AB}$, and Alice wants to send a data qubit $|\psi\rangle_{A'}$. She performs a CNOT[a]$_{A\to A'}$, where the data qubit is the "control" qubit, and the entangled qubit on her side acts as the "target". She then applies an H gate on the data qubit and measures both qubits in her possession, obtaining classical bits (a, b). Alice sends the measurements to Bob, and he can apply the corrections $Z^a X^b$ to his qubit [12, 13].

[a] The effect of this gate is $\text{CNOT}(|i\rangle\,|j\rangle) \mapsto |i\rangle\,|i+j \mod 2\rangle$ where we call i the control and j the target.

Many quantum systems are not perfectly closed. Therefore to be able to talk about *open quantum systems*, it is important to introduce an additional Operator [12],

Definition 2.1.3 (Density operator)**.** An operator ρ is called a density operator if it

1. is positive, $\rho \geq 0$,
2. is self-adjoint, $\rho^{\dagger} = \rho$,
3. has trace 1, $\text{Tr}\{\rho\} = 1$.

Mixed states can be written in the density operator formalism as

$$\rho = \sum_k p_k \left|\psi_k\right\rangle \left\langle\psi_k\right|, \quad \text{with} \ \sum_k p_k = 1, \tag{2.4}$$

and called pure if there is one state with $p = 1$. A pure state can then be represented as $\rho = |\psi\rangle\,\langle\psi|$ [14].

To be able to quantify the similarity between two arbitrary quantum states, we first need to introduce the Fidelity of the two quantum states [12].

Definition 2.1.4 (Fidelity)**.** Given two density matrices ρ and σ, the fidelity is defined as

$$F(\rho, \sigma) = \left(\mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2. \tag{2.5}$$

If $\sigma = |\psi\rangle\langle\psi|$ is a pure state, then the Fidelity can be written as $F(\rho, \sigma) = \langle\psi|\rho|\psi\rangle$.

A limiting factor in building large-scale quantum networks is the *no-cloning theorem.* This theorem states that quantum mechanics forbids the copying of unknown quantum states [8]. Since this is an important theorem, the proof will be outlined below.

Suppose there is a pure state $|\psi\rangle$ to be copied, and $|s\rangle$ a target state. Construct a unitary U such that $|\Psi\rangle = U(|\psi\rangle|s\rangle) = |\psi\rangle|\psi\rangle$. Assuming this copying device works for any state, doing the same for a state $|\psi\rangle$ yields the state $|\Phi\rangle = U(|\phi\rangle|s\rangle) = |\phi\rangle|\phi\rangle$. Taking the inner product for both cases leads to

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2. \tag{2.6}$$

This holds for either $\langle\psi|\phi\rangle = 0$ or $\langle\psi|\phi\rangle = 1$, thus the states are either equal or orthogonal.

No device can copy any general quantum state [12].

2.1.2 Quantum noise and channels

Often encountered in quantum mechanics are the Hermitian and Unitary *Pauli matrices.*

$$\sigma_0 = \mathbb{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = \mathrm{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \mathrm{Y} := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \mathrm{Z} := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.7}$$

Since these form a basis for the Hilbert space of 2 × 2 Hermitian matrices $\mathcal{H}_2(\mathbb{C})$ they have found wide use in quantum information and can be used to model quantum channels [14, 12].

We use these operators to introduce the computational basis (Z - basis) as the eigenstate of Z with the eigenvalues $Z|0\rangle = +|0\rangle$ and $Z|1\rangle = -|1\rangle$. Similar to this we introduce the orthonormal conjugate basis (X - basis) as the eigenstates corresponding to $X|+\rangle = +|=\rangle$ and $X|-\rangle = -|-\rangle$[1].

[1] Explicitly these states can be written down as

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Just like classical systems, quantum systems suffer from noise. Since real systems are not perfectly closed, they interact with their environment. This interaction manifests itself as noise. One way of modeling this is to consider *quantum operations*. Take an initial state ρ and a final state ρ', then a quantum operation $\mathcal{E}(\cdot)$ is the map such that $\rho' = \mathcal{E}(\rho)$. These operations can be represented using the operator-sum representation as [12]

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger, \tag{2.8}$$

with the operation elements E_k known as the *Kraus operators* and obey $\sum_k E_k^\dagger E_k = \mathbb{1}$.

Definition 2.1.5 (Quantum Channel)**.** A quantum channel $\mathcal{E} : \mathcal{H}_n \mapsto \mathcal{H}_n$ is a completely positive, trace-preserving map (CPTP) that maps one density operator to another. Completely positive meaning $(\mathbb{1} \otimes \mathcal{E})(\rho) \geq 0$ and trace-preserving $\mathrm{Tr}\{\mathcal{E}(\rho)\} = \mathrm{Tr}\{\rho\}$.

Two examples of important quantum channels are the

1. Depolarizing channel:
A channel that depolarizes the qubit with probability p and leaves the state unchanged with probability $1 - p$. One can write the Kraus Operators as,

$$E_i \in \left\{ \sqrt{1 - \frac{3}{4} p \mathbb{1}}, \quad \frac{\sqrt{p}}{2} X, \quad \frac{\sqrt{p}}{2} Y, \quad \frac{\sqrt{p}}{2} Z \right\}.$$

2. Dephasing channel:
A channel that adds a phase of (-1) to the state $|1\rangle$ with a probability of $1 - p$. One can write the Kraus Operators as,

$$E_i \in \left\{ \sqrt{p} \mathbb{1}, \quad \sqrt{1 - p} Z \right\}.$$

2.2 Quantum communication

2.2.1 Stages of development and applications

We present a brief summary on the stages of development of the quantum internet and its application. For a more thorough presentation refer to [6].

One can roughly break down the development into the following points:

1 Prepare and measure: This is the first stage to offer ”end-to-end quantum functionality”. It enables QKD without needing to trust intermediary repeater nodes. *Applications:* Include QKD and two-party cryptography.

2 Entanglement distribution: Enables end-to-end entanglement creation - either deterministically (succeeds with probability (almost) one) or in a heralded way (where we communicate the success of entanglement generation). *Applications:* Device independence for QKD.

3 Quantum memory: End nodes have the ability to store a quantum state in memory. Can now transfer unknown qubits from one node to another. *Application:* Able to perform blind quantum computation.

4 Few-qubit fault-tolerant: Fault-tolerant execution of local operation on logical qubits. Enables to extend storage time arbitrarily. *Applications:* Fault-tolerant gates enables distributed quantum computing.

5 Quantum computing network: Final stage. Consists of quantum computers that can exchange quantum communication as they please. *Applications:* In principle, all protocols can be realized. A possibility in the future might be quantum cloud computing.

2.2.2 The BB84 protocol

When looking at the performance of a system, it is instructive to compare the initial and final states in order to quantify the error the quantum system has undergone. The concept of the secret key rate (SKR) is introduced on the basis of the BB84 protocol - the first QKD protocol introduced by C. H. Bennett and G. Brassard [4].

The protocol itself is also known as a ”prepare and measure protocol.” [15] This protocol only uses quantum properties in the first two steps, namely the preparation of a quantum state and subsequently in the delivery and measurement of said state. The following steps happen using classical post-processing using an authenticated classical channel. Two parties, Alice and Bob, can exploit a quantum channel to produce a secret key. In the presence of an Eavesdropper (Eve) trying to tap this channel, it will cause disturbances to this channel, and Alice and Bob can learn of this attack by seeing a change in the statistics [16].

The protocol consists of the following six steps [17, 18]:

1. *Prepare:* Alice chooses N (where N is large) random classical bits X_i^c and encodes these into qubits, either in the $X-$ basis or the $Z-$ basis.
2. *Delivery + measurement:* She then uses a quantum channel to send the qubits to Bob. He measures them with a basis he chooses at random and gets a classical bit string Y_i^c.
3. *Basis Sifting:* They communicate via a classical, authenticated channel, the basis they used for encoding/measurement. They discard all the bits where the bases do not agree.
4. *Parameter Estimation:* Take a small subset chosen at random from the remaining bit string and compare it with each other to obtain an estimate on the error rate (how much disagreement there is between X_i^c and Y_i^c). If this error exceeds a certain threshold, the protocol is aborted since this might indicate the presence of an Eavesdropper. If successful, Alice and Bob hold a string of bits $n \leq N$ bits called the raw key.
5. *Information reconciliation:* Alice sends information such that Bob can correct the remaining Bit string Y_i^c.
6. *Privacy Amplification:* Having removed the errors, they can turn their partially secret raw key into a fully secure key of length $l \leq n$.

2.2.3 Secret fraction and secret key rate

When looking at infinitely long keys ($N \to \infty$), one can define the secret key fraction as the fraction of the length of the final secret key l and the length of the raw key

$$r = \lim_{N \to \infty} l/n. \tag{2.9}$$

The extraction of a secret key from the raw key requires classical post-processing, where the focus here will be on one-way post-processing. The formulas are instructive and do not cover the whole depth but rather are intended to give a rough understanding of the quantities used.

This extractable secret key fraction is given by the Devetak-Winter bound [19, 20]

$$r = I(A : B) - \min(I_{EA}, I_{EB}), \tag{2.10}$$

where $I(X : Y)$ is the mutual Information between to Random Variables X and Y and I_{EA} is given by

$$I_{AE} = \max_{\text{Eve}} \chi(A : E). \tag{2.11}$$

We will not derive the secret key fraction but will present the equation in the case of the BB84 Protocol as,

$$r = \max\{0, 1 - h[e_X] - h[e_Z]\}, \tag{2.12}$$

with $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ the binary entropy and e_X (e_Z) the quantum bit error rate (QBER) in the X (Z) basis [21].

The secret key fraction will decrease when increasing the QBER. Once it passes a critical threshold the secret key fraction will drop to zero. In the example of depolarizing noise (where $e_X = e_Z$), the Protocol can tolerate an error of up to 11%, and anything above that will yield a rate of zero [22].

Furthermore, one can compute the Secrete key rate SKR as the ratio between the secret key fraction and the average distribution time $\langle DT \rangle$ [21],

$$SKR = \frac{r}{\langle DT \rangle}. \tag{2.13}$$

Finite key

The definitions and formulas presented hold in the asymptotic limit of infinitely long keys with i.e., $N \to \infty$. Naturally, the question that presents itself is what impact a finite key will have on the secret key rate. Since this is out of the scope of this thesis, a brief summary of the main points will be presented, and the interested reader is referred to additional work, such as [23, 24, 25].

When considering finite keys (in BB84), a reduction in the secret key fraction r is expected. This can be (roughly) broken into two reasons. Firstly, Step 4. *Parameter Estimation* is now conducted on a finite number of samples where one needs to consider the worst-case consistent with statistical fluctuations. Secondly, Equation (2.10) contains terms that vanish in the asymptotic limit. The rest of this work focuses on infinite keys since the main goal of the secret key rate is to work as a measure of performance [18].

2.3 Quantum Repeaters

Telecommunication networks involve distances that are several hundreds or thousands of kilometers long. Due to these long distances, the signals' strength decreases. Akin to asking a friend to pass on a message to a faraway living friend, classically, the issue of a weak signal can be circumvented. To do this one breaks down one long link, connecting two nodes, into several smaller links with repeater stations between these smaller links. These repeater stations copy, amplify and re-transmit the incoming signal [12]. In order to send quantum information, or in the case of the BB84 protocol, sending entangled states, copying these states is prohibited by Quantum mechanics. Quantum mechanics forbids copying quantum information due to the No-cloning theorem introduced in Chapter 2; thus, alternative approaches need to be found.

One way of doing this is to introduce a so-called *quantum repeater*. This repeater works analogously to the classical system in the sense that one takes a link connecting two parties, Alice (A) and Charlie (C), and breaks them down into smaller so-called *elementary links*. As illustrated in Figure 2.1, A and C are connected to the repeater between them, Bob (B). The repeater does not necessarily need to be located equidistant to the neighboring nodes. We consider the case of

B consisting of two memories B_1 and B_2. Three generations of quantum repeaters exist. The first generation using heralded entanglement generation as well as heralded entanglement purification. The second and third generation both use quantum error correction to overcome larger distances [26]. Quantum repeaters have not been realized experimentally yet, but many theoretical proposals have been proposed [27, 28, 29]. The rest of this project will deal with the former, the so-called first generation of quantum repeaters.

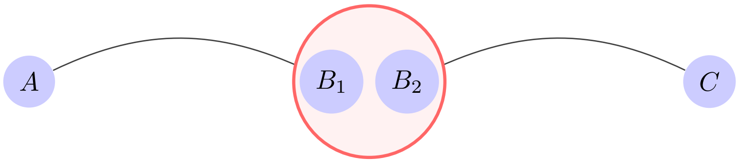


Figure 2.1: Quantum repeater, with the end-nodes Alice (A) and Charlie (C). The repeater, Bob (B), is denoted as the red circle consisting of two memories B_1 and B_2, and located between the end-nodes.

2.3.1 Mode of operation

A quantum repeater connecting two parties, where all nodes are connected by quantum and classical communication channels and allow for two-way signaling, can be broken up into the building blocks of:

Entanglement generation: An entangled pair $|\Phi\rangle$ is created and shared between two adjacent nodes A and B, this is the aforementioned elementary link. The probability of success of creating such an entangled link of Length L in an optical fiber is $p = e^{-L/L_0}$, where L_0 is the attenuation length [30, 31]. Since current link success probabilities are low, the qubits need to be stored in the repeater while another link is created. Storage can be achieved by using a *quantum memory*. Once both parties have established a link to the repeater, they can continue and perform an

Entanglement swap: As illustrated in Figure 2.2, Bob shares an entangled state with Alice $|\Phi\rangle_{AB_1}$ and an entangled state with Charlie $|\Phi\rangle_{B_2C}$. Bob performs the teleportation protocol (Chapter 2) as to entangle A and C and subsequently measures its qubits and delivers the results to the end-nodes. This procedure, therefore, takes the initial state of the complete system and delivers the final state

$$|\Phi\rangle_{AB_1} |\Phi\rangle_{B_2C} \mapsto |\Phi\rangle_{AC} |\Phi\rangle_{B_1B_2} . \tag{2.14}$$

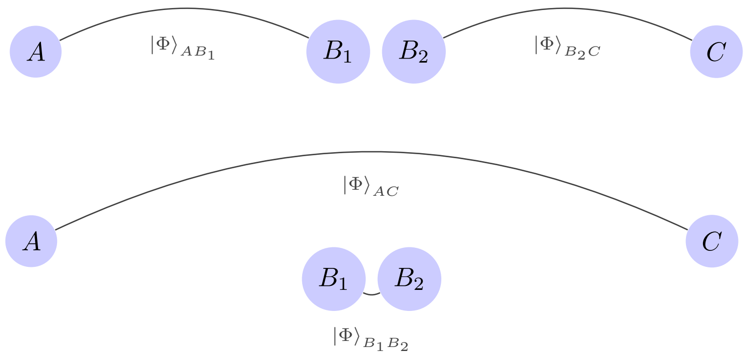


Figure 2.2: Entanglement swap, where B acts as repeater and A and C are the end-nodes. For readability, the red circle from the previous figure for the repeater has been omitted.

Both processes (entanglement generation and swap) are noisy operations which degrade the fidelity of the state. To counter this, one can employ so-called

Entanglement distillation: This works by consuming (multiple) lower quality states to establish a higher quality state [32, 33, 34, 35].

2.3.2 Decoherence - characterizing coherence times

Quantum decoherence is the process whereby quantum information is lost due to interaction with the environment [36, 37, 38]. Two quantities that characterize this quantum decoherence are the *relaxation time* T_1 and the *dephasing time* T_2 [39, 40, 41].

Relaxation time T_1: It measures the time for energy relaxation from the excited state $|1\rangle$ to the state $|0\rangle$. This decay is exponential and is characterized by the probability of being in state $|1\rangle$ such that $\Pr(|1\rangle) = e^{-t/T_1}$. To evaluate this time, follow the protocol presented below.

Protocol 1 Probing the relaxation time T_1.

Steps:

1. Initialize the qubit into the state $|0\rangle$,
2. apply an $X-$ Gate,
3. wait for time t,
4. measure the probability of being in state $|1\rangle$,
5. Fit an exponential curve to the data points to obtain T_1.

Dephasing time T_2: It measures the time for a superposed state to lose the phase information (i.e. going from $|+\rangle \mapsto |0/1\rangle$). To evaluate T_2, the following protocol can be used:

Protocol 2 Probing the dephasing time T_2.

Steps:

1. initialize the qubit into the state $|0\rangle$,
2. apply an H - Gate[2],
3. wait for time t,
4. apply an H - Gate again,
5. measure the probability of being in state $|0\rangle$,
6. Fit an exponential curve to the data points to obtain T_2.

Coherence times of one qubit to another can vary due to a multitude of parameters, resulting in a spread around a mean coherence time [42, 43]. Even for a single qubit, statistical errors introduce an uncertainty in this coherence time.

2.3.3 Implementing a memory and simplifying models

Implementing a quantum repeater experimentally requires that a qubit can be stored while further links are created and subsequently swapped. Several proposals have been brought forward, such as trapped ions [44, 45], atomic ensembles [46, 47, 48] and nitrogen-vacancy centres [49, 50, 10]. Several models of quantum memories and ways to optimize these exist [51, 52, 53], and since the exact physical realization of such a memory is not required for this project, two such simplified models will be presented [27, 54].

The decoherence on the stored qubit can be modeled as the combination of a *depolarizing* - and a *dephasing*- Channel introduced in Section 2.1.2. Instead of writing the depolarizing channel with its Kraus operators, the equivalent channel is presented in its *Werner form* with dimension d as

$$D_{\text{depol}}\left[\rho\right] = w_1\rho + (1-w_1)\frac{\mathbb{1}_d}{d}, \tag{2.15}$$

and the dephasing channel as,

$$D_{\text{dephase}}\left[\rho\right] = w_2\rho + (1-w_2)Z\rho Z. \tag{2.16}$$

Here, the Werner parameters w_1 and w_2 are assumed to have an exponential decay depending on the time t spent in the memory and the coherence time T_1, T_2 introduced in the previous section,

[2] $H\,|0\rangle = |+\rangle$.

$$w_1 = e^{-t/T_1}, \tag{2.17}$$

$$w_2 = \frac{1}{2}\left(1 + e^{-t/2T_2}\right). \tag{2.18}$$

2.3.4 Introducing a cutoff time

Quantum repeaters suffer from noise. One of the sources of noise are quantum memories mentioned above. To perform a *swap*, the link which has been created first needs to sit in the quantum memory, where it starts to decohere. This decoherence may lower the states' quality than one is willing to tolerate, and one way to address this decrease in quality is to introduce a cutoff time.

What is a cutoff

A *cutoff time* τ, is the *maximal time* the qubit is allowed to stay in the quantum memory. Once this time has been reached, the qubit in the memory is discarded, and the end-node and the repeater need to re-start the process of generating a link. We also define the extreme cases of having no quantum memory ($\tau = 0$) or using no cutoff ($\tau = \infty$).

Benefit of a cutoff time

Once a link has been created between an end-node and a repeater, i.e., a link between A and B, the qubit needs to wait in the memory until the second link has been created and can then subsequently be swapped. The qubit idling in the quantum memory starts to decohere while waiting on the second entangled qubit. This decoherence leads to a *reduction in the states' quality.* To illustrate this example, assume we have exponential noise on our quantum memory and the Bell state $|\Phi^+\rangle$ as an initial state. Then the resulting fidelity can be expressed as

$$F = \frac{1}{4}\left(1 + 3 \cdot e^{-t/T}\right), \tag{2.19}$$

where t is the time the qubit spends in the memory.

When looking at the same setup but now using a cutoff, we *limit the maximal reduction in the states' quality.* In the case of the fidelity, the cutoff assures that the lowest delivered fidelity is

$$F = \frac{1}{4}\left(1 + 3 \cdot e^{-\tau/T}\right). \tag{2.20}$$

The *benefit* of using a cutoff is a higher quality of the delivered state, as illustrated in Figure 2.3, where the red curve denotes the fidelity when using a cutoff, which is higher than the case of using no cutoff in blue. Using a cutoff comes at the cost of *longer waiting times until end-to-end entanglement is established.* Increasing the state's quality reduces our QBER and thus improves our secret key fraction r, while at the same time increasing the average distribution time $\langle DT\rangle$.

Thus, there is a trade-off between a higher fractional key rate and a higher distribution time, i.e., what error we allow vs. how long we want to wait.

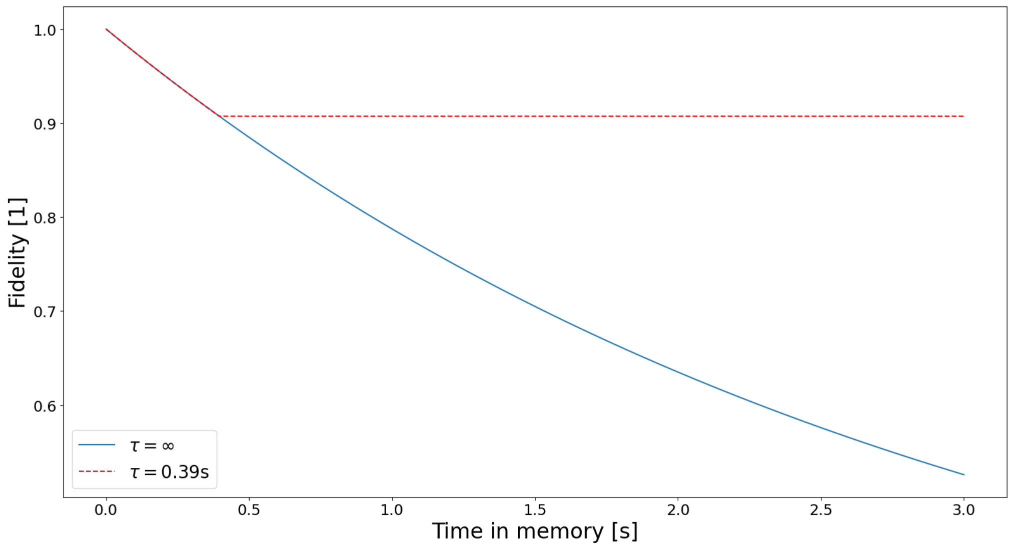


Figure 2.3: Fidelity of a state ρ, using a cutoff in red and no cutoff in blue. The values chosen are to illustrate the fidelity decrease and were chosen as $T = 3$s for the coherence time, and $\tau = 0.39s$ for the cutoff time.

Optimal cutoff time

When using such a cutoff as described above when looking at the secret key rate, this secret key rate attains a maximal value for a certain cutoff time [27]. We call this the *optimal cutoff* τ^*, denoted by an asterisk. This optimal cutoff thus obeys the equation

$$\tau^* = \arg\max_{\tau} SKR(\tau). \tag{2.21}$$

We introduce three variables necessary to analyze the model in the next chapter. These variables are the

- Cutoff time τ: This is the maximal time (in seconds) the qubit is stored in the memory. Once this time is reached, the memory discards the qubit.
- Cutoff $\xi = \tau/\Delta t$: Gives the relationship between the cutoff time and the round time Δt introduced in the next chapter. Used in the subsequent analytical derivations.
- Cutoff rounds $n_{\text{cut}} = \lfloor \xi \rfloor$: This is the number of rounds that can succeed before the qubit is discarded. It is used for deriving the equations in Chapter 3.

For completeness, all three variables are introduced. The most important two are the cutoff time τ and the cutoff ξ. The *cutoff* is used later for analytical derivations. In contrast, the *cutoff time* is used in plots to facilitate the understanding of the relationship of a cutoff time with respect to the coherence time.

Chapter 3

The secret key rate for a single quantum repeater

As explained in the previous chapter, creating long-distance entanglement between two parties is a non-trivial task. This chapter elaborates on the setup of a three-node network, i.e., two parties and one repeater between them, and emphasizes the derived equations [55]. These equations form the basis of the rest of this thesis.

Section 3.1 introduces the problem statement, the parameters, and the assumptions taken. Section 3.2 elaborates on the protocol used when no cutoff time is used and introduces the equations for the average distribution time and the QBER derived from this. The last section, Section 3.3, describes the protocol used when using a cutoff and introduces the equations for the average distribution time and the QBER when using a cutoff.

3.1 Problem statement and the model description

We will consider a three-node network consisting of the end-nodes Alice (A) and Charlie (C), as well as the repeater Bob (B). To be able to verify the performance of the repeater, we will be using entanglement-based QKD (Chapter 2). Similar to [27], entanglement generation will proceed sequentially. Meaning Bob can only create entanglement one link at a time, and thus the scheme needs to succeed independently on Alice and Charlie. Alice and Charlie measure their respective qubit as soon as a link is established. The repeater, Bob, can store the qubit in its quantum memory and waits until both links have been established. He performs a *swap* and joins both links as soon as this succeeds - establishing end-to-end entanglement. Throughout this work, for ease of calculations, we neglect classical communications between the nodes as well as the time gate operations take.

Following setup will be considered,

- *swap* is instantaneous and deterministic (succeeds with $p_{\text{SWAP}} = 1$),
- an elementary link has length L,
- entanglement generation takes time Δt and succeeds with probability p,
- symmetric setup: $L, p, \Delta t$ is the same for $A - B$ and $B - C$,
- sequential repeater: B can only create a link with one neighbor at a time, i.e., he can either create a link $A - B$ *or* $B - C$, but not both at the same time.

As a model of the *quantum memory*, we will be considering a depolarizing channel with exponential noise and a joint coherence time of T (Chapter 2). Thus a state Bell State ρ idling in the quantum memory for a time t will be mapped to,

$$\rho \mapsto e^{-t/T}\rho + \left(1 - e^{-t/T}\right)\frac{\mathbb{1}}{4}. \tag{3.1}$$

When sending a signal over an optical fiber, the signal strength decreases exponentially as a function of the length of the fiber, here denoted as the link length L. This decrease in the signal strength is called *attenuation* [56]. Thus we model the success probability of creating a link of length L during *entanglement generation* as [27]

$$p = 0.5 \cdot e^{-L/L_0} = 0.5 \cdot 10^{-\alpha L/10}, \tag{3.2}$$

where L_0 is the attenuation length and α the attenuation coefficient [57]. Since creating one link takes time Δt, we call this the *round time*, given by [58]

$$\Delta t = L/c_{\text{fiber}}, \tag{3.3}$$

Where c_{fiber} is the speed of light in the fiber.

3.2 Analysis in the absence of a cutoff time

Before examining how the cutoff time affects the secret key rate, we investigate the average distribution time and the QBER when *not* using a cutoff. The exact derivations can be found in [55].

Protocol 3 End-to-end entanglement generation

Setup: No cutoff ($\tau = \infty$).

Goal: Create Entanglement between A and C via a Repeater node B.

Steps:

```
1 Generate link $L_1$ between $A$ and $B$.
2 $A$ measures the qubit immediately, $B$ stores the qubit in memory.
3 Generate link $L_2$ between $B$ and $C$.
4 Measure qubit of $C$ immediately.
5 Swap is performed by $B$ on the new and stored qubit.
6 → End-to-End entanglement is achieved.
```

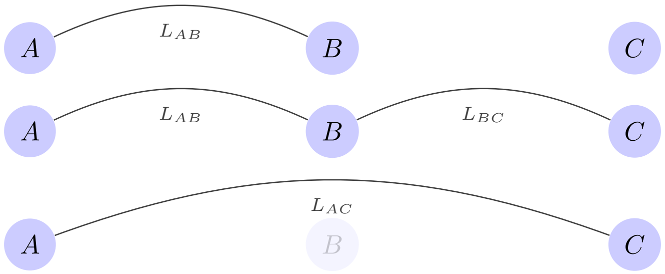


Figure 3.1: Establishment of end-to-end entanglement between A and C following Protocol 3 in the absence of a cutoff time τ.

Using the above protocol, B first creates a link with A, as seen in Figure 3.1. Generating a link between them succeeds after n_1 attempts, and generating a link between B and C succeeds after n_2 attempts. Since generating a link in this setup is probabilistic, the number of attempts n_i is a geometrically distributed random variable with probability p. A random variable X that is geometrically distributed is characterized by its probability mass function $\Pr(X = k) = (1-p)^{k-1}p$, where $k = \{1, 2, \dots\}$ is the number of trials and p the probability of success at each trial. Its expectation value is $\langle X \rangle = 1/p$.

Since B can only create a link with one end-node after another (sequentially), the random variables n_1 and n_2 are independent of each other. Thus the distribution time DT^{∞} when not using a cutoff ($\tau = \infty$) for creating end-to-end entanglement is the summation of the time it takes to generate a link between $A - B$ and $B - C$,

$$DT^{\infty} = DT^{\infty}_{AB} + DT^{\infty}_{BC} = n_1 \Delta t + n_2 \Delta t = \Delta t \left(n_1 + n_2\right) = \Delta t n, \tag{3.4}$$

with the random variable $n = n_1 + n_2$. The average distribution time needed to establish the connection between $A - C$ is the expectation value of Equation (3.4),

$$\langle DT^{\infty}\rangle = \Delta t\,\langle n\rangle = \Delta t\left(\langle n_1\rangle + \langle n_2\rangle\right) = \frac{2\Delta t}{p}, \tag{3.5}$$

where we used the linearity of the expectation as well as the independence of n_1 and n_2.

While waiting for the second link to be created, the qubit in the memory undergoes depolarization for a time $t = n_i\Delta t$, thus leaving the final state,

$$\rho \mapsto e^{-n_i\Delta t/T}\rho + \left(1 - e^{-n_i\Delta t/T}\right)\frac{\mathbb{1}}{4}. \tag{3.6}$$

Using this state, we find the average QBER given by the equation

$$\langle e_Z\rangle = \frac{1}{2} - \frac{1}{2}\left\langle e^{-n_i\Delta t/T}\right\rangle = \frac{1}{2} - \frac{1}{2}\frac{p}{p + e^{\Delta t/T} - 1}. \tag{3.7}$$

Where we used the expectation value of an exponential calculated in the Appendix.

3.3 Analysis in the presence of a cutoff time

In the presence of a cutoff time τ, the protocol below proceeds equal to the previous section up to the point where the first link is created. We will be using the definitions for a cutoff introduced in Section 2.3.4.

Protocol 4 End-to-end entanglement generation

Setup: Cutoff ($\tau \neq \infty$).

Goal: Create Entanglement between A and C via a Repeater node B, while guaranteeing that the maximal time spent in memory is not greater than the cutoff τ.

Steps:

1. Generate link L_1 between A and B.
2. A measures the qubit immediately; B stores the qubit in memory.
3. Generate link L_2 between B and C.
   (a) Cutoff: If L_2 is delivered in time $t > \tau \rightarrow$ discard link L_1,
   $\Rightarrow$ Start at Step 1, with the Roles reversed.

   (b) Cutoff: If L_2 is delivered in time $t \leq \tau \rightarrow$ keep link.
4. Measure qubit of C immediately.
5. BSM is performed by B on the new and stored qubit.
6. $\rightarrow$ End-to-End entanglement is achieved.

As an example, seen in Figure 3.2, a link between A and B has been created, and the qubit is stored in B. The time spent in the memory exceeds the threshold of τ, and thus the qubit is discarded.

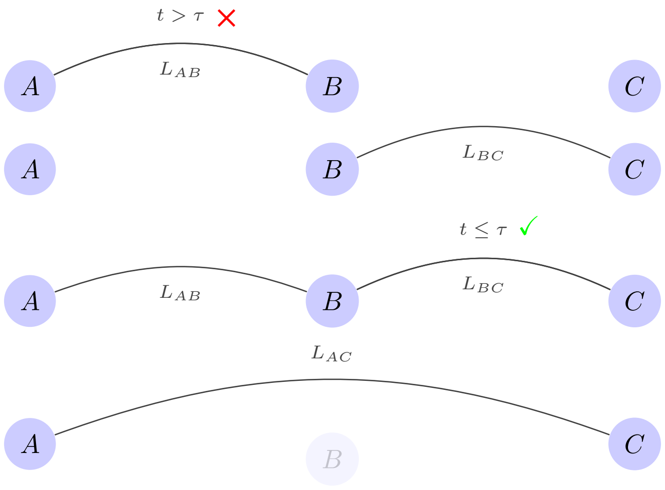


Figure 3.2: Establishment of end-to-end entanglement between A and C following Protocol 4 in the presence of a cutoff time τ.

Now a link between B and C is established, and a link between A and B can be created while the qubit idles in the memory. As soon as both links are established and the idling qubit does not exceed τ, B swaps both links and establishes end-to-end entanglement.

Calculating the average distribution time in the presence of a cutoff is more intricate, and for the sake of brevity, the resulting equations will be presented. For a derivation of the distribution time, we refer to [55] and for a derivation of the QBER we refer to [54].

The average distribution time for a cutoff time is

$$\langle DT \rangle = \frac{\Delta t}{p} \left(1 + \frac{1}{1 - (1-p)^{n_{\text{cut}}}} \right), \tag{3.8}$$

where $n_{\text{cut}} = \lfloor \tau / \Delta t \rfloor$ is the maximum number of rounds of entanglement generation before the cutoff time is exceeded and $\lfloor \cdot \rfloor$ the flooring operator.

The resulting QBER, using the same definitions as above, is

$$\langle e_Z \rangle = \frac{1}{2} - \frac{p e^{-\Delta t/T}}{2\,(1 - (1-p)^{n_{\text{cut}}})} \frac{1 - [e^{-\Delta t/T}(1-p)]^{n_{\text{cut}}}}{1 - e^{-\Delta t/T}(1-p)}. \tag{3.9}$$

Part II
Influence of coherence time drift on the secret key rate

The main contributions of this thesis are:

We numerically evaluate the optimal cutoff time for different coherence times. Using this, we assess the *factor of improvement* of using an optimal cutoff time in the secret key rate compared to abstaining from using one while varying the coherence time. Previous work investigated the secret key rate as a function of the distance using an optimal cutoff [54] or the secret key rate as a function of the cutoff for different schemes [27].

We introduce the *first-order approximation to the cutoff* to establish a functional relationship between the cutoff and the coherence time.

We introduce the notion of *loss in secret key rate*. Given the maximal deviations in coherence time from a mean and the optimal cutoff time of that mean coherence time, one can now calculate the *approximate loss in secret key rate* - where the loss is the difference between the secret key rate with the cutoff optimized to the deviated coherence time, and the secret key rate optimized for the mean coherence time.

Chapter 4

Understanding drift in the coherence time

As seen in the chapters before, creating a working quantum repeater is still in its infancy - a factor limiting its performance being the quality of memory. One way of improving the fidelity, or rather in the case of QKD, the secret key rate, is to implement a cutoff as introduced in chapter 2. This cutoff time is a timer on your quantum memory and discards the qubit once the time runs out.

Section 4.1 presents the parameters we fix throughout this project, defines what we mean by a drift in coherence time, and introduces bounds on the cutoff. Section 4.2 explains the effect of the drift on the secret key rate using different coherence times to illustrate it further. Section 4.3 follows with introducing an algorithm to calculate the optimal cutoff times as a function of the coherence times and uses these to calculate a factor of improvement for the secret key rate when using an optimal cutoff time compared to no cutoff time.

Section 4.4 introduces the conditions for an optimal secret key rate and elaborates on the problems associated with finding an optimal cutoff. Section 4.5 delves deeper into how to quantify the change in cutoff when the coherence time drifts. Section 4.6 concludes with a relationship between the difference in cutoff and a difference in the coherence time.

4.1 Important parameters and definitions

To understand how to find an optimal cutoff time, we first proceed by fixing parameters that we do not wish to vary, such as the link length. Further, we explain what is meant by a *drift in coherence time.*

4.1.1 Fixing the link length

Parameter	Symbol	Value	Unit
Link Length	L	100	[km]
speed	c_{fiber}	$2 \cdot 10^5$	$\left[\frac{\text{km}}{\text{s}}\right]$
attenuation coefficient	α	0.25	$\left[\frac{\text{dB}}{\text{km}}\right]$
success probability	p	$0.5 \cdot 10^{-5/2}$	[1]
round time	Δt	$5 \cdot 10^{-4}$	[s]

Table 4.1: Parameters that are being kept fixed throughout the whole calculations.

In [54] the secret key rate as a function of the elementary link length was investigated as well as the role of the cutoff rounds on the secret key rate for different protocols proposed. Therefore, we will fix the link length in this work and accordingly fix the success probability of link creation p as well as the round time Δt.

To fully fix the parameters mentioned above, we need to specify further the *attenuation losses* and the *speed of light in the fiber* introduced in Chapter 3. Attenuation losses vary depending on the fiber used, with values for the attenuation coefficient ranging from 0.14dB/km to 0.4dB/km [54]. We will choose a value of $\alpha = 0.25$ as a value that lies between them. Furthermore, we set the speed of light in glass fiber as $c_{\text{fiber}} = 2 \cdot 10^5$m/s [58]. Thus, according to Equation 3.2 for the success probability and Equation 3.3 for the round time, we can calculate the values shown in Table 4.1. Fixing the values from the table above, our secret key rate is a function of coherence time T and the cutoff time τ introduced in the previous chapter.

4.1.2 A drift in coherence time

To understand why we want to vary the coherence time, we first need to introduce what a *drift in coherence time* means. This means that the coherence time starts changing from the mean coherence time T_0, or *drifting*, with maximal deviations given by δT. Therefore the coherence time experience drift will be an element of

$$T \in [T_0 - \delta T, T_0 + \delta T]\,. \tag{4.1}$$

This is inspired by the statistical uncertainty inherent when measuring the coherence time, where one fits a predefined function to the experimentally obtained data, whether it may it be an exponential function, as in the case for Chapter 2, or a Gaussian distribution with mean coherence time T_0 as in [43].

The *optimal cutoff* introduced in Section 2.3.4 is the cutoff that maximizes the secret key rate for a coherence time T_0. Thus a cutoff optimized for a coherence time T_0 might not be the optimal cutoff for a drifted coherence time $T_0 \pm \delta T$.

4.1.3 Bounding the cutoff time

The optimal cutoff time τ^*, is the cutoff that maximizes the secret key rate for a given coherence time. Before continuing, we will explain the limits we impose on our cutoff - this aids when numerically looking for optimal cutoff times later.

Chapter 3 introduces the cutoff rounds as $n_{\text{cut}} = \lfloor \tau/\Delta t \rfloor$. Any cutoff time lower than the round time will floor to zero, therefore imposing a lower limit on our cutoff time as $\tau = \Delta t$. On the other hand, the coherence time is the time our state maintains its quantum properties. Thus we impose the maximal cutoff time to be not greater than the coherence time T. We can conclude that our cutoff time should lay in the interval

$$\tau \in (\Delta t, T]. \tag{4.2}$$

Two extreme cases are the case of $\tau = 0$, corresponding to the case of not having a quantum memory, and the case of $\tau = \infty$, which corresponds to the case of not using a cutoff time. When using superscripts for functions of the form X^∞ we always understand a cutoff time using the latter extreme case.

4.2 The evolution of the secret key rate for different coherence times

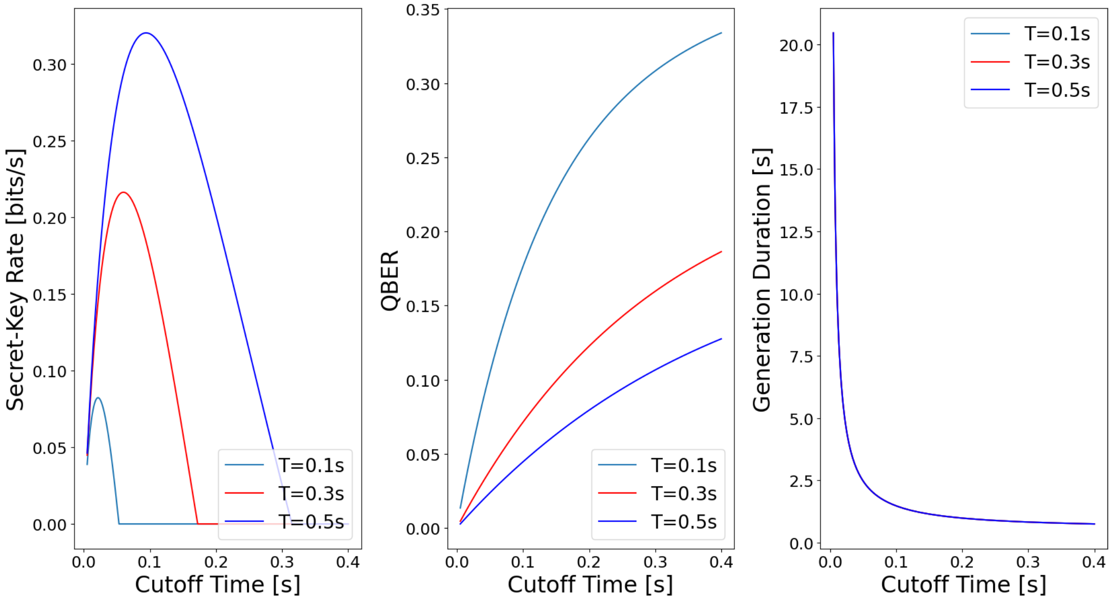
In Chapter 3, we explained the optimal secret key rate as the maximal secret key rate obtained when varying the cutoff time. In this section, we plot the secret key rate as a function of the cutoff time τ for different coherence times. We will investigate coherence times of the same order as the average generation time of one link

($T \sim \Delta t/p \approx 0.3$s), and the cases of one and two orders of magnitude greater. Thus, we will plot the coherence times $T_0 \in \{0.3, \quad 3, \quad 30\}$s with maximal deviations of $\delta T = \frac{2}{3}T_0$. The maximal deviations were picked large to illustrate better the change in secret key rate for different coherence times.

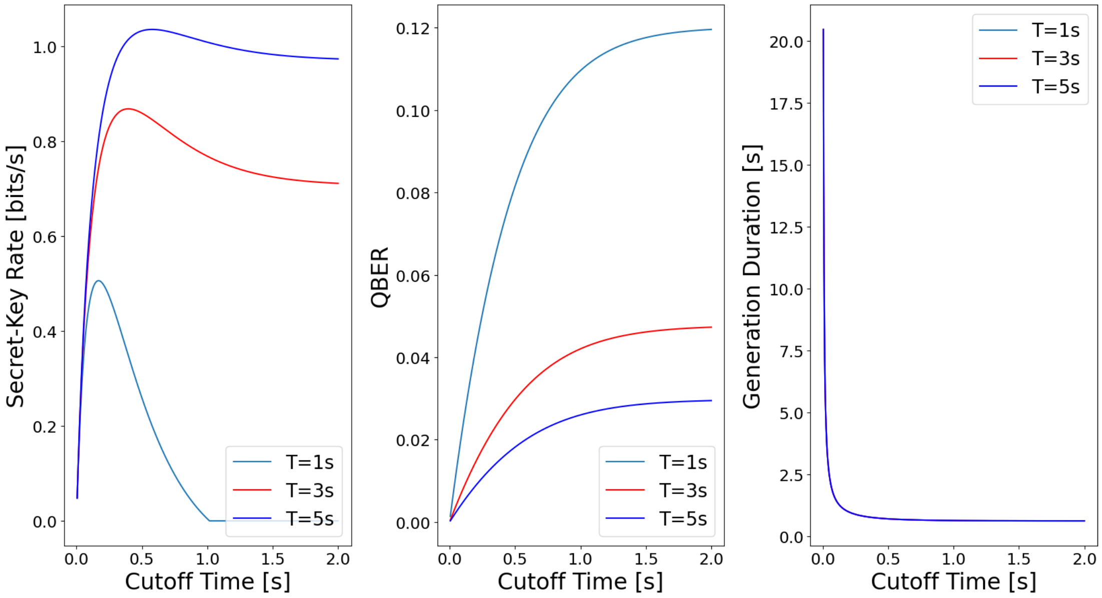
When observing the secret key rates plotted in Figure 4.1 as functions of the cutoff time, we can make the following statements,

- For coherence times $T \sim \Delta t/p$ using a cutoff time yields not only an improvement but is **necessary** to achieve a non-zero secret key. When looking at a specific coherence time (i.e., 0.3s) even **small deviations from the optimal cutoff lead to a significant decrease in the secret key rate.** The QBER keeps increasing and passes the maximal tolerable error threshold of 11%. This is due to the fact that the coherence times are similar to the generation time for one link, not using a cutoff lets the qubit decohere before it can be distributed. The generation duration, or the average distribution time, increases rapidly for short cutoff times and is independent of the chosen coherence time. Variations in this cutoff transfer to bigger variations in the resulting secret key rate.
- For coherence times $T \sim 10 \cdot \Delta t/p$ the cutoff yields an improvement, though it is not strictly necessary to use one for non-zero keys. **Deviations from the optimal cutoff lead to a more subtle change in secret key rate than before**. The QBER starts saturating earlier.
- For coherence times $T \sim 100 \cdot \Delta t/p$ the optimal secret key rate is difficult to identify graphically from Figure 4.1c. An optimal cutoff can be obtained when analyzing the data, even though the optimal secret key rate approaches the value for the secret key rate in the absence of a cutoff. **Deviations from the optimal cutoff seem to lead to barely noticeable changes in the secret key rate.**

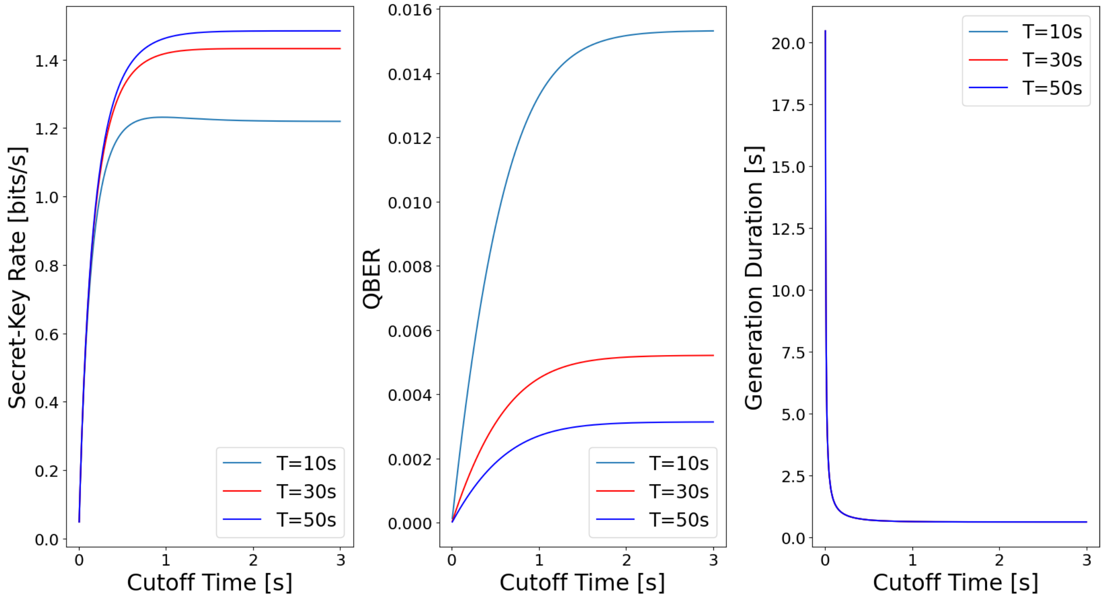
These initial findings provide a good basis and motivation to delve deeper into the next chapter, making it clear that the optimal secret key rate changes for different coherence times. However, it is yet unclear **how sensitive** this optimum is to changes (drifts) in the coherence time.



(a) The lowest order of magnitude for coherence times $T \in \{0.1, 0.3, 0.5\}$. High sensitivity is observed with respect to variations in the cutoff, secret key rate goes to zero for higher values of τ.



(b) Order of magnitude higher than (a) for coherence times $T \in \{1, 3, 5\}$. Sensitivity is lower, nonetheless, a clear optimal cutoff can be found.



(c) Highest order of magnitude for coherence times $T \in \{10, 30, 50\}$. No apparent sensitivity can be observed, cutoffs seem to have a small impact.

Figure 4.1: The Secret key rate (left), the QBER (middle), and the Generation duration (right) for different coherence times Ts when varying the cutoff time τ. Generation duration is independent of the coherence time and thus equal for all three plots.

4.3 Maximal achievable gain

As seen in the previous section as well as in [54, 27], using a cutoff leads to higher secret key rates compared to not using cutoffs. Before continuing with the question of how to express this sensitivity to drifts, we want to elaborate on the question

How much do we gain when using an optimal cutoff vs. not using a cutoff as a function of the coherence time?

In analogy to classical electronics [59] we define the maximal achievable gain G, as the ratio between the secret key rate using the optimal cutoff (SKR^*) and the secret key rate in the absence of such a cutoff (SKR^∞)

$$G = \begin{cases} 0 & SKR^* = 0, \\ \frac{SKR^*}{SKR^\infty} & SKR^* \neq 0. \end{cases} \tag{4.3}$$

Therefore yielding the explicit formula of

$$G = 2 \cdot \frac{1 - q^{\tau/\Delta t}}{2 - q^{\tau/\Delta t}} \cdot \frac{1 - 2h(e_z^*)}{1 - 2h(e_z^\infty)}, \tag{4.4}$$

whenever $SKR^* \neq 0$ and the QBER e_z^* (e_z^∞) for the optimal (no-cutoff) case.

We use Algorithm 1 to calculate the optimal cutoff times τ^* as a function of the coherence time. As seen in Figure 4.2, a coherence time of $T \leq 1.12\text{s} \approx 4\Delta t/p$ means that no secret key can be produced without a cutoff. The gain (Figure 4.2) rapidly decreases to unity for coherence times $T \geq 3 \approx 10\Delta t/p$. Using this numerical approach, we can conclude that for coherence times below $10\Delta t/p$ a cutoff is important for achieving higher secret key rates.

Algorithm 1: Obtaining optimal cutoff.

```
Data: List: coherence times $T$,
            cutoffs with $\tau \in (\Delta t, T]$,
            secret key rates SKR
Result: List: optimal cutoffs $\tau^*$.
for $T_i$ in $T$ do
    for $\tau_i$ in $\tau$ do
        $SKR(T_i, \tau_i)$
        Add $SKR(T_i, \tau_i)$ to SKR ;        /* Add the value to the SKR list */
    end
    $\tau_i^* = \arg\max_\tau$ SKR ;     /* Find the tau where SKR has the maximal value */
    Add $\tau_i^*$ to $\tau^*$
end
```

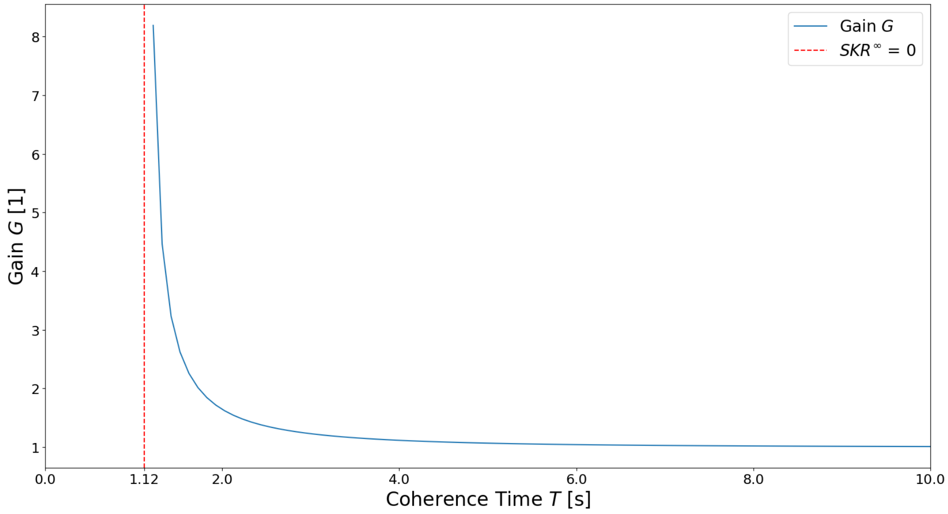


Figure 4.2: Factor of improvement when using an optimal cutoff vs. not using a cutoff for the secret key rate. In blue the Gain G and in red the first value of the coherence time where the secret key rate goes to zero

4.4 The conditions for an optimum

Being interested in finding a cutoff that maximizes the secret key rate, several modifications need to be implemented to make secret key rate differentiable with respect to our cutoff time.

In Chapter 3 we introduced the *cutoff* $\xi = \tau/\Delta t \in \mathbb{R}$. We take this cutoff as the analytic continuation of $n_{\text{cut}} = \lfloor \xi \rfloor$, since we are assuming small round times. Thus, finding the optimum with respect to τ is the same as finding an optimum with respect to ξ up to a multiplicative constant. Next, one relaxes the constraint on the secret key fraction and writes it as $r = 1 - 2h(e_Z)$ (omitting the $\max\{\cdot\}$), since for depolarizing noise, the QBER in the X - basis and in the Z - basis are the same. Lastly, for the sake of simplicity, the $\langle \cdot \rangle$ of the QBER will be dropped. Whenever we write e_Z the average QBER will be implied.

We can further define an optimal secret key rate as the unique solution to the equation

$$\partial_\xi SKR = \frac{\partial_\xi r \langle DT \rangle - r \partial_\xi \langle DT \rangle}{\langle DT \rangle^2} = 0 \tag{4.5}$$

$$\frac{\partial_\xi r}{r} = \frac{\partial_\xi \langle DT \rangle}{\langle DT \rangle}, \tag{4.6}$$

$$\frac{2}{\ln 2} \cdot \frac{\partial_\xi e_Z \cdot \ln e_\theta}{1 - 2h(e_Z)} = \ln q \frac{q^\xi}{(2 - q^\xi)(1 - q^\xi)} \tag{4.7}$$

for $e_\theta = \frac{e_Z}{1-e_Z}$ and $\partial_\xi e_Z$ derived in the Appendix. The condition of non-zero rate ($r > 0$) is implied, and $\langle DT \rangle$ is the average distribution time (generation time). Therefore, the goal is to find the cutoff that obeys the above condition, making it a function of the coherence time, effectively finding a relationship for the optimal cutoff of the form $\xi^* = \xi(T)$.

Due to the highly non-trivial nature of $h(\cdot)$ in Equation 4.7, we were unable to solve this equation for an optimal cutoff ξ^*. Nonetheless, this condition is going to be valuable for later, even though, for the optimal cutoff, we must rely on the cutoffs found numerically in Chapter 4.

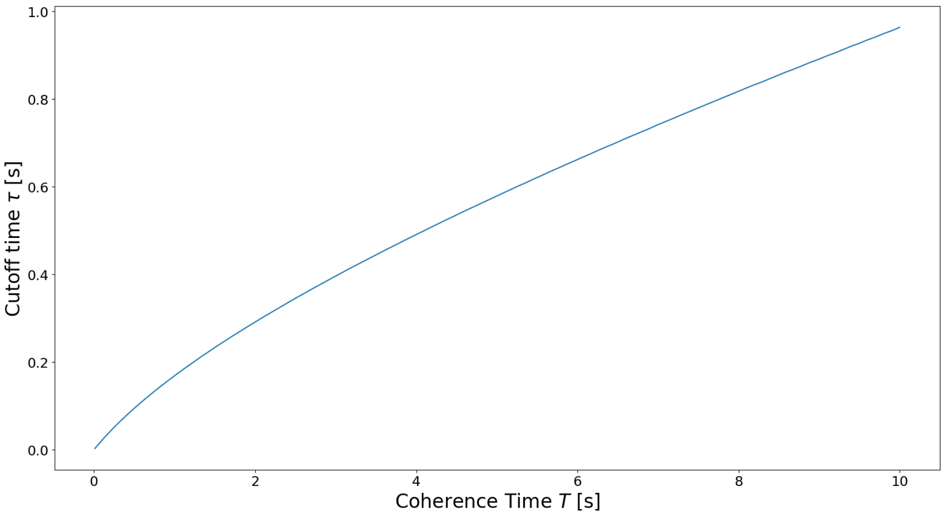


Figure 4.3: The optimal cutoff time τ as a function over the coherence time T.

As seen in Figure 4.3 the cutoff τ behaves approximately linear for higher coherence times but loses much of this linearity as the coherence times gets smaller.

4.5 Quantifying the effect on the optimal cutoff when varying the coherence time

Having found these cutoffs numerically, the question that arises is how sensitive these cutoffs are to deviations in the coherence time. From the previous chapter we deducted that the cutoff is more sensitive the smaller the coherence time. Calculating this sensitivity might help us in understanding if this is really the case, and if not, we could proceed to investigate why not.

Calculating this sensitivity can be done by defining the condition for the optimum as an implicit function, $R(T, \xi) = \partial_\xi SKR = 0$. We use that the optimal cutoff a function of the coherence time is and use the chain rule to differentiate with respect to T to arrive at

$$\partial_T R \cdot \frac{dT}{dT} + \partial_\xi R \cdot \frac{d\xi}{dT} = 0. \tag{4.8}$$

Solving for $d\xi/dT$ and plugging in $R = \partial_\xi SKR$ we arrive at the expression

$$\frac{d\xi}{dT} = -\frac{\partial_T \partial_\xi SKR}{\partial_\xi^2 SKR}. \tag{4.9}$$

Using the previously found optimal cutoffs ξ^* and the relationship $d\tau/dt = \Delta t \cdot d\xi/dT$ the derivative is evaluated in Figure 4.4 with respect to a varying coherence time T. Doing this serves two purposes. First, analyzing the magnitude gives information about how quickly the optimal cutoff changes. Second, the sign gives information about the behavior of the derivative.

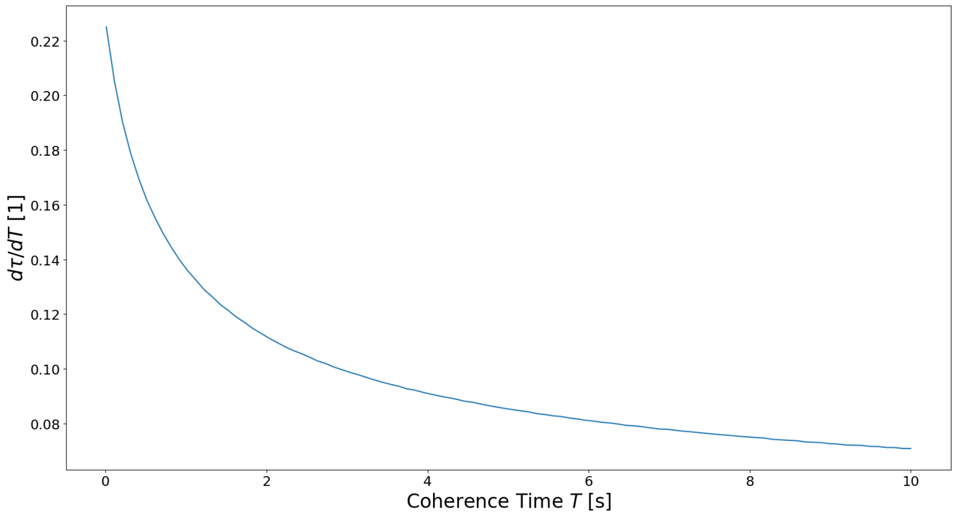


Figure 4.4: The derivative of the cutoff $d\tau/dT$ versus the coherence time T, evaluated for the numerically evaluated optimal cutoff times τ^* in Chapter 4

Since the derivative in Figure 4.4 is positive for all coherence times the cutoff keeps increasing, even though the rate at which it does keeps decreasing.

4.6 Approximating the optimal cutoff time using leading order expansions

Anticipating the next chapter, we want to establish a relationship between a change in cutoff and a change in coherence time. To achieve this we want to approximate the optimal cutoff to first-order for the mean coherence time T_0 and its associated optimal cutoff ξ_0. We proceed similar to the previous section and use $\partial_\xi SKR = R(T, \xi)$ and arrive at

$$R(\xi, T) = R(T_0, \xi_0) + (\partial_T\ R)|_{T_0,\xi_0}\, \Delta T + (\partial_\xi\ R)|_{T_0,\xi_0}\, \Delta\xi + \mathcal{O}(\Delta T^2, \Delta\xi^2) = 0. \quad (4.10)$$

where $\Delta T = T - T_0$, with the mean coherence time T_0 (fixed) and T (variable) and $\Delta\xi = \xi - \xi_0$, with the associated optimal cutoff ξ_0 (fixed) and ξ (variable). By construction we have $R(T_0, \xi_0) = 0$. Solving for $\Delta\xi$ we can write to first-order

$$\Delta\xi = -\left.\frac{\partial_T \partial_\xi SKR}{\partial_\xi^2 SKR}\right|_{T_0,\xi_0} \Delta T. \tag{4.11}$$

We have found a relationship of the form $\Delta\xi = A \cdot \Delta T$, where we identify $A = \frac{\partial_T \partial_\xi SKR}{\partial_\xi^2 SKR}$. We can use the equation above and solve it for ξ to get the linear approximation to the optimal cutoff (neglecting higher-order terms),

$$\xi(T) = -\left.\frac{\partial_T \partial_\xi SKR}{\partial_\xi^2 SKR}\right|_{T_0,\xi_0} (T - T_0) + \xi_0, \tag{4.12}$$

$$\xi(T) = A\left(T_0, \xi_0\right) \cdot (T - T_0) + \xi_0. \tag{4.13}$$

To verify this approximation, the numerically evaluated cutoff and the linearization are plotted with respect to a varying coherence time. We use a mean coherence time of $T_0 = 3$s, a maximal deviation of $T_0 \pm \frac{1}{3} T_0 = 3\text{s} \pm 1\text{s}$, and an associated optimal cutoff time of $\tau_0 = 0.396$s. The derivatives for the secret key rate, derived in the Appendix, are evaluated at the mean coherence time T_0 and the associated cutoff τ_0.

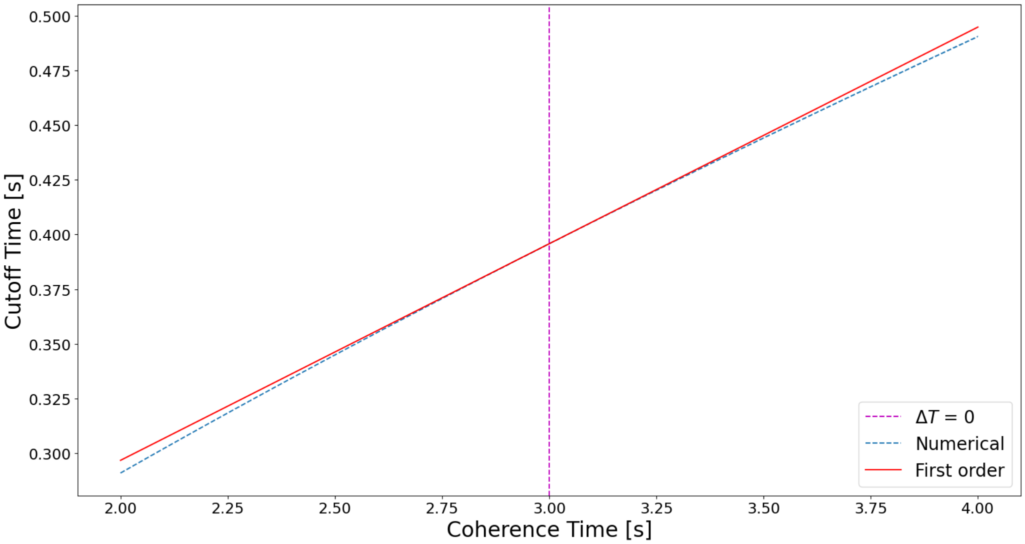


Figure 4.5: Linearization of the cutoff τ as a function of the coherence time T, around the mean coherence time $T_0 = 3\text{s}, \tau_0 = 0.396\text{s}$. The range is limited to $T_0 \pm \frac{1}{3}T_0$.

As seen in Figure 4.5 the approximation resembles the true cutoff in the provided range, with a maximal error e of 2%, as shown in Appendix C. For small deviations around the mean coherence time, the cutoff can be approximated by a linear function.

Chapter 5

Quantifying the sensitivity

The previous chapter introduced the meaning of drift in the coherence time and showed a functional relationship between the cutoff and the coherence time. Both these results will be used throughout this Chapter to motivate and quantify the resulting loss in secret key rate due to drift.

Section 5.1 explains how to quantify this loss and derives the second-order approximation. Section 5.2 presents the sensitivity parameter derived and its interpretation. Section 5.3 presents an analysis of the validity of the approximations introduced. Finally, Section 5.4 compares the two regimes of low and high sensitivity.

5.1 Quantifying the loss in secret key rate

Throughout this work, we have seen

1. that using a cutoff improves the secret key rate,
2. what the factor of improvement is when using a cutoff compared to the absence of one.

A continuation of this poses the question: *What is the secret key rate we lose when the coherence time starts drifting?*

To elaborate on what is meant by losing secret key rate, consider the following scenario: As presented in Chapter 4, we have the mean coherence time T_0 and deviations around the mean such that the coherence time is bound to the region $T \in [T_0 \pm \delta T]$.

Next, we find the optimal cutoff for our expected coherence time $\xi_0 = \xi(T_0)$. If our coherence time starts trailing to a new value $T_1 = T_0 \pm \delta T$, the optimal cutoff will start to shift as well to a new cutoff $\xi_1 = \xi(T_1)$. The resulting secret key rate, initially optimized to ξ_0, will thus be lower than the optimal secret key rate using ξ_1.

This can be seen in Figure 5.1, where the two secret key rates as functions of the cutoff time τ[1] are plotted for different coherence times. Assuming the expected coherence time is $T_0 = 3$s (red), we can find a cutoff time as $\tau_0 = 0.39$s, rounded to two decimal points for readability. If we now start decreasing the coherence time, we arrive at the maximal deviation where $T_1 = 1$s, we can see that the optimal cutoff for this curve (blue) would be in fact lower, $\tau_1 =$. The intersection of the magenta line with the blue curve is the secret key rate we observe when using the cutoff or the expected coherence time τ_0, which is lower than we could get maximally. *This reduction is what we term a loss in secret key rate.*

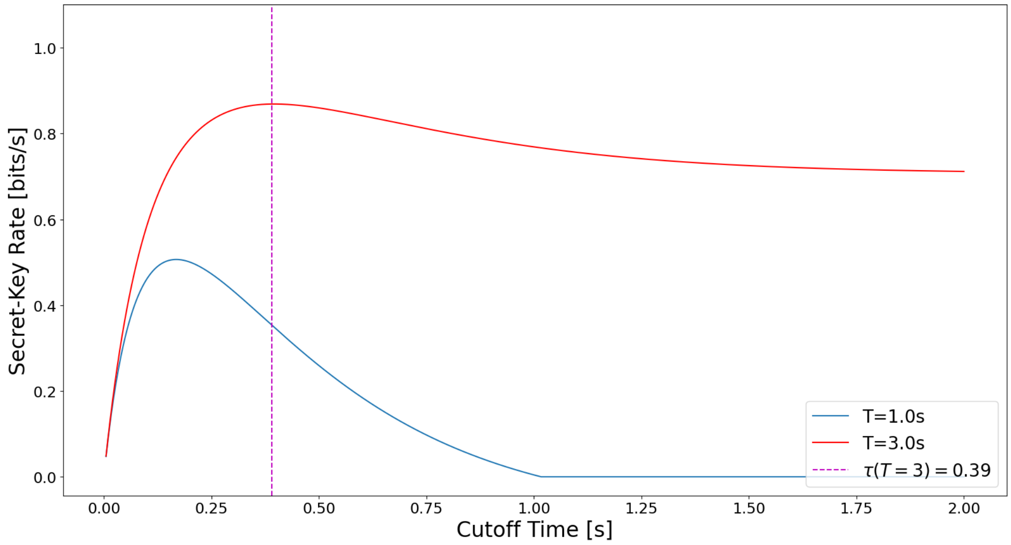


Figure 5.1: Secret key rate for a coherence time $T_0 = 3$s (red) and a coherence time $T_1 = 1$s (blue). The optimal cutoff time is $\tau_0(T = 3) = 0.39$s (vertical magenta line).

More generally, this *loss in secret key rate* can be understood as the difference between the optimal secret key rate for every coherence time $SKR(T, \xi(T))$, where

[1] To go from a cutoff time to the cutoff use $\tau = \xi \cdot \Delta t$.

$\xi(T)$ is the optimal cutoff as a function of the coherence time T and the secret key rate $SKR(T, \xi_0)$ that uses a cutoff $\xi_0 = \xi(T_0)$ optimized for a specific coherence time T_0,

$$\Delta SKR = SKR(T, \xi(T)) - SKR(T, \xi_0). \tag{5.1}$$

By construction $\Delta SKR \geq 0$, since the optimized secret key rate for every coherence time is never lower than a sub-optimal one.

To better understand what the loss is for small deviations around the expected coherence time T_0, and since we were unable to find a closed-form for $\xi(T)$, we proceed similarly as when approximating the cutoff and expand the loss to first-order around (T_0, ξ_0),

$$\begin{aligned} SKR(T, \xi) &= SKR(T_0, \xi_0) + \partial_\xi \, SKR|_{T_0,\xi_0} \, \Delta\xi + \partial_T \, SKR|_{T_0,\xi_0} \, \Delta T, \\ SKR(T, \xi_0) &= SKR(T_0, \xi_0) + \partial_T \, SKR|_{T_0,\xi_0} \, \Delta T, \\ \Delta SKR &= \partial_\xi \, SKR|_{T_0,\xi_0} \, \Delta\xi, \end{aligned}$$

with $\Delta T = T - T_0$, $\Delta\xi = \xi - \xi_0$. In the linear expansion, the loss of secret key rate is $\Delta SKR = \partial_\xi \, SKR|_{T_0,\xi_0} \, \Delta\xi = 0$ - coming from the flatness around the maximum[2]. To calculate the resulting loss, we extend this approximation to second-order and employ the functional relationship between a difference in cutoff and a difference in coherence time introduced in Equation 4.11, termed A. This way our loss will only be a function of the maximum deviation from our expected coherence time, the expected coherence time T_0 and the associated optimal cutoff ξ_0,

$$\begin{aligned} \Delta SKR(T, \xi) &= \frac{1}{2}\partial_\xi^2 \, SKR|_{T_0,\xi_0} \, \Delta\xi^2 + \partial_T \partial_\xi \, SKR|_{T_0,\xi_0} \, \Delta T \Delta\xi \\ &= \left[\frac{1}{2} A \partial_T \partial_\xi \, SKR|_{T_0,\xi_0}\right] \Delta T^2 \end{aligned} \tag{5.2}$$

with $\Delta T = T - T_0$, $\Delta\xi = \xi - \xi_0$ from above.

[2] This is akin to using the method of steepest descent where a function is approximated around its maximum/minimum and a constant term and its second derivative are left.

Computationally it would be feasible to calculate the exact losses for two points. On the other hand, this approach gives a way to better understand how the loss evolves as a single function of the deviation from the expected coherence time, ΔT.

5.2 Deriving and understanding the sensitivity parameter

The loss in Equation 5.3 yields an absolute value in bits/second. We can (with a little algebra) rewrite our expression as the loss with respect to a certain secret key rate, the relative deviation around T_0 and a prefactor B such that

$$\begin{aligned}\Delta SKR(T,\xi) &= \left[\frac{1}{2}A\partial_T\partial_\xi\ SKR|_{T_0,\xi_0}\right]\Delta T^2\\ \frac{\Delta SKR(T,\xi)}{SKR^*} &= \frac{1}{2}\left[\frac{T_0^2}{SKR^*}\cdot A\partial_T\partial_\xi\ SKR|_{T_0,\xi_0}\right]\left(\frac{\Delta T}{T_0}\right)^2 \\ &= B\cdot\left(\frac{\Delta T}{T_0}\right)^2.\end{aligned} \tag{5.3}$$

As before $SKR^* = SKR(T_0, \xi_0)$ is the optimal secret key rate for the expected coherence time T_0 and the associated cutoff ξ_0. The factor $B = B(T_0, \xi_0)$ is evaluated at the cutoff and coherence time and a non-zero secret key rate and a non-zero coherence time are assumed. Using Equation 5.3, one can

1 calculate the loss relative to a reference key rate SKR^* for a given range ΔT,

2 interpret the prefactor B as a form of sensitivity parameter.

Focusing on the second point, the B - value influences the shape of the parabola of the quadratic approximation. A large value means that per unit change of the coherence time T, the resulting change in ΔSKR is large. A smaller value means smaller ΔSKR per unit change of T. We can, therefore, interpret this prefactor as a form of *sensitivity factor*. To understand how this value changes depending on the expected coherence time, we use the numerically found cutoff times and evaluate B for every coherence time and its associated cutoff time. This is done to better understand B, the computational costs can be kept lower if computing the cutoff $\xi(T)$ first and then using them in all subsequent steps for B.

Next, we start varying our optimal coherence time from $T_0 = 0.001$s to $T_0 = 10$s. These values were chosen to give a great enough range to give us insights (range

$\sim 30 \cdot \Delta t/p$) but not too great as to be computationally unfeasible. Consequently, evaluating this sensitivity factor for all coherence times and the optimal cutoffs $T_0, \xi(T)$ yields how *strong* the magnitude of the loss decreases.

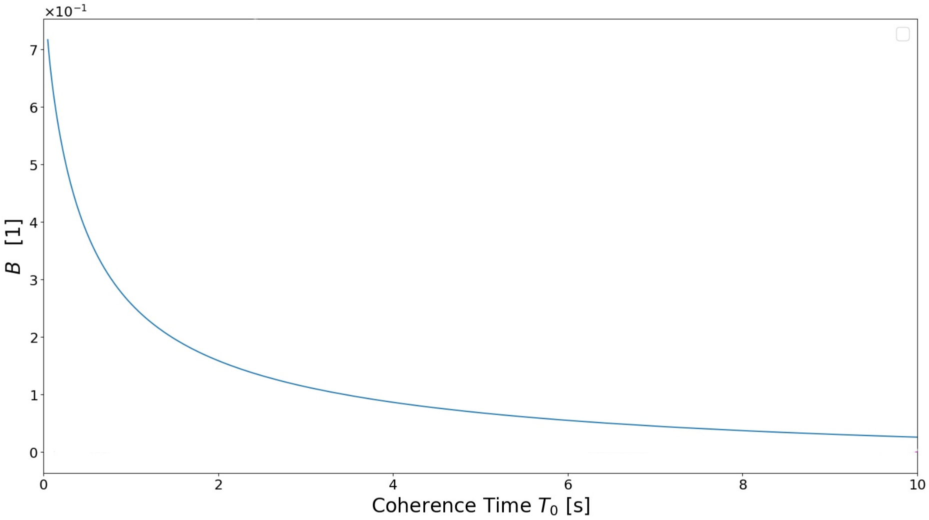


Figure 5.2: Sensitivity Parameter B as a function of the coherence time T_0, where for every coherence time the optimal cutoff ξ_0 has to be used.

Doing this, we can see in Figure 5.2 that similar to the sensitivity of the cutoff to the coherence time, the B - value decreases rapidly for higher coherence times and is greatest for small coherence times, i.e., in the vicinity of $T \sim \Delta t/p$. Thus when the relative deviations $\Delta T/T_0$ are equal throughout all coherence times, we see that small coherence times lead to a comparatively higher loss,

$\Rightarrow$ Relative deviation around T_0 is important **and** absolute value of T_0.

5.3 Analysing the validity of the approximation

When approximating a function, the question arises of how good this approximation to the original function is. To do this we use Equation 5.3 and compare it to a numerical evaluation of $\Delta SKR/SKR^*$ as a function of the coherence time. Using a coherence time of $T_0 = 3$s and the associated optimal cutoff time of $\tau = 0.39$s as seen in Figure 5.3 below.

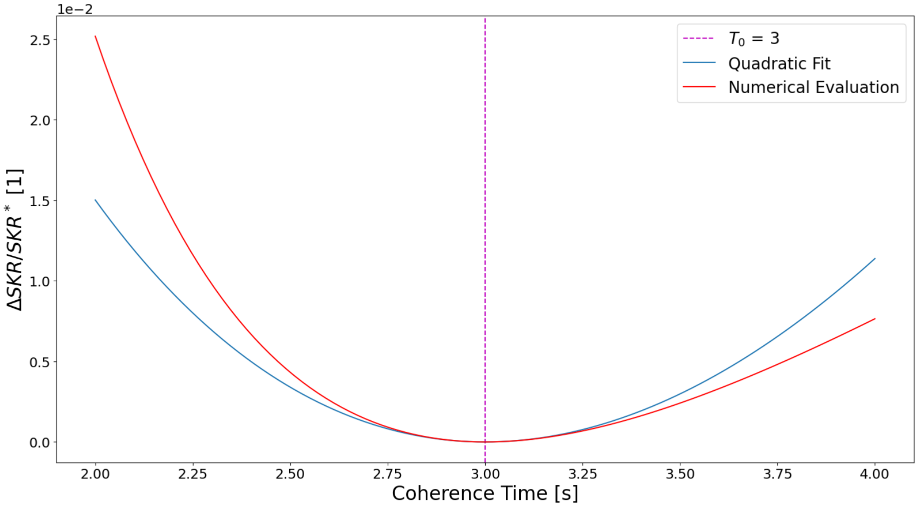


Figure 5.3: Loss in secret key rate relative to an optimal secret key rate SKR^* for a drift in coherence time. We plot the quadratic fit (blue), the numerically evaluated loss (red) and the chosen mean coherence time T_0 for the quadratic fit (magenta vertical line).

Since the second-order approximation loses all information about asymmetries, it weighs lower and higher coherence times equally - whereas shown before the optimal cutoff, and therefore the secret key rate is more sensitive to deviations when the coherence time is low as opposed to when the coherence times are high. Since for higher coherence times (i.e. when using coherence times of the order $T = 10$s) the sensitivity is lower, and thus a lower loss, the approximation is more accurate as the deviations become more symmetrical around T_0.

To evaluate the accuracy of the approximation, introduce the accuracy score

$$\delta = \frac{\Delta SKR^{\text{num}}}{SKR^*} - B \cdot \left(\frac{\Delta T}{T_0}\right)^2, \tag{5.4}$$

where the first term $\Delta SKR^{\text{num}}/SKR^*$ is the difference in loss evaluated numerically with respect to SKR^* and the second term is the second-order approximation. This accuracy score gives information on *how accurate the approximation compared to the real value is.*

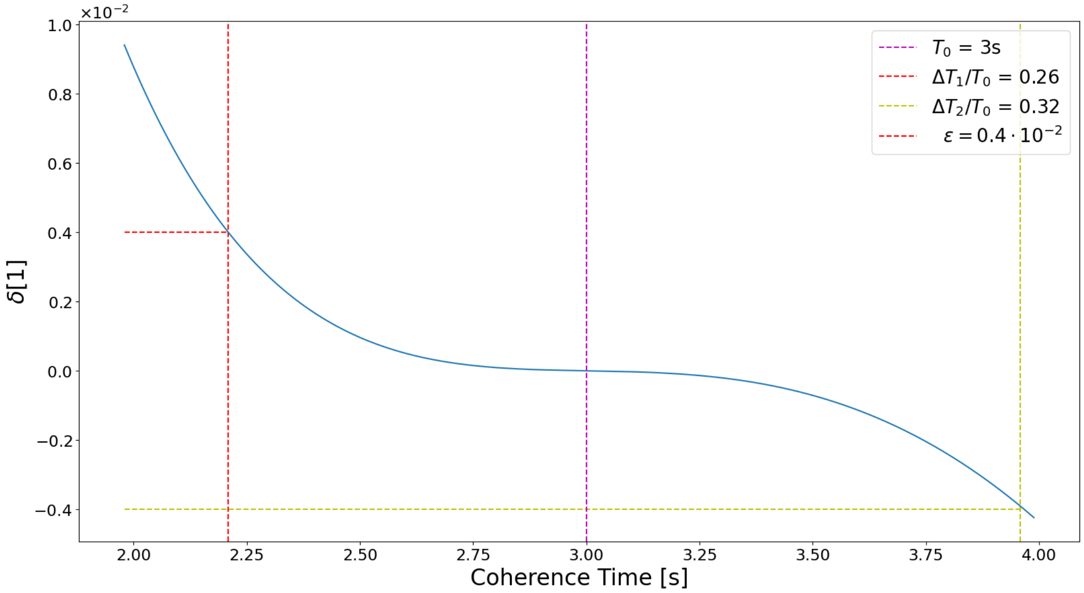


Figure 5.4: Accuracy score δ as a function of the coherence change ΔT. We choose error thresholds ε indicated by the red and yellow horizontal line intersecting the accuracy score (blue). The chosen mean coherence time T_0 in magenta.

Doing this for the coherence time $T_0 = 3$s, we set a maximal error threshold ε, in this case, $\varepsilon = 0.4 \cdot 10^{-2}$. Figure 5.4 shows the accuracy δ in blue, with the magenta line the chosen T_0 where $\delta = 0$. Finding the intersection of the error threshold with our blue curve (red and yellow line), one can find two ranges for the coherence time, ΔT_1 (red) and ΔT_2 (yellow). Thus the range of validity in this given example is

$$\Rightarrow T_0 \pm \min(\Delta T_1, \Delta T_2) = T_0 \pm 0.26 \cdot T_0. \tag{5.5}$$

5.4 Comparing high and low sensitivity regimes

Thus, so far, we can state the following points:

- Given Equation 5.3 we can calculate the approximate loss in secret key rate when having a drift in coherence time.
- With Equation 5.4 we introduce an accuracy score to investigate how good our second-order approximation is to the numerical loss in secret key rate.
- From this accuracy score, and by setting a certain error threshold, we can get a range of validity where our approximation is below this threshold.

We can thus make statements about the *approximate* loss in secret key rate. Now, in Figure 5.2, we can see that **decreasing** the coherence time **increases** the sensitivity, and therefore the loss also increases, whereas **increasing** the coherence time **decreases** the sensitivity and the loss.

We can see this when plotting the loss in secret key rate in Figure 5.4, where the numerically evaluated loss has an asymmetry around the mean T_0, whereas our quadratic fit is symmetric around T_0.

Comparing these higher and lower sensitivity regimes, we conclude that it might be possible to argue that the second-order approximation is a lower bound when drifting towards lower coherence times and an upper bound when drifting towards higher coherence times. If it is indeed a bound needs to be proven mathematically, to be able to make such statements and therefore further research is necessary.

Chapter 6

Conclusions and outlook

We summarize the results obtained in this thesis and conclude with ideas that might extend on the work done so far.

6.1 Summary and conclusions

The aim of this thesis was to gain an understanding on what effect a drift in coherence time might have on a system with two end-nodes and one quantum repeater using cutoff times. We achieved this by considering depolarizing noise for the memory to keep the results independent of the specific physical implementation.

In Chapter 4, we introduce two things: First, what is meant by a drift in the coherence time - a fluctuation around a coherence time T_0 with maximal deviations $\pm\delta T$. To gain a deeper insight into how fluctuations around a coherence time impact the secret key rate, we plot the secret key rate for a coherence time T_0 as well as a lower and higher coherence time. We consider coherence times $T_0 \sim \Delta t/p$ as well as for the cases where $T_0 \gg \Delta t/p$, where $\Delta t/p$ is the average time it takes for one link to be created. The cutoff has the most significant impact whenever the coherence time is close to $\Delta t/p$. Having seen the differences in cutoff times for different coherence times motivates us to delve into the second point, to numerically evaluate the optimal cutoff as a function of the coherence time. Using these cutoffs, the maximal gain one can achieve for the secret key rate when using a cutoff time is compared to the secret key rate in the absence of such a cutoff time. In the vicinity of $T \sim \Delta t/p$ the gain is the greatest and keeps decreasing rapidly towards zero.

Chapter 4 also introduces the analytical condition of finding the cutoff time that maximizes the secret key rate. We were unable to analytically express the cutoff time as a function of the coherence time. Nonetheless, this condition was further used to express the first-order approximation to the cutoff as a function of the coherence time, $\Delta\xi = A \cdot \Delta T$. This allows us to find a relationship between the cutoff and the coherence time. Additionally, we analyzed how sensitive the cutoff is to variations in the coherence time by calculating the derivative of the cutoff time with respect to the coherence time, $d\tau/dT$. Calculating this derivative, is equal to calculating the first-order approximation and then evaluating A for all coherence times and associated optimal cutoffs. Evaluating the derivative of the cutoff time showed that the cutoff is very sensitive whenever the coherence time is of the same order as $\Delta t/p$.

Finally, Chapter 5 introduces what is meant by the loss in secret key rate when experiencing a drift in coherence time. It was defined as the difference in secret key rate for the case when the cutoff was optimized for the maximal drift ($\xi(T_0 \pm \delta T)$) and the case where the cutoff was optimized for the mean value (ξ_0). The loss in secret key rate was approximated to second-order in ΔT, for the expected coherence time T_0 and the cutoff ξ_0. The second-order approximation yields a concise expression for the loss as a function of ΔT. This approximation is less accurate the smaller the coherence time gets. Still, due to the asymmetry in the loss, it empirically seems it could be used as a lower bound when the deviation is negative ($T_0 - \delta T$) and as an upper bound when the deviation is positive ($T_0 + \delta T$).

6.2 Future outlook

Many approaches were considered and investigated during this project, yet not all were fruitful. Nevertheless, they might inspire further work on understanding how a drift in coherence time might affect the secret key rate.

A closed-form solution of the optimal cutoff as a function of the coherence time is useful in delivering more precise statements about the loss in secret key rate as well as the sensitivity. Due to the complicated nature of Equation 4.7 it is not easy to explicitly solve this for a cutoff ξ. A possible approach might be to try and find an approximate closed-form of the cutoff as a function of the coherence time. The following points might also help as a starting point,

Approximating equations:
We were unable to explicitly solve the equations for the optimal secret key rate for a specific cutoff ξ. Following approximations might yield a solution:

- Approximating the binary entropy function could yield a solvable model in the sense that $\ln(1-x) \approx -x$ for small x could be used. Another solution might be to use an alternate function that approximates the binary function.
- Approximating terms involving exponentials. Terms containing $\xi \cdot \beta = \frac{\tau}{T}$ might be approximated by $e^{-\beta\xi} \approx 1 - \beta\xi$. For the values used for p and Δt (Chapter 4), $\xi \cdot \beta$ empirically does not seem to exceed a value of 0.4 thus keeping the error of this approximation to $\approx 10\%$.
- Approximating terms containing $q^{\xi} = (1-p)^{\xi} \approx e^{-\xi \cdot p}$, for small values of p, similar to [60]. Taylor approximating this seems to only hold for small values of the cutoff ξ, and the more this increases, the more significant the error.

Exponential distribution:
Instead of using the geometric distribution as a probability mass function, one could replace this with an exponential distribution similar to [60, 61]. For small values of p, this is again a useful approximation and might help find a closed-form expression for the cutoff as a function of the coherence time. The ideal route would be to find this closed-form expression using the exponential distribution and then using it as the optimal cutoff for the model presented here using the geometric distribution.

Fitting a function:
Given the numerically found cutoff times, one can fit a function using a least-squares method. Given the function's form, this might help figure out which terms in Equation 4.7 might be negligible or could be simplified.

Using the optimal cutoff times for the loss:
Assuming a closed-form of the cutoff ξ is found, one could then calculate the loss in secret key rate (Chapter 5) directly. Whether doing this will lead to a more accurate result depends on the accuracy of the closed-form expression.

New parameter:
An interesting idea might be to introduce a new parameter that is a function of both the coherence time and the cutoff time, i.e., involving $\frac{\tau}{T} = \xi\beta$. This would reduce the space of parameters and might help simplify the search for an optimal secret key rate. Nonetheless, terms containing either the coherence time or the cutoff will need

to be replaced accordingly as this might raise issues.

Multiple nodes:
Using numerical simulations (Netsquid) to verify how the loss in secret key rate scales for multiple nodes. Having found an expression for the loss in secret key rate in the case of the three node network, it might be possible to extend the loss to larger networks using Netsquid. Since we are dealing with a depolarizing channel, we would expect the maximal noise to scale exponentially with the number of nodes. Using a *swap-asap* scheme [62] we might be able to perform better than this when looking at the *loss in secret key rate with drift.* The problem that might arise here is the long time it takes to optimize a cutoff time for a coherence time in Netsquid.

References

[1] Richard P Feynman. "Simulating physics with computers". In: *Feynman and computation.* CRC Press, 2018, pp. 133–153.

[2] Peter W Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th annual symposium on foundations of computer science.* Ieee. 1994, pp. 124–134.

[3] Claude Elwood Shannon. "A mathematical theory of communication". In: *The Bell system technical journal* 27.3 (1948), pp. 379–423.

[4] Charles H Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *arXiv preprint arXiv:2003.06557* (2020).

[5] Manuel Castells. "The impact of the internet on society: a global perspective". In: *Change* 19 (2014), pp. 127–148.

[6] Stephanie Wehner, David Elkouss, and Ronald Hanson. "Quantum internet: A vision for the road ahead". In: *Science* 362.6412 (2018), eaam9288.

[7] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. "Universal blind quantum computation". In: *2009 50th Annual IEEE Symposium on Foundations of Computer Science.* IEEE. 2009, pp. 517–526.

[8] William K Wootters and Wojciech H Zurek. "A single quantum cannot be cloned". In: *Nature* 299.5886 (1982), pp. 802–803.

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

[10] Simon Baier et al. "Realization of a Multi-Node Quantum Network of Remote Solid-State Qubits". In: *Quantum Information and Measurement.* Optical Society of America. 2021, M2A–2.

[11] Roberto Ferrara. *Lecture Notes for Algorithms in Quantum Theory.* Dec. 2020.

[12] Michael A Nielsen and Isaac Chuang. *Quantum computation and quantum information.* 2002.

[13] Wojciech Kozlowski and Stephanie Wehner. "Towards large-scale quantum networks". In: *Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication.* 2019, pp. 1–7.

[14] Michael Wolf. *Mathematical Introduction to Quantum Information Processing.* June 2019.

[15] Stefano Pirandola et al. “Advances in quantum cryptography”. In: *Advances in Optics and Photonics* 12.4 (2020), pp. 1012–1236.

[16] Mark M Wilde. “From classical to quantum Shannon theory”. In: *arXiv preprint arXiv:1106.1445* (2011).

[17] Renato Renner. “Security of quantum key distribution”. In: *International Journal of Quantum Information* 6.01 (2008), pp. 1–127.

[18] Valerio Scarani et al. “The security of practical quantum key distribution”. In: *Reviews of modern physics* 81.3 (2009), p. 1301.

[19] Igor Devetak and Andreas Winter. “Distillation of secret key and entanglement from quantum states”. In: *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences* 461.2053 (2005), pp. 207–235.

[20] Renner Renato, N Gisin, and B Kraus. “An information-theoretic security proof for QKD protocols”. In: *Phys Rev A (arXiv: quant-ph/0502064)* 72.1 (2005).

[21] Boxi Li, Tim Coopmans, and David Elkouss. “Efficient optimization of cut-offs in quantum repeater chains”. In: *2020 IEEE International Conference on Quantum Computing and Engineering (QCE)*. IEEE. 2020, pp. 158–168.

[22] Gláucia Murta et al. “Key rates for quantum key distribution protocols with asymmetric noise”. In: *Physical Review A* 101.6 (2020), p. 062321.

[23] Hang Liu et al. “Tight finite-key analysis for quantum key distribution without monitoring signal disturbance”. In: *npj Quantum Information* 7.1 (2021), pp. 1–6.

[24] Lana Sheridan, Thinh Phuc Le, and Valerio Scarani. “Finite-key security against coherent attacks in quantum key distribution”. In: *New Journal of Physics* 12.12 (2010), p. 123019.

[25] Ian George, Jie Lin, and Norbert Lütkenhaus. “Numerical calculations of the finite key rate for general quantum key distribution protocols”. In: *Physical Review Research* 3.1 (2021), p. 013274.

[26] Sreraman Muralidharan et al. “Optimal architectures for long distance quantum communication”. In: *Scientific reports* 6.1 (2016), pp. 1–10.

[27] Filip Rozpedek et al. “Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission”. In: *Physical Review A* 99.5 (2019), p. 052330.

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

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

[30] Stefan Langenfeld et al. “Quantum repeater node demonstrating unconditionally secure key distribution”. In: *Physical Review Letters* 126.23 (2021), p. 230506.

[31] Riccardo Bassoli et al. “Quantum communication networks”. In: *Foundations in Signal* (2021).

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

[33] Wolfgang Dür and Hans J Briegel. “Entanglement purification and quantum error correction”. In: *Reports on Progress in Physics* 70.8 (2007), p. 1381.

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

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

[36] Wojciech Hubert Zurek. “Decoherence, einselection, and the quantum origins of the classical”. In: *Reviews of modern physics* 75.3 (2003), p. 715.

[37] Dave Morris Bacon. *Decoherence, control, and symmetry in quantum computers.* University of California, Berkeley, 2001.

[38] Daniel A Lidar and K Birgitta Whaley. “Decoherence-free subspaces and subsystems”. In: *Irreversible quantum dynamics.* Springer, 2003, pp. 83–120.

[39] Mahdi Naghiloo. “Introduction to experimental quantum measurement with superconducting qubits”. In: *arXiv preprint arXiv:1904.09291* (2019).

[40] Robert S Sutor. *Dancing with Qubits: How quantum computing works and how it can change the world.* Packt Publishing Ltd, 2019.

[41] David Press et al. “Ultrafast optical spin echo in a single quantum dot”. In: *Nature Photonics* 4.6 (2010), pp. 367–370.

[42] Swamit S Tannu and Moinuddin K Qureshi. “Not all qubits are created equal: a case for variability-aware policies for NISQ-era quantum computers”. In: *Proceedings of the Twenty-Fourth International Conference on Architectural Support for Programming Languages and Operating Systems.* 2019, pp. 987–999.

[43] Michiel Adriaan Rol. “Control for programmable superconducting quantum systems”. In: (2020).

[44] Michael J Biercuk et al. “Optimized dynamical decoupling in a model quantum memory”. In: *Nature* 458.7241 (2009), pp. 996–1000.

[45] Pengfei Wang et al. “Single ion-qubit exceeding one hour coherence time”. In: *arXiv preprint arXiv:2008.00251* (2020).

[46] Joshua Nunn. “Quantum memory in atomic ensembles”. In: (2008).

[47] Thierry Chanelière, Gabriel Hétet, and Nicolas Sangouard. “Quantum optical memory protocols in atomic ensembles”. In: *Advances In Atomic, Molecular, and Optical Physics.* Vol. 67. Elsevier, 2018, pp. 77–150.

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

[49] Andreas Reiserer et al. “Robust quantum-network memory using decoherence-protected subspaces of nuclear spins”. In: *Physical Review X* 6.2 (2016), p. 021040.

[50] Hannes Bernien et al. “Heralded entanglement between solid-state qubits separated by three metres”. In: *Nature* 497.7447 (2013), pp. 86–90.

[51] Laszlo Gyongyosi and Sandor Imre. “Optimizing high-efficiency quantum memory with quantum machine learning for near-term quantum devices”. In: *Scientific reports* 10.1 (2020), pp. 1–24.

[52] Chiara Macchiavello, G Massimo Palma, and Shashank Virmani. “Entangled states maximize the two qubit channel capacity for some Pauli channels with memory”. In: *arXiv preprint quant-ph/0307016* (2003).

[53] A Yu Kitaev. “Fault-tolerant quantum computation by anyons”. In: *Annals of Physics* 303.1 (2003), pp. 2–30.

[54] Kenneth Rozpedek Filip arond Goodenough et al. “Parameter regimes for a single sequential quantum repeater”. In: *Quantum Science and Technology* 3.3 (2018), p. 034002.

[55] Guus Avis. To be published.

[56] John G Webster and Halit Eren. *Measurement, Instrumentation, and Sensors Handbook: Two-Volume Set.* CRC press, 2018.

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

[58] Julian Rabbie et al. “Designing quantum networks using preexisting infrastructure”. In: *npj Quantum Information* 8.1 (2022), pp. 1–12.

[59] David M Pozar. *Microwave engineering.* John wiley & sons, 2011.

[60] Viacheslav V Kuzmin and Denis V Vasilyev. “Diagrammatic technique for simulation of large-scale quantum repeater networks with dissipating quantum memories”. In: *Physical Review A* 103.3 (2021), p. 032618.

[61] Tim Coopmans, Sebastiaan Brand, and David Elkouss. “Improved analytical bounds on delivery times of long-distance entanglement”. In: *Physical Review A* 105.1 (2022), p. 012608.

[62] Tim Coopmans et al. “Netsquid, a network simulator for quantum information using discrete events”. In: *Communications Physics* 4.1 (2021), pp. 1–15.

[63] Gareth James et al. *An introduction to statistical learning.* Vol. 112. Springer, 2013.

Appendix A

Proofs

A.1 Expectation values for the QBER

No cutoff: Given a random variable n_i that follows a geometric distribution with parameter p, we can then calculate the expectation value of the exponential with some parameter a as,

$$\begin{aligned}
\left\langle e^{-a \cdot n_i} \right\rangle &= \sum_{j=1}^{\infty} p(1-p)^{j-1} \cdot e^{-aj} && \text{(A.1)} \\
&= pe^{-a} \sum_{k=0}^{\infty} (e^{-a}(1-p))^k && \text{(A.2)} \\
&= \frac{pe^{-a}}{1 - e^{-a}(1-p)} && \text{(A.3)} \\
&= \frac{p}{p + e^{a} - 1} && \text{(A.4)}
\end{aligned}$$

Using a cutoff: Given a random variable n_i that follows a geometric distribution with parameter p, we can then calculate the expectation value of the exponential with some parameter a for the first trials until the cutoff rounds n_{cut} are reached as [54],

$$\left\langle e^{-a\cdot n_i}\right\rangle = \frac{\sum_{j=1}^{n_{\text{cut}}} p(1-p)^{j-1}\cdot e^{-aj}}{\sum_{j=1}^{n_{\text{cut}}} p(1-p)^{j-1}} \tag{A.5}$$

$$= \frac{pe^{-a}}{1-(1-p)^{n_{\text{cut}}}}\frac{1-((1-p)e^{-a})^{n_{\text{cut}}}}{1-e^{-a}(1-p)} \tag{A.6}$$

A.2 Bell states in X - Basis

Using the states in basis states, we can rewrite the Bell states as

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|{+}{+}\right\rangle + \left|{-}{-}\right\rangle\right), \quad \left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|{+}{-}\right\rangle - \left|{-}{+}\right\rangle\right), \tag{A.7a}$$

$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|{+}{+}\right\rangle - \left|{-}{-}\right\rangle\right), \quad \left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|{+}{-}\right\rangle - \left|{-}{+}\right\rangle\right). \tag{A.7b}$$

A.3 Symmetry of the Werner state $\rho(w)$

For simplicity, assuming our state is in Werner form with the Bell state $|\phi^+\rangle$,

$$\rho(w) = w\left|\phi^+\right\rangle\left\langle\phi^+\right| + (1-w)\frac{\mathbb{1}}{4}. \tag{A.8}$$

We want to show that our QBER in the X - and Z - basis is equal.
Proof: We can write $e_Z(w)$ in the Z - Basis as

$$\begin{aligned}
e_Z(w) &= \langle 01|\,\rho(w)\,|01\rangle + \langle 10|\,\rho(w)\,|10\rangle \\
&= w\left\langle 01\middle|\phi^+\right\rangle\left\langle\phi^+\middle|01\right\rangle + (1-w)\langle 01|\,\frac{\mathbb{1}}{4}\,|01\rangle + w\left\langle 10\middle|\phi^+\right\rangle\left\langle\phi^+\middle|10\right\rangle + (1-w)\langle 10|\,\frac{\mathbb{1}}{4}\,|10\rangle \\
&= w\left(\left|\left\langle 01\middle|\phi^+\right\rangle\right|^2 + \left|\left\langle 10\middle|\phi^+\right\rangle\right|^2\right) + \frac{1-w}{2} \\
&= \frac{1-w}{2}
\end{aligned}$$

and in the X - basis as

$$\begin{aligned}
e_X(w) &= \langle +-|\, \rho(w)\, |+-\rangle + \langle -+|\, \rho(w)\, |-+\rangle \\
&= w \left\langle +- \middle| \phi^+ \right\rangle \left\langle \phi^+ \middle| +- \right\rangle + (1-w) \langle +-|\, \frac{\mathbb{1}}{4}\, |+-\rangle + w \left\langle -+ \middle| \phi^+ \right\rangle \left\langle \phi^+ \middle| -+ \right\rangle + (1-w) \langle -+|\, \frac{\mathbb{1}}{4}\, |-+\rangle \\
&= w \left(\left| \left\langle +- \middle| \phi^+ \right\rangle \right|^2 + \left| \left\langle -+ \middle| \phi^+ \right\rangle \right|^2 \right) + \frac{1-w}{2} \\
&= \frac{1-w}{2}
\end{aligned}$$

since we can write our Bell state in X - basis as $|\phi^+\rangle \propto |{+}{+}\rangle + |{-}{-}\rangle$.

Appendix B

Derivatives

Throughout this work we used the derivative of the secret key rate but did not explicitly write out every term. This appendix will serve to show the derivatives used. To aid in readability, we will introduce a few abbreviations:

$$q = 1 - p, \quad \textit{probability of failure.} \tag{B.1a}$$

$$\beta = \frac{\Delta t}{T}, \quad \textit{decay factor.} \tag{B.1b}$$

$$\mu = qe^{-\beta}, \quad \textit{decayed probability of failure.} \tag{B.1c}$$

$$e_\theta = \frac{e_z}{1 - e_z} \quad . \tag{B.1d}$$

B.1 Derivatives of the rate, distribution time and the secret key rate

Finding the partial derivatives leads to

$$
\begin{aligned}
\partial_\xi SKR &= \frac{\langle DT\rangle \partial_\xi r - \partial_\xi \langle DT\rangle r}{\langle DT\rangle^2}, && \text{(B.2)}\\
\partial_T\partial_\xi SKR &= \frac{\langle DT\rangle \partial_T\partial_\xi r - \partial_\xi \langle DT\rangle \partial_T r}{\langle DT\rangle^2}, && \text{(B.3)}\\
\partial_\xi^2 SKR &= \frac{\partial_\xi^2 r \langle DT\rangle + \partial_\xi r \partial_\xi \langle DT\rangle - \partial_\xi r \partial_\xi \langle DT\rangle - r\partial_\xi^2 \langle DT\rangle}{\langle DT\rangle^4} - \partial_\xi SKR \cdot \frac{\partial_\xi \langle DT\rangle}{\langle DT\rangle},\\
&= \frac{\partial_\xi^2 r \langle DT\rangle - r\partial_\xi^2 \langle DT\rangle}{\langle DT\rangle^4} - \partial_\xi SKR \cdot \frac{\partial_\xi \langle DT\rangle}{\langle DT\rangle},\\
&= \frac{\partial_\xi^2 r \langle DT\rangle - r\partial_\xi^2 \langle DT\rangle}{\langle DT\rangle^4}. && \text{(B.4)}
\end{aligned}
$$

In the last step we used, the partial derivative of the secret key rate vanishes if evaluated at the optimal cutoff i.e. $\partial_\xi SKR = 0$ evaluated at ξ_0.

As a next step, we will find the partial derivatives with respect to the cutoff and the coherence time. We note that the distribution time is only explicitly a function of the cutoff and not the coherence time, $\langle DT\rangle = \langle DT\rangle(\xi)$. The rate is explicitly dependent on the cutoff as well as the coherence time $r = r(T, \xi)$. Thus, the partial derivatives of the rate can be found to be

$$
\begin{aligned}
\partial_j r &= \frac{2}{\ln 2}\left[\partial_j e_z \cdot \ln e_\theta\right], \quad \text{For } j \in \{T, \xi\}, && \text{(B.5)}\\
\partial_j\partial_i r &= \frac{2}{\ln 2}\left[\partial_j\partial_i e_z \cdot \ln e_\theta + \frac{\partial_i e_z \partial_j e_z}{e_z(1-e_z)}\right], && \text{(B.6)}\\
\partial_T\partial_\xi r &= \frac{2}{\ln 2}\left[\partial_T\partial_\xi e_z \cdot \ln e_\theta + \frac{\partial_\xi e_z \partial_T e_z}{e_z(1-e_z)}\right], && \text{(B.7)}\\
\partial_\xi^2 r &= \frac{2}{\ln 2}\left[\partial_\xi^2 e_z \ln e_\theta + \frac{(\partial_\xi e_z)^2}{e_z(1-e_z)}\right], && \text{(B.8)}\\
\partial_T^2 r &= \frac{2}{\ln 2}\left[\partial_T^2 e_z \ln e_\theta + \frac{(\partial_T e_z)^2}{e_z(1-e_z)}\right]. && \text{(B.9)}
\end{aligned}
$$

Similar to the rate r, we find the derivatives of the distribution time $\langle DT\rangle$ with respect to the cutoff ξ and rewrite them as functions of the distribution time,

$$\partial_\xi \langle DT \rangle = \frac{\Delta t}{p} \ln(q) \frac{q^\xi}{[1-q^\xi]^2} = \ln(q) \frac{q^\xi}{(2-q^\xi)(1-q^\xi)} \cdot \langle DT \rangle \,, \tag{B.10}$$

$$\partial_\xi^2 \langle DT \rangle = \frac{\Delta t}{p} \left(\frac{q^\xi (q^\xi + 1) \ln^2 q}{(1-q^\xi)^3} \right) = \left(\frac{q^\xi (q^\xi + 1) \ln^2 q}{(2-q^\xi)(1-q^\xi)^2} \right) \cdot \langle DT \rangle \,. \tag{B.11}$$

B.2 Derivatives for the QBER

The main difficulty, both in terms of finding the derivatives as well as in writing the equations in a concise form, lies in the QBER. The QBER can be rewritten as

$$e_z = \frac{1}{2} - \frac{1}{2} \frac{pe^{-\beta}}{1-q^\xi} \frac{1-\mu^\xi}{1-\mu} = \frac{1}{2} - \omega \cdot (1-\mu^\xi), \tag{B.12}$$

where we introduce $\omega = \frac{pe^{-\beta}}{2(1-\mu)(1-q^\xi)}$, for conciseness. This factor appears in the derivatives as well, making the formulas shorter. Next, we need to use the derivatives for the formerly introduced factor as well as the decay factor β and the decayed probability of failure μ.

These derivatives can be found to be

$$\begin{aligned} \partial_T \beta &= -\frac{\beta}{T}, \\ \partial_\xi \mu^\xi &= \mu^\xi (\ln q - \beta) = \mu^\xi \ln \mu, \quad \partial_T \mu^\xi = \frac{\beta}{T} \xi \mu^\xi, \\ \partial_\xi \omega &= \omega \cdot \frac{q^\xi}{1-q^\xi} \ln q, \qquad \partial_T \omega = \omega \cdot \frac{\beta}{T} \frac{1}{1-\mu}. \end{aligned}$$

$$\partial_\xi e_z = \omega \cdot \left[\ln q \frac{q^\xi - \mu^\xi}{q^\xi - 1} - \beta \mu^\xi\right] \tag{B.13}$$

$$\partial_\xi^2 e_z = -\omega \left\{ \frac{2\beta \ln q \mu^\xi}{1 - q^\xi} + \frac{(q^\xi + 1)\ln^2 q (q^\xi - \mu^\xi)}{(1 - q^\xi)^2} - \beta^2 \mu^\xi \right\} \tag{B.14}$$

$$\partial_T e_Z = \frac{\beta}{T} \omega \left(\xi \mu^\xi - \frac{1 - \mu^\xi}{1 - \mu} \right) \tag{B.15}$$

$$\begin{aligned} \partial_T \partial_\xi e_z &= -\frac{\beta}{2T} \frac{p e^{-\beta}}{(1 - q^\xi)^2} \frac{1}{1 - \mu} \left\{ \mu^\xi [(1 - \beta\xi)(1 - q^\xi) + \xi \ln(q)] + \frac{\ln(q)(q^\xi - \mu^\xi) + \beta \mu^\xi (1 - q^\xi))}{1 - \mu} \right\} \\ &= -\frac{\beta}{T} \frac{\omega}{1 - q^\xi} \left\{ \mu^\xi [(1 - \beta\xi)(1 - q^\xi) + \xi \ln(q)] + \frac{\ln(q)(q^\xi - \mu^\xi) + \beta \mu^\xi (1 - q^\xi))}{1 - \mu} \right\} \end{aligned} \tag{B.16}$$

Appendix C

Optimal cutoff time as function of the coherence time

To find the optimal cutoff time, we use Algorithm 1. We will show a few examples for the measured run-time. This algorithm may be optimized as to improve the speed.

We use the algorithm from Chapter 4 to find the optimal cutoff for different ranges of the coherence time. Seen in Table C.1, are the different run times, where N_T is the number of elements the coherence time list has, N_τ is the number of elements of the optimal cutoff time list, T is the range of the coherence times, and t_{run} run is the run time.

T [s]	N_T	N_τ	t_{run} [s]
$[0.01, 4]$	10^4	10^3	866
$[2, 4]$	$5 \cdot 10^3$	$5 \cdot 10^3$	2002
$[7.9, 12.1]$	$5 \cdot 10^3$	$5 \cdot 10^3$	1978
$[0.1, 0.5]$	$5 \cdot 10^3$	$5 \cdot 10^3$	1998

Table C.1: Run-time of Algorithm 1

Inspired by [63], we define the normalized residual e, which is the difference between the numerical value of the optimal cutoff time τ^{num} and the estimated, or rather linearized value for the cutoff time τ^{lin}

$$\mathrm{e} = \frac{\tau^{\mathrm{num}} - \tau^{\mathrm{lin}}}{\tau^{\mathrm{num}}}. \tag{C.1}$$

As seen in the figures below, we can linearize the cutoff times up to an error of a few percent for all three mean coherence times. The parabolic form of the residuals indicate a non-linear relationship of the optimal cutoff to the coherence time. As seen from Figure 4.4, the smaller the coherence time, the greater the change in cutoff time with respect to the coherence time. The plots below indicate similar residuals for the different mean coherence times, which could be because the accuracy of the optimal cutoff found numerically is too low. To verify this, we would need to run the algorithm with higher accuracy, which becomes prohibitively expensive for higher coherence times since the relative deviation $\delta T = T_0/n$, where n is an integer, increases rapidly for greater mean coherence times.

If the accuracy is not the problem, it might be that the cutoff changes rapidly for small mean coherence times; however, since we consider relative deviations, this might cancel each other out. *Since we did not come to a conclusion, this discussion was excluded from the main part.*

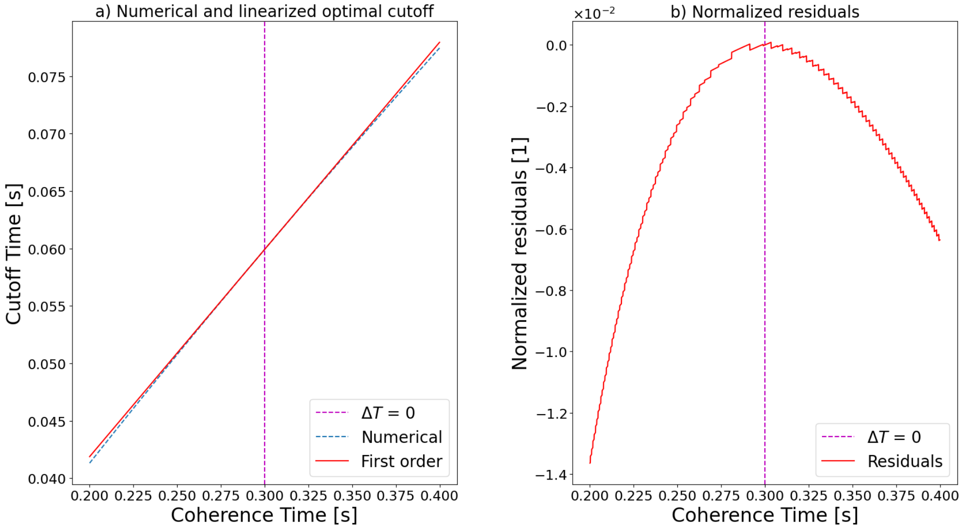


Figure C.1: (a) Numerically found optimal cutoff (dashed blue) and the linearized cutoff (red) for a coherence time $T_0 = 0.3$s and an associated cutoff time $\tau_0 = 0.060$s. (b) Normalized residuals as a function of the coherence time.

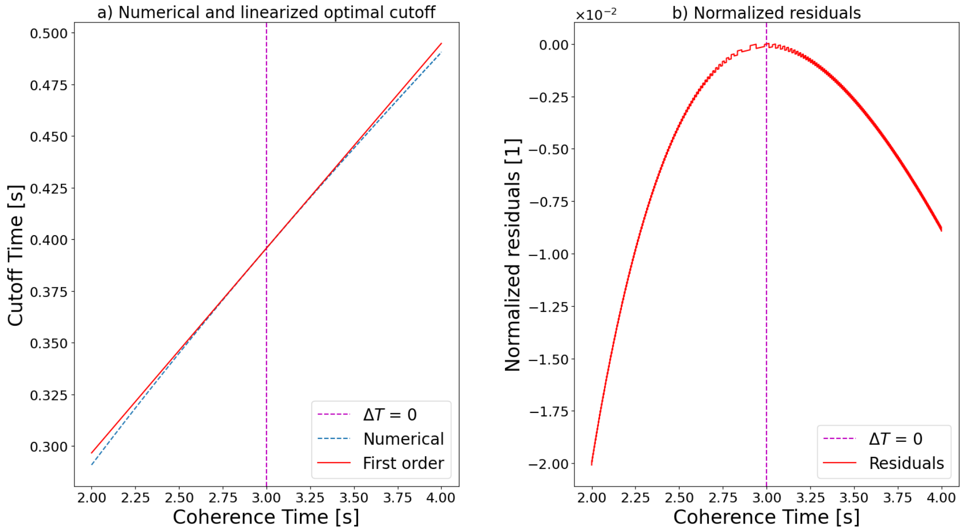


Figure C.2: (a) Numerically found optimal cutoff (dashed blue) and the linearized cutoff (red) for a coherence time $T_0 = 3$s and an associated cutoff time $\tau_0 = 0.396$s. (b) Normalized residuals as a function of the coherence time.

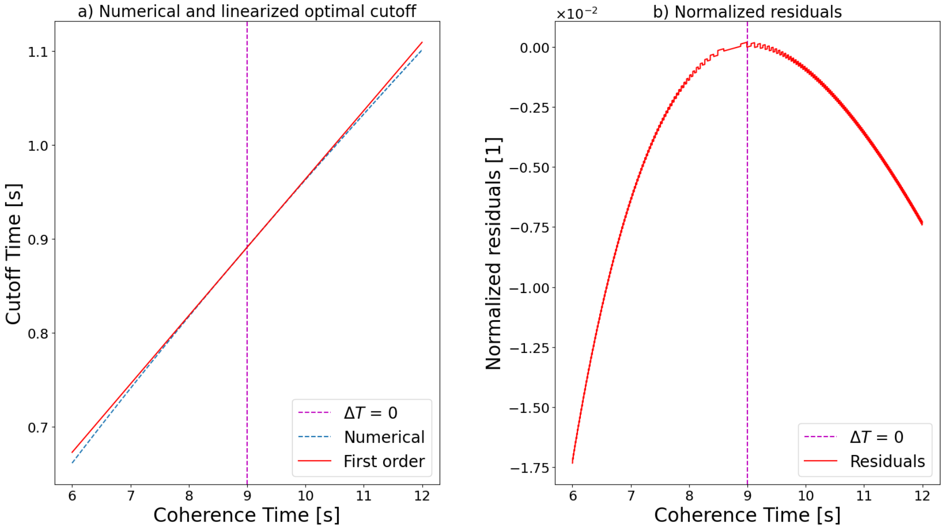


Figure C.3: (a) Numerically found optimal cutoff (dashed blue) and the linearized cutoff (red) for a coherence time $T_0 = 9$s and an associated cutoff time $\tau_0 =$ s. (b) Normalized residuals as a function of the coherence time.