Decoherence Estimation
in Quantum Theory and Beyond

Corsin Pfister
(M.Sc., ETH Zürich)

A thesis submitted for the degree of
Doctor of Philosophy

Centre for Quantum Technologies
National University of Singapore

Declaration

I hereby declare that this thesis is my original work and it has been written by me in its entirety. I have duly acknowledged all the sources of information which have been used in the thesis. This thesis has also not been submitted for any degree in any university previously.

Corsin Pfister
17 May 2016

Acknowledgments

I would like to thank my supervisor, Stephanie Wehner, for allowing me to conduct a PhD in quantum information theory. I am grateful for the effort, time and resources that she invested to make my time as a PhD student a great learning experience. I highly appreciate the personal and scientific freedom that I enjoyed, and I am grateful for her efforts to connect me with many interesting researchers all over the world.

I want to thank my collaborators, Jedrzej Kaniewski, Marco Tomamichel, Atul Mantri, Robert Schmucker, Nathan McMahon, Gerard Milburn, Patrick J. Coles and Norbert Lütkenhaus, who made research a fun experience for me and from whom I learned a lot.

I would like to thank Terry Rudolph, Markus P. Müller, Anthony J. Short, Renato Renner, Robert Spekkens, Lucien Hardy and Norbert Lütkenhaus for their hospitality and for giving me the opportunity to visit their research groups.

I want to express my gratitude to my office mates and group members Marco Tomamichel and Le Phuc Thinh, who spent countless hours answering my questions, discussing things I was interested in and helping me solve difficult problems. I would like to thank Markus P. Müller, Lluis Masanes, Tobias Fritz and Matthew Pusey for many deeply inspiring discussions at multiple occasions and locations as well as through the exchange of lots of emails.

I am indebted to Jedrzej Kaniewski and Filip Rozpedek, who have read a preliminary version of my thesis. I would also like to thank Le Phuc Thinh, Mark Steudtner and David Elkouss for making very useful comments on parts of my thesis.

Special thanks go to Evon Tan and Chantal Smith for their constant efforts to make life at the institute so smooth. Thanks to their outstanding skills in solving administrational problems, I could focus on research. Without their help, my life as a researcher would have been a lot harder.

A big thanks goes to Markus Baden, Nick Lewty, Dominik Stahl, Si-Hui Tan, Martin Isbjörn-Trappe, Sven Hobbie, Cord Müller and many more for spending so many hours of pleasure with me and for making my time in Singapore a very happy one.

Finally, I thank my parents Cornelia and Felix, my brother Nicolin and my beloved girlfriend Dorvis Chung for all their love and support. I am deeply grateful for having you in my life and for feeling your care and support even during times when we live far away from each other.

Abstract

The quantum physics literature provides many different characterizations of decoherence. Most of them have in common that they describe decoherence as a kind of influence on a quantum system upon interacting with an another system. In the spirit of quantum information theory, we adapt a particular viewpoint on decoherence which describes it as the loss of information into a system that is possibly controlled by an adversary. We use a quantitative framework for decoherence that builds on operational characterizations of the min-entropy that have been developed in the quantum information literature. It characterizes decoherence as an influence on quantum channels that reduces their suitability for a variety of quantifiable tasks such as the distribution of secret cryptographic keys of a certain length or the distribution of a certain number of maximally entangled qubit pairs. This allows for a quantitative and operational characterization of decoherence via operational characterizations of the min-entropy.

In this thesis, we present a series of results about the estimation of the min-entropy, subdivided into three parts. The first part concerns the estimation of a quantum adversary's uncertainty about classical information—expressed by the smooth min-entropy—as it is done in protocols for quantum key distribution (QKD). We analyze this form of min-entropy estimation in detail and find that some of the more recently suggested QKD protocols have previously unnoticed security loopholes. We show that the specifics of the sifting subroutine of a QKD protocol are crucial for security by pointing out mistakes in the security analysis in the literature and by presenting eavesdropping attacks on those problematic protocols. We provide solutions to the identified problems and present a formalized analysis of the min-entropy estimate that incorporates the sifting stage of QKD protocols.

In the second part, we extend ideas from QKD to a protocol that allows to estimate an adversary's uncertainty about *quantum* information, expressed by the fully quantum smooth min-entropy. Roughly speaking, we show that a protocol that resembles the parallel execution of two QKD protocols can be used to lower bound the min-entropy of some unmeasured qubits. We explain how this result may influence the ongoing search for protocols for entanglement distribution.

The third part is dedicated to the development of a framework that allows the estimation of decoherence even in experiments that cannot be correctly described by quantum theory. Inspired by an equivalent formulation of the min-entropy that relates it to the fidelity with a maximally entangled state, we define a decoherence quantity for a very general class of probabilistic theories that reduces to the min-entropy in the special case of quantum theory.

This entails a definition of maximal entanglement for generalized probabilistic theories. Using techniques from semidefinite and linear programming, we show how bounds on this quantity can be estimated through Bell-type experiments. This allows to test models for decoherence that cannot be described by quantum theory. As an example application, we devise an experimental test of a model for gravitational decoherence that has been suggested in the literature.

List of Publications

This thesis is based on the following publications and preprints:

- Chapter 5 is based on the publication listed as reference [Pfi+16],

  Sifting attacks in finite-size quantum key distribution
  Corsin Pfister, Norbert Lütkenhaus, Stephanie Wehner and Patrick J. Coles
  New Journal of Physics **18**, 053001 (2016).

- Chapter 6 is based on a yet unpublished paper [Pfi+] with the following preliminary title,

  Capacity tomography of quantum channels with correlated errors
  Corsin Pfister, Atul Mantri, Marco Tomamichel and Stephanie Wehner
  In preparation.

- Chapter 7 is based on the preprint listed as reference [Pfi+15],

  Understanding nature from experimental observations: a theory independent test for gravitational decoherence
  Corsin Pfister, Jedrzej Kaniewski, Marco Tomamichel, Atul Mantri, Robin Schmucker, Nathan McMahon, Gerard Milburn and Stephanie Wehner
  arXiv:1503.00577 [quant-phys]
  (under review at Nature Communications).

During his graduate studies, the author also completed the publication listed as reference [PW13],

An information-theoretic principle implies that any discrete physical theory is classical
Corsin Pfister and Stephanie Wehner
Nature Communications **4**, 1851 (2013).

Contents

Part I

Introduction

Chapter 1

Introduction

Quantum theory describes the laws that govern the behavior of elementary particles. Some phenomena predicted by quantum theory—and observed in laboratories around the world—defy an explanation in terms of the classical laws of physics that we encounter with macroscopic objects in everyday life. In the popular literature, this has led to a mystification of the so-called *quantum effects*. They are often described as *limitations*. For example, Heisenberg's uncertainty principle famously states that one cannot know both the position and the momentum of a particle. Another example is the no-cloning theorem, stating that there cannot be a process that copies an arbitrary quantum state.

Quantum information theory takes a different viewpoint. It does not see the quantum effects as limitations, but instead as useful properties that can be exploited to our benefit (for an interesting exposition of this viewpoint with a historical account, see for example the introduction of the thesis of van Assche [Ass06]). While in general, the range of such useful effects and their suggested applications is very broad, we center our attention on a particular type of phenomenon.

We will discuss *decoherence* and its estimation. Quantum decoherence estimation enables information processing tasks that are impossible to achieve classically. Moreover, we will see how the concept of decoherence estimation can be generalized to more general probabilistic theories that include quantum theory as a special case. We will describe these applications in more detail when we look at the summary of the results of this thesis in section 1.4.

Before we come to that, we start with an informal warm-up. In the following sections, we will recapitulate some of the properties of decoherence processes that have been declared as the defining characteristics of decoherence. There is no commonly accepted definition of decoherence. We will briefly touch on some characterizations that can be found in the literature, but due to the very widespread use of the word, we necessarily miss out some of the meanings behind the term "decoherence". For more extensive treatments of various meanings of decoherence, the reader is advised to consult the corresponding review literature, such as [Zur03], [Sch05].

In this thesis, we adopt a particular viewpoint on decoherence that may be summarized in one sentence as follows: *decoherence is the loss of information into the environment*. This is not a new understanding but rather a viewpoint that is ubiquitous in quantum information science. In the arguably

most well-known textbook on quantum information theory [NC00], Nielsen and Chuang write "A key concept in understanding the merit of a particular quantum computer realization is the notion of *quantum noise* (sometimes called *decoherence*)" and "Generally speaking, anything which causes loss of (quantum) information is a noise process".

We will approach this viewpoint through a series of examples. While many of the characterizations of decoherence refer to the density matrix formalism and are of a more theoretical interest, we aim for an operational and quantitative treatment. The goal of sections 1.2 and 1.3 is to get some intuition about the benefits of such a treatment when dealing with information processing tasks. Before we come to that, we will look at some other characterizations of decoherence in section 1.1.

1.1 What is decoherence?

The origin of the word "decoherence" seems to be unclear. However, it has been an established notion in the physics community, at least since an article by Zurek [Zur91] popularized it to the broader scientific community [Sch05]. Although virtually all quantum physicists have encountered the word "decoherence" and most of them have developed some familiarity with it, there is no generally accepted definition of this term. If you were to ask three physicists what decoherence is, you may very well get three different answers that use very different vocabulary, such as "the vanishing of the off-diagonal terms of a system's density matrix", "the emergence of classical behavior of quantum systems" [Joo+03] or, as mentioned above, "the loss of information into the environment". While each of these explanations is meaningful in its own right, their widespread coexistence illustrates that the term "decoherence" does not refer to one single idea. Instead, it is associated with a multitude of overlapping ideas that share similarities. One such similarity is that most of the characterizations of decoherence can—in some sense—be seen as a loss of information.

To make things more concrete, it is helpful to look at some simple example. Let us consider a spin-$\frac{1}{2}$ particle in the state "up" with respect to the z-direction, $|0\rangle = |\uparrow_z\rangle$. If the spin of this system was measured with respect to the z-direction, it would yield the outcome "up". However, if the system was measured with respect to the x-direction, it would yield the outcomes "up" and "down" with equal probability, because the system is in a superposition of the two eigenstates in the x-direction,

$$|0\rangle = |\uparrow_z\rangle = \frac{|\uparrow_x\rangle + |\downarrow_x\rangle}{\sqrt{2}} = \frac{|+\rangle + |-\rangle}{\sqrt{2}}\,. \tag{1.1}$$

This situation changes if the measurements are carried out after a dynamic evolution of the system. If the particle undergoes some process in which it interacts with another system, its state will change and, in general, it will no longer be a pure state but instead become mixed (see figure 1.1). In the most extreme case, the state will become the fully mixed state $\mathbb{1}/2$.

While this state would still reproduce the same probability distribution if measured along the x-direction, it has lost its spin-information along the z-

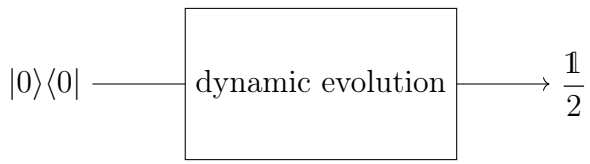


Figure 1.1: A simple decoherence process. We will often consider a decoherence process as a "black box", that is, we only see the system before and after the process, but we do not know what systems it interacts with.

direction. This can also be seen as the state losing its "coherence terms", that is, the off-diagonal terms of the density matrix in the x-basis vanish:

$$|0\rangle\langle 0| = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}_x \quad \mapsto \quad \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}_x = \frac{\mathbb{1}}{2}\,. \tag{1.2}$$

This is sometimes described as decoherence.

The loss of the coherence terms is often interpreted as a loss of *phase information*. To see why, let us consider a different type of system. Instead of a spin-$\frac{1}{2}$ system with the z- and x-direction as bases, let us consider a photon with the diagonal polarizations and the horizontal/vertical polarizations as bases. Consider a beam of diagonally polarized photons sent through a Mach-Zehnder interferometer [Mac92; Zeh91] (see figure 1.2). A polarizing beam splitter (PBS) splits the beam into beams of horizontal and vertical polarization. After travelling through their respective arm, the two beams hit another PBS, and two photon detectors are set up at the two sides of the second PBS to see which exit the photons take. By varying the length difference between the two arms of the interferometer, a relative phase between the horizontal and the vertical component of the beam can be introduced, and the relative detection frequency of the two detectors shows an interference pattern. If the Mach-Zehnder interferometer is modified by removing the second PBS, then the setup constitutes a measurement in the horizontal/vertical basis,[1] which decoheres the photons that were originally diagonally polarized into the fully mixed state. The relative detection frequencies no longer have a dependency on the length of the arms, and hence, phase information is lost.

This description of decoherence as a loss of phase information is rather specific to a particular setting. Moreover, a loss of the coherence terms is basis-specific: while the example above describes full decoherence, leading to the basis-independent fully mixed state, partial decoherence that merely reduces the magnitude of the off-diagonal terms depends on the basis in which the system decoheres. One may therefore want to use another characteristic of an evolution like (1.2) to characterize decoherence: it turns a pure state into a mixed state. An operation that does that can obviously not be unitary, which is another feature of decoherence.

We said that the dynamic evolution of the system is a process in which the system interacts with other systems. For a better understanding of decoherence, it is helpful to incorporate these other systems into the picture. Since

[1] A better way to look at this is that the first PBS entangles the polarization degree of freedom with the path degree of freedom (c.f. the diagram in figure 1.3).

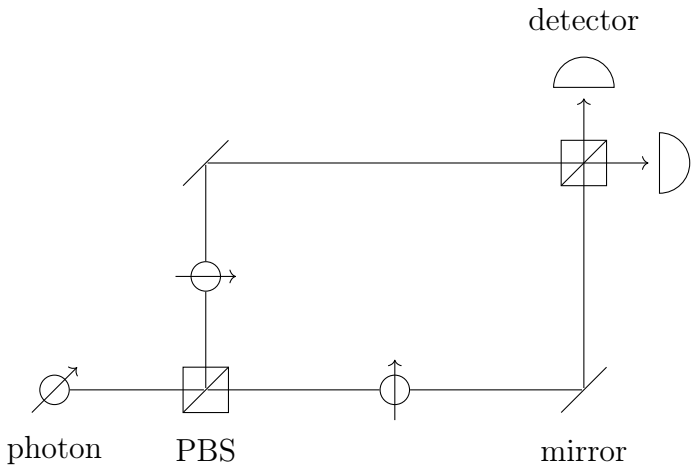


Figure 1.2: Loss of phase information in a modified Mach-Zehnder interferometer. In a Mach-Zehnder interferometer, varying the relative length of the arms yields interference patterns that show the relative phase of the two components. If the second polarizing beam splitter (PBS) is removed, the phase information gets lost.

we have several systems now, it is a good idea to give them their own names. The system of interest that we looked at above shall be denoted by A, and the systems that it interacts with can be grouped together to a system E. The latter is often referred to as the *environment*. Incorporating the environment into the picture leads to a closed system which, according to the postulates of quantum mechanics, evolves unitarily. We shall call this the *purified picture*, in contrast to the single-system picture that we had above in figure 1.1.

Let us consider a concrete example of a dynamic evolution. For our purposes, a particularly useful example is the one in which the environment measures system A in the x-basis, recording the outcome in a system E. As a circuit diagram, this can be written as in figure 1.3.

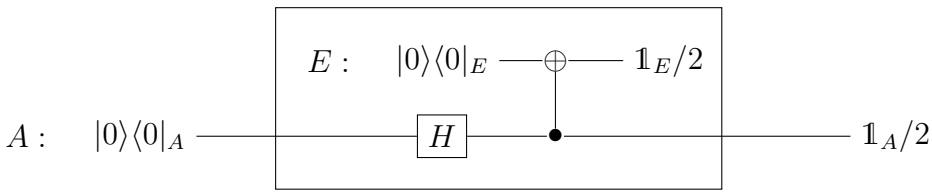


Figure 1.3: Measurement as a unitary evolution. For our purposes, a particularly important example of a decoherence process is a measurement. It fits seamlessly with the axiom of unitary evolution of closed systems. In this diagram, H denotes the *Hadamard gate*, and right of that, we see a *CNOT gate*. The reader unfamiliar with the circuit representation of a measurement is referred to [NC00].

How does the picture change when incorporating system E? The overall process transforms the joint state as

$$|0\rangle_A \otimes |0\rangle_E \quad \mapsto \quad \frac{|0\rangle_A \otimes |0\rangle_E + |1\rangle_A \otimes |1\rangle_E}{\sqrt{2}} =: |\Phi\rangle_{AE}\,, \tag{1.3}$$

that is, it turns the initial product state into an entangled state. In contrast, observing system A alone, we see a transformation which, in the Kraus representation, reads

$$|0\rangle\langle 0| \mapsto \sum_{x=+,-} |x\rangle\langle x||0\rangle\langle 0||x\rangle\langle x| = \frac{\mathbb{1}}{2}\,. \tag{1.4}$$

While, as we noted above, an observer without side information (who sees (1.4)) has lost the information about the z-component of the particle's spin, an observer holding system E has access to that information: (s)he just needs to check in which state system E is in order to know the z-component of the spin. The fact that information is lost in the single-system picture but preserved in the purified picture has led some authors to defining decoherence as "the loss of information into the environment".

Moreover, while the transformation on system A alone, equation (1.2), is not unitary, the measurement as a transformation on the joint system AE *is* unitary (since it can be written as a quantum circuit). Thus, while in the single-system picture, we see a fully mixed output state, the overall state in the purified picture is pure. The coherence terms are preserved, as they can be obtained back by reversing the unitary on AE.

Single-system picture	**Purified picture**
• information lost (z-spin, phase)	• information accessible
• coherence terms lost	• coherence terms preserved
• non-unitary	• unitary
• mixed output state	• pure output state

Table 1.1: Comparison of the single-system picture and the purified picture. Each of the listed differences between the single-system picture (in which the system is an open system) and the purified picture (in which the overall system is closed) can be seen as a characteristic of decoherence.

This discussion gives us some of the characterizations of decoherence in the form of differences between the single-system picture and the purified picture. We have summarized the discussed properties in table 1.1.

1.2 Asymptotic quantification of decoherence

The decoherence process that we considered in the previous section, namely the measurement in figure 1.3 and equation (1.4), is an extreme case of decoherence: the coherence terms vanish completely. In the single-system picture, this can be seen as the action of the *phase damping channel* of full strength (we will discuss channels in more detail in section 3.1.2. In general, the channel is given by

$$\rho_A \mapsto \left(1 - \frac{p}{2}\right)\rho_A + \frac{p}{2}\sigma_x\rho_A\sigma_x\,. \tag{1.5}$$

where σ_x is the Pauli operator

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} . \tag{1.6}$$

For $p = 1$, this gives the same channel as in (1.4), and for $p = 0$, the channel just leaves the system invariant. What about intermediate cases of decoherence? Can the characteristics that we identified in the previous section be used to derive a quantitative measure of decoherence?

The characteristics we identified compare the single-system picture with a purified picture. Thus, if we want to use some characteristics of table 1.1 for a quantification of decoherence, we need to answer the following question. Given a channel

$$\mathcal{C}_A : \rho_A \mapsto \mathcal{C}_A(\rho_A) , \tag{1.7}$$

is there a unitary U_{AE} and an environment system E in a state $|\psi\rangle\langle\psi|_E$ such that

$$\mathrm{tr}(U_{AE}(\rho_A \otimes |\psi\rangle\langle\psi|_E)U_{AE}^\dagger) = \mathcal{C}(\rho_A) \quad \text{for all density operators } \rho_A\,? \tag{1.8}$$

A corollary of the *Stinespring dilation theorem* [Sti55] states that every channel can be extended this way. Such an extension is called a *channel purification*, and for a given channel, all such purifications are equivalent in a certain sense. We will see this more formally in section 3.3, but for now, it is sufficient to know that we can always unambiguously refer to a purification of the channel.

Which of the characteristics of table 1.1 could we use to quantify decoherence? The loss of the coherence terms and the loss of information (in the sense of changing an observable's probability distribution) are unsatisfactory, as they are basis-dependent. There also seems to be no straightforward measure of "non-unitarity". Instead, as a first step towards a quantitative treatment of decoherence, we could use a measure of "mixedness" to compare the single-system picture with the purified picture.

One such measure is the *von Neumann-entropy* H of a system S, defined by

$$H(S) = -\mathrm{tr}(\rho_S \log \rho_S) , \tag{1.9}$$

where log denotes the binary logarithm. It can be seen as such a measure, because $H(S) = 0$ iff ρ_S is pure, and $H(S)$ is maximal when ρ_S is fully mixed. If we compare the mixedness of the overall state with the mixedness of the output state in the single-system picture, we get

$$H(AE) - H(A) = H(AE) - H(E) \tag{1.10}$$
$$=: H(A|E) , \tag{1.11}$$

the first equality follows from the fact that $H(A) = H(E)$ when the state of the system AE is pure. The quantity $H(A|E)$ is called the conditional von Neumann entropy. It can be seen as a measure for how much information an observer holding system E has about system A.

Here, we motivated the conditional von Neumann entropy in a rather ad-hoc way. The purpose of this was just to connect the characteristics of decoherence that are typically stressed in the physics literature with the quantitative treatment that we are aiming for. In quantum information theory, the von Neumann entropy has been formulated in a rigorous framework of axioms and operational characterizations. One such operational characterization is the connection between the *coherent information*, defined by Schumacher and Nielsen [SN96], and the *channel capacity*.

To discuss the coherent information, we need to extend the above picture. For increased convenience in the discussion below, we now distinguish between the input system and the output system of the channel, giving them distinct labels A' and B, respectively (see figure 1.4). Thus, we consider a channel $\mathcal{C}_{A'\to B}$. The initial state $\rho_{A'}$ of the system may not be a pure state, in general. However, we can consider a *purification* of $\rho_{A'}$, that is, a reference system A and a bipartite pure state $|\psi\rangle_{A'A}$ such that $\mathrm{tr}_A(|\psi\rangle\langle\psi|_{A'A}) = \rho_{A'}$ (we will discuss this in more detail in section 3.3).

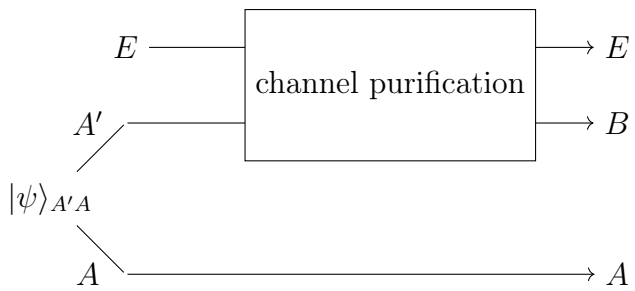


Figure 1.4: Diagram for the coherent information. The initial state $\rho_{A'}$ of the system is purified by a reference system A. Taking this into account, the overall system after the channel consists of three subsystems A, B and E.

In this setting, the coherent information is defined with respect to the state ρ_{AB} as

$$I(A\rangle B)_\rho := H(B) - H(AB) \tag{1.12}$$
$$= -H(A|B)_\rho\,. \tag{1.13}$$

Taking the channel purification E into account, we can write this as

$$I(A\rangle B)_\rho = -H(A|B)_\rho \tag{1.14}$$
$$= H(A|E)\,, \tag{1.15}$$

where the last equality follows from the fact that the overall state ρ_{ABE} is pure [NC00].

The coherent information $I(A\rangle B)_\rho$ has been shown to be related to the quantum channel capacity $Q(\mathcal{C}_{A'\to B})$ of the channel, which is known as the Lloyd-Shor-Devetak (LSD) theorem [Llo97; Sho02; Dev05]. Roughly speaking, the quantum capacity quantifies how much quantum information can be transmitted through the channel (for more information, we refer to quantum

information textbooks such as [Wil13]. The LSD theorem states that

$$Q(\mathcal{C}_{A'\to B}) = \lim_{n\to\infty} \frac{1}{n} \max_{\rho_{(A')^n}\in\mathcal{S}(\mathcal{H}_{A'}^{\otimes n})} I(A^n\rangle B^n)_\rho \,, \tag{1.16}$$

where $I(A^n\rangle B^n)_\rho$ is the coherent information for $\rho_{A^nB^n} = \mathbb{1}_A^{\otimes n}\otimes\mathcal{C}_{A'\to B}^{\otimes n}(\rho_{A^n(A')^n})$ and $\rho_{A^n(A')^n}$ is a purification of $\rho_{(A')^n}$. The state $\mathbb{1}_A^{\otimes n}\otimes\mathcal{C}_{A'\to B}^{\otimes n}(\rho_{A^n(A')^n})$ results from the n-fold use of the channel $\mathcal{C}_{A'\to B}$ to transmit $(A')^n$, i.e. n copies of system A', while the purification A^n of $(A')^n$ remains unchanged. Thus, the r.h.s. of (1.16) is the coherent information in the limit of infinitely many channel uses. Likewise, the quantum capacity $Q(\mathcal{C}_{A'\to B})$ is the limit of the achievable rate for quantum data transmission in the limit of infinitely many channel uses. One says that the quantum capacity, and therefore the coherent information, is an *asymptotic quantity*. This has the disadvantage that from the coherent information, only very limited statements about finitely many uses of the channel can be made.

The von Neumann entropy has other very important roles, such as in the asymptotic analysis of *quantum key distribution* (QKD), discovered by Bennett and Brassard [BB84] and Ekert [Eke91]. To discuss this, it is helpful to switch to the information-theoretic paradigm, in which the systems A and E are controlled by *parties* with intentions and interests, rather than being dead physical objects. In a QKD protocol there are three parties A, B and E, called Alice, Bob and Eve. It is a cryptographic protocol in which Alice wants to send a secret key to Bob using a public channel such that the eavesdropper Eve (who has control over the channel) cannot learn it. Here, a key is a string of random bits that Alice and Bob want to use for encrypting messages in a *one-time pad*.[2]

Classically, a secure exchange of secret keys through public communication is impossible without relying on assumptions of computational hardness. Quantum mechanically, however, it is (in principle) possible to do this securely by the use of decoherence estimation. For our purposes, it is particularly insightful to consider this in an *entanglement-based* protocol, invented by Ekert, rather than in a *prepare-and-measure* protocol, as invented by Bennett and Brassard.

In a simple entanglement-based QKD protocol, Alice prepares maximally entangled pairs of qubits and sends one half of each pair to Bob using a quantum channel. The quantum channel is insecure, so there could be an eavesdropper Eve trying to read out the quantum information that Alice sends to Bob (see figure 1.5). For each pair, Alice and Bob independently measure their qubit in either the Pauli-$\mathbb{X}$ basis or the Pauli-$\mathbb{Z}$ basis, where the basis is chosen at random. Afterwards, Alice and Bob compare part of their data. If they do that in a clever way, they can determine with high confidence whether an eavesdropper was present. More precisely, from the compared data, they can bound the amount of information that any eavesdropper (or any channel purification) has about the data that Alice and Bob did *not* compare. The

[2] The one-time pad is a symmetric key cipher that allows for perfectly secret communication between two parties over a public communication channel. The one-time pad requires the use of a secret key. Fore more information about the one-time pad and symmetric key ciphers in general, see [Sti05].

bound is of the form $H(X|E) \geq f(\beta)$, where X is the data that Alice holds and has not communicated, and where $f(\beta)$ just stands symbolically for a function of parameters that they determined in the comparison. This is called *parameter estimation*. (We will learn more about concrete QKD protocols in chapter 5.) Thus, they can determine how secret their information is by means of experiment—which is something without a classical analogue. It is a form of decoherence estimation that allows Alice and Bob to do QKD.

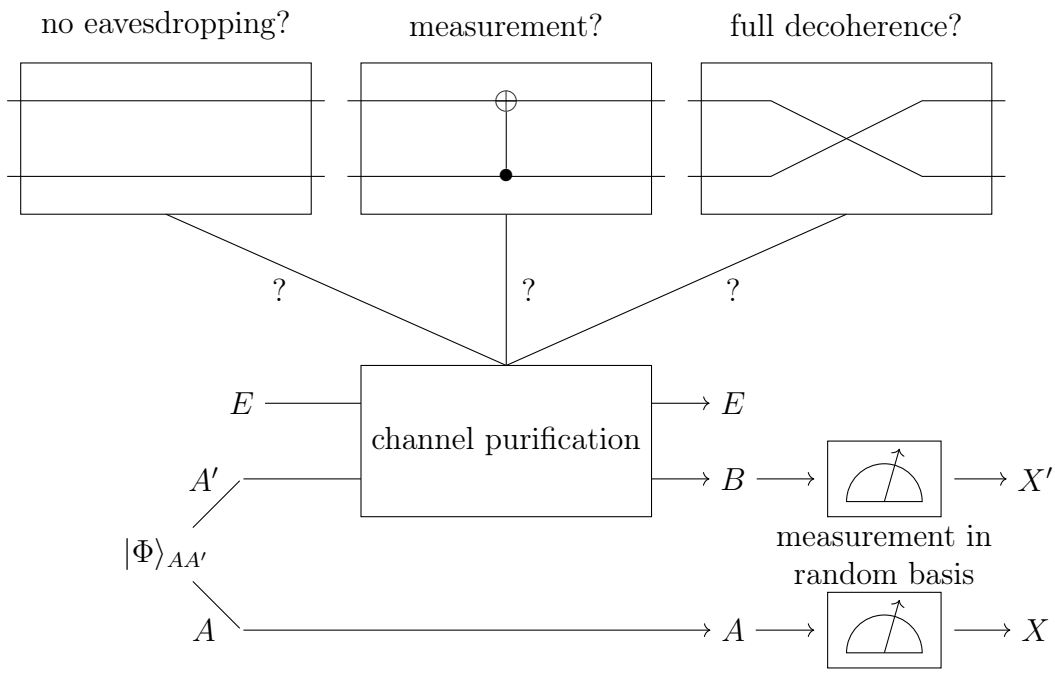


Figure 1.5: Diagram for an entanglement-based QKD protocol. By comparing measurement statistics, Alice and Bob can lower bound the conditional von Neumann entropy $H(X|E)$. If there is no eavesdropping, they will find that $H(X|E) = n$, where n is the number of bits in the outcome string X. If Eve measures every qubit passing the channel, she gets classically correlated with Alice, $H(A|E) = 0$. In the most extreme case, Eve keeps the sent qubit and forwards another system to Bob, thereby creating entanglement with Alice, in which case $H(A|E) = -n$.

Apart from QKD, the (conditional) von Neumann entropy has many more operational characterizations that we will not cover here. However, it has a huge drawback concerning its practical applicability: it is an *asymptotic* quantity. For the QKD example, this means that security proofs based on the von Neumann entropy only hold in the limit where Alice and Bob exchange infinitely many (qu)bits. Since real-world applications are always finite, this means that the results are never applicable for actual QKD protocols.

1.3 Quantification of single-shot decoherence

To make quantum key distribution applicable in practice, one needs to account for the fact that Alice and Bob only exchange a finite amount of data. Thus,

their statistical tests can only give them a bounded confidence about an eavesdropper's knowledge. Concretely, speaking in the last section's language, Alice and Bob can never conclude with certainty that there was no decoherence in the transmission (in which case $H(X|E) = n$) when they only exchange a finite amount of data. However, the one time pad encryption, for which Alice and Bob want the key, only works with perfectly secret keys if perfect security is required.

Thus, in actual QKD protocols, one needs a method to turn keys with partial uncertainty of Eve into smaller keys with (almost) full uncertainty of Eve. This is done with *quantum leftover hashing* [Tom+11]. It turns an n-bit string X about which Eve has partial knowledge into an l-bit string (with $l < n$) about which Eve has (almost) no information. The quantum leftover hashing lemma, which we will encounter in chapter 4, states the conditions under which this is possible. These conditions are not formulated in terms of the von Neumann entropy but in terms of the smooth conditional *min-entropy*, introduced by Renato Renner [Ren05]. (We will see its formal definition in chapter 3.) Roughly speaking, the quantum leftover hashing lemma [Tom+11] states that from a string X with $H^{\varepsilon}_{\min}(X|E) > l$, one can extract an l-bit key K which is approximately uniformly random and uncorrelated with Eve, that is

$$\rho_{KE} \approx \pi_K \otimes \rho_E \,, \quad \text{where} \quad \pi_K = \frac{\mathbb{1}_K}{2^l} \,. \tag{1.17}$$

We will see the precise statement (and also the role of the parameter ε in chapter 4. Thus, finite-size QKD protocols work with the min-entropy rather than the von Neumann entropy. Again, the estimation of the min-entropy $H^{\varepsilon}_{\min}(X|E)$ can be seen as a form of decoherence estimation.

The motivation for the min-entropy that we have just given is an application-specific one and might seem quite far away from the more intuitive characterizations of decoherence that we mentioned further above. There are, however, other characterizations of the min-entropy that bring us back to a more intuitive picture. For example, the (non-smooth) min-entropy can be seen as a measure for how far away Eve is from a situation in which she is maximally entangled with Alice. More precisely, it has been shown [KRS09] that

$$H_{\min}(A|E)_\rho = -\log d_A \max_{\mathcal{R}_{E\to A'}} F^2(\Phi_{AA'}, \mathbb{1}_A \otimes \mathcal{R}_{E\to A'}(\rho_{AE})) \,, \tag{1.18}$$

Here, the maximum is taken over all operations $\mathcal{R}_{E\to A'}$ that Eve can perform on her part of the system, F is the *fidelity* that measures how close two states are, and $\Phi_{AA'}$ is the maximally entangled state

$$|\Phi\rangle_{AA'} = \frac{1}{\sqrt{d_A}} \sum_{i=1}^{d_A} |i\rangle_A \otimes |i\rangle_{A'} \,. \tag{1.19}$$

(For a definition of the fidelity F, see definition 3.14.) Thus, the min-entropy measures how close Eve can bring herself to sharing the state $\Phi_{AA'}$ with Alice.

1.4 Summary of the results presented in this thesis

In the previous sections, we have seen that decoherence can be thought of in many different terms: some that are more intuitive, but which refer explicitly to the mathematical representation of a state as a density operator, and some that are very application-specific. In this thesis, we will see three different results, all of which have in common that they concern decoherence in some sense, and technically correspond to bounding the min-entropy.

The first result concerns QKD protocols, and will be presented in chapter 5. We will investigate in detail how QKD protocols estimate the conditional min-entropy $H^{\varepsilon}_{\min}(X|E)$. We will find that an error has spread in the more recent QKD literature that leads to an incorrect bound on the min-entropy. More precisely, we analyze *iterative sifting*, a recently suggested procedure in which Alice and Bob communicate past measurement basis choices to ensure that they end up with enough bits measured in the same basis. We find that iterative sifting leads to two previously unnoticed problems that break the security proof of the QKD protocol. We will see attack strategies that exploit these problems, and see how the protocol can be modified to avoid them. We present a detailed formal proof of the min-entropy bound for the resulting protocol, thereby seeing at what point iterative sifting breaks the security proof of QKD.

In chapter 6, we will use ideas from QKD to devise a protocol that achieves the distribution of secret *quantum* information. While in QKD, the goal is to distribute a classical random bit string which is decoupled from Eve, we will see a protocol in which Alice sends qubits to Bob that are decoupled from Eve. The protocol can be thought of as a modified QKD protocol, in which qubits are measured at random in the $\mathbb{X}$-basis, in the $\mathbb{Z}$-basis, or not at all. As we will see, Alice and Bob can then exchange and analyze their measurement results in the $\mathbb{X}$- and $\mathbb{Z}$-basis to obtain a bound $H^{\varepsilon}_{\min}(A|E)$, where A is the system of Alice's unmeasured qubits. Such a protocol can be extended to a protocol where Alice and Bob process their unmeasured qubits to distill entanglement between each other.

Finally, chapter 7 is dedicated to the question of how decoherence can be estimated in situations where quantum theory may no longer be a correct description of nature. This is interesting for the investigation of phenomena for which there is no quantum description. For example, since there is no consistent theory of quantum gravity, effects of gravitational decoherence are likely to fall outside of the realm of quantum theory. We will generalize the probabilistic structure of quantum theory to a framework of generalized probabilistic theories where quantum theory forms a special case. This framework is general enough to encompass any theory with probabilistic measurement outcomes satisfying a set of minimal assumptions. This way, one may hope to have a framework at hand that is general enough to encompass the theory that correctly describes gravitational decoherence, without knowing which theory exactly it is. For these generalized probabilistic theories, we derive a framework of decoherence estimation. Taking expression (1.18) as an inspiration, we derive a generalized decoherence quantity $\mathrm{Dec}(A|E)$ for any probabilistic theory

that has a notion of a "maximally correlated state", in analogy to maximally entangled states in quantum theory. We will show that this quantity can be estimated by CHSH measurements performed on a maximally correlated particle pair, where one half of the pair undergoes the decoherence process in question. This way, one obtains a bound of the form $\mathrm{Dec}(A|E) \leq f(\beta)$, where f is a function of the measured CHSH parameter β. This way, one can test proposed models for gravitational decoherence by calculating $\mathrm{Dec}(A|E)$ for these models and checking whether the obtained value is compatible with the experimentally derived bound of the form $\mathrm{Dec}(A|E) \leq f(\beta)$. This might provide a useful falsification tool in the search for a model for gravitational decoherence. As an example application of this framework, we will suggest an optomechanical experiment to test Diosi's theory of gravitational decoherence.

1.5 Outline of the thesis

The general structure of this thesis is as follows. It is divided into four parts: introduction (part I), preliminaries (part II), contributions (part III) and appendix (part IV).

The preliminaries serve as a summary of the technical prerequisites that are required to understand the contributions made in this thesis. They should more be considered as a reminder than as an introduction for beginners. They start with a lookup-table of our conventions and notation before we recapitulate some formal details of discrete probability theory in chapter 2. In chapter 3, we revise the definitions of the quantum framework as it is typically used in quantum information theory, including min- and max-entropy formalism. In chapter 4, we will recapitulate those operational characterizations of the min-entropy that are relevant for our contributions.

Part III forms the main part of this thesis, and is dedicated to the results that we have summarized in the previous section: the problems of iterative sifting in QKD (chapter 5), the protocol for the distribution of secret quantum information (chapter 6), and the decoherence estimation framework for generalized probabilistic theories (chapter 7). We will round things off in chapter 8, where we make some concluding remarks and have an outlook on future research that may follow up the contributions of this thesis.

Finally, part IV consists of the appendix.

Part II

Preliminaries

General conventions

- We use the -1 superscript notation to denote preimages of elements or subsets under maps. For example, for a map $f : A \to B$, an element $y \in B$ and a subset $S \subseteq B$, we write

$$f^{-1}(y) = \{x \in A \mid f(x) = y\}\,, \tag{1.20}$$
$$f^{-1}(S) = \{x \in A \mid f(x) \in S\}\,. \tag{1.21}$$

- The logarithm is with respect to base 2, i.e. $\log := \log_2$.
- The natural logarithm (to base e) is denoted by ln.
- We denote the positive integers by $\mathbb{N}_+ := \{1, 2, 3, \ldots\}$.
- For $n \in \mathbb{N}_+$, we write $[n] := \{1, \ldots, n\}$,
- We use the following notation for multinomial coefficients:

$$\binom{n}{n_1, n_2, \ldots, n_k} := \frac{n!}{n_1! n_2! \ldots n_k!}\,. \tag{1.22}$$

Chapter 2

Discrete probability theory

In most of the quantum information literature—especially research papers—elements of probability theory such as random variables or conditionings are addressed rather implicitly. For example, when a quantity is said to be a random variable, the underlying probability space and the form of the random variable as a map are typically not modeled explicitly. The more formally inclined reader is then left to figure out the underlying probability space structure himself. This is usually not a problem, and leaving the precise mathematics implicit can save space in research publications to talk about the more central topics of the paper.

In much of the material presented in this thesis, however, these elements of probability theory are very central. In chapter 5, for example, we will look at some probabilistic aspects of a QKD protocol in great detail and point out mistakes that occurred in current research literature. These mistakes would have probably not been made if the underlying probability space structure had been treated more formally. For this reason, we will model probability spaces and random variables explicitly whenever this is useful and feasible. The material in this section is a recap of the aspects of probability theory that need to be understood in order to grasp our probability space models on a formal level. It is more a reminder and an indication of our notational conventions rather than a complete introduction to the subject.

2.1 Probability spaces, random variables and events

Probability theory is the theory of *probability spaces*. In general, a probability space is given by a triple $(\Omega, \mathcal{E}, \mu)$, where Ω is a set, $\mathcal{E}$ is a sigma-algebra and μ is a measure. However, for our purposes, it is not necessary to know what a sigma-algebra or a measure is. We will only deal with cases in which the set Ω is countable (i.e. finite or countably infinite). In this case, probability theory can be reduced to the study of *discrete* probability spaces, which are defined as follows.

Definition 2.1 : *A* ***discrete probability space*** *is a pair* (Ω, P)*, where* Ω *is a countable set (called the* ***sample space****) and* P *is a* ***probability mass***

function *on Ω, that is, a function $P : \Omega \to [0,1]$ such that*

$$\sum_{\omega \in \Omega} P(\omega) = 1\,. \tag{2.1}$$

The elements of Ω are called ***elementary events****.*

We will often say "probability distribution" when we mean a probability mass function. Since discrete probability spaces are the only probability spaces that we will encounter, it is unnecessarily cumbersome to refer to "discrete" probability spaces all the time. Instead, we make the following convention.

Convention 2.2 : *Throughout this thesis, the term "probability space" refers to a discrete probability space.*

Definition 2.3 : *Let (Ω, P) be a probability space. A* ***random variable*** *X on (Ω, P) is a map $X : \Omega \to \Omega_X$ to some set Ω_X. The set Ω_X is the* ***codomain*** *of X. The* ***probability distribution*** *P_X* ***of a random variable*** *X is given by the probability mass function*

$$\begin{array}{rccl} P_X : & \Omega_X & \to & [0,1] \\ & x & \mapsto & \displaystyle\sum_{\omega \in X^{-1}(x)} P(\omega)\,. \end{array} \tag{2.2}$$

Convention 2.4 : *Throughout this thesis, we will write random variables in uppercase letters (such as X) and its values, i.e. the elements of its codomain, in lowercase letters (such as x).*

Remark 2.5: A random variable X on a probability space (Ω, P) as in definition 2.3 induces a probability space (Ω_X, P_X). The following diagram helps to see the relation between the probability spaces (Ω, P) and (Ω_X, P_X).

$$\begin{tikzcd} \Omega \arrow[r, "X"] \arrow[dr, "P"'] & \Omega_X \arrow[d, "P_X"] \\ & {[0,1]} \end{tikzcd} \tag{2.3}$$

Remark 2.6: Roughly speaking, one can say that "functions of random variables are again random variables". In more detail, consider a probability space (Ω, P) and a random variable $X : \Omega \to \Omega_X$. Then, for a map $f : \Omega_X \to \Omega_Y$ to some set Ω_Y, there are two equivalent ways in which we can see Ω_Y as the codomain of a random variable Y: either, we see $Y = f \circ X$ as a random variable on the probability space (Ω, P), or we consider f as a random variable on the probability space (Ω_X, P_X). The relation between these two views can be seen in the following diagram:

$$\begin{tikzcd} \Omega \arrow[r, "X"] \arrow[rr, bend left, "Y=f\circ X"] \arrow[dr, "P"'] & \Omega_X \arrow[r, "f"] \arrow[d, "P_X"] & \Omega_Y \arrow[dl, "P_Y"] \\ & {[0,1]} & \end{tikzcd} \tag{2.4}$$

In this case, where a random variable Y is defined via a map f, we write $Y = f(X)$ and say that the random variable Y is a function of the random variable X.

Definition 2.7 : *Let (Ω, P) be a probability space, let X, Y be random variables on (Ω, P). Then the* ***joint probability distribution*** *of X and Y is the probability mass function*

$$\begin{array}{rccl} P_{XY}: & \Omega_{XY} & \to & [0,1] \\ & (x,y) & \mapsto & \displaystyle\sum_{\omega \in (X \times Y)^{-1}(x,y)} P(\omega)\,, \end{array} \tag{2.5}$$

where $\Omega_{XY} = \Omega_X \times \Omega_Y$ and where $X \times Y$ is the map

$$\begin{array}{rccl} X \times Y: & \Omega & \to & \Omega_X \times \Omega_Y \\ & \omega & \mapsto & (X(\omega), Y(\omega))\,. \end{array} \tag{2.6}$$

This gives rise to a probability space (Ω_{XY}, P_{XY}).

Remark 2.8: In analogy to remark 2.5, we point out that two random variables X and Y on a probability space (Ω, P) also induce a probability space (Ω_{XY}, P_{XY}). Moreover, definition 2.7 generalizes to joint distributions $P_{X_1 \ldots X_n}$ on $\Omega_{X_1 \ldots X_n}$ for any number n of random variables in the obvious way, leading to probability spaces $(\Omega_{X_1 \ldots X_n}, P_{X_1 \ldots X_n})$.

Definition 2.9 : *For a probability space (Ω, P), an* ***event*** *A is a subset $A \subseteq \Omega$ of the sample space Ω. The probability of an event A is defined by*

$$P[A] = \sum_{\omega \in A} P(\omega)\,. \tag{2.7}$$

Convention 2.10 : *Note the different notations we use for probabilities: for elementary events $\omega \in \Omega$, we write $P(\omega)$, for values x of a random variable X, we write $P_X(x)$, and for events $A \subseteq \Omega$, we write $P[A]$ (in square brackets).*

All events that we will consider are given by equalities or inequalities involving random variables. For example, if (Ω, P) is a probability space and X is a random variable, then the set

$$(X = x) := \{\omega \in \Omega \mid X(\omega) = x\} \tag{2.8}$$

is an event. It has the probability

$$P[X = x] = \sum_{\omega \in (X=x)} P(\omega) = \sum_{\omega \in X^{-1}(x)} P(\omega) = P_X(x)\,. \tag{2.9}$$

We will often consider random variables whose codomains are subsets of the real numbers. In that case, the set Ω_X is an ordered set, so we can consider events of the form

$$(X \leq x) := \{\omega \in \Omega \mid X(\omega) \leq x\}\,. \tag{2.10}$$

Such events have the probability

$$P[X \leq x] = \sum_{\omega \in (X \leq x)} P(\omega) = \sum_{x' \leq x} P_X(x')\,. \tag{2.11}$$

For two random variables X and Y, we can consider events like

$$(X + Y \leq 8 \wedge X \geq 3) := \{\omega \in \Omega \mid X(\omega) + Y(\omega) \leq 8 \text{ and } X(\omega) \geq 3\}\,, \quad (2.12)$$

where $\wedge$ denotes the logical "and". More generally, we interpret any equality or inequality involving random variables (such as the left hand side in equations (2.8), (2.10) and (2.12)) as an event. All random variables that we will consider are of this form. For the definitions in this chapter, we denote events by A and B and think of them as placeholders for equalities or inequalities involving random variables.

Definition 2.11 : *Let (Ω, P) be a probability space, let A and B be events such that $P[B] \neq 0$. The* ***conditional probability*** *$P[A|B]$ of A conditioned on B (or A given B) is defined as*

$$P[A|B] = \frac{P[A \cap B]}{P[B]}\,. \quad (2.13)$$

If A is of the form $X = x$ for a random variable X, we write

$$P_{X|B}(x) := P[X = x|B] = \frac{P[(X = x) \cap B]}{P[B]}\,. \quad (2.14)$$

If, in addition, B is of the form $Y = y$ for a random variable Y, we write

$$P_{X|Y}(x|y) := P[X = x|Y = y] = \frac{P_{XY}(x, y)}{P_Y(y)}\,. \quad (2.15)$$

We will make use of the *law of total probability*, which can be formulated in terms of random variables X and Y as follows.

Proposition 2.12 (Law of total probability): *For two random variables X and Y, it holds that*

$$P_X(x) = \sum_{\substack{y \in \Omega_Y \\ P_Y(y) \neq 0}} P_Y(y) P_{X|Y}(x|y)\,. \quad (2.16)$$

We will also make use of the following result.

Theorem 2.13 (Bayes' Theorem): *Let A, B be events such that $P[A] \neq 0$ and $P[B] \neq 0$. Then*

$$P[A|B] := \frac{P[A]P[B|A]}{P[B]}\,. \quad (2.17)$$

In chapter 5, when we talk about efficiencies of protocols, we will see that efficiencies are random variables. In order to compare efficiencies of protocols, we will compare their *expectation values*, which are defined as follows.

Definition 2.14 : *For a random variable X, the* ***expectation value*** *$\langle X \rangle$ of X is defined as*

$$\langle X \rangle := \sum_{x \in \Omega_X} P_X(x)\, x\,. \quad (2.18)$$

The expectation value of a random variable can be decomposed in a way similar to the law of total probability above as shown by the following proposition.

Proposition 2.15 : *For random variables X and Y, it holds that*

$$\langle X \rangle = \sum_{\substack{y \in \Omega_Y \\ P_Y(y) \neq 0}} P_Y(y) \langle X | Y = y \rangle \,, \tag{2.19}$$

where

$$\langle X | Y = y \rangle := \sum_{x \in \Omega_X} P_{X|Y}(x|y)\, x \tag{2.20}$$

Definition 2.16 : *The quantity $\langle X | Y = y \rangle$ as in equation (2.20) is called the* ***conditional expectation*** *of X given the event $Y = y$.*

Chapter 3

Quantum information theory

In this chapter, we give a summarized overview of some basics of quantum information theory. The material presented here should not be seen as an introduction to the topic but as reminder of well-established definitions and results in quantum information theory. It also serves as a means to introduce our notational conventions. For an introduction to quantum information theory, we recommend the textbooks by Nielesn and Chuang [NC00] and by Wilde [Wil13]. For an introduction to quantum measurements with an account on its history, see [Kra83].

3.1 Basic definitions of the quantum formalism

3.1.1 States

In quantum theory, a system is associated with a complex Hilbert space $\mathcal{H}$. Throughout this thesis, we restrict ourselves to systems whose Hilbert space is finite-dimensional. In other words, all quantum systems that we consider are associated with a finite-dimensional complex inner product space, and we will always denote such a space by the symbol $\mathcal{H}$.

Convention 3.1 : *Throughout this thesis, quantum systems are assumed to be finite-dimensional, and the symbol $\mathcal{H}$ always denotes finite-dimensional complex inner product spaces.*

We assume that the reader has some familiarity with linear algebra. We use the *bra-ket notation* (or *Dirac notation*), i.e. we denote vectors by a "ket" $|\psi\rangle \in \mathcal{H}$ and their dual vectors by a "bra" $\langle\psi| \in \mathcal{H}^*$. We assume that this notation is clear. Readers unfamiliar with this notation are referred to any standard textbook on quantum mechanics or quantum information theory, such as [Wil13].

For operators on $\mathcal{H}$, we use the following notation.

Definition 3.2 : *The space of* ***endomorphisms*** *on $\mathcal{H}$, given by*

$$\mathrm{End}(\mathcal{H}) := \{L : \mathcal{H} \to \mathcal{H} \mid L \textit{ linear}\} \ , \tag{3.1}$$

is a vector space. The ***Hermitian operators*** *on $\mathcal{H}$,*

$$\mathrm{Herm}(\mathcal{H}) := \left\{L \in \mathrm{End}(\mathcal{H}) \mid L^\dagger = L\right\} \tag{3.2}$$

(where $L^\dagger$ denotes the Hermitian adjoint of L) form a linear subspace of $\mathrm{End}(\mathcal{H})$. *The* ***states*** *(or* ***density operators****) ρ on $\mathcal{H}$ are given by*

$$\mathcal{S}(\mathcal{H}) := \{\rho \in \mathrm{Herm}(\mathcal{H}) \mid \rho \geq 0, \mathrm{tr}(\rho) = 1\}\,, \tag{3.3}$$

where $\rho \geq 0$ means that the operator ρ is positive and $\mathrm{tr}(\rho)$ denotes the trace of the operator ρ. It is often convenient to consider the ***subnormalized states*** *on $\mathcal{H}$, given by*

$$\mathcal{S}^{\leq}(\mathcal{H}) := \{\rho \in \mathrm{Herm}(\mathcal{H}) \mid \rho \geq 0, \mathrm{tr}(\rho) \leq 1\}\,. \tag{3.4}$$

An important distinction among quantum states is the distinction between *pure* and *mixed* states. Pure states can be thought of as states of maximal knowledge. We assume that this interpretation is clear and will not recall it here. The reader unfamiliar with this concept is referred to textbooks on quantum information theory, such as [NC00] or [Wil13].

Definition 3.3 : *Let $\rho \in \mathcal{S}(\mathcal{H})$ be a state. The state ρ is* ***pure*** *if there is a normalized vector $|\psi\rangle \in \mathcal{H}$ such that $\rho = |\psi\rangle\langle\psi|$.*

While the usage of the term "pure state" in the literature is clear, the usage of the term "mixed state" is not. Some authors call a state ρ mixed if it is not pure. Other authors use the term as a synonym for "density operator", meaning that they do not assume that the state is pure (but allowing for that case). We will call a state mixed if it is not pure.

To distinguish between spaces corresponding to different systems, we use subscripts, i.e. $\mathcal{H}_A$, $\mathcal{H}_B$ is the space associated with system A, B, respectively. Joint systems of several subsystems are associated with the tensor product of the spaces of the subsystems, e.g. the space of the joint system AB consisting of subsystems A and B is given by $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. Instead of "joint" system, we will also write "composite" system. A composite system consisting of two or three subsystems, is also called a "bipartite" or "tripartite" system, respectively.

Definition 3.4 : *For a subnormalized state $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ of a composite system AB, the* ***reduced state*** *on system A is defined as*

$$\rho_A := \mathrm{tr}_B(\rho_{AB})\,, \tag{3.5}$$

where tr_B is the ***partial trace*** *over B, that is, tr_B is the unique linear operator $\mathrm{tr}_B : \mathrm{End}(\mathcal{H}_{AB}) \to \mathrm{End}(\mathcal{H}_A)$ such that*

$$\mathrm{tr}_B(V \otimes W) = V\mathrm{tr}(W) \quad \forall V \in \mathrm{End}(\mathcal{H}_A)\,, \forall W \in \mathrm{End}(\mathcal{H}_B)\,. \tag{3.6}$$

Likewise, the reduced state on system B is defined as $\rho_B = \mathrm{tr}_A(\rho_{AB})$.

It holds that $\mathrm{tr}_A(\mathrm{tr}_B(\rho_{AB})) = \mathrm{tr}_B(\mathrm{tr}_A(\rho_{AB})) = \mathrm{tr}(\rho_{AB})$. Definition 3.4 extends to partial traces over arbitrarily many subsystems of arbitrary composite systems.

Convention 3.5 : *In contexts where a state of a composite system has already been defined, we will refer to the reduced states of the system simply by omitting the subscripts of traced-out systems. For example, in a context where a density operator $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_{ABC})$ has already been defined, we will simply write ρ_A and implicitly mean $\rho_A = \mathrm{tr}_B(\mathrm{tr}_C(\rho_{ABC}))$.*

A particularly important type of state is a *maximally entangled state*, defined as follows.

Definition 3.6 : *Consider two systems A and A' of equal dimension. A state $\rho_{AA'}$ is a maximally entangled state if it is of the form*

$$\rho_{AA'} = |\Phi\rangle\langle\Phi|_{AA'}\,, \quad \text{where} \quad |\Phi\rangle_{AA'} = \frac{\sum_{i=1}^{d_A} |i\rangle_A \otimes |i\rangle_{A'}}{\sqrt{d_A}} \tag{3.7}$$

for some orthonormal basis $(|i\rangle_A)_{i=1}^{d_A}$ of A and some orthonormal basis $(|i\rangle_{A'})_{i=1}^{d_A}$ of A'.

Maximally entangled states are basis-dependent, that is, for different choices of the bases $(|i\rangle_A)_{i=1}^{d_A}$ and $(|i\rangle_A)_{i=1}^{d_{A'}}$, we get different states of the form as in equation (3.7). Nonetheless, in many situations it is common to refer to *the* maximally entangled state. Lemmata 3.7 and 3.8 will help us to understand in which situations it is safe to do so. The following lemma can be found in [Tom12].

Lemma 3.7 (Mirror lemma): *Let $\rho_{AA'} = |\Phi\rangle\langle\Phi|_{AA'}$ be a maximally entangled state (with $|\Phi\rangle_{AA'}$ as in equation (3.7)), let U_A be a unitary on A, let $U_{A'}$ be the unitary on $\mathcal{H}_{A'}$ that acts the same way with respect to the basis $(|i\rangle_{A'})_{i=1}^{d_A}$ as U_A acts with respect to $(|i\rangle_{A'})_{i=1}^{d_A}$.*[1] *Then*

$$(U_A \otimes \mathbb{1}_{A'})|\Phi\rangle_{AA'} = (\mathbb{1}_A \otimes U_{A'}^T)|\Phi\rangle_{AA'}\,, \tag{3.8}$$

where $U_{A'}^T$ denotes the transpose of $U_{A'}$ with respect to the basis $(|i\rangle_{A'})_{i=1}^{d_A}$.

Lemma 3.7 can be proved by simple direct calculation, which we omit here. The mirror lemma states that the application of a unitary on one half of a system in a maximally entangled state corresponds to the applicaton of another unitary on the other half. This allows to prove the following, lemma, which is widely used in quantum information (see, for example, [NC00] and [Wil13]).

Lemma 3.8 : *Let $\rho_{AA'}$ and $\sigma_{AA'}$ be maximally entangle states of the same system AA'. Then there is a unitary $U_{A'}$ on $\mathcal{H}_{A'}$ such that*

$$\rho_{AA'} = (\mathbb{1}_A \otimes U_{A'})\sigma_{AA'}(\mathbb{1}_A \otimes U_{A'}^\dagger)\,. \tag{3.9}$$

Proof. Let $|\Phi\rangle_{AA'}, |\Psi\rangle_{AA'} \in \mathcal{H}_{AA'}$ be such that

$$\rho_{AA'} = |\Phi\rangle\langle\Phi|_{AA'}\,, \quad \sigma_{AA'} = |\Psi\rangle\langle\Psi|_{AA'}\,. \tag{3.10}$$

Since any two bases are related by a unitary, there is a unitary V_A on $\mathcal{H}_A$ and a unitary $W_{A'}$ on $\mathcal{H}_{A'}$ such that

$$|\Phi\rangle_{AA'} = (V_A \otimes W_{A'})|\Psi\rangle_{AA'} \tag{3.11}$$

$$= (\mathbb{1}_A \otimes W_{A'})(V_A \otimes \mathbb{1}_{A'})|\Psi\rangle_{AA'}\,. \tag{3.12}$$

According to the mirror lemma, it holds that

$$(V_A \otimes \mathbb{1}_{A'})|\Psi\rangle_{AA'} = (\mathbb{1}_A \otimes V_{A'}^T)|\Phi\rangle_{AA'}\,, \tag{3.13}$$

[1] More precisely, $U_{A'} = S_{A'\to A}^{-1} U_A S_{A\to A'}$, where $S_{A\to A'}$ maps the basis $(|i\rangle_A)_{i=1}^{d_A}$ to the basis $(|i\rangle_{A'})_{i=1}^{d_A}$.

Inserting (3.13) into (3.12) yields

$$|\Phi\rangle_{AA'} = (\mathbb{1}_A \otimes W_{A'})(\mathbb{1}_A \otimes V_{A'}^T)|\Psi\rangle_{AA'} \tag{3.14}$$
$$= (\mathbb{1}_A \otimes W_{A'}V_{A'}^T)|\Psi\rangle_{AA'} \tag{3.15}$$
$$= (\mathbb{1}_A \otimes U_{A'})|\Psi\rangle_{AA'}\,, \tag{3.16}$$

where $U_A = W_{A'}V_{A'}^T$ is a unitary. □

Lemma 3.8 tells us that when we consider functions of states that are invariant under local unitaries on one system, then any two maximally entangled states yield the same function value. In this sense, all maximally entangled states are equivalent.

Another important special state that we consider is the *maximally mixed state*, defined as follows.

Definition 3.9 : *Consider a d_A-dimensional system A. The maximally mixed state on A, denoted by π_A, is given by*

$$\pi_A = \frac{1}{d_A}\sum_{i=1}^{d_A} |i\rangle\langle i|\,, \tag{3.17}$$

where $\{|i\rangle\}_{i=1}^{d_A}$ is any basis of $\mathcal{H}_A$ (the state is independent of the choice of the basis).

An important property of maximally entangled states is that the reduced state (on either side) is always a maximally mixed state.

3.1.2 Evolution

An *evolution* of a quantum system is any process that changes the state of the system. This may also involve a change of the type of quantum system. In simple terms, an evolution is a map from the states $\mathcal{S}(\mathcal{H}_A)$ of a quantum system A to the states $\mathcal{S}(\mathcal{H}_B)$ of a quantum system B. Quantum information scientists like to think of the evolution of a quantum system as a *channel* $\mathcal{C}_{A\to B}$: it takes a system A in some state ρ_A as its input and outputs a system B in a state ρ_B:

$$A \longrightarrow \boxed{\text{quantum channel } \mathcal{C}_{A\to B}} \longrightarrow B \tag{3.18}$$

In order to correspond to a physical evolution of the system, the map $\mathcal{C}_{A\to B}$ needs to satisfy three properties. Firstly, such a map needs to preserve the trace of the state, $\mathrm{tr}(\mathcal{C}_{A\to B}(\rho_A)) = \mathrm{tr}(\rho_A)$. Secondly, considerations of probabilistic consistency require the map $\mathcal{C}_{A\to B}$ to be linear [NC00]. Thirdly, it needs to map positive operators to positive operators (otherwise, states would not be mapped to states), that is, it needs to be a positive map:

$$\mathcal{C}_{A\to B}(\rho_A) \geq 0 \quad \forall\, \rho_A \geq 0\,. \tag{3.19}$$

Consistency considerations lead to a requirement stronger than (3.19): it needs to remain a positive map even if it becomes part of a larger evolution in which

another system remains unchanged:

$$\begin{array}{ccc} E & \longrightarrow & E \\ A & \boxed{\text{quantum channel } \mathcal{C}_{A\to B}} \longrightarrow & B \end{array} \tag{3.20}$$

This is summarized in the following formal definition of a quantum channel.

Definition 3.10 : *Let A and B be quantum systems. A* ***quantum channel*** *from A to B is a linear map*

$$\mathcal{C}_{A\to B} : \mathrm{End}(\mathcal{H}_A) \to \mathrm{End}(\mathcal{H}_B) \tag{3.21}$$

which is trace-preserving, i.e.

$$\mathrm{tr}(\mathcal{C}_{A\to B}(\rho_A)) = \mathrm{tr}(\rho_A) \quad \forall\, \rho_A \in \mathrm{End}(\mathcal{H}_A)\,, \tag{3.22}$$

and which is completely positive. That is, for any quantum system E of any dimension $d_E \in \mathbb{N}_+$, the map $\mathcal{C}_{A\to B}\otimes\mathbb{1}_E$ (with $\mathbb{1}_E$ denoting the identity channel $\mathbb{1}_E(\rho_E) = \rho_E$) is a positive map,

$$(\mathcal{C}_{A\to B} \otimes \mathbb{1}_E)(\rho_{AE}) \geq 0 \quad \forall\, \rho_{AE} \in \mathcal{H}_{AE}\,. \tag{3.23}$$

Such a map is called a ***trace-preserving completely positive map*** *(abbreviated as* ***TPCPM****).*[2]

For some situations, it is convenient to introduce the following notation.

Definition 3.11 : *For vector spaces V and W, we denote the vector space of linear maps from V to W by $\mathrm{Hom}(V, W)$. It is the space of* ***homomorphisms*** *from V to W. In particular, we denote the space of linear maps from $\mathrm{End}(\mathcal{H}_A)$ to $\mathrm{End}(\mathcal{H}_B)$ by $\mathrm{Hom}(\mathrm{End}(\mathcal{H}_A), \mathrm{End}(\mathcal{H}_B))$.*

By virtue of definition 3.11, we can denote channels $\mathcal{C}_{A\to B}$ as special elements of the vector space $\mathrm{Hom}(\mathrm{End}(\mathcal{H}_A), \mathrm{End}(\mathcal{H}_B))$. In this thesis, we consider two physical situations that we will describe by quantum channels. In the first situation, a party Alice sends some quantum information to a distant party Bob, and thereby uses some sort of quantum channel, for example, a glass fiber. This situation is typically considered in protocols where secret information is communicated. In such a situation, one is not allowed to make assumptions about the quantum channel that is implemented by the glass fiber, as it is possible that some eavesdropper modifies the fiber. In this case, we need to consider *channel purifications*, which we will discuss in section 3.3.

The second situation that we consider are measurements. These are processes that change the state of a quantum system, and since a channel is the most general description of such a process, it can be described as a quantum channel. We will see this in the second half of section 3.1.3 below.

[2] According to this definition, the terms "channel" and "TPCPM" are equivalent. In practice, the term channel is preferred when speaking of the evolution of a system in a physical sense, while the term TPCPM refers to the map as a mathematical object. However, this distinction is often not very strict.

3.1.3 Measurements

Measurement statistics

The statistics of a measurement on a quantum system are completely described by a *positive operator valued measure* (POVM), defined as follows.

Definition 3.12 : *Let A be a quantum system. A* ***positive operator valued measure*** *is a set $\{M_i\}_{i=1}^n$ of positive operators on $\mathcal{H}_A$ such that*

$$\sum_{i=1}^{n} M_i = \mathbb{1}_A \,, \tag{3.24}$$

where $\mathbb{1}_A$ is the identity operator on $\mathcal{H}_A$.[3] *If system A is initially in a state ρ_A and is measured with respect to the POVM, then the probability of an outcome $i \in [n]$ is given by $\mathrm{tr}(M_i \rho_A)$.*

We will often consider measurements on *qubit* systems. A system A is a qubit system if $\mathcal{H}_A$ is isomorphic to $\mathbb{C}^2$. We will speak of measurements with respect to the $\mathbb{X}$-basis and with respect to the $\mathbb{Z}$-basis. This is a very common terminology, and just means that measurements are performed with respect to the POVMs

$$\mathbb{X} = \{\mathbb{X}_0, \mathbb{X}_1\} \,, \quad \mathbb{Z} = \{\mathbb{Z}_0, \mathbb{Z}_1\} \,, \tag{3.25}$$

where

$$\mathbb{X}_0 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} , \qquad \mathbb{Z}_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} , \tag{3.26}$$

$$\mathbb{X}_1 = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} , \qquad \mathbb{Z}_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} . \tag{3.27}$$

They correspond to measurements in the eigenbasis of the Pauli operators σ_x and σ_z, respectively. These POVMs are in fact projective measurements, i.e. each of the four operators above are orthogonal projectors. For projective measurements, it is straightforward to assign post-measurement states (see further below).

It is common and handy to use a special notation for the *eigenstates* of these measurements, which can be represented as $|v\rangle\langle v|$ for some eigenvector $|v\rangle$ of one of the projectors in (3.26) and (3.27). For $\mathbb{Z} = \{\mathbb{Z}_0, \mathbb{Z}_1\}$, the eigenvectors are

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} , \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} , \tag{3.28}$$

and for $\mathbb{X} = \{\mathbb{X}_0, \mathbb{X}_1\}$, we have the eigenvectors

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} , \qquad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} . \tag{3.29}$$

[3] We use the same symbol $\mathbb{1}$ for the identity operator and the identity channel, as the identity channel can be seen as the multiplication with the identity operator.

Note that

$$\mathrm{tr}(\mathbb{Z}_0|0\rangle\langle 0|) = \mathrm{tr}(\mathbb{Z}_1|1\rangle\langle 1|) = \mathrm{tr}(\mathbb{X}_0|+\rangle\langle +|) = \mathrm{tr}(\mathbb{X}_1|-\rangle\langle -|) = 1\,, \tag{3.30}$$

so if a system is in an eigenstate of a basis, it has a definite outcome.

In chapter 5, we will consider product measurements on multiple qubits. As an example, for a system composed of n qubits, one can consider the product POVM

$$\{\mathbb{Z}_{z_1} \otimes \mathbb{Z}_{z_2} \otimes \ldots \otimes \mathbb{Z}_{z_n} \mid z_i \in \{0,1\}\, \forall\, i \in [n]\}\,, \tag{3.31}$$

which corresponds to each qubit being measured in the $\mathbb{Z}$-basis. Instead of denoting outcomes by numbers $z_1, \ldots, z_n \in \{0,1\}$, we can denote a set of outcomes by a string

$$z = (z_1, \ldots, z_n) \in \{0,1\}^n\,. \tag{3.32}$$

This way, the POVM (3.31) can be rewritten as

$$\{\Pi_Z(z)\}_{z\in\{0,1\}^n}\,, \quad \text{where} \quad \Pi_Z(z) = \bigotimes_{i=1}^{n} \mathbb{Z}_{z_i}\,. \tag{3.33}$$

The reader may wonder why we have added a subscript Z in the notation for the projector $\Pi_Z(z)$. This will become clear in the following paragraph.

For an n-qubit system A in a state ρ_A, the numbers $\mathrm{tr}(\Pi_Z(z)\rho_A)$ indexed by $z \in \{0,1\}^n$ form a probability distribution. Thus, we can consider the probability space induced by the measurement. In most cases, there is no benefit in doing so, but when we study QKD measurement statistics in detail in section 5.8, this will prove useful. It will allow us to connect the formalism of classical probability spaces that we recapitulated in chapter 2 with the statistics of quantum measurements. This allows us to formally speak of the *random variables* of measurement outcomes and functions thereof. For our above example, we can consider the probability space (Ω_Z, P_Z), where $\Omega_Z = \{0,1\}^n$ and where

$$\begin{array}{rccl} P_Z: & \Omega_Z & \to & [0,1]\,, \\ & z & \mapsto & \mathrm{tr}(\Pi_Z(z)\rho_A)\,. \end{array} \tag{3.34}$$

On this probability space, the random variable Z of the outcome string z is simply given by the identity map,

$$\begin{array}{rccl} Z: & \Omega_Z & \to & \Omega_Z\,, \\ & z & \mapsto & z\,. \end{array} \tag{3.35}$$

This formalism can be extended to distributed measurements of several parties. Consider a joint quantum system AB, where both A and B are n-qubit systems. Then we can describe the statistics of a measurement where both Alice and Bob measure all their qubits in the $\mathbb{Z}$-basis by the POVM

$$\{\Pi_{ZZ'}(z,z')\}_{z,z'\in\{0,1\}^n}\,, \quad \text{where} \quad \Pi_{ZZ'}(z,z') = \left(\bigotimes_{i=1}^{n} \mathbb{Z}_{z_i}\right) \otimes \left(\bigotimes_{i=1}^{n} \mathbb{Z}_{z'_i}\right)\,. \tag{3.36}$$

This induces the probability space $(\Omega_{ZZ'}, P_{ZZ'})$, where $\Omega_{ZZ'} = \{0,1\}^n \times \{0,1\}^n$ and where

$$\begin{array}{rccl} P_{ZZ'}: & \Omega_{ZZ'} & \to & [0,1]\,, \\ & (z,z') & \mapsto & \mathrm{tr}(\Pi_{ZZ'}(z,z')\rho_{AB})\,. \end{array} \tag{3.37}$$

On this probability space, the random variables Z and Z' of the outcome strings z and z' are simply the projections on the respective component, e.g.

$$\begin{array}{rccll} Z: & \Omega_{ZZ'} & \to & \Omega_Z & (=\{0,1\}^n)\,, \\ & (z,z') & \mapsto & z\,. & \end{array} \tag{3.38}$$

This induction of probability spaces is essentially just a change of notation, but a particularly useful one. It allows to readily apply the formalism of classical probability spaces on measurement statistics of quantum systems. At the same time, we can infer properties of the probability distributions from properties of the state. (This will be very useful when we discuss the uniform sampling property and the absence of a basis information leak of sifting protocols in section 5.8.)

Post-measurement states

If a projective measurement $\{\Pi_i\}_i$ is performed on a system A which is initially in a state ρ_A and yields outcome k, then after the measurement, the system is in the post-measurement state ρ'_A, given by

$$\rho'_A = \frac{\Pi_k \rho_A \Pi_k}{\mathrm{tr}(\Pi_k \rho_A)}\,. \tag{3.39}$$

However, typically, after a quantum system is measured, it is no longer available in an experiment (for example, a measured photon may be absorbed). Moreover, not all measurements are projective measurements. Non-projective measurements arise from projective measurements on larger composite systems [NC00].

Even in such situations, it makes sense to consider a post-measurement state, where the outcome of the measurement outcome is stored in a classical register. For example, if a qubit system A is initially in a state ρ_A and then is measured with respect to the $\mathbb{X}$-basis, we consider the post-measurement state

$$\rho_X = \sum_x P_X(x)|x\rangle\langle x|\,, \tag{3.40}$$

where $\{|x\rangle\}_{x=0,1}$ is a fixed basis of a classical register system X and where

$$P_X(x) = \mathrm{tr}(\mathbb{X}_x \rho_A)\,. \tag{3.41}$$

The transformation $\rho_A \mapsto \rho_X$ is a quantum channel. A density operator of the form (3.40), i.e. a state which is diagonal in a fixed basis, is called a *classical state*. Why is it beneficial to consider such a density operator instead of just considering the outcome probabilities $P_X(x)$?

One case where this is useful is the case where an adversary holds quantum side information. Consider the case where a party Alice and an adversary Eve

share a quantum system ρ_{AE}. If Alice performs a measurement in the $\mathbb{X}$-basis on her system, we can consider the post-measurement state

$$\rho_{XE} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_E^x \,, \tag{3.42}$$

where P_X is as above and where

$$\rho_E^x = \frac{\mathrm{tr}_A((\mathbb{X}_x \otimes \mathbb{1}_E)\rho_{AE}(\mathbb{X}_x \otimes \mathbb{1}_E))}{P_X(x)} \,. \tag{3.43}$$

The state transformation $\rho_{AE} \mapsto \rho_{XE}$ is a quantum channel. A state of the form (3.42) is called a *classical-quantum state*, or CQ-state, for short. Given this state, Eve can perform operations (e.g. measurements) on system E in order to learn something about the value of the random variable X. In this case, where Eve holds quantum side information rather than classical side information, Eve is strictly more powerful than if she would only hold classical information [KR11], which makes it necessary to incorporate Alice's measurement result into a quantum state as in (3.42). An important application of this is the *quantum leftover hashing lemma* that we will see in section 4.2 and use in section 5.8.

Intercept-resend attacks

Another case where it is useful for us to consider post-measurement states are *intercept-resend attacks* in QKD, which we will consider in section 5.5. Say that Alice sends a quantum system A to Bob. Eve intercepts the sent quantum system and performs a projective measurement on it (say Eve measures in the $\mathbb{Z}$-basis, see figure 3.1). Then Eve prepares the system in an eigenstate associated with the measurement outcome (see equation (3.30)) and sends it to Bob. This yields the same state for Bob as the post-measurement state of equation (3.39), but physically it is not a post-measurement state but a newly prepared state.

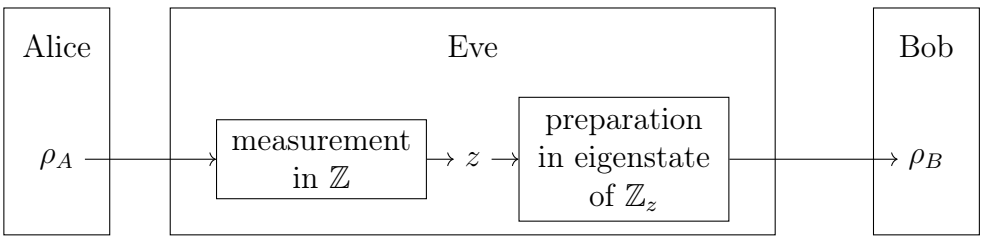


Figure 3.1: An intercept-resend attack. Alice wants to send a quantum system A in some state ρ_A to Bob. Eve intercepts system A and measures it (with respect to the $\mathbb{Z}$-basis, for example). Then Eve reprepares system A in the eigenstate corresponding to the measurement outcome and sends it to Bob.

This changes the state of the system ρ_A to a state ρ_B which, in general, differs from ρ_A. In section 5.5, when we determine error rates for intercept-resend attacks in entanglement-based QKD protocols, it is important to understand

how exactly the state is changed. We will consider the case where Alice prepares a qubit pair in a maximally entangled state

$$|\Phi\rangle_{AA'} = \frac{|0\rangle_A \otimes |0\rangle_{A'} + |1\rangle_A \otimes |1\rangle_{A'}}{\sqrt{2}} \tag{3.44}$$

and sends system A' to Bob. Thereby, Eve intercepts this transmission with an intercept-resend attack (see figure 3.2).

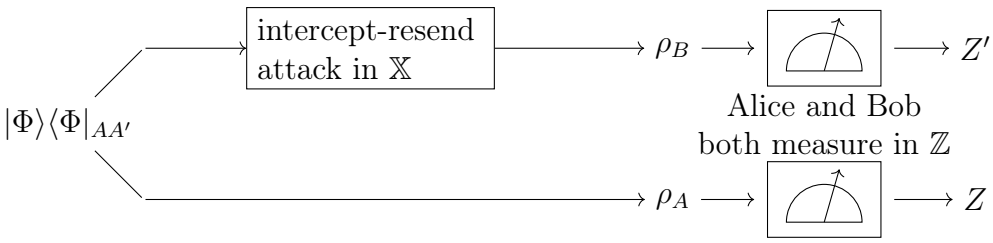


Figure 3.2: Intercept-resend attack in an entanglement-based QKD protocol. In an entanglement-based QKD protocol, Alice prepares a qubit pair in a maximally entangled state and sends on half to Bob. In an intercept-resend attack, the transmission is intercepted by Eve, who performs an attack as shown in figure 3.1 above. Then Alice and Bob measure their half of the system in a randomly chosen basis. If Alice and Bob happen to choose the same basis, but Eve chooses a different basis, then there is a non-zero probability that Alice's and Bob's measurement outcomes differ. If Eve measures in $\mathbb{X}$ and Alice and Bob measure in $\mathbb{Z}$ (or vice versa), we get that $P[Z \neq Z'] = 1/2$ (or $P[X \neq X'] = 1/2$, respectively).

In this case, if Eve attacks in the $\mathbb{Z}$-basis and obtains an outcome z, then Bob will receive $|0\rangle_B$ if $z = 0$ and $|1\rangle_B$ if $z = 1$ (as one can see from (3.30) above). Moreover, Alice obtains the post-measurement state (c.f. equation (3.43) above)

$$\rho_A^z = \frac{\mathrm{tr}_B((\mathbb{1}_A \otimes \mathbb{Z}_z)|\Phi\rangle\langle\Phi|_{AB}(\mathbb{1}_A \otimes \mathbb{Z}_z)}{\mathrm{tr}((\mathbb{1}_A \otimes \mathbb{Z}_z)|\Phi\rangle\langle\Phi|_{AB})}\,, \tag{3.45}$$

which is $\rho_A^0 = |0\rangle\langle 0|$ if $z = 0$ and $\rho_A^1 = |1\rangle\langle 1|$ if $z = 1$. Thus, taken together, Alice and Bob receive the state

$$\begin{aligned} &|0\rangle_A \otimes |0\rangle_{A'} \quad \text{if } z = 0\,, \\ &|1\rangle_A \otimes |1\rangle_{A'} \quad \text{if } z = 1\,. \end{aligned} \tag{3.46}$$

Analogously, if Eve attacks in the $\mathbb{X}$-basis, then Alice and Bob receive the state

$$\begin{aligned} &|+\rangle_A \otimes |+\rangle_{A'} \quad \text{if } x = 0\,, \\ &|-\rangle_A \otimes |-\rangle_{A'} \quad \text{if } x = 1\,. \end{aligned} \tag{3.47}$$

where

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\,, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}\,. \tag{3.48}$$

For the error rate calculations in section 5.5, we will consider the case where Alice and Bob measure in the same basis ($\mathbb{X}$ or $\mathbb{Z}$). From (3.46) and (3.47), we get that if Eve attacks in the same basis as Alice and Bob measure their systems, then Alice and Bob will get the same outcome with certainty. However, if Eve attacks in $\mathbb{X}$ and Alice and Bob measure in $\mathbb{Z}$ (or vice versa), then Alice and Bob get different outcomes with probability $1/2$, because for $i = 0, 1$, we get that

$$\mathrm{tr}((\mathbb{X}_0 \otimes \mathbb{X}_1)(|i\rangle\langle i|_A \otimes |i\rangle\langle i|_B)) = \mathrm{tr}((\mathbb{X}_1 \otimes \mathbb{X}_0)(|i\rangle\langle i|_A \otimes |i\rangle\langle i|_B)) = \frac{1}{4}\,, \tag{3.49}$$

and for $i = +, -$, we get

$$\mathrm{tr}((\mathbb{Z}_0 \otimes \mathbb{Z}_1)(|i\rangle\langle i|_A \otimes |i\rangle\langle i|_B)) = \mathrm{tr}((\mathbb{Z}_1 \otimes \mathbb{Z}_0)(|i\rangle\langle i|_A \otimes |i\rangle\langle i|_B)) = \frac{1}{4}\,. \tag{3.50}$$

We will speak of an *error* when Alice and Bob get different measurement outcomes despite measuring in the same basis. The above shows that if Alice and Bob measure in the same basis as Eve's attack, they will have no error, but if Eve uses a different basis than Alice and Bob, the error probability is $1/2$.

3.2 Distance measures

Many of the definitions that we will see below make use of distance measures between quantum states. We will not go far beyond the mere definitions here. For more information about these measures, see [NC00] (for the trace distance and the fidelity) and [Tom12] (for the generalized fidelity and the purified distance). Another good source for distance measures and the distinguishability of quantum states with a large collection of references is the PhD thesis of Christopher Fuchs [Fuc95].

We start with the definition of the *trace distance* and the *fidelity*. They are defined in terms of the *trace norm*, which is defined as follows.

Definition 3.13 : *On the vector space* $\mathrm{End}(\mathcal{H})$*, we will use the following norms. The* ***trace norm*** *is given by*

$$\begin{array}{rccc} \|\cdot\|_1 : & \mathrm{End}(\mathcal{H}) & \to & \mathbb{R}\,, \\ & L & \mapsto & \mathrm{tr}\left(\sqrt{L^\dagger L}\right)\,. \end{array} \tag{3.51}$$

Definition 3.14 : *Let* $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ *be states. The* ***trace distance*** *between* ρ *and* σ *is defined as*

$$D(\rho, \sigma) := \frac{1}{2}\|\rho - \sigma\|_1\,. \tag{3.52}$$

The ***fidelity*** *between* ρ *and* σ *is defined as*

$$F(\rho, \sigma) := \left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1 \tag{3.53}$$

$$= \mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\,. \tag{3.54}$$

As the following lemma shows, the trace distance and the fidelity share a symmetry property that is very practical in practive: they are invariant under under the simultaneous application of a unitary.

Lemma 3.15 : *Let $\rho, \sigma \in \mathcal{H}$ be states, let U be a unitary on $\mathcal{H}$. Then*

$$D(U\rho U^\dagger, U\sigma U^\dagger) = D(\rho, \sigma)\,, \tag{3.55}$$

$$F(U\rho U^\dagger, U\sigma U^\dagger) = F(\rho, \sigma)\,. \tag{3.56}$$

Another useful fact is that for two states that are diagonal in the same basis, the trace distance and the fidelity become functions of the diagonal distributions. Consider two states

$$\rho = \sum_x P_X(x)\ |x\rangle\langle x|\,, \quad \sigma = \sum_x Q_X(x)\ |x\rangle\langle x|\,. \tag{3.57}$$

The trace distance between these two states is given by

$$D(\rho, \sigma) = \frac{1}{2}\sum_x |P_X(x) - Q_X(x)| \tag{3.58}$$

$$=: d(P_X, Q_X)\,, \tag{3.59}$$

where $d(P_X, Q_X)$ is the *total variation distance* or *classical trace distance* between the probability distributions P_X and Q_X. The fidelity between these two states is given by

$$F(\rho, \sigma) = \sum_x \sqrt{P_X(x)Q_X(x)} \tag{3.60}$$

$$= b(P_X, Q_X)\,, \tag{3.61}$$

where $b(P_X, Q_X)$ is the *Bhattacharyya coefficient* or *classical fidelity* between the probability distributions P_X and Q_X.

Such a connection between the quantum trace distance and fidelity and their classical counterparts does not only hold for states that are diagonal in the same basis. In a modified way, it holds for any pair of states. The probability distributions P_X and Q_X can be seen as the probability distributions over the outcomes that one would get if the systems were measured in the basis with respect to which they are diagonal. Extending on this idea, one may also consider the classical fidelity or the classical trace distance between probability distributions induced by the states when measured in other bases. Roughly speaking, it turns out that the trace distance and the fidelity equal their classical counterparts of the measurement-induced distributions when the basis is chosen such that the two states look as different as possible (as measured by the classical quantities). The following proposition states this formally.

Proposition 3.16 : *For two quantum states ρ and σ of the same system, it holds that*

$$D(\rho, \sigma) = \max_{\{M_i\}_i} \sum_i |\mathrm{tr}(M_i\rho) - \mathrm{tr}(M_i\sigma)|\,, \tag{3.62}$$

$$F(\rho, \sigma) = \min_{\{M_i\}_i} \sum_i \sqrt{\mathrm{tr}(M_i\rho)\mathrm{tr}(M_i\sigma)}\,, \tag{3.63}$$

where the optimizations run over all POVMs $\{M_i\}_i$ of the system.

For a proof of proposition 3.16, see [NC00]. When the two states are diagonal in the same basis, then the optima in (3.62) and (3.63) are achieved for the measurement in that basis. The connection between the classical trace distance / classical fidelity and their quantum counterparts will be important for us when we define distance measures for generalized probabilistic theories in chapter 7.

Now we will recapitulate the definitions of the *generalized fidelity* and the *purified distance*. For our purposes, their role is to allow us to formally define the smooth min- and max-entropy in section 3.4 below. To avoid potential confusion for readers that have seen definitions of the smooth min- and max-entropy elsewhere, we point out that the preferred definition of these quantities has changed over time. Since they have first been defined in Renato Renner's seminal work on quantum key distribution [Ren05], different distance measures have been used for the smoothing of the min- and the max-entropy (among other aspects that changed). In this thesis, we will follow the definitions in [Tom12], which use the purified distance for smoothing.

The purified distance is defined in terms of the generalized fidelity as follows.

Definition 3.17 : *Let $\rho, \sigma \in \mathcal{S}^{\leq}(\mathcal{H})$ be subnormalized states. The* ***generalized fidelity*** *between ρ and σ is defined as*

$$F(\rho, \sigma) := \left\| \sqrt{\rho}\sqrt{\sigma} \right\|_1 + \sqrt{(1 - \mathrm{tr}\rho)(1 - \mathrm{tr}\sigma)}\,,$$

The ***purified distance*** *between ρ and σ is defined as*

$$P(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)^2}\,.$$

Note that for normalized states ρ and σ that are diagonal in the same basis (as in (3.57)), the purified distance is given by

$$F(\rho, \sigma) = \sqrt{1 - \left(\sum_x \sqrt{P_X(x) Q_X(x)} \right)^2}\,. \tag{3.64}$$

The purified distance enters the definition of the smooth min- and max-entropy below (definition 3.28) in the form of the *ε-ball* with respect to the purified distance. It is defined as follows.

Definition 3.18 (ε-ball): *Let $\rho \in \mathcal{S}^{\leq}(\mathcal{H})$ be a subnormalized state and let $0 \leq \varepsilon \leq \sqrt{\mathrm{tr}(\rho)}$. We define the* ***$\varepsilon$-ball around*** *$\rho$ as*

$$B^{\varepsilon}(\rho) := \{\sigma \in \mathcal{S}^{\leq}(\mathcal{H}) \mid P(\sigma, \rho) \leq \varepsilon\}\,,$$

Another measure that we will use is the *operator norm*. We will use it when we define the preparation quality for the smooth min-max uncertainty relation (theorem 3.30). It is defined as follows.

Definition 3.19 (Operator norm): *For a Hilbert space $\mathcal{H}$, the* ***operator norm*** *on $\mathrm{End}(\mathcal{H})$ is defined as*

$$\begin{aligned} \|\cdot\|_\infty : \quad \mathrm{End}(\mathcal{H}) &\to \mathbb{R}\,, \\ L &\mapsto \sup_{|\psi\rangle \in \mathcal{H}} \frac{\|L|\psi\rangle\|_{\mathcal{H}}}{\||\psi\rangle\|_{\mathcal{H}}}\,, \end{aligned} \tag{3.65}$$

where $\|\cdot\|_{\mathcal{H}}$ denotes the norm on the Hilbert space $\mathcal{H}$.

3.3 State purification and channel purification

In section 3.1.2, we said that the general evolution of a system (which is not assumed to be closed) is given by a TPCPM. In the introduction, we briefly mentioned that every channel can, in an essentially unique way, be seen as the effect of a unitary evolution of a larger, closed system, of which the original system is a subsystem. In this section, we make this statement more precise by recapitulating the concept of *channel purification*. Before we come to that, we start with an easy warm-up and first look at *state purification*.

3.3.1 State purification

In quantum information theory, mixed states are interpreted as states of incomplete knowledge about the preparation of the system. It turns out that any system in a mixed state can be seen as part of a larger system in a pure state. This is called a purification of the mixed state, and is defined as follows.

Definition 3.20 : *Let ρ_A be a state of a system A. A* ***purification*** *of ρ_A is a pure state ρ_{AE}, where E is some other system, such that $\mathrm{tr}_E(\rho_{AE}) = \rho_A$. Such a system E is called a* ***purifying system****.*

In the case where the state ρ_A is pure, it can be seen as its own purification, in which case E is the trivial system with $\mathcal{H}_E \simeq \mathbb{C}$ so that $\mathcal{H}_{AE} \simeq \mathcal{H}_A$. In general, for every d_A-dimensional system, one can find a purification with a purifying system E of at most the same dimension as A, $d_E \leq d_A$ [NC00].

For a mixed state, a purifying system E is necessarily correlated with A, i.e. ρ_{AE} is not a product state. This is of utmost importance in cryptographic settings, where A is a system whose state encodes information that is meant to be secret and where E is a system that may be controlled by an adversary who tries to learn something about the information encoded in A.

Purifications are not unique. However, as we argue in the following, all purifications of a state are equivalent when it comes to assessing an eavesdropper's ability to learn about the information encoded in A. The following proposition is a first step in this direction.

Proposition 3.21 : *Let ρ_A be a state of a system A and let E be a fixed system that is large enough to purify A. Then any two purifications ρ_{AE} and σ_{AE} of ρ_A are related by a unitary on the purifying system. That is, for any two such purifications, there is a unitary U_E on E such that*

$$\sigma_{AE} = (\mathbb{1}_A \otimes U_E)\rho_{AE}(\mathbb{1}_A \otimes U_E^\dagger)\,. \tag{3.66}$$

For a proof, see [NC00]. Proposition 3.21 tells us that as long as we consider a fixed purifying system held by Eve, it does not matter which purification we consider since Eve can switch between any of them by applying a unitary on the system that she controls. Does this picture change if we allow Eve to have any purifying system rather than a fixed one?

To answer this question, let us consider a state ρ_A of a system A and a purification ρ_{AE}, where the dimension of E is the smallest possible to purify A.[4] Clearly, if we allow Eve to hold a different purifying system E' of equal

[4] It can be shown that the smallest such dimension is $d_E = \mathrm{rank}(\rho_A)$ [NC00].

dimension, nothing changes concerning Eve's abilities, so we need to consider the case where Eve holds a larger purifying system E'. There are two such cases: (a) $\mathcal{H}_E$ is a linear subspace of $\mathcal{H}_{E'}$, (b) E is part of a composite system $E' = ER$. The following proposition gives us the necessary information for these two cases.

Proposition 3.22 : *Let ρ_{AE} be a pure state of some joint system AE. Then the following holds:*

(a) The reduced states ρ_A and ρ_E have the same spectrum.

(b) Every state ρ_{AER} for some system R with $\mathrm{tr}_R(\rho_{AER}) = \rho_{AE}$ satisfies $\rho_{AER} = \rho_{AE} \otimes \rho_R$.

Proofs of these statements can be found in [NC00]. Two states having the same spectrum implies that they have the same rank. Therefore, part (a) of the proposition tells us that allowing Eve to hold a larger system E' does not change anything for Eve because the purification cannot have support on the extra dimensions. Part (b) means that any additional systems do not help either because they are necessarily uncorrelated with the already purified system AE. Eve can always add or remove such an uncorrelated system.

The essence of the above discussion is that in cryptographic settings, it does not matter which purification is considered. Eve is equally powerful in any purification. The above can elegantly be summarized by stating that any two purifications of a state are related by an isometry [Wil13].

3.3.2 Channel purification

We have just seen that every state can, in an essentially unique way, be purified. In other words, any system in a state of incomplete information can be seen as part of a larger system with complete information. If anything is correlated with a system A, then it is found in the purification.

Now let us consider a situation where Alice wants to send quantum information to Bob. She encodes the information in a system A and sends it through a channel to Bob who receives it as a system B. In general, the state ρ_B received by Bob is not pure, even if the input system ρ_A to the channel is pure. Thus, information about the system has been lost in the transfer. Where did it go?

If Alice and Bob use the channel in a cryptographic setting, where the information encoded in A is meant to be confidential, they need to assume that the information that they lost in the transfer is held by Eve. Since we said above that anything that is correlated with B must be contained in its purification, this means that Eve needs to be assumed to hold a purification ρ_{BE} of ρ_B. However, the situation is insufficiently described by just one such purification, because that purification purifies the output ρ_B for a given input state ρ_A. It could be that some input states get strongly decohered, whereas others are not decohered at all. One needs to find a description that not only purifies one particular output state, but the whole channel. That is, given a channel

$$\mathcal{C}_{A\to B} : \mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_B)\,, \tag{3.67}$$

we are looking for a map $\mathcal{S}(\mathcal{H}_A) \to \mathcal{S}(\mathcal{H}_{BE})$ that maps an input state ρ_A to a purification ρ_{BE} of the output $\mathcal{C}_{A\to B}(\rho_A)$ of the channel. A special case[5] of the *Stinespring dilation theorem* [Sti55] states that there is always such a map.

Theorem 3.23 (Stinespring dilation theorem): *Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces of finite dimension d_A and d_B, let $\mathcal{C} : \mathrm{End}(\mathcal{H}_A) \to \mathrm{End}(\mathcal{H}_B)$ be a TPCPM. Then there is a Hilbert space $\mathcal{H}_E$ of dimension $d_E \leq d_A d_B$ and an isometry*

$$V : \mathcal{H}_A \to \mathcal{H}_{BE} \tag{3.68}$$

such that

$$\mathrm{tr}_E(V\rho_A V^\dagger) = \mathcal{C}(\rho_A) \quad \forall\, \rho_A \in \mathrm{End}(\mathcal{H}_A)\,. \tag{3.69}$$

At first glance, one may be surprised to find that the dimension of the purifying system E satisfies only $d_E \leq d_A d_B$ rather than $d_E \leq d_B$. The reason, however, is simple. In the case where the input state ρ_A is not pure, we also need to consider a purifying system A' for the input system (see figure 3.3). The purifying system A' can be chosen such that $d_{A'} \leq d_A$ (see the previous subsection). Thus, E needs to purify $A'B$ and thus $d_E \leq d_{A'} d_B \leq d_A d_B$.

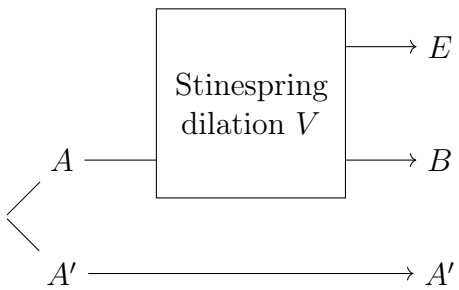


Figure 3.3: Stinespring dilation of a channel. Every channel can be seen as the visible part of an operation that preserves the information encoded in the initial state.

The fact that the Stinespring dilation V of a channel $\mathcal{C}$ is an isometry means that no information is "lost" but rather leaked to Eve. This is because isometries preserve Hilbert space angles and therefore the distinguishability of quantum information. From an information-theoretic point of view, the Stinespring dilation of a channel is the ultimate answer to the question of what Alice and Bob need to consider when they ask themselves where the information that they communicate over the channel is leaked: if information is leaked away from B, it is contained in the output of a Stinespring dilation of the channel.

Some people refer to a Stinespring dilation of a channel as a *channel purification*. For our treatment of decoherence in generalized probabilistic theories (and for foundational aspects of quantum theory), it is interesting to note that

[5] In full generality, the Stinespring dilation theorem makes a statement for arbitrary (not necessarily finite-dimensional) Hilbert spaces, while we only consider the finite-dimensional case here.

a Stinespring dilation of a channel can in turn be seen as part of a unitary with a larger input system (see figure 3.4). We consider an additional input system E' of dimension $d_{E'} = d_B d_E / d_A$ (such that $d_A d_{E'} = d_B d_E$) in a fixed pure state $|\psi\rangle\langle\psi|_{E'}$. Then we define a map

$$\widetilde{U} : \operatorname{span}\Big\{ |\phi\rangle_A \otimes |\psi\rangle_{E'} \,\Big|\, |\phi\rangle_A \in \mathcal{H}_A \Big\} \to \mathcal{H}_{BE} \tag{3.70}$$

as the linear extension of

$$|\phi\rangle_A \otimes |\psi\rangle_{E'} \mapsto V|\phi\rangle_A \quad \forall\, |\phi\rangle_A \in \mathcal{H}_A\,. \tag{3.71}$$

It is not difficult to see that such a map is an isometry and that it can be extended to a unitary $U : \mathcal{H}_{AE'} \mapsto \mathcal{H}_{BE}$. Some authors call such a unitary extension a channel purification (and therefore use this term in a different way than people who call a Stinespring dilation this way).

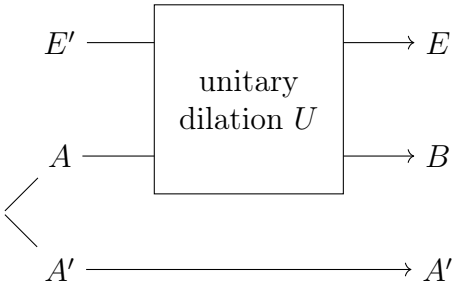


Figure 3.4: Unitary dilation of a channel. Every channel can be seen as the visible part of a unitary evolution of a larger, closed system.

This reconciles channels with the unitary evolution postulate of quantum theory: non-unitary channels are evolutions of open systems that behave unitarily when the scope is extended to include the whole, closed system. It will also help us in the formulation of a decoherence estimation framework for generalized probabilistic theories, as it allows us to see the overall operation acting on one large system rather than mapping from a smaller input system to a larger output system.

3.3.3 Choi-Jamiolkowski representation of a channel

In section 4.4, when we discuss the *decoupling theorem*, we will refer to the *Choi-Jamiolkowski representation* of a channel. It is a way to represent a channel $\mathcal{C}_{A\to S}$ as a bipartite state $\tau_{A'S}$. This representation is given in the form of a map which is called the *Choi-Jamiolkowski isomorphism*. This isomorphism has first been considered by Choi [Cho75]. In the quantum information community, it has become a habit to name it after Jamiolkowski as well, who studied a similar but different isomorphism [Jam72] that was introduced by de Pillis [Pil67]. Both isomorphisms have a relation to the Stinespring dilation theorem that we encountered in the last section; for more information, see [Pau03].

The Choi-Jamiolkowski isomorphism is defined as follows.

Definition 3.24 : *Let A and S be quantum systems, let A' be a copy of A (that is, a quantum system of the same dimension), let $(|i\rangle_A)_{i=1}^{d_A}$ and $(|i\rangle_{A'})_{i=1}^{d_A}$ be a basis of $\mathcal{H}_A$ and $\mathcal{H}_{A'}$, respectively, let*

$$|\Phi\rangle_{A'A} = \frac{1}{\sqrt{d_A}} \sum_{i=1}^{d_A} |i\rangle_{A'} \otimes |i\rangle_A \,. \tag{3.72}$$

*The **Choi Jamiolkowski isomorphism** with respect to the bases $(|i\rangle_A)_{i=1}^{d_A}$ and $(|i\rangle_{A'})_{i=1}^{d_A}$ is the linear map*

$$\begin{array}{rccl} \tau: & \mathrm{Hom}(\mathrm{End}(\mathcal{H}_A), \mathrm{End}(\mathcal{H}_S)) & \to & \mathrm{End}(\mathcal{H}_{A'} \otimes \mathcal{H}_S) \\ & \mathcal{C}_{A\to S} & \mapsto & (\mathbb{1}_{A'} \otimes \mathcal{C}_{A\to S})|\Phi\rangle\langle\Phi|_{A'A} \,. \end{array} \tag{3.73}$$

For a channel $\mathcal{C}_{A\to S}$, the state

$$\tau^{\mathcal{C}}_{A'S} := \tau(\mathcal{C}_{A\to S}) \tag{3.74}$$

*is the **Choi-Jamiolkowski representation** of $\mathcal{C}_{A\to S}$ with respect to the bases $(|i\rangle_A)_{i=1}^{d_A}$ and $(|i\rangle_{A'})_{i=1}^{d_A}$. When the channel $\mathcal{C}$ is clear from the context, we drop the superscript $\mathcal{C}$ and write $\tau_{A'S}$ instead of $\tau^{\mathcal{C}}_{A'S}$.*

The map (3.73) is an isomorphism of vector spaces, that is, it is a bijective linear map. More interestingly, the restriction of τ to channels (TPCPMs) bijectively maps the set of all channels from A to S to the set of all bipartite states $\rho_{A'S}$ for which $\mathrm{tr}_S(\rho_{A'S}) = \mathbb{1}_{A'}/d_A$. This is because of the following two equivalences:

- $\mathcal{C}_{A\to S}$ is completely positive $\iff$ $\tau^{\mathcal{C}}_{A'S}$ is positive,
- $\mathcal{C}_{A\to S}$ is trace-preserving $\iff$ $\mathrm{tr}_S(\tau^{\mathcal{C}}_{A'S}) = \mathbb{1}_{A'}/d_A$

The Choi-Jamiolkowski isomorphism is not a *canonical* isomorphism: it depends on the choice of the bases $(|i\rangle_A)_{i=1}^{d_A}$ and $(|i\rangle_{A'})_{i=1}^{d_A}$. Nonetheless, in many situations, it is common to refer to *the* Choi-Jamiolkowski representation of a channel. This is similar to referring to *the* maximally entangled state, although there are many (see the discussion at the end of section 3.1.1). These two things are related, as becomes apparent in the proof of the following proposition.

Lemma 3.25 : *Let A and S be quantum systems, let $\mathcal{C}_{A\to S}$ be a channel from A to S, let $\tau_{A'S}$ and $\tau'_{A'S}$ each be a Choi-Jamiolkowski representation of $\mathcal{C}_{A\to S}$ (with respect to different bases, in general). Then there is a unitary $U_{A'}$ on A' such that*

$$\tau_{A'S} = (U_{A'} \otimes \mathbb{1}_S)\tau'_{A'S}(U^\dagger_{A'} \otimes \mathbb{1}_S) \,. \tag{3.75}$$

Proof. According to definition 3.24,

$$\tau_{A'S} = (\mathbb{1}_{A'} \otimes \mathcal{C}_{A\to S})|\Phi\rangle\langle\Phi|_{A'A} \,, \tag{3.76}$$

$$\tau'_{A'S} = (\mathbb{1}_{A'} \otimes \mathcal{C}_{A\to S})|\Psi\rangle\langle\Psi|_{A'A} \,, \tag{3.77}$$

where $|\Phi\rangle\langle\Phi|_{A'A}$ and $|\Psi\rangle\langle\Psi|_{A'A}$ are maximally entangled. By virtue of lemma 3.8, there is a unitary $V_{A'}$ on A' such that

$$|\Phi\rangle_{A'A} = (\mathbb{1}_{A'} \otimes V_A)|\Psi\rangle_{A'A} \,. \tag{3.78}$$

By the mirror lemma (see lemma 3.7),

$$(\mathbb{1}_{A'} \otimes V_A)|\Psi\rangle_{A'A} = (V_{A'}^T \otimes \mathbb{1}_A)|\Psi\rangle_{A'A} \,. \tag{3.79}$$

Thus,

$$\begin{aligned}
\tau_{A'S} &= (\mathbb{1}_{A'} \otimes \mathcal{C}_{A\to S})(V_{A'}^T \otimes \mathbb{1}_A)|\Psi\rangle\langle\Psi|_{A'A}((V_{A'}^T)^\dagger \otimes \mathbb{1}_A) && (3.80)\\
&= (V_{A'}^T \otimes \mathbb{1}_S)(\mathbb{1}_{A'} \otimes \mathcal{C}_{A\to S})|\Psi\rangle\langle\Psi|_{A'A}((V_{A'}^T)^\dagger \otimes \mathbb{1}_S) && (3.81)\\
&= (V_{A'}^T \otimes \mathbb{1}_S)\tau'_{A'S}((V_{A'}^T)^\dagger \otimes \mathbb{1}_S) && (3.82)\\
&= (U_{A'} \otimes \mathbb{1}_S)\tau'_{A'S}(U_{A'}^\dagger \otimes \mathbb{1}_S)\,, && (3.83)
\end{aligned}$$

where $U_{A'} = V_{A'}^T$. □

Lemma 3.25 is similar to lemma 3.8. A difference is that in lemma 3.25, the unitary is a unitary on the A' system (which is not transformed by the map $\mathbb{1}_{A'} \otimes \mathcal{C}_{A\to S}$), while in lemma 3.8, either side has a unitary that transforms the two states into one another.

The important consequence of lemma 3.25 is that as long as we are only interested in functions that are invariant under unitaries on A', it does not matter which Choi-Jamiolkowski representation of a channel we consider. When we look at the decoupling theorem in section 4.4, an important quantity will be the min-entropy of the Choi-Jamiolkowski representation of a channel. As we will see in the following section, this quantity is invariant under local unitaries (see lemma 3.29).

3.4 Min- and max-entropy

In this section, we recapitulate the definitions and some basic properties of the smooth min- and max-entropy of quantum states. The quantification of uncertainty by means of entropic quantities is an intensely studied subject in (quantum) information theory. Entropy as an uncertainty measure was introduced in a semial work by Shannon [Sha48], which is seen as the founding work of classical information theory. Von Neumann introduced an analogous entropic measure for quantum states [Neu27]. Since then, many different entropic measures have been introduced. In this thesis, we consider the conditional min- and max-entropy for quantum states, or min- and max-entropy, for short, which has been introduced by Renner [Ren05]. The concept of entropy smoothing, which Renner developed for the min- and max-entropy for quantum states [Ren05], goes back to Cachin and Maurer [CM97; Cac97], who introduced it for classical Rényi entropies [Rén60].

We will not go far beyond merely stating the definitions and properties of the (smooth) min- and max-entropy here. In chapter 4, we will have a closer look at characterizations of the (smooth) min-entropy that are relevant

for our purposes. We can see these characterizations as the motivation for the min-entropy. Thus, we postpone the motivation for the (smooth) min- and max-entropy formalism to a later point. More information on the smooth min- and max-entropy formalism can be found in [Tom12].

We start with the definitions of the non-smooth versions of the min- and max-entropy.

Definition 3.26 : *Let $\rho_{AB} \in \mathcal{S}^{\leq}(\mathcal{H}_{AB})$ be a subnormalized bipartite state. The **min-entropy** of A conditioned on B for the state ρ_{AB} is defined as*

$$H_{\min}(A|B)_\rho := \max_{\sigma \in \mathcal{S}^{\leq}(\mathcal{H}_B)} \sup\{\lambda \in \mathbb{R} \mid \rho_{AB} \leq 2^{-\lambda} I_A \otimes \sigma_B\} \,. \tag{3.84}$$

*The **max-entropy** of A given B for the state ρ_{AB} is defined as*

$$H_{\max}(A|B)_\rho := \max_{\sigma \in \mathcal{S}^{\leq}(\mathcal{H}_B)} \log \left\| \sqrt{\rho_{AB}} \sqrt{I_A \otimes \sigma_B} \right\|_1^2 \,. \tag{3.85}$$

We will often drop the state subscript when it is clear from context for which state the entropy is evaluated. For our proofs in section 5.8, it will be useful to have a simplified expression for $H_{\max}(X|Y)$ for the case where X and Y are classical systems, i.e. for the case where the state ρ_{XY} is of the form

$$\rho_{XY} = \sum_{x,y} P_{XY}(x,y) \; |x\rangle\langle x| \otimes |y\rangle\langle y| \tag{3.86}$$

for some probability distribution P_{XY}. In this case, the max-entropy can be written as [Tom12]

$$H_{\max}(X|Y) = \log \left(\sum_y \left(\sum_x \sqrt{P_{XY}(x,y)} \right)^2 \right) \tag{3.87}$$

$$= \log \sum_y P_Y(y) 2^{H_{\max}(X)_{P^y}} \,, \tag{3.88}$$

where $H_{\max}(X)_{P^y}$ is the unconditional max-entropy of the distribution $P_{X|Y=y}(X)$, namely

$$H_{\max}(X)_{P^y} = 2 \log \sum_x \sqrt{P_{X|Y=y}(x)} \,. \tag{3.89}$$

We will often consider min- and max-entropies for reduced states of already defined states. The following convention makes that easier.

Convention 3.27 : *In contexts where a multipartite state ρ is already defined, the min-entropy $H_{\min}(\,\cdot\,|\,\cdot\,)_\rho$ and the max-entropy $H_{\max}(\,\cdot\,|\,\cdot\,)_\rho$ are evaluated for the reduced state associated with the labels in $H_{\min}(\,\cdot\,|\,\cdot\,)_\rho$ and $H_{\max}(\,\cdot\,|\,\cdot\,)_\rho$. For example, for a tripartite state $\rho_{ABC} \in \mathcal{S}^{\leq}(\mathcal{H}_{ABC})$, the min-entropy $H_{\min}(A|B)_\rho$ is evaluated for the reduced state $\rho_{AB} = \mathrm{tr}_C(\rho_{ABC})$. The same convention holds for the smooth min- and max-entropies that we will define below.*

The smooth min- and max-entropies are defined as optimization problems, where the min- and max-entropy is optimized over all states that are ε-close to the state in question. Thereby, "closeness" is measured in the purified distance that we defined in section 3.2 (see the definition of the ε-ball, definition 3.18).

Definition 3.28 : *Let $\rho_{AB} \in \mathcal{S}^{\leq}(\mathcal{H}_{AB})$ be a bipartite state and let $\varepsilon \geq 0$. We define the* ***ε-smooth min- and max-entropies*** *of A conditioned on B for the state ρ_{AB} as*

$$H^{\varepsilon}_{\max}(A|B)_\rho := \min_{\rho' \in B^{\varepsilon}(\rho)} H_{\max}(A|B)_{\rho'} \,,$$
$$H^{\varepsilon}_{\min}(A|B)_\rho := \max_{\rho' \in B^{\varepsilon}(\rho)} H_{\min}(A|B)_{\rho'} \,.$$

An important property of the smooth min- and max-entropy is that these quantities are invariant under local unitaries, as stated by the following lemma.

Lemma 3.29 : *Let $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ be a bipartite state, let U_A and U_B be unitaries on system A and B, respectively, let $\varepsilon \geq 0$. Then*

$$H^{\varepsilon}_{\min}(A|B)_\rho = H^{\varepsilon}_{\min}(A|B)_\sigma \,, \tag{3.90}$$
$$H^{\varepsilon}_{\max}(A|B)_\rho = H^{\varepsilon}_{\max}(A|B)_\sigma \,, \tag{3.91}$$

where

$$\sigma_{AB} = (U_A \otimes U_B)\rho_{AB}(U_A^\dagger \otimes U_B^\dagger) \,. \tag{3.92}$$

A proof of lemma 3.29 (or of a more general statement in terms of isometries) can be found in [Tom12]. As we will see in chapter 4, the smooth min-entropy $H^{\varepsilon}_{\min}(A|E)$ quantifies the number of uniformly random bits that can be extracted from A such that E is fully decoupled from these bits (that is, Eve has no knowledge about them). This is called *privacy amplification*, and will be discussed in section 4.2. This is very important in quantum key distribution, where E is a purifying system of a composite system AB in which Alice and Bob hold information. Alice and Bob cannot estimate $H^{\varepsilon}_{\min}(A|E)$, directly. However, they can estimate $H^{\varepsilon}_{\max}(A|B)$ and then use the *smooth min-max uncertainty*, proved by Tomamichel and Renner [TR11]. Here we directly formulate it for the qubit case that we are interested in.

Theorem 3.30 (Smooth min-max uncertainty): *Let $\rho_{ABE} \in \mathcal{S}(\mathcal{H}_{ABE})$ be a pure tripartite state where A is an n-qubit system, let $\mathbb{X} = \{\mathbb{X}_0, \mathbb{X}_1\}$ and $\mathbb{Z} = \{\mathbb{Z}_0, \mathbb{Z}_1\}$ be qubit POVMs. Consider the states ρ_{XBE} and ρ_{ZBE} that arise from measuring all of the n qubits of system A with respect to $\mathbb{X}$ and $\mathbb{Z}$, respectively, and storing the outcomes in a classical register X and Z, respectively (c.f. section 3.1.3),*

$$\rho_{XBE} = \sum_{x \in \{0,1\}^n} P_X(x)\ |x\rangle\langle x| \otimes \rho^x_{BE} \,, \tag{3.93}$$
$$\rho_{ZBE} = \sum_{z \in \{0,1\}^n} P_Z(z)\ |z\rangle\langle z| \otimes \rho^z_{BE} \,. \tag{3.94}$$

Then for $\varepsilon \geq 0$,

$$H^{\varepsilon}_{\min}(X|E)_\rho + H^{\varepsilon}_{\max}(Z|B)_\rho \geq nq \,, \tag{3.95}$$

where

$$q = -\log \max_{i,j} \left\| \sqrt{\mathbb{X}_i}\sqrt{\mathbb{Z}_j} \right\|^2_\infty \,. \tag{3.96}$$

The parameter q is the ***preparation quality****. If $\mathbb{X}$ and $\mathbb{Z}$ are mutually unbiased such as the Pauli measurements in equations (3.26) and (3.27), then $q = 1$.*

In a QKD protocol, Alice and Bob estimate $H^{\varepsilon}_{\max}(Z|B)$ by performing a measurement on B. This is because measurements on the side information can only increase the max-entropy, as stated in the following lemma.

Lemma 3.31 : *Let $\varepsilon \geq 0$ and $\rho_{ZB} \in \mathcal{S}^{\leq}(\mathcal{H}_{AB})$ be a bipartite state. Let $\rho_{ZZ'}$ arise from a measurement on system B. Then*

$$H^{\varepsilon}_{max}(Z|B) \leq H^{\varepsilon}_{max}(Z|Z')\,. \tag{3.97}$$

Lemma 3.31 is a corollary of a general *data processing inequality*, proved by Tomamichel [Tom12]. Applying inequality (3.97) to inequality (3.95), we get the following corollary.

Corollary 3.32 : *Let $\rho_{ABE} \in \mathcal{S}(\mathcal{H}_{ABE})$ be a pure tripartite state where A and B are n-qubit systems, let $\mathbb{X}$, $\mathbb{Z}$, q, ε, ρ_{XBE} be as in theorem 3.30 and let $\rho_{ZZ'E}$ arise from measuring all of the $2n$ qubits of A and B with respect to $\mathbb{Z}$. Then*

$$H^{\varepsilon}_{\min}(X|E)_{\rho} + H^{\varepsilon}_{max}(Z|Z')_{\rho} \geq nq\,. \tag{3.98}$$

We will use the uncertainty relation in the form of inequality (3.98) when we prove the security of protocols in section 5.8. Another useful lemma for QKD concerns the reduction of the min-entropy upon learning some classical information. This is important because in a QKD protocol, Alice and Bob communicate classical information about A and need to estimate the implications on the eavesdropper's uncertainty. The following lemma provides a bound for this case. We will use it in the next chapter.

Lemma 3.33 : *Let ρ_{AEY} be a QQC-state, let $0 \leq \varepsilon < 1$. Then*

$$H^{\varepsilon}_{\min}(A|EY) \geq H^{\varepsilon}_{\min}(A|E) - \log d_Y\,. \tag{3.99}$$

A proof of lemma 3.33 can be found in [Tom12].

Chapter 4

Operational characterizations of the min-entropy

In section 3.4, we gave the mathematical definitions of the min-entropy $H_{\min}(A|B)$ and the smooth min-entropy $H^{\varepsilon}_{\min}(A|B)$. In this section, we want to breathe life into these quantities by giving them operational interpretations. In other words, we demonstrate that the min-entropy quantifies how well some operational tasks can be performed, given a quantum state with a certain min-entropy as a resource. The material presented in this section is a selection of some results that have been shown in [KRS09; Tom+11; Dup+10; Tom+12], without any claim on completeness. Of particular importance for our purposes are the characterizations of the min-entropy in terms of the length of an extractable shared secret key (section 4.3), in terms of state merging (section 4.5) and in terms of the minimal distance to the maximally entangled state (section 4.6), whereas the characterizations of section 4.1, section 4.2 and section 4.4 should be seen as preparation.

4.1 Maximal guessing probability

The first characterization that we look at is not of direct relevance for the work presented in this thesis, but it is very suitable for an easy warm-up. In their work on the operational interpretation of the min- and max-entropy [KRS09], König, Renner and Schaffner give several characterizations of the min- and the max-entropy. One of them concerns the special case of classical information X, held by Alice, with quantum side information E, held by Eve. That is, Alice and Bob share a bipartite quantum system in a classical-quantum state (CQ-state)

$$\rho_{XE} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_E^x \,. \tag{4.1}$$

Now consider the task where Eve has to guess the value of X. To this end, she measures her part of the quantum system and makes a guess depending on the outcome of that measurement. For a POVM $\mathcal{M} = \{M_x\}_x$ on E, Eve's probability of guessing correctly is given by

$$p_{\text{guess}}(X|E)_{\mathcal{M}} = \sum_x P_X(x)\mathrm{tr}(M_x\rho_E^x) \,, \tag{4.2}$$

and the guessing probability using an optimal POVM $\mathcal{M}$ is given by

$$p_{\text{guess}}(X|E) := \max_{\mathcal{M}} p_{\text{guess}}(X|E)_{\mathcal{M}} \,. \tag{4.3}$$

König, Renner and Schaffner show that

$$p_{\text{guess}}(X|E) = 2^{-H_{\min}(X|E)} \,. \tag{4.4}$$

Therefore, $H_{\min}(A|E)$ can be seen as expressing the uncertainty of Eve about the classical information X as a decreasing function of her optimal probability of guessing X correctly, $H_{\min}(X|E) = -\log p_{\text{guess}}(X|E)$.

4.2 Privacy amplification

In this section, we look at *privacy amplification*. The concept of privacy amplification goes back to work by Bennett et al. [BBR88], who introduced it in the context of quantum key distribution [Ben+92; Ben+95]. The technical result that enables privacy amplification is the *leftover hashing lemma*, which also has other applications (see [Sti02] for an overview). The first formulation of the leftover hashing lemma was made by Impagliazzo et al. [ILL89], who introduced it in the context of pseudorandom number generation. The analysis of the more general case of leftover hashing against quantum side information (also called *quantum* leftover hashing), which is the relevant case for us, was initiated by König, Maurer and Renner [KMR05; RK05]. Here, we present the quantum leftover hashing lemma in a further developed form that has been derived by Tomamichel et al. [Tom+11]. For other examples of further development in quantum leftover hashing, see [HT16] and references therein.

As in the previous section, we consider the case where Alice holds classical information X and Eve holds quantum side information E, but this time we give a characterization of the smooth min-entropy instead of the unsmoothed one. Let us assume that the quantum system X is a bit string of length n. Eve has some knowledge about that bit string, quantified by $H^{\varepsilon}_{\min}(X|E)$. Now one may ask the following question: Is it possible for Alice to map the n-bit string X to a shorter bit string K of length $l < n$ such that K is uniformly random and uncorrelated with Eve? More precisely, is there an operation mapping the n-bit system X to an l-bit system K such that the resulting state is

$$\rho_{KE} = \pi_K \otimes \rho_E \,, \tag{4.5}$$

where

$$\pi_K = \frac{1}{2^l} \sum_{k \in \{0,1\}^l} |k\rangle\langle k| \tag{4.6}$$

is the maximally mixed state on the l-bit string? Such an operation is called privacy amplification, because it turns a string about which Eve has partial knowledge into a string about which Eve has no knowledge. It can be seen as the extraction of secret uniform randomness: system K in the maximally

mixed state provides Alice with uniform randomness, and this randomness is secret because Eve's system E is fully decoupled (i.e. uncorrelated) from system K.

In general, it is not possible to achieve condition (4.5) perfectly. However, it is possible for Alice to achieve this condition *approximately*. Let us assume that Alice is satisfied if the resulting state satisfies

$$\frac{1}{2}\|\rho_{KE} - \pi_K \otimes \rho_E\|_1 \leq \Delta \tag{4.7}$$

for some small enough Δ. The idea is that if the initial uncertainty of Eve $H^{\varepsilon}_{\min}(X|E)$ is large enough and the length l of Alice's resulting string K is small enough, then this might be possible.

As it turns out, such a thing cannot be achieved using a fixed function, in general. However, the *quantum leftover hashing lemma* [Tom+11] states that this can be achieved by a so-called *two-universal hashing*. The idea is as follows. Alice applies a function $f : \{0,1\}^n \to \{0,1\}^l$ to map her n-bit string X to an l-bit string K, but instead of using a fixed function, she randomly chooses f from a family $\mathcal{F}$ which is two-universal, that is

$$\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}} \delta_{f(x),f(y)} \leq 2^{-l} \quad \text{for all } x, y \in \{0,1\}^n \text{ with } x \neq y\,, \tag{4.8}$$

where δ denotes the Kronecker delta. Inequality (4.8) means that for every pair $x, y \in \{0,1\}^n$ of non-identical strings, the probability that a function $f \in \mathcal{F}$, chosen uniformly at random, maps x and y to the same l-bit string is not higher than if they would be assigned to random elements of $\{0,1\}^l$.

Let us write the initial state as

$$\rho_{XE} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho^x_E \tag{4.9}$$

$$= \sum_x |x\rangle\langle x| \otimes \sigma^x_E\,, \tag{4.10}$$

where the first equation is equation (4.1) and where for each x, σ^x_E is the subnormalized state

$$\sigma^x_E = P_X(x)\rho^x_E\,. \tag{4.11}$$

Suppose that Alice chooses a function $f \in \mathcal{F}$ uniformly at random, applies it to the bit string X to obtain a bit string K and keeps a record of her choice of function in a register F. Then the resulting state ρ_{KEF} is given by

$$\rho_{KEF} = \frac{1}{|\mathcal{F}|}\sum_f \sum_k |k\rangle\langle k| \otimes \sigma^{[f,k]}_E \otimes |f\rangle\langle f|\,, \tag{4.12}$$

where

$$\sigma^{[f,k]}_E := \sum_{x\in f^{-1}(k)} \sigma^x_E\,. \tag{4.13}$$

The reader may wonder why it is helpful to consider an extra register F with a record of the choice of the function f. The reason is that it helps to formulate a strong result: it turns out that the bit string K is approximately uniformly random and decoupled from Eve *even* if Eve is given that register F (i.e. even if Eve knows which function $f \in \mathcal{F}$ has been applied). This is the statement of the *quantum leftover hashing lemma*, formulated and proved by Tomamichel et al. [Tom+11].

Theorem 4.1 (Quantum leftover hashing lemma): *Let $\mathcal{F}$ be a two-universal family of functions $f : \{0,1\}^n \to \{0,1\}^l$, let ρ_{XE} and ρ_{KEF} be defined as in equations (4.1) and (4.12), respectively. Then*

$$\frac{1}{2}\|\rho_{KEF} - \pi_K \otimes \rho_{EF}\|_1 \leq \Delta\,, \tag{4.14}$$

where

$$\Delta \leq \varepsilon + \frac{1}{2}\sqrt{2^{l-H^{\varepsilon}_{\min}(X|E)}} \tag{4.15}$$

and where π_K is the maximally mixed state as in equation (4.6).

Therefore, considering the bipartite system EF as the system that Eve controls after the hashing, i.e. $E' = EF$, we can rewrite inequality (4.14) as

$$\|\rho_{KE'} - \pi_K \otimes \rho_{E'}\|_1 \leq \Delta\,, \tag{4.16}$$

so the condition of (4.7) is satisfied even if Eve is fully informed about how Alice transformed the string X into the string K. A randomness extraction process with this property is called a *strong extractor*. This property will be of major importance in the following subsection.

The distance Δ, which quantifies how far the extraction is from a perfect extraction, has the expected behavior: the smaller the resulting string length l and the higher Eve's initial uncertainty $H^{\varepsilon}_{\min}(X|E)$ about X is, the better the extraction performs. For a fixed distance Δ, inequality (4.15) can be solved for the maximal length l that can be extracted within distance Δ,

$$l = \left\lfloor H^{\varepsilon}_{\min}(X|E) - 2\log\frac{1}{2(\Delta-\varepsilon)}\right\rfloor\,. \tag{4.17}$$

Equation (4.17) shows that $H^{\varepsilon}_{\min}(X|E)$ quantifies the length of a secret uniformly random bit string that can be extracted from X.

4.3 Extraction of a shared secret key

Building on the quantum leftover hashing lemma presented in the last subsection, we will now look into the important role that the smooth min-entropy plays in quantum key distribution (QKD). To this end, we extend the bipartite setting of the last subsection to a tripartite setting. We consider three parties Alice, Bob and Eve, where Alice and Bob are cooperating parties that trust each other and Eve is an adversary. Consider the case where Alice, Bob and Eve share the CCQ-state

$$\rho_{XX'E} = \sum_{x,x'} P_{XX'}(x,x')\ |x\rangle\langle x| \otimes |x'\rangle\langle x'| \otimes \rho_E^{x,x'}\,, \tag{4.18}$$

where Alice holds system X, Bob holds system X' and Eve holds system E. Analogously to the previous subsection, we consider X and X' to be classical bit strings of length n with quantum side information E under the control of Eve.

In contrast to the previous subsection, where Alice's task was to extract secret uniform randomness of a single system, we now consider the task where Alice and Bob cooperatively extract a *shared secret key*. This means that they want to end up in a situation in which Alice holds a bit string K, Bob holds a bit string K' (the two copies of the shared key) and Eve holds some quantum side information E'' (the reason for the use of a double prime will become clear below) such that two properties, called *correctness* and *secrecy*, are satisfied. To achieve these conditions, they are allowed to perform classical post-processing of their data X and X'. Thereby, they communicate over a classical communication channel which is *public* and *authenticated*. This means that Eve can read but not modify all of the messages that Alice and Bob exchange.

Here we closely follow [Tom+12] in the formulation of the correctness and secrecy conditions. In order to formulate these two conditions, it is helpful to to see the keys as random variables induced by the final state $\rho_{KK'E''}$, jointly distributed according to

$$P_{KK'}(k,k') = \langle k| \otimes \langle k'|\rho_{KK'}|k\rangle \otimes |k'\rangle \,. \tag{4.19}$$

The *ideal* secrecy and correctness conditions read as follows:

- **Correctness**: Alice's and Bob's keys are identical, $K = K'$.
- **Secrecy**: The key is uniformly random and uncorrelated with Eve, i.e. $\rho_{KE''} = \pi_K \otimes \rho_{E''}$ where π_K is the maximally mixed state on the key register and $\rho_{E'}$ is the reduced state of Eve.

Note that the secrecy condition is identical to the secrecy condition in equality (4.5) above, the only difference being that it is now formulated for the reduced state $\rho_{KE''}$ of a tripartite state $\rho_{KK'E''}$. Note that if secrecy and correctness are satisfied simultaneously, then the secrecy condition also holds for Bob, i.e. $\rho_{K'E''} = \pi_{K'} \otimes \rho_{E''}$. Correctness and secrecy together form the *security* conditions, i.e. we say that we are given security when we are given correctness and secrecy.

In analogy to the previous subsection, the ideal security conditions stated above cannot be achieved in general. Instead, approximate security conditions need to be introduced. They are formulated with respect to parameters $\varepsilon_{\text{cor}}, \Delta > 0$ and the final state $\rho_{KK'E''}$ as follows:

- **ε_{cor}-correctness:** The probability that Alice's and Bob's key differ is bounded by ε_{cor}, i.e.

$$P[K \neq K'] \leq \varepsilon_{\text{cor}} \,. \tag{4.20}$$

- **Δ-secrecy:** The key K is Δ-indistinguishable from a key which is uniformly random and uncorrelated with Eve. More precisely,

$$\frac{1}{2}\|\rho_{KE''} - \pi_K \otimes \rho_{E''}\|_1 \leq \Delta \,. \tag{4.21}$$

Again, the Δ-secrecy condition (4.21) is the same as the condition in inequality (4.7), just that it is formulated with respect to $\rho_{KK'E''}$.

Now we want to see how Alice and Bob can cooperatively transform the initial state $\rho_{XX'E}$ into an ε_{cor}-correct and Δ-secret state $\rho_{KK'E''}$. The idea is to do this in two sequential steps:

- In the first step, they execute an error correcting code and perform a hash comparison (EC & HC) in order to achieve ε_{cor}-correctness,
- In the second step, they perform a privacy amplification (PA) (c.f. section 4.2), where both Alice and Bob hash down their string to a shorter string about which Eve has almost no knowledge. This way, they achieve Δ-secrecy.

Figure 4.1 shows a diagram that helps to keep the overview during the following discussion.

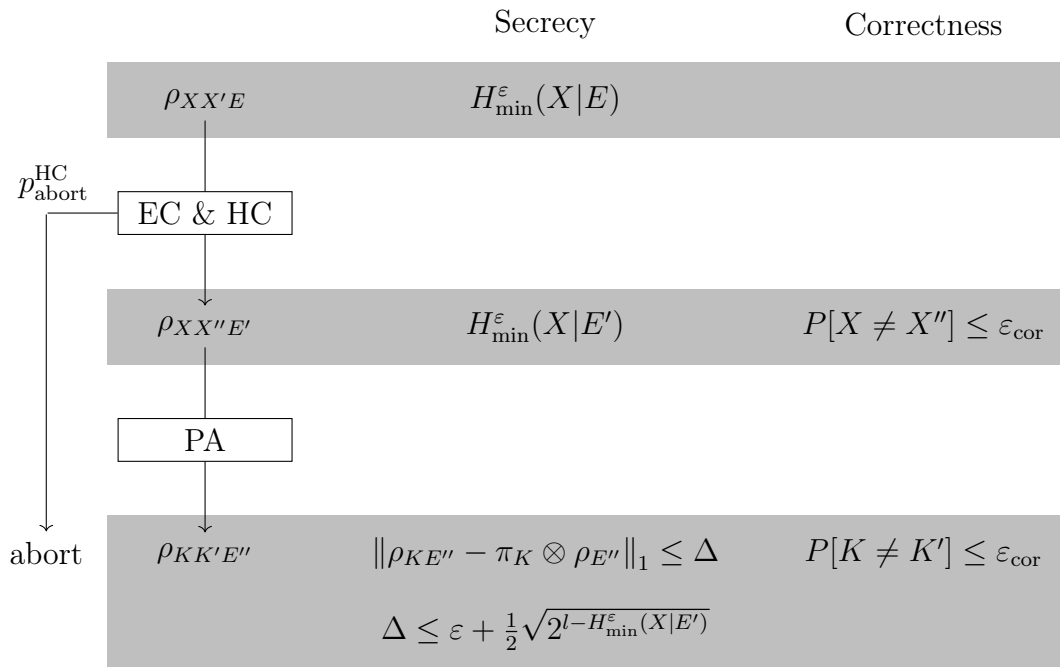


Figure 4.1: Extraction of a shared secret key from a tripartite state.

The goal of the first step (EC & HC) is that the bit strings X and X' of Alice and Bob are transformed into identical bit strings. To this end, they communicate over the public authenticated channel, thereby leaking as little information about the string as possible. This is known as *information reconciliation*. This subject was studied, for example, by Brassard and Salvail [BS94], building on earlier work by other authors [Rob85; BBR88; Ben+92]. For more about information reconciliation, see [Tom+14] and references therein. Here, we prefer to call it error correction and hash comparison instead of information reconciliation, because it refers more specifically to what kind of scheme we have in mind.

In that scheme, Alice and Bob carry out an error correcting code, considering Alice's bit string X as the "correct" bit string and Bob's bit string X'

as the bit string that needs to be corrected. The details of the applied code are not important for our purposes. For us, it is sufficient to understand what the code achieves: Alice's bit string X remains unchanged, Bob's bit string X' gets mapped to a "corrected" bit string X'' and, since Alice and Bob need to communicate over a public channel, Eve receives $\mathrm{leak}_{\mathrm{EC}}$ bits of information about X for some $\mathrm{leak}_{\mathrm{EC}} \in \mathbb{N}$. For more information about error correcting codes, see [HP10].

After the error correction, Alice and Bob perform a hash comparison to check whether $X = X''$. Alice randomly chooses a function g from an $\varepsilon_{\mathrm{cor}}$-almost universal family $\mathcal{G}$ of hash functions $g : \{0,1\}^n \to \{0,1\}^{n'}$, that is, a family $\mathcal{G}$ such that

$$\frac{1}{|\mathcal{G}|} \sum_{g \in \mathcal{G}} \delta_{g(x),g(y)} \leq \varepsilon_{\mathrm{cor}} \quad \text{for all } x, y \in \{0,1\}^n \text{ with } x \neq y\,. \tag{4.22}$$

Such a family can always be chosen such that $n' = \lceil \log(1/\varepsilon_{\mathrm{cor}}) \rceil$. Then, Alice applies g to her string to obtain an n'-bit string $g(X)$ and sends both the choice of the function g and the string $g(X)$ to Bob. This gives Eve another $\lceil \log(1/\varepsilon_{\mathrm{cor}}) \rceil$ bits of information about X (the choice of the function g is uncorrelated with X and thus does not give Eve more information about X). This allows Bob to check whether $g(X) = g(X'')$. If $g(X) \neq g(X'')$, then necessarily $X \neq X''$, so Alice and Bob abort. If $g(X) = g(X'')$, then $X = X''$ with probability $1 - \varepsilon_{\mathrm{cor}}$ and they continue the protocol.

After EC & HC, Alice, Bob and Eve share a system in the overall state $\rho_{XX''E'}$, where E' is Eve's system E, together with the information about X that was communicated over the public channel during the error correction ($\mathrm{leak}_{\mathrm{EC}}$ bits) and during hash comparison ($\lceil \log(1/\varepsilon_{\mathrm{cor}}) \rceil$ bits). As we have just argued, this state satisfies $P[X \neq X''] \leq \varepsilon_{\mathrm{cor}}$ which, as we will see below, turns into the correctness condition (see figure 4.1). For the secrecy condition in the next step, we need to bound the information $H^{\varepsilon}_{\min}(X|E')$ as a function of the initial uncertainty $H^{\varepsilon}_{\min}(X|E)$ (note the difference: E vs. E'). Let us denote the classical register with the $\mathrm{leak}_{\mathrm{EC}} + \lceil \log(1/\varepsilon_{\mathrm{cor}}) \rceil$ bits of information that Eve holds by F, so that $E' = EF$. Then we have

$$\begin{aligned} H^{\varepsilon}_{\min}(X|E') &= H^{\varepsilon}_{\min}(X|EF) && (4.23)\\ &\geq H^{\varepsilon}_{\min}(X|E) - \log d_F && (4.24)\\ &= H^{\varepsilon}_{\min}(X|E) - \mathrm{leak}_{\mathrm{EC}} - \lceil \log(1/\varepsilon_{\mathrm{cor}}) \rceil\,, && (4.25) \end{aligned}$$

where we used lemma 3.33 for the inequality.

Now Alice and Bob hold strings X and X'' which are identical with probability $1 - \varepsilon_{\mathrm{cor}}$ and about which Eve has partial uncertainty, expressed by inequality (4.25). Now Alice and Bob can make use of the quantum leftover hashing lemma (theorem 4.1) and perform a simultaneous privacy amplification. To this end, Alice chooses a function $f \in \mathcal{F}$ uniformly at random, where $\mathcal{F}$ is a two-universal family of hashing functions $f : \{0,1\}^n \to \{0,1\}^l$. Then Alice communicates the choice of f to Bob. Since their communication is public, Eve gets this information too, and stores it in a register F. Therefore, Eve holds side information $E'' = E'F$. Then both Alice and Bob hash down their string using the function f, ending up with l-bit strings $K = f(X)$

and $K' = f(X'')$. According to the quantum leftover hashing lemma of the previous subsection, the resulting state $\rho_{KK'E'F}$ satisfies

$$\frac{1}{2}\|\rho_{KE'F} - \pi_K \otimes \rho_{E'F}\|_1 \leq \Delta\,, \tag{4.26}$$

where

$$\Delta \leq \varepsilon + \frac{1}{2}\sqrt{2^{l-H^{\varepsilon}_{\min}(X|E')}}\,. \tag{4.27}$$

Rewriting inequality (4.26) with the substitution $E'' = E'F$ and using the bound (4.25) in inequality (4.27) gives

$$\frac{1}{2}\|\rho_{KE''} - \pi_K \otimes \rho_{E''}\|_1 \leq \Delta\,, \tag{4.28}$$

with

$$\Delta \leq \varepsilon + \frac{1}{2}\sqrt{2^{l-H^{\varepsilon}_{\min}(X|E)-\mathrm{leak}_{\mathrm{EC}}-\lceil\log(1/\varepsilon_{\mathrm{cor}})\rceil}}\,. \tag{4.29}$$

Thus, the secrecy condition (4.20) is fulfilled with a distance Δ that accounts for the $\mathrm{leak}_{\mathrm{EC}} + \lceil\log(1/\varepsilon_{\mathrm{cor}})\rceil$ bits of information that were communicated for EC & HC.

The correctness condition $P[K \neq K'] \leq \varepsilon_{\mathrm{cor}}$ follows trivially from the inequality $P[X \neq X''] \leq \varepsilon_{\mathrm{cor}}$, because the hashing only increases the likelihood that the strings coincide. Note the importance of the fact that the hashing is a strong extractor: since Alice and Bob need to use the same hashing function to preserve correctness, they had to communicate the choice of f. This is why it is important that inequality (4.28) holds with register F.

In practice, Alice and Bob fix the secrecy parameter Δ in advance and then extract a key of the largest length compatible with Δ. Solving inequality (4.29) for that maximal l gives

$$l = \left\lfloor H^{\varepsilon}_{\min}(X|E) - 2\log\frac{1}{2(\Delta-\varepsilon)\rceil} - \mathrm{leak}_{\mathrm{EC}} - \lceil\log(1/\varepsilon_{\mathrm{cor}})\rceil\right\rfloor\,. \tag{4.30}$$

We conclude the following.

Proposition 4.2 : *Given $\varepsilon \geq 0$, $\varepsilon_{cor} > 0$, a CCQ-state $\rho_{XX'E}$ and an error correcting code that communicates leak_{EC} bits of information, Alice can probabilistically extract a ε_{cor}-correct and Δ-secret shared key K, K' of length l, with l given in equality (4.30) and Δ bounded in inequality (4.27).*

For Alice and Bob to know the length l of the keys that they can extract, they need to have a bound on $H^{\varepsilon}_{\min}(X|E)$. The extraction is probabilistic because Alice and Bob may abort during the hash comparison with some probability $p^{\mathrm{HC}}_{\mathrm{abort}}$. The probability $p^{\mathrm{HC}}_{\mathrm{abort}}$ is a function of the state $\rho_{XX'}$ and thus not known in practical situations. However, this is not a problem: If Alice know $H^{\varepsilon}_{\min}(X|E)$ for a given $\varepsilon \geq 0$, then *conditioned on passing* the hash comparison, they know that their shared key satisfies the desired security condition. The important point is that Alice and Bob need to know $H^{\varepsilon}_{\min}(X|E)$ for a known, given $\varepsilon > 0$. Note also the relation between ε and Δ: for a Δ-secret key, ε needs to be sufficiently much smaller than Δ, see equation (4.30).

4.3.1 Application to secret communication and quantum key distribution

What is the use of proposition 4.2? Imagine a situation where Alice and Bob are at distant locations, and they want to generate a shared key for the use in a one-time pad. According to proposition 4.2, all that Alice and Bob need to achieve is to run a protocol at the end of which they share a state $\rho_{XX'E}$ with Eve such that the min-entropy $H^{\varepsilon}_{\min}(X|E)$ is bounded from below. Then, if that protocol is followed by error correction, hash comparison and privacy amplification, they have distributed a secure shared key. The resulting protocol is thus a key distribution protocol, a *quantum key distribution* (QKD) protocol. Thus, we can say that proposition 4.2 reduces the task of finding a QKD protocol to finding a protocol that distributes a state $\rho_{XX'E}$ with n-bit strings X and X' such that the min-entropy $H^{\varepsilon}_{\min}(X|E)$ is bounded from below.

A typical QKD protocol consists of the following subroutines:

(i) Preparation, distribution, measurement and sifting,

(ii) Parameter estimation,

(iii) Error correction and hash comparison,

(iv) Privacy amplification.

Proposition 4.2 allows us to separate subroutines (i) and (ii) from subroutines (iii) and (iv). Hence, we are looking for a protocol consisting of subroutines (i) and (ii) which produces a state $\rho_{XX'E}$ with a lower-bounded entropy $H^{\varepsilon}_{\min}(X|E)$. For increased convenience in chapter 5, we shall make the following convention.

Convention 4.3 : *We call a protocol that distributes bit strings X and X' to Alice and Bob in an overall state $\rho_{XX'E}$ with a lower bounded min-entropy $H^{\varepsilon}_{\min}(X|E)$ a* ***raw key distribution protocol****.*

In chapter 5, we discuss raw key distribution protocols in detail. We find that many QKD protocols in the literature use combinations of subroutines (i) and (ii) with a serious security flaw, i.e. with a wrong estimation of $H^{\varepsilon}_{\min}(X|E)$. (We will see later what exactly that means.) Reducing QKD to these two subroutines is therefore very convenient for our purposes.

4.4 Decoupling

In section 4.2, looked at the quantum leftover hashing lemma. Roughly speaking, it states that if a classical system X with quantum side information E has a sufficiently high min-entropy $H^{\varepsilon}_{\min}(X|E)$, then X can be mapped to a bit string K which is almost fully decoupled from E. Note that here, the system that is decoupled from Eve is a *classical* system.

This raises the question whether this can be generalized to a fully quantum setting, where not only the side information E is assumed to be a quantum

register, but where also the information to be decoupled is quantum information. For example, one may consider a system AE, where A is an n-qubit system, and ask the following question: if $H^{\varepsilon}_{\min}(A|E)$ is sufficiently high, is there an operation that maps the n-qubit system A to a smaller l-qubit system S (with $l < n$) such that S is almost fully decoupled from E? This could be seen as a generalization of leftover hashing to the case where the hashed information is quantum information. The *decoupling theorem*, which we will state in theorem 4.4 below, states such a generalization, using a decoupling operation for quantum information. The first form of the decoupling theorem was derived by Abeyesinghe et al. [Abe+09]. It was used by Hayden et al. to find a new proof of the LSD theorem that relates the coherent information to the channel capacity [Hay+08]. The one-shot version of the decoupling theorem that we consider here was derived by Berta [Ber08] and Dupuis et al. [Dup09; Dup+10].

For devising such a decoupling operation, one needs to come up with an analogue of the random hashing functions $f \in \mathcal{F}$ used in the leftover hashing (see section 4.2 which acts on quantum systems instead of on bit strings. To gain some intuition, let us oversimplify the action of the hashing functions $f \in \mathcal{F}$. Actual constructions of families of two-universal hash functions are more involved, but for now, we can think of hash functions $f : \{0,1\}^n \to \{0,1\}^l$ as being composed of a permutation of the n bits, followed by the discarding of some bits. To get different functions of the family $\mathcal{F}$, one varies the permutation, but discards the same bits. A bit more formally, we can write the hashing that transforms the state ρ_{XE} into a state ρ_{KE} as

$$\rho_{KE} = \frac{1}{|\mathcal{F}|} \sum_{\sigma \in S_{\mathcal{F}}} \operatorname{tr}_{X_1 \ldots X_{n-l}} (U_\sigma \otimes \mathbb{1}_E) \rho_{XE} (U_\sigma^\dagger \otimes \mathbb{1}_E) \,. \tag{4.31}$$

where U_σ is a unitary that permutes the bits of X according to the permutation σ and where $S_{\mathcal{F}}$ is a set of permutations of the n bits that defines the family $\mathcal{F}$ of hash functions. For simplicity, we just consider the first $n - l$ bits to be discarded to map an n-bit string to an l-bit string. The attentative reader may have noticed that in contrast to equation (4.12), we do not consider the case where Eve is given the hash function f that has been applied; there is no F register in the side information. Indeed, we modify the situation here insofar as we do not consider strong extractors.

More generally, the operation mapping ρ_{XE} to ρ_{KE} can be thought of as not only involving unitaries that just permute the bits but which also perform reversible operations on those bits themselves, such as bit flips. Such combinations of system permutations and bit flips would again be unitaries, so more generally, we could write

$$\rho_{KE} = \frac{1}{|\mathcal{F}|} \sum_{U_X \in \mathcal{U}_{\mathcal{F}}} \operatorname{tr}_{X_1 \ldots X_{n-l}} (U_X \otimes \mathbb{1}_E) \rho_{XE} (U_X^\dagger \otimes \mathbb{1}_E) \,, \tag{4.32}$$

where now $\mathcal{U}_{\mathcal{F}}$ is a set of unitaries that defines the family $\mathcal{F}$.

The operation producing the state (4.32) is tailored for classical bit strings. They are composed of clearly distinct subsystems (the individual bits), and each of these subsystems has a clearly distinct basis (consisting of $|0\rangle$ and $|1\rangle$).

The permutations of the systems and the trace operation $\mathrm{tr}_{X_1 \ldots X_{n-l}}$ assume a distinct subdivision into subsystems, and the bit flips act in a particular basis. For general quantum systems, such distinctions are not given, in general. For a general decoupling, we must therefore think of a generalization of these operations.

Now consider the case where we have a quantum system AE in a state ρ_{AE} that we want to map it to a smaller quantum system SE such that the resulting state ρ_{SE} is almost decoupled from E. As an analogue of the trace operation $\mathrm{tr}_{X_1 \ldots X_{n-l}}$ that discards particular subsystems, we consider any TPCPM $\mathcal{T}_{A\to S}$ that maps the quantum system A to a smaller quantum system S. Secondly, we replace the set $\mathcal{U}_{\mathcal{F}}$ of unitaries by the whole unitary group $\mathbb{U}_A$ of system A. Accordingly, the summation over the set $\mathcal{U}_{\mathcal{F}}$ becomes a *Haar measure* integral over the group $\mathbb{U}_A$,

$$\frac{1}{|\mathcal{F}|} \sum_{U \in \mathcal{U}_{\mathcal{F}}} \quad \to \quad \int\limits_{U_A \in \mathbb{U}_A} dU_A \,. \tag{4.33}$$

Thus, as an analogue of equation (4.32), we can write

$$\rho_{SE} = \int\limits_{U_A \in \mathbb{U}_A} (\mathcal{T}_{A\to S} \otimes \mathbb{1}_E)(U_A \otimes \mathbb{1}_E)\rho_{AE}(U_A^\dagger \otimes \mathbb{1}_E) dU_A \,, \tag{4.34}$$

or using the shorthand notation $\mathcal{T}_{A\to S} := (\mathcal{T}_{A\to S} \otimes \mathbb{1}_E)$ and $U_A := (U_A \otimes \mathbb{1}_E)$,

$$\rho_{SE} = \int\limits_{U_A \in \mathbb{U}_A} \mathcal{T}_{A\to S}(U_A \rho_{AE} U_A^\dagger) dU_A \,. \tag{4.35}$$

The state ρ_{SE} can be seen as resulting from applying a random unitary, followed by mapping the large system A down to a smaller system S using a fixed map $\mathcal{T}_{A\to S}$.

The motivation of equation (4.35) was a bit vague, but it servers the purpose of giving an intuition for the operations involved in the decoupling theorem. Now we are ready to state it formally (see [Dup+10]).

Theorem 4.4 (Decoupling theorem): *Let $\rho_{AE} \in \mathcal{S}(\mathcal{H}_{AE})$ be a bipartite state, let S be another quantum system, let $\mathcal{T}_{A\to S}$ be a TPCPM, let $\tau_{A'S}$ be its Choi-Jamiolkowski representation. Then, for every $\varepsilon > 0$, it holds that*

$$\int\limits_{U_A \in \mathbb{U}_A} \left\| \mathcal{T}_{A\to S}(U_A \rho_{AE} U_A^\dagger) - \tau_S \otimes \rho_E \right\|_1 dU_A \leq 2^{-\frac{1}{2}H^\varepsilon_{\min}(A|E)_\rho - \frac{1}{2}H^\varepsilon_{\min}(A'|S)_\tau} + 12\varepsilon \,. \tag{4.36}$$

Note that by lemmata 3.25 and 3.29, it does not matter which Choi-Jamiolkowski representation $\tau_{A'S}$ of $\mathcal{T}_{A\to S}$ is chosen. Inequality (4.36) states a bound for the expected difference of the transformed state from the fully decoupled state $\tau_B \otimes \rho_E$. The bound depends on the initial uncertainty $H^\varepsilon_{\min}(A|E)_\rho$ that Eve has about A, as well as the min-entropy $H^\varepsilon_{\min}(A|S)_\tau$ of the Choi-Jamiolkowsi representation τ_{AS} of the map $\mathcal{T}_{A\to S}$. The latter quantifies how suitable the map $\mathcal{T}_{A\to S}$ is for decoupling.

As already mentioned above, the decoupling theorem does not make a statement about how suitable the decoupling is as a strong extractor, which contrasts with the quantum leftover hashing lemma. Another difference is that here, Alice chooses from a continuous set of unitaries, instead of from a finite set of hashing functions. However, it is possible to state decoupling theorems for finite sets of unitaries. We will not cover such constructions. The interested reader is referred to the decoupling theorem for *unitary approximate two-designs* [HP07; Sze+13].

4.5 Quantum state merging

In the last section, we have seen how Alice can decouple her system A from another system E in the case where the min-entropy $H^{\varepsilon}_{\min}(A|E)$ is high. It is not immediately obvious why this is useful, as the quantum information that Alice decouples from Eve is not distributed but only held by Alice. However, the decoupling theorem has important implications for protocols with distributed information. Here, we are going to see one such protocol, called *quantum state merging*. The information presented in this section can be found in [Dup+10]. We will first explain quantum state merging, and then explain its relation to decoupling further below.

The notion has been introduced by Horodecki, Oppenheim and Winter [HOW05; HOW06]. Initially, quantum state merging was considered in the asymptotic limit. Here, we consider the more general one-shot version, which has first been investigated in [Ber08], and preliminary results appeared in [KRS09]. The result that we present in theorem 4.6 below has been shown in [Dup+10]. We start by giving the formal definition of quantum state merging. Since the definition is not easy to absorb at first, the reader may have a look at the diagram and the explaining caption of figure 4.2 while reading definition 4.5.

Definition 4.5 : *Let $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ be a bipartite state purified by a state ρ_{ABE}, let A_0 and B_0 be K-dimensional systems, let B_0 and B_1 be L-dimensional systems. A TPCPM*

$$\mathcal{E} : \mathrm{End}(\mathcal{H}_{AA_0BB_0}) \to \mathrm{End}(\mathcal{H}_{A_1B_1B'B}) \tag{4.37}$$

is a ***quantum state merging of the state*** *ρ_{AB} with error $\varepsilon \geq 0$ if $\mathcal{E}$ is a local operation and classical forward communication process for the bipartition $AA_0 \to A_1$ vs. $BB_0 \to B_1B'B$ and*

$$(\mathcal{E} \otimes \mathbb{1}_E)(|\Phi\rangle\langle\Phi|^K_{A_0B_0} \otimes \rho_{ABE}) \approx_\varepsilon |\Phi\rangle\langle\Phi|^L_{A_1B_1} \otimes \rho_{BB'E}\,, \tag{4.38}$$

where $|\Phi\rangle\langle\Phi|^K$ and $|\Phi\rangle\langle\Phi|^L$ are maximally entangled states of the pairs A_0B_0 and A_1B_1, respectively, and where the symbol $\approx_\varepsilon$ denotes ε-closeness in the purified distance. The number

$$l^\varepsilon := \log K - \log L \tag{4.39}$$

is the ***entanglement cost*** *of the quantum state merging.*[1]

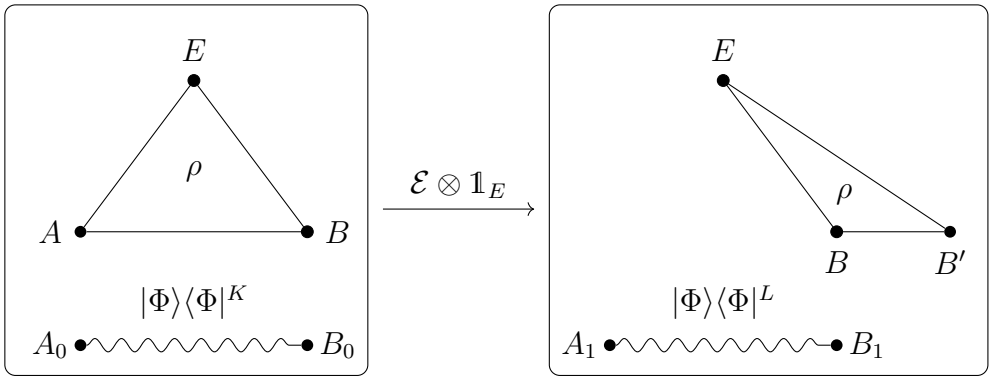


Figure 4.2: Quantum state merging. Alice and Bob share a bipartite system in a state ρ_{AB}, purified by some state ρ_{ABE}. The goal of Alice and Bob is to transfer the information encoded in A to a system B' on Bob's side, thereby reproducing the correlations with both B and E. In other words, they want to reproduce the state ρ_{AB} on Bob's side, such that the purification remains intact with the same purifying system. To achieve this, Alice and Bob are provided with a pair A_0B_0 of K-dimensional systems in a maximally entangled state $|\Phi\rangle\langle\Phi|^K_{A_0B_0}$. Alice and Bob cooperatively implement a TPCPM $\mathcal{E}$ from system AA_0BB_0 to system $A_1B_1B'B$ by performing local operations on their systems, as well as classical communication from Alice to Bob. The effect of this operation is that the state ρ is moved from system ABE to the system $B'BE$, and instead of a K-dimensional maximally entangled pair A_0B_0, they hold a pair A_1B_1 of L-dimensional systems in the maximally entangled state $|\Phi\rangle\langle\Phi|^L$. If the min-entropy $H^\varepsilon_{\min}(A|E)_\rho$ of the state ρ_{ABE} is sufficiently high, quantum state merging can be achieved with L being larger than K. If K is a power of 2, then the state $|\Phi\rangle\langle\Phi|^K$ is identical to the state of $\log K$ ebits. Thus, quantum state merging for a high min-entropy $H^\varepsilon_{\min}(A|E)_\rho$ can be seen as expanding about $\log K$ ebits to about $\log L$ ebits.

The entanglement cost l^ε quantifies how many *ebits* Alice and Bob need to use up in order to transfer the state. The word "ebit" is a common term to refer to a pair of maximally entangled qubits. Ebits are an extremely important resource not only in quantum state merging but in a large variety of information processing tasks. For our purposes, the most interesting aspect of quantum state merging is that if the entanglement cost is negative, then Alice and Bob share more entanglement after the protocol than they did before the protocol. Thus, a quantum state merging with negative entanglement cost can be seen as an entanglement expansion: Alice and Bob end up with more entanglement than they started with. It cannot be seen as entanglement creation, because in general, some initial entanglement is required for the existence of a quantum state merging protocol of the desired (negative) entanglement cost. This constitutes an interesting analogy to QKD, which should be seen as a secret key expansion instead of a secret key generation, because an initial secret key is needed for authentication.

In order to use quantum state merging for entanglement expansion, it is

[1] This state merging-related entanglement cost is not to be confused with other meanings of the same term (for another meaning of entanglement cost, see [Hor+09], for example).

crucial to know for which states the entanglement cost is negative. The following theorem answers this question by bounding the minimal entanglement cost of a state merging of a state ρ_{AB} in terms of the min-entropy.

Theorem 4.6 : *For a bipartite state $\rho_{AB} \in \mathcal{S}(\mathcal{H}AB)$ with min-entropy $H^{\varepsilon}_{\min}(A|E)_\rho$ (where ρ_{ABE} purifies ρ_{AB}), there is a quantum state merging with error $\varepsilon > 0$ whose entanglement cost l^ε satisfies*

$$l^\varepsilon \leq -H^{\varepsilon^2/13}_{\min}(A|E)_\rho + 4\log(1/\varepsilon) + 2\log(13)\,. \tag{4.40}$$

Conversely, the entanglement cost l^ε of every state merging of ρ_{AB} satisfies

$$l^\varepsilon \geq -H^{4\sqrt{2\varepsilon}+3\varepsilon}_{\min}(A|E)_\rho - 2\log\left(\frac{1}{\varepsilon}\right)\,. \tag{4.41}$$

The statement of inequality (4.40) is called the *achievability* part of theorem 4.6, and the statement of inequality (4.41) is the *converse* part of the theorem. In Chapter 6, we will present a protocol that distributes n-qubit systems A and B to Alice and Bob, respectively, and prove that the min-entropy $H^{\varepsilon}_{\min}(A|E)$ of the state ρ_{ABE} of these systems (for a purifying system E) is bounded from below. At first sight, one might think that this protocol, in combination with theorem 4.6, provides a protocol for entanglement expansion. However, this is not true. The problem is that the achievability part of the theorem only states that for states with a sufficiently high entropy, there *exists* a quantum state merging protocol that leads to entanglement expansion. It does not state how this protocol looks like. In particular, it does not provide a fixed protocol that performs entanglement expansion for *all* states whose min-entropy satisfies a particular bound. Nonetheless, theorem 4.6 is a highly important result, as it provides achievability limits that future designers of entanglement expansion protocols can aim for.

The proof of (4.6), which can be found in [Dup+10], makes use of the decoupling theorem. The first part of a state merging protocol is constructed as a decoupling operation. While this first part of the protocol is a fixed construction, the second part of the protocol is only shown to exist. As the interested reader may verify, this existence statement boils down to the existence of a unitary as per lemma 3.8. If the state ρ_{ABE} was known, then the unitary could be constructed. However, as long as a min-entropy bound is all that one knows about the state, the unitary can only be shown to exist.

The construction of protocols that produce the desired output for *all* states satisfying a min-entropy bound is an active research topic. State merging protocols with this property have been referred to as *universal* quantum state merging protocols. Preliminary results on such protocols for the asymptotic case of many independent uses of the same channel can be found in [BBJ13].

4.6 Maximal achievable fidelity with a maximally entangled state

The last characterization of the min-entropy that we look at will be very useful in chapter 7, when we generalize the min-entropy to a decoherence quantity

for a more general family of probabilistic theories. In contrast to the characterizations that we have seen in the last three subsections, we now consider a characterization of the *unsmoothed* min-entropy rather than the smooth one. It is given in the form of the following proposition, which has been proved by König, Renner and Schaffner [KRS09].

Proposition 4.7 : *Let $\rho_{AE} \in \mathcal{S}(\mathcal{H}_{AE})$ be a bipartite state, let A' be a system of the same dimension as A ($d_A = d_{A'}$), let $|\Phi\rangle\langle\Phi|_{AA'} \in \mathcal{S}(\mathcal{H}_{AA'})$ be a maximally entangled state.*[2] *Then*

$$H_{\min}(A|E)_\rho = -\log d_A \max_{\mathcal{R}_{E\to A'}} F^2(|\Phi\rangle\langle\Phi|_{AA'}, \mathbb{1}_A \otimes \mathcal{R}_{E\to A'}(\rho_{AE}))\,, \tag{4.42}$$

where F is the fidelity and where the maximization runs over all channels $\mathcal{R}_{E\to A'}$.

Equation (4.42) gives us a new interpretation of the min-entropy: for a state ρ_{AE}, the min-entropy $H_{\min}(A|E)$ can be interpreted as a measure for how well Eve, who controls system E, can entangle her system with system A (see figure 4.3). By choosing a *recovery map* $\mathcal{R}_{E\to A'}$ and applying it to her system, she transforms the state ρ_{AE} into the state $\mathbb{1}_A \otimes \mathcal{R}_{E\to A'}(\rho_{AE})$. Thus, the maximum in equation (4.42) evaluates to the maximal squared fidelity that Eve can achieve with the maximally entangled state $|\Phi\rangle\langle\Phi|_{AA'}$. Note that for a larger achievable fidelity, the min-entropy decreases.

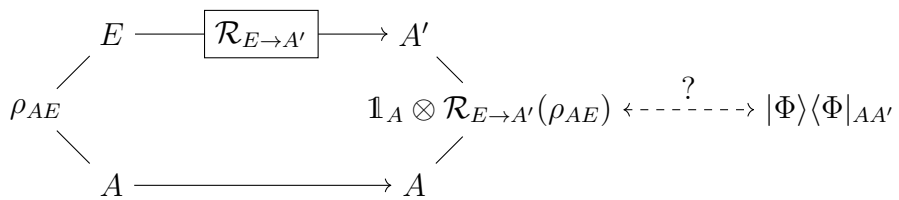


Figure 4.3: Alternative interpretation of the min-entropy. Consider a state ρ_{AE} shared by Alice and Bob. Suppose that Eve tries to get her system maximally entangled with the system controlled by Alice. To this end, she applies a recovery map $\mathcal{R}_{E\to A'}$ on her system, chosen to get as close as possible to the maximally entangled state $|\Phi\rangle\langle\Phi|_{AA'}$. Here, "as close as possible" means that Eve tries to transform ρ_{AE} into a state $\rho_{AA'}$ such that the fidelity with $|\Phi\rangle\langle\Phi|_{AA'}$ is as high as possible. It turns out that $H_{\min}(A|E)$ is a measure for how well she can do that.

Note that the choice of the maximally entangled state is irrelevant: by virtue of lemmata 3.8 and 3.15, it holds that for two maximally entangled states $|\Phi\rangle\langle\Phi|_{AA'}$ and $|\Psi\rangle\langle\Psi|_{AA'}$,

$$\begin{aligned}
&F^2(|\Phi\rangle\langle\Phi|_{AA'}, \mathbb{1}_A \otimes \mathcal{R}_{E\to A'}(\rho_{AE})) && (4.43)\\
&= F^2((\mathbb{1}_A \otimes U_{A'})|\Psi\rangle\langle\Psi|_{AA'}(\mathbb{1}_A \otimes U_{A'}^\dagger), \mathbb{1}_A \otimes \mathcal{R}_{E\to A'}(\rho_{AE})) && (4.44)\\
&= F^2(|\Psi\rangle\langle\Psi|_{AA'}, (\mathbb{1}_A \otimes U_{A'}^\dagger)(\mathbb{1}_A \otimes \mathcal{R}_{E\to A'})(\rho_{AE})(\mathbb{1}_A \otimes U_{A'})) && (4.45)\\
&= F^2(|\Psi\rangle\langle\Psi|_{AA'}, (\mathbb{1}_A \otimes \widetilde{\mathcal{R}}_{E\to A'})(\rho_{AE}))\,, && (4.46)
\end{aligned}$$

for some unitary U_A, where $\widetilde{\mathcal{R}}_{E\to A'}$ is the channel $\mathcal{R}_{E\to A'}$, followed by the unitary $U_A^\dagger$. Since $\mathcal{R}_{E\to A'} \mapsto \widetilde{\mathcal{R}}_{E\to A'}$ is a bijection on the set of unitaries on A,

[2] As we will explain below, the choice of the maximally entangled state does not matter.

we get that

$$\begin{aligned}&\max_{\mathcal{R}_{E\to A'}} F^2(|\Psi\rangle\langle\Psi|_{AA'}, \mathbb{1}_A \otimes \widetilde{\mathcal{R}}_{E\to A'}(\rho_{AE}))\\ &= \max_{\mathcal{R}_{E\to A'}} F^2(|\Psi\rangle\langle\Psi|_{AA'}, \mathbb{1}_A \otimes \mathcal{R}_{E\to A'}(\rho_{AE}))\,.\end{aligned} \tag{4.47}$$

Thus, the choice of the maximally entangled state does not matter.

Part III

Contributions

Chapter 5

Sifting attacks in quantum key distribution

5.1 Introduction

In section 4.3, we have seen that a quantum key distribution protocol can be divided into two parts:

- In the first part, classical n-bit strings X and X' are distributed to Alice and Bob, respectively, about which Eve has some quantum side information E. Eve's knowledge about the bit strings is limited in a certain way, namely in that the min-entropy $H^{\varepsilon}_{\min}(X|E)$ of the overall state $\rho_{XX'E}$ is bounded from below. We call this first part of a QKD protocol a *raw key distribution protocol*. It is the part of a QKD protocol where the data is generated and sifted (we will explain below what this means).

- In the second part, Alice and Bob execute an error correcting code and make a hash comparison to establish the correctness condition, inequality (4.20). Then they perform privacy amplification, in which they map the n-bit strings to shorter l-bit strings using two-universal hashing. This turns the lower bound on $H^{\varepsilon}_{\min}(X|E)$ of the raw key distribution protocol into the security condition of inequality (4.21). This part of a QKD protocol is referred to as the *classical post-processing* of the protocol.

In this chapter, we analyze the first part, the raw key distribution protocol, in detail, whereas the classical post-processing will no longer be treated. Readers interested in classical post-processing topics are referred to the PhD thesis of Gilles van Assche [Ass06].

We will point out a serious security flaw that has been spread in the more recent QKD literature. It has the consequence that the min-entropy $H^{\varepsilon}_{\min}(X|E)$ is not bounded correctly. To get an idea of what the problem is, let us have a brief look at what a raw key distribution protocol looks like. As we mentioned briefly in section 4.3 (see page 55), a reduced QKD protocol can itself be split into two parts:

(i) Preparation, distribution, measurement and sifting,

(ii) Parameter estimation.

We refer to subroutine (i) collectively as "sifting". Even though the word sifting usually only refers to the process of discarding part of the data acquired in the measurements, we refer to the preparation, distribution, measurement and sifting together as "sifting", because they are intertwined in *iterative sifting*, the protocol that we will analyze in detail.

There are many different protocols in the QKD literature, and the details of (i) and (ii) depend on the particular protocol. To make things more concrete, we will now have a brief and informal look at an example protocol. It is defined with respect to two parameters $n \in \mathbb{N}$ and $q_{\text{tol}} \in [0, 1]$, where n is the length of the resulting bit strings X and X' and q_{tol} is an error tolerance parameter. The protocol goes as follows.

(i) Sifting protocol: Let $m = (4 + \delta)n$ be an integer, where $\delta > 0$ is some small number. The first two steps of the protocol are repeated m times (we say they perform m *rounds*). In round $r \in [m]$, Alice and Bob do the following:

Step 1: Alice prepares a qubit pair in a maximally entangled state and sends one half to Bob using a quantum channel controlled by Eve.

Step 2: Alice and Bob independently choose a basis $A_r, B_r \in \{0, 1\}$ at random, where 0 and 1 are equally likely and where 0 stands for the $\mathbb{X}$-basis and 1 stands for the $\mathbb{Z}$-basis. Then they measure their half of the qubit pair in that basis and store the outcome $Y_r, Y'_r \in \{0, 1\}$.

After these m rounds of repetition, Alice and Bob carry out the rest of the protocol in one single run.

Step 3: Alice and Bob communicate their basis choices A_r, B_r for $r \in [m]$ and determine the sets

$$U(m) = \{r \in [m] \mid A_r = B_r = 0\}\,, \tag{5.1}$$
$$V(m) = \{r \in [m] \mid A_r = B_r = 1\}\,. \tag{5.2}$$

If $|U(m)| < n$ or $|V(m)| < n$, they abort the protocol. We say that n is their *quota* for the $\mathbb{X}$-basis and the $\mathbb{Z}$-basis. If $|U(m)| \geq n$ and $|V(m)| \geq n$, they choose subsets $U \subseteq U(m)$ and $V \subseteq V(m)$, each of size n, uniformly at random, i.e. each subset of size n has the same likelihood of being chosen. Then they discard the rest of the data. This discarding of data is called *sifting*. With the data of the remaining $2n$ rounds, they continue with parameter estimation.

(ii) Parameter estimation (PE) protocol: Alice and Bob choose a subset $W \subset U \cup V$ of size n fully at random. This determines the *test bits*.

They communicate their measurement results Y_r, Y'_r with $r \in W$. This allows them to determine the *test bit error rate* Λ_{test}, defined as

$$\Lambda_{\text{test}} := \frac{1}{n} \sum_{r \in W} Y_r \oplus Y'_r \,. \tag{5.3}$$

If $\Lambda_{\text{test}} > q_{\text{tol}}$, they abort the protocol. Otherwise, they use the remaining n measurement outcomes, which we call the *raw key bits* or just *key bits*, as their bit strings X and X'.

This is a simple example of a raw key distribution protocol. It is essentially identical to a protocol considered by Shor and Preskill [SP00]. The only difference is that here, we formulate it as an entanglement-based protocol instead of a prepare-and-measure protocol.[1] Compared with other protocols that we will look at, it is an inefficient protocol, but in contrast to the problematic protocol that we will discuss below, it is a secure protocol. Instead of deriving a formal lower bound on the min-entropy $H^{\varepsilon}_{\min}(X|E)$, we will give some intuitive arguments for why Eve cannot have too much knowledge about X (and X').

Let us put ourselves in Eve's shoes. In order to gain information about X, she may want to intercept the qubits sent from Alice to Bob. More precisely, let us say that she performs an *intercept-resend attack*. This means that Eve measures some of the qubits that Alice sends through the channel and resends each of these qubits in the eigenstate associated with the measurement outcome. Since Alice and Bob choose their bases at random, Eve does not know in which basis to attack. On the other hand, if she knew which of the rounds are key rounds (i.e. if she knew which measurement results end up in the raw key), she could decide to only attack in these rounds. Then all test bits would be unaffected, and her attack would not be detected. However, Eve does not know that, because the key bits are sampled uniformly at random from the bits where Alice and Bob measured in the same basis. Therefore, since Eve really wants to gain information about X, we assume that she attacks in every round. Since she does not know the encoding basis, she can either use a fixed basis or randomize her basis choice. In either case, she will introduce an expected error rate of 25%,[2] so if q_{tol} is set significantly below 25%, then Eve's attack will be detected.

Hence, we can say that a central assumption in QKD is that Eve has no knowledge about which rounds are test rounds and which rounds are key rounds. In the Shor-Preskill protocol that we just discussed, this assumption is satisfied. Below, we will have a close look at another raw key distribution protocol which has been used in recent literature. We will show that that protocol violates this assumption, i.e. Eve has (partial) knowledge about which rounds are key rounds and which rounds are test rounds. As we will show, this breaks the security proof of the protocol.

[1] In a prepare-and-measure protocol, Alice chooses two random bits A_r and Y_r in each round r and prepares a single qubit (instead of a pair) in the state Y_r in the basis A_r. Then she sends this qubit to Bob. On Bob's side, nothing changes. From a security point of view, these two situations are equivalent.

[2] We assume here that the $\mathbb{X}$-basis and the $\mathbb{Z}$-basis are complementary, e.g. they correspond to the σ_x- and σ_z-Pauli bases. In that case, measuring in the wrong basis leads to an error in 50% of the cases (see the discussion in section 3.1.3). Since Eve chooses the wrong basis with probability 1/2, this leads to an expected error rate of 25%.

5.1.1 Summary of the results

The raw key distribution protocol that we criticize is composed of two sub-protocols which we call *iterative sifting* and *single-basis parameter estimation*. In contrast to the Shor-Preskill protocol above, where measurement choices are only communicated when all the quantum communication is completed, iterative sifting involves an iterative procedure where Alice and Bob communicate previous basis choice after each completed round until a quota is met. This protocol design is chosen to increase the efficiency of the protocol, meaning that less quantum communication is necessary for the same length of the raw keys. We will describe iterative sifting and its efficiency motivation in detail in section 5.2. This sifting scheme was part of theoretical protocols [Tom+12; Lim+13; Cur+14; Lim+14] and has found experimental implementations [Bac+13]. As we describe in section 5.4, we find that iterative sifting leads to two previously unnoticed security issues. In a nutshell, these problems are:

- *Non-uniform sampling*: The sampling probability, due to which the key bits are chosen, is not uniform. In other words, there is an a priori bias: Eve knows ahead of time that some rounds are more likely to end up in the sample than others.

- *Basis information leak*: Alice and Bob's public communication about their previous basis choices (which, in iterative sifting, happens before the quantum communication is over) allows Eve to update her knowledge about which of the upcoming (qu)bits will end up in the sample. As a consequence, the quantum information that passes through the channel thereafter can be correlated to this knowledge of Eve.

In section 5.5, we describe intercept-resend attack strategies for Eve that exploit these two security issues. As a figure of merit, we calculate the expected error rates for these attacks and find that they reach values far below the value of 25% which is expected for secure protocols such as the Shor-Preskill protocol above.

How can these problems be avoided? One way would be to fall back on protocols such as the one above. However, this way one would lose all the efficiency benefits of iterative sifting. Instead, in section 5.6, we construct a protocol that shows much of the efficiency benefits of iterative sifting, yet suffers from neither of the two problems we describe. In section 5.8, we show how the security of a raw key distribution protocol can be proved formally. We develop two formal criteria for a sifting protocol and show that they are sufficient to guarantee a correct estimation of min-entropy. Then we show that our suggested protocol satisfies these two criteria, whereas iterative sifting does not.

5.2 Raw key distribution protocols and efficiency

Further below in this section, we introduce the problematic iterative sifting protocol. Since iterative sifting was designed with efficiency in mind, it is

very helpful for its discussion to talk about the efficiency of raw key distribution protocols. Thus, we shall approach iterative sifting through some other examples that illustrate efficiency aspects.

There are several efficiency aspects, but maybe the most obvious one is the number of raw key bits per number of qubits of quantum communication. In the Shor-Preskill protocol above, $m = (4 + \delta)n$ qubits are sent for n bits of raw key, so the fraction is $n/(4 + \delta)n \approx 1/4$ for small δ.[3] For the discussion of efficiency, it is helpful to visualize the m rounds of the protocol as a bar and to subdivide it into three parts (see figure 5.1): the $\mathbb{X}$-*agreements*, where both measured in $\mathbb{X}$, the $\mathbb{Z}$-*agreements*, where both measured in $\mathbb{Z}$, and the *disagreements*, where Alice and Bob measure in different bases. In the Shor-Preskill protocol, the probability p_x of choosing the $\mathbb{X}$-basis and the probability p_z of choosing the $\mathbb{Z}$-basis are both $1/2$. Thus, speaking in expectation values, the $\mathbb{X}$-agreements and the $\mathbb{Z}$-agreements each are about $m/4$ bits in size, and there are about $m/2$ bits of disagreements. During parameter estimation, one half of the agreements are used for testing (i.e. for determining Λ_{test}), so there are about $m/4$ of bits left for the raw key.

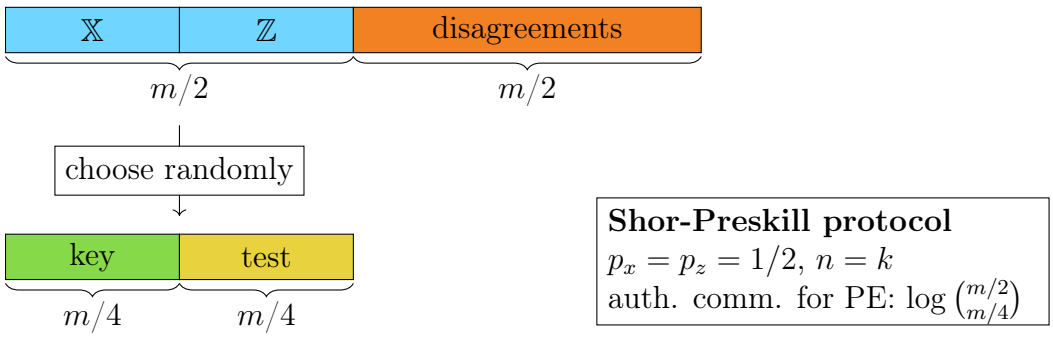


Figure 5.1: Efficiency of the Shor-Preskill protocol. In this protocol, the basis choice probabilities and the quota are symmetric. In other protocols below, we will distinguish between an $\mathbb{X}$-quota n and a $\mathbb{Z}$-quota k, but here we have $n = k$. The meaning of the authenticated communication for parameter estimation will be explained below.

How could this efficiency be increased? Lo, Chau and Ardehali (LCA) suggested to use biased basis choice probabilities $p_x > p_z$ to increase the efficiency [LCA05]. The idea behind this suggestion is that the expectation value $2p_xp_zm$ of the number of disagreements becomes smaller this way. Hence, less data is discarded during sifting (see figure 5.2). While in the Shor-Preskill protocol, the quota for the $\mathbb{X}$- and $\mathbb{Z}$-agreements that need to be met are symmetric (recall that they abort unless they have at least n $\mathbb{X}$-agreements and at least n $\mathbb{Z}$-agreements), one now has asymmetric quota. We denote the quota for the $\mathbb{X}$-agreements by n and the quota for the $\mathbb{Z}$-agreements by k, so we have $n > k$.

[3] This is a naïve efficiency estimation, because it does not account for the fact that Alice and Bob may abort the protocol, in which case the final secret key length is 0, not n. For the discussion in this subsection, this naïve notion of efficiency shall be sufficient. We will analyze efficiency in more detail in section 5.6.

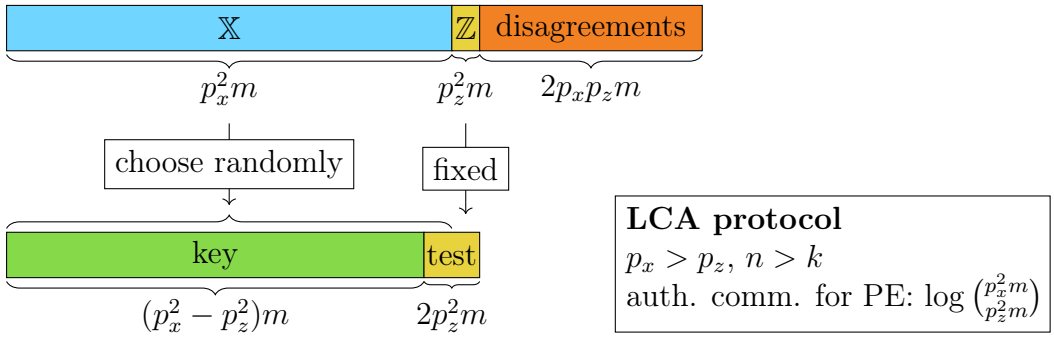


Figure 5.2: Efficiency of the LCA-protocol. The number of disagreements can be significantly reduced by choosing asymmetric basis choice probabilities and quota. The proportions in this figure are drawn for $p_x = 0.8$.

As LCA noted, it would not be secure in this case to sample the test bits from the union of the $\mathbb{X}$- and $\mathbb{Z}$-agreements uniformly. Instead, they make a somewhat peculiar suggestion for parameter estimation. They suggest to determine *two* error rates: one error rate is determined for the k $\mathbb{Z}$-agreements that they keep for parameter estimation, and the other rate is determined for a randomly chosen subset of the $\mathbb{X}$-agreements of the same size k. Only if both error rates are below a certain threshold value, Alice and Bob use the remaining $n - k$ $\mathbb{X}$-agreements as the raw key. The ratio of raw key bits per qubit of quantum communication, when the quota n and k are chosen proportional to the probabilities of the $\mathbb{X}$- and $\mathbb{Z}$-agreements, is about $(p_x^2 - p_z^2)m/m = (p_x^2 - p_z^2)$ and can therefore be much higher than the value of one quarter for the Shor-Preskill protocol.

Is it really necessary to determine two error rates? As we prove in section 5.7, it turns out that the LCA protocol is still secure when it is modified such that only the error rate on the $\mathbb{Z}$-agreements is estimated. This means that parameter estimation is done in only one basis. Therefore, we call it *single-basis parameter estimation* (SBPE). Then, all the sifted $\mathbb{X}$-agreements are used for the raw key. This has several advantages. Firstly, it simplifies the protocol. Secondly, the ratio of raw key bits per sent qubit increases to $p_x^2 m/m = p_x^2$ (see figure 5.3). Thirdly, Alice and Bob do not have to choose the test bits at random, i.e. they do not need any randomness for the choice of the sample. This is an advantage because this way, Alice and Bob do not have to communicate their choice of the sample. To understand the importance of this, let us say a few words on *authentication*.

In QKD, the communication between Alice and Bob needs to be *authenticated* in order to prevent a *man-in-the-middle attack*. Authentication requires some small initial secret key shared between Alice and Bob, and the more Alice and Bob need to communicate, the larger this initial key needs to be. In this sense, QKD should actually be regarded as secret-key expansion rather than secret key generation. Hence, avoiding authenticated communication reduces the required size of the initial shared secret key. In this modified scheme, the randomness cost for parameter estimation (PE) that needs to be communicated is 0, while it is $\log \binom{m/2}{m/4}$ bits for the Shor-Preskill protocol and about

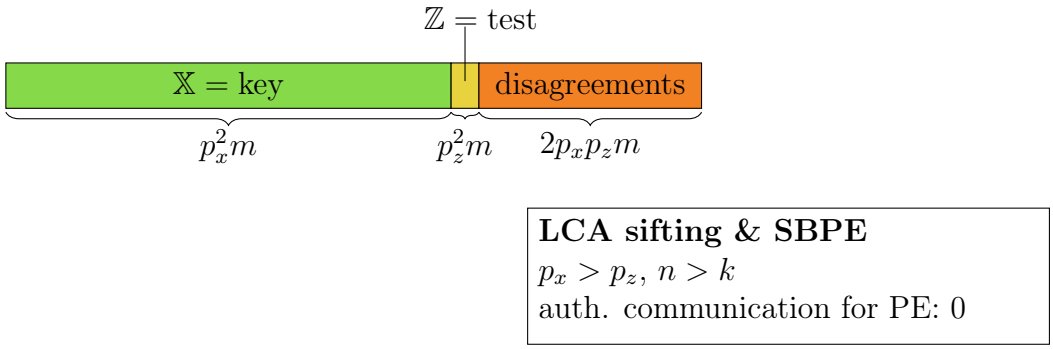


Figure 5.3: Efficiency of LCA sifting with single-basis parameter estimation.

$\log \binom{p_x^2 m}{p_z^2 m}$ bits for the LCA protocol.[4] For more information about authentication in QKD, see the aforementioned book by Gilles van Assche [Ass06]. As we discuss in more detail in section 5.6, we recommend the use of LCA sifting and SBPE as a raw key distribution protocol. It is efficient, and we formally prove its security in sections 5.7 and 5.8.

So far, we only discussed unproblematic modifications of raw key distribution protocols. Now we discuss modifications that lead to iterative sifting which, as we will show in the next section, raises security issues. One may be tempted to say that LCA sifting with SBPE is still unnecessarily inefficient, because the number of rounds is fixed to a number m instead of being variable depending on basis agreements that Alice and Bob have during the quantum communication. With a fixed number of rounds, two undesired things can happen: Alice and Bob may not meet the quota, in which case they need to abort, or they keep the quantum communication running even though they already met the quota. For this reason, some authors [Tom+12; Lim+13; Cur+14; Lim+14; Bac+13] decided to make a further modification of the reduced QKD protocol: after each round of quantum communication, Alice and Bob communicate their basis choice of the past round. This way, they can determine how many $\mathbb{X}$-agreements and $\mathbb{Z}$-agreements they already had. If they have less than n $\mathbb{X}$-agreements or less than k $\mathbb{Z}$-agreements, they continue the quantum communication. Once they met both quota, they terminate the quantum communication. At that point, they may have too many $\mathbb{X}$-agreements or too many $\mathbb{Z}$-agreements (but not both). In that case, they choose a subset of size n or k at random, respectively. We will write out the iterative sifting protocol in detail in the next section.

The advantage of iterative sifting is that Alice and Bob never have to abort due to quota restrictions, and on the other hand, the quantum communication never runs longer than necessary for meeting the quota. The underlying assumption is that since Alice and Bob only communicate basis choices of previous rounds, but not of upcoming rounds, Eve does not get any advantage. However, as we show in the next section, this assumption is wrong. Iterative sifting breaks the security proofs that were presented for these protocols.

[4] The binomial coefficient gives the number of possible sample choices. Therefore, the authenticated communication cost in bits is the logarithm of the binomial coefficient.

5.3 Iterative sifting

The iterative sifting protocol has been formulated in slightly different ways in the literature, where the differences lie mostly in the choice of the wording and in whether it is realized as a prepare-and-measure protocol [Tom+12; Bac+13; Cur+14; Lim+14] or as an entanglement-based protocol [Lim+13]. These details are irrelevant for the problems that we describe. We formulate protocols as entanglement-based protocols, because it makes the formal treatment in section 5.8 easier. Another difference is that some of the above-mentioned references take into consideration that sometimes, a measurement may not take place (no-detection event) or may have an inconclusive outcome. This is done by adding a third symbol $\emptyset$ to the set of possible outcomes, turning the otherwise dichotomic measurements into trichotomic ones with symbols $\{0, 1, \emptyset\}$. We choose not to do so, because the problems that we describe arise independently of whether no-detection events or inconclusive measurements take place. Incorporating them would not solve the problems that we address but rather complicate things and distract from the main issues that we want to point out.

For a formal write-up of the protocol, it is useful to clarify some notational conventions. The protocol involves quantities that are random (such as Alice's and Bob's basis choices A_r and B_r or the raw key X and its elements $X_1, \ldots, X_n$). Mathematically, this means that they form random variables. We follow convention 2.4 and denote random variables by uppercase letters, whereas we denote concrete values of the random variables by lowercase letters. Fixed numbers, such as the quota n and k, will also be denoted by lowercase letters. It is useful to give their sum its own letter l.

Convention 5.1 : *From now on, l is defined as $l := n + k$, the sum of the $\mathbb{X}$- and the $\mathbb{Z}$-quota. This is to be clearly distinguished from the secret key length in chapter 4.*

From now on, we split up raw key distribution protocols into a sifting protocol and a PE protocol. After the sifting protocol, Alice and Bob have sifted measurement outcomes and sifted basis choices. Above, we did not give them their own symbols, but in the following we will denote them as follows. Alice's sifted measurement outcomes form an l-bit string, and we denote its random variable by $S = (S_i)_{i=1}^l$. Likewise, we denote Bob's measurement outcome string by $T = (T_i)_{i=1}^l$ and the sifted basis choice string by $\Theta = (\vartheta_i)_{i=1}^l$. In the PE, these strings S, T and Θ are then transformed into the raw keys X and X' (see figure 5.4).

We have written out iterative sifting in protocol 5.1. There, and in the rest of this thesis, we use the notation $\{0, 1\}_k^l$ for the set of all l-bit strings with Hamming weight k,

$$\{0, 1\}_k^l := \left\{ (\vartheta_i)_{i=1}^l \in \{0, 1\}^l \,\middle|\, \sum_{i=1}^l \vartheta_i = k \right\} . \tag{5.4}$$

In the protocol, Alice iteratively prepares qubit pairs in a maximally entangled state and sends one half of the pair to Bob (step 1). Then, Alice and Bob each measure their qubit with respect to a basis $a_i, b_i \in \{0, 1\}$, respectively, where 0 stands for the $\mathbb{X}$-basis and 1 stands for the $\mathbb{Z}$-basis (step 2).

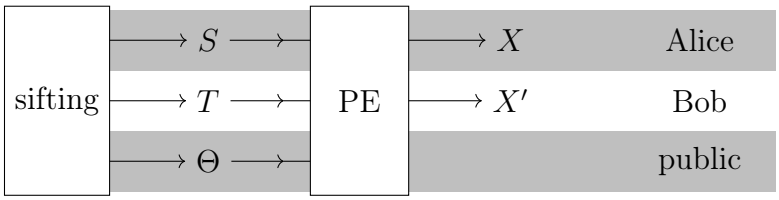


Figure 5.4: Subdivision of reduced QKD into sifting and parameter estimation (PE). A sifting protocol produces l-bit strings of sifted measurement outcomes for Alice (S) and for Bob (T), as well as an l-bit string of sifted basis choices (Θ). These three strings are transformed into the raw keys X and X' in the PE.

Thereby, the $\mathbb{X}$-basis is chosen with probability p_x and the $\mathbb{Z}$-basis is chosen with probability p_z. These probabilities p_x and p_z are parameters of the protocol. The important and problematic parts of the protocol are step 3 and the subsequent check of the termination condition (TC): after *each* measurement, Alice and Bob communicate their basis choice over an authenticated classical channel. With this information at hand, they then check whether the termination condition is satisfied: if they have at least n $\mathbb{X}$-agreements and at least k $\mathbb{Z}$-agreements, the termination condition is satisfied and they enter the *final phase* of the protocol by continuing with step 4. These quota n and k are parameters of the protocol. If the condition is not met, they repeat the steps 1 to 3 (which we call the *loop phase* of the protocol) until they meet this condition. Because of this iteration, whose termination condition depends on the history[5] of the protocol run up to that point, we call it the iterative sifting protocol. Its number of rounds is a random variable that we denote by M. We denote possible values of M by m.

After the loop phase of the protocol, in which the whole data is generated, Alice and Bob enter the final phase of the protocol, in which this data is sifted. This sifting consists of discarding data of rounds in which Alice and Bob measured in different bases, as well as randomly discarding a surplus of basis agreements, where a "surplus" refers to having more than n $\mathbb{X}$-agreements or more than k $\mathbb{Z}$-agreements. This discarding of surplus is done to simplify the analysis of the protocol, which is easier if the number of bits where both measured in the $\mathbb{X}$ ($\mathbb{Z}$) basis is fixed to a number n (k). After throwing away the surplus, Alice and Bob relabel their data in an order-preserving way in step 5, resulting in sifted measurement outcome strings S and T as well as a sifted basis choice string Θ. This is just done so that the labels of the output string elements are always $i = 1, 2, \ldots, l$ without gaps, which is useful for later analysis. It does not correspond to a practically relevant process. The idea behind the order-preserving relabeling is shown in figure 5.5.

Iterative sifting is problematic, but to fully understand why, one needs to see how the output of the iterative sifting protocol is processed in the subsequent PE. As we mentioned in section 5.2, protocols from the literature that

[5] By the *history* of a protocol run, we mean the record of everything that happened during the run of the protocol. In the case of iterative sifting, this means the random bits a_r, b_r, the measurement outcomes y_r, y'_r etc.

Iterative Sifting

Parameters: $n, k \in \mathbb{N}_+$, $p_x, p_z \in [0,1]$ with $p_x + p_z = 1$.

Outputs:
- Alice: l-bit string $(S_i)_{i=1}^l \in \{0,1\}^l$ (sifted outcomes),
- Bob: l-bit string $(T_i)_{i=1}^l \in \{0,1\}^l$ (sifted outcomes),
- public: l-bit string $(\Theta_i)_{i=1}^l \in \{0,1\}_k^l$ (sifted basis choices)

The protocol

Loop phase: Steps 1 to 3 are iterated round-wise (round index $r = 1, 2, \ldots$) until the termination condition (TC) after step 3 is reached. In round r, Alice and Bob do:

Step 1: Alice prepares a qubit pair in a maximally entangled state and sends one half to Bob.

Step 2: Alice and Bob independently choose a basis $A_r, B_r \in \{0,1\}$ at random with probability p_x, p_z, where 0 stands for the $\mathbb{X}$-basis and 1 stands for the $\mathbb{Z}$-basis. Then they measure their part of the qubit pair in that basis and get an outcome $Y_r, Y_r' \in \{0,1\}$, respectively.

Step 3: Alice and Bob communicate their basis choice A_r and B_r over a public authenticated channel. Then they determine the sets

$$U(r) := \{j \in [r] \mid A_j = B_j = 0\}\,,$$
$$V(r) := \{j \in [r] \mid A_j = B_j = 1\}$$

TC: If the condition ($|U(r)| \geq n$ and $|V(r)| \geq k$) is reached, Alice and Bob set $M := r$ and proceed with step 4. Otherwise, they increment r by one and repeat from step 1.

Final phase: The following steps are performed only once:

Step 4: Alice and Bob choose a subset $U \subseteq U(M)$ of size n at random, i.e. each subset of size n is equally likely to be chosen. Analogously, they choose a subset $V \subseteq V(M)$ of size k at random. Then they discard the bits A_r, B_r, Y_r and Y_r' for which $r \notin U \cup V$.

Step 5: Let R_i be the i-th element of $U \cup V$. Then Alice determines $(S_i)_{i=1}^l \in \{0,1\}^l$, Bob determines $(T_i)_{i=1}^l \in \{0,1\}^l$ and together they determine $(\Theta_i)_{i=1}^l \in \{0,1\}_k^l$, where for every $i \in [l]$,

$$S_i = Y_{R_i}\,, \quad T_i = Y'_{R_i}\,, \quad \Theta_i = A_{R_i}\,(= B_{R_i})\,.$$

Step 6: Alice locally outputs $(S_i)_{i=1}^l$, Bob locally outputs $(T_i)_{i=1}^l$, and they publicly output $(\Theta_i)_{i=1}^l$.

Protocol 5.1: The iterative sifting protocol.

$$u = \{2, 5, 7\}\,, \qquad v = \{4, 10\}$$

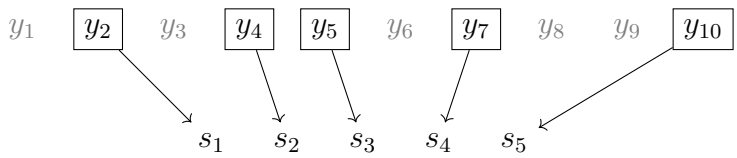


Figure 5.5: Example of an order-preserving relabeling (step 5 of the iterative sifting protocol). For this simple example, we have chosen the quota $n = 3$, $k = 2$, and hence $l = 5$. Suppose that the termination condition is reached after 10 rounds, and that Alice chooses the subsets $u = \{2, 5, 7\}$ and $v = \{4, 10\}$. Then Alice's sifted measurement outcomes are simply $s_1 = y_2$, $s_2 = y_4$, $s_3 = y_5$, $s_4 = y_7$, $s_5 = y_{10}$. The strings $(t_i)_{i=1}^5$ and $(\vartheta_i)_{i=1}^5$ are chosen the same way, i.e. $t_1 = y'_2, \ldots, t_5 = y'_{10}$ and $\vartheta_1 = a_2, \ldots, \vartheta_5 = a_{10}$.

use iterative sifting use single-basis parameter estimation (SBPE). To make clear what we are talking about, we have written out the SBPE protocol in protocol 5.2. It is a very simple protocol, parametrized by $n, k \in \mathbb{N}$ and an error tolerance rate $q_{\text{tol}} \in [0, 1]$. Alice and Bob communicate the test bits, i.e. those bits S_i, T_i for which $\Theta_i = 1$, and then determine the test bit error rate Λ_{test}. If Λ_{test} exceeds q_{tol}, they abort; otherwise, they use the bits S_i, T_i with $\Theta_i = 0$ as the raw key. The reordering in step 3 is analogous to the reordering in step 5 of protocol 5.1. Again, we consider this reordering for the analysis in sections 5.7 and 5.8, which is easier if X and X' are simply elements of $\{0, 1\}^n$.

It is important to emphasize that if the output of iterative sifting serves as the input of SBPE, then the bits that result from measurements in the $\mathbb{X}$-basis are used for the raw key, and the bits that result from measurements in the $\mathbb{Z}$-basis are used for parameter estimation (i.e. they form the *sample* for the parameter estimation). Hence, the sample is determined by the basis choice. In contrast to the Shor-Preskill protocol, no additional randomness is used to choose the sample. This is not necessarily a problem by itself. However, as we will show in the next section, in iterative sifting, some rounds are more likely to end up in the sample than other rounds. This leads to non-uniform sampling, which is a problem since uniform sampling is one of the assumptions that enter the analysis of the parameter estimation. This seems to have gone unnoticed so far, as we found that protocols in the literature that use iterative sifting as a subroutine use SBPE as a subroutine for parameter estimation [Tom+12; Lim+13; Cur+14; Lim+14; Bac+13].

5.4 The two security issues with iterative sifting

5.4.1 Non-uniform sampling

To show that iterative sifting leads to non-uniform sampling, we calculate the sampling probabilities for some example parameters $k, n \in \mathbb{N}$ as functions of the probabilities p_x and p_z. By a sampling probability, we mean the probability that some subset of k of the $l = n+k$ bits is used as a sample for the parameter

Single-Basis Parameter Estimation (SBPE)

Parameters: $n, k \in \mathbb{N}$, $q_{\text{tol}} \in [0,1]$.

Inputs:
- Alice: l-bit string $S = (S_i)_{i=1}^l \in \{0,1\}^l$ (sifted outcomes),
- Bob: l-bit string $T = (T_i)_{i=1}^l \in \{0,1\}^l$ (sifted outcomes),
- public: l-bit string $\Theta = (\Theta_i)_{i=1}^l \in \{0,1\}_k^l$ (sifted basis choices)

Outputs:
- Alice: n-bit string $X = (X_j)_{j=1}^n \in \{0,1\}^n$ (raw key),
- Bob: n-bit string $X' = (X'_j)_{j=1}^n \in \{0,1\}^n$ (raw key).

The protocol

Step 1: Alice and Bob communicate their test bits, i.e. the bits S_i and T_i with i for which $\Theta_i = 1$, over a public authenticated channel.

Step 2: Alice and Bob determine the *test bit error rate*

$$\Lambda_{\text{test}} := \frac{1}{k} \sum_{i=1}^{l} \Theta_i (S_i \oplus T_i)$$

and perform the *correlation test*: if $\Lambda_{\text{test}} \leq q_{\text{tol}}$, they continue the protocol and move on to Step 3. If $\Lambda_{\text{test}} > q_{\text{tol}}$, they abort and output $X = X' = \perp$.

Step 3: Let I_j be the j-th element of $\{I \in [l] \mid \Theta_I = 0\}$. Then Alice outputs the n-bit string $(X_j)_{j=1}^n$ and Bob outputs the n-bit string $(X'_j)_{j=1}^n$, where

$$X_j = S_{I_j}\,, \quad X'_j = T_{I_j}\,.$$

Protocol 5.2: The single-basis parameter estimation (SBPE) protocol.

estimation, i.e. the sampling probabilities are $P_\Theta(\vartheta)$ for $\vartheta \in \{0,1\}_k^l$. We say that sampling is uniform if $P_\Theta(\vartheta)$ is the same for all $\vartheta \in \{0,1\}_k^l$, and non-uniform otherwise. It turns out that the calculation of the values of $P_\Theta(\vartheta)$ is non-trivial even for small values of n and k (as we will see in the proof of proposition 5.2 below). While non-uniform sampling already arises in the case of the smallest possible parameters $k = n = 1$, the results are even more interesting in cases where $k \neq n$. Let us consider iterative sifting (Protocol 5.1) with $n = 1$, $k = 2$ and arbitrary $p_x, p_z \in [0,1]$. We denote strings without brackets and commas. For example, we write $110 \in \{0,1\}_2^3$ instead of $(1,1,0) \in \{0,1\}_2^3$. The possible values of the random variable Θ are 110, 101 and 011. The probabilities of these strings are given as follows.

Proposition 5.2 : *For the iterative sifting protocol as in Protocol 5.1 with*

$n = 1$ and $k = 2$, it holds that

$$P_\Theta(110) = g_z^2\,, \quad \textit{where} \quad g_z = \frac{p_z^2}{p_z^2 + p_x^2}\,. \tag{5.5}$$

For the other two possible values of Θ, it holds that

$$P_\Theta(011) = P_\Theta(101) = \frac{1 - g_z^2}{2}\,. \tag{5.6}$$

A fully formalized proof of proposition 5.2 in accordance with the definitions in chapter 2 would require to model the sample space Ω of the probability space on which Θ is defined. This set models all the randomness that influences Θ, namely the basis choices $A = A_1, A_2, \ldots$ and $B = B_1, B_2, \ldots$ of Alice and Bob, as well as the choices of the subsets U and V. (However, Θ is independent of the outcome strings Y and Y'.) For example, an element of Ω can be modeled as

$$\omega = (\underbrace{1011101}_{a}, \underbrace{0101001}_{b}, \underbrace{\{6\}}_{u}, \underbrace{\{4,7\}}_{v})\,, \tag{5.7}$$

its probability would be

$$P(\omega) = p_x^2 p_z^5 \cdot p_x^4 p_z^3 \cdot \binom{2}{1}^{-1} \cdot \binom{2}{2}^{-1} \tag{5.8}$$

$$= \frac{1}{2} p_x^6 p_z^8\,, \tag{5.9}$$

and it would be mapped to

$$\vartheta = \Theta(\omega) = 101\,. \tag{5.10}$$

Another example is as follows:

$$\omega' = (101, 101, \{2\}, \{1,3\})\,, \tag{5.11}$$

$$P(\omega') = p_x p_z^2 \cdot p_x p_z^2 \cdot \binom{1}{1}^{-1} \cdot \binom{2}{2}^{-1} \tag{5.12}$$

$$= p_x^2 p_z^4\,, \tag{5.13}$$

$$\Theta(\omega') = 101\,. \tag{5.14}$$

Both ω and ω' lie in the preimage of 101 under Θ, so both of them appear in the sum

$$P_\Theta(101) = \sum_{\omega \in \Theta^{-1}(101)} P(\omega)\,. \tag{5.15}$$

In general, the preimages of the sifted basis choice strings ϑ are sets of tuples ω where the length of a and b is not bounded. At the same time, not all such tuples are elements of Ω (for example, the last entry of a and b needs to be a basis agreement in iterative sifting).

This makes the set Ω hard to model. However, our primary goal here is to show that iterative sifting with SBPE leads to non-uniform sampling. To

this end, it is sufficient to calculate the probability of two samples and to see that they are unequal. For these calculations, it seems exaggerated to have the underlying sample space explicitly written out. In order to avoid unnecessarily complicating things, we therefore only deal with the relevant events, random variables and their probability mass functions directly, assuming that the reader understands what probability space they are meant to be defined on. In section 5.6, when we treat LCA sifting in detail, we will give a full probability space model for that protocol (which is easier than a probability space model for iterative sifting).

For the calculation of equations (5.5) and (5.6), it is useful to introduce the random variables N_x, N_z and N_d, standing for the number of $\mathbb{X}$-agreements, $\mathbb{Z}$-agreements and disagreements in a protocol run, respectively. In this notation, the sampling probabilities can be calculated as follows.

Proof of Proposition 5.2. We first write out the sequence of equalities that lead to the claim. We explain each equality below. The sequence of equalities looks as follows:

$$P_\Theta(110) = \sum_{n_x=1}^{\infty}\sum_{n_z=2}^{\infty}\sum_{n_d=0}^{\infty} P_{\Theta N_x N_z N_d}(110, n_x, n_z, n_d) \tag{5.16}$$

$$= \sum_{n_z=2}^{\infty}\sum_{n_d=0}^{\infty} P_{\Theta N_x N_z N_d}(110, 1, n_z, n_d) \tag{5.17}$$

$$= \sum_{n_z=2}^{\infty}\sum_{n_d=0}^{\infty} p_x^2 (p_z^2)^k (2p_x p_z)^d \binom{n_z + n_d}{n_d} \tag{5.18}$$

$$= g_z^2\,, \quad \text{where } g_z = \frac{p_z^2}{p_z^2 + p_x^2}\,. \tag{5.19}$$

Equation (5.16) is just stating that P_Θ is the marginal of $P_{\Theta N_x N_z N_d}$. The ranges of the sums can be explained as follows. The iterative sifting protocol always runs until there have been at least n $\mathbb{X}$-agreements and at least k $\mathbb{Z}$-agreements. Therefore,

$$P_{\Theta N_x N_z N_d}(\vartheta, n_x, n_z, n_d) = 0 \quad \text{if } n_x < n \text{ or } n_z < k\,. \tag{5.20}$$

In our case, $n = 1$ and $k = 2$, hence the limits of the sums.

Equation (5.17) follows from

$$P_{\Theta N_x N_z N_d}(110, n_x, n_z, n_d) = 0 \quad \text{for } n_x \geq 2\,. \tag{5.21}$$

One can see (5.21) as follows: if $N_x \geq 2$, then necessarily $N_z = 2$, because $N_x > n \wedge N_z > k$ is impossible in iterative sifting (the loop phase of the protocol is terminated as soon as both quota are met). This means that during the random discarding, no $\mathbb{Z}$-agreement gets discarded. Moreover, if $N_x \geq 2$, then the last round of the loop phase must be a $\mathbb{Z}$-agreement. Since this $\mathbb{Z}$-agreement is not discarded, we have that Θ must necessarily end in a 1 if $N_x \geq 2$, so $\Theta = 110$ is impossible in that case.

To see why Equation (5.18) holds, note that the event

$$\Theta = 110 \wedge N_x = 1 \wedge N_z = n_z \wedge N_d = n_d \tag{5.22}$$

consists of all runs of the protocol in which one $\mathbb{X}$-agreement, n_z $\mathbb{Z}$-agreements and n_d disagreements occurred, and where the $\mathbb{X}$-agreement was the last round of the loop phase. This is because in every such run, one necessarily ends up with $\Theta = 110$, and if $\Theta = 110$, then the last round of the loop phase must be an $\mathbb{X}$-agreement. There are $\binom{n_z+n_d}{n_d}$ such runs, and each of them has the probability $p_x^2(p_z^2)^{n_z}(2p_xp_z)^{n_d}$, and therefore

$$P_{\Theta N_x N_z N_d}(110, 1, n_z, n_d) = \binom{n_z + n_d}{n_d} p_x^2 (p_z^2)^{n_z} (2p_x p_z)^{n_d} \,. \tag{5.23}$$

This explains Equation (5.18). Finally, equation (5.19) is just an evaluation of the expression in the line above. This shows $P_\Theta(110) = g_z^2$.

It remains to be shown that $P_\Theta(101) = P_\Theta(011) = (1 - g_z^2)/2$. In analogy to the above, it holds that

$$P_\Theta(101) = \sum_{n_x=1}^{\infty} \sum_{n_z=2}^{\infty} \sum_{n_d=0}^{\infty} P_{\Theta N_x N_z N_d}(101, n_x, n_z, n_d) \tag{5.24}$$

$$= \sum_{n_x=2}^{\infty} \sum_{n_d=0}^{\infty} P_{\Theta N_x N_z N_d}(101, n_x, 2, n_d) \,. \tag{5.25}$$

Equation (5.24) is, in analogy to Equation (5.16), stating that P_Θ is the marginal of $P_{\Theta N_x N_z N_d}$, and the same argumentation for the limits of the sums applies. Equation (5.25) is explained by a similar reasoning as for Equation (5.17): it follows from

$$P_{\Theta N_x N_z N_d}(101, n_x, n_z, n_d) = 0 \quad \text{for } n_z \geq 3 \,. \tag{5.26}$$

For Equation (5.26), note that if $N_z \geq 3$, then $N_x = 1$ because $N_x > n \wedge N_z > k$ is impossible in iterative sifting. Thus, no $\mathbb{X}$-agreement gets discarded. Moreover, if $N_z \geq 3$, then the last round of the loop phase must be an $\mathbb{X}$-agreement. Since this $\mathbb{X}$-agreement is not discarded, Θ necessarily ends in a 0 if $N_z \geq 3$, so $\Theta = 101$ is impossible in this case.

Analogously, it holds that

$$P_\Theta(011) = \sum_{n_x=1}^{\infty} \sum_{n_z=2}^{\infty} \sum_{n_d=0}^{\infty} P_{\Theta N_x N_z N_d}(011, n_x, n_z, n_d) \tag{5.27}$$

$$= \sum_{n_x=2}^{\infty} \sum_{n_d=0}^{\infty} P_{\Theta N_x N_z N_d}(011, n_x, 2, n_d) \,. \tag{5.28}$$

The next step is to realize that for every $n_x \geq 2$ and for every $n_d \in \{0, 1, 2, \ldots\}$, it holds that

$$P_{\Theta N_x N_z N_d}(101, n_x, 2, n_d) = P_{\Theta N_x N_z N_d}(011, n_x, 2, n_d) \,. \tag{5.29}$$

This is because the event

$$(\Theta = 101, N_x = n_x, N_z = 2, N_d = n_d) \tag{5.30}$$

and the event

$$(\Theta = 011, N_x = n_x, N_z = 2, N_d = n_d) \tag{5.31}$$

consist of equally many histories of the protocol, and each of these histories has the same probability. Equations (5.25), (5.28) and (5.29) imply $P_\Theta(101) = P_\Theta(011)$. Since $P_\Theta(011) + P_\Theta(101) + P_\Theta(110) = 1$ and $P(110) = g_z^2$, it holds that $P_\Theta(011) = P_\Theta(101) = (1 - g_z^2)/2$ as claimed. □

Proposition 5.2 shows that different samples have different probabilities, in general. In order for the sampling probability P_Θ to be uniform, in the case where $n = 1$ and $k = 2$, we need to have $P_\Theta(\vartheta) = 1/3$ for $\vartheta = 011, 101, 110$. This holds if and only if $g_z = g_z^*$, where $g_z^* = 1/\sqrt{3}$, which in turn is equivalent to $p_z = p_z^*$, where

$$p_z^* = \frac{\left(3 + 2\sqrt{3}\right)\left(1 + \sqrt{\sqrt{3} - 1}\right)}{\sqrt{3}} \approx 0.539\,. \tag{5.32}$$

This is bad news for iterative sifting: it means that iterative sifting leads to non-uniform sampling for all values of p_z except $p_z = p_z^*$. Interestingly, the value of p_z^* does not seem to be a probability that has been considered in the QKD literature. In particular, p_z^* corresponds to neither the symmetric case $p_z = 1/2$ nor to a certain asymmetric probability which has been suggested to be chosen in order to maximize the key rate [Tom+12].

The value g_z can be interpreted as the probability that in a certain round of the loop phase, Alice and Bob have a $\mathbb{Z}$-agreement, given that they have an agreement in that round (this conditional is why the p_z^2 is renormalized with the factor $1/(p_z^2 + p_x^2)$). Hence, g_z^2 is the probability that Alice and Bob's first two basis agreements are $\mathbb{Z}$-agreements. Therefore, $P_\Theta(110) = g_z^2$ is what one would intuitively expect: to end up with $\Theta = 110$, the first two basis agreements need to be $\mathbb{Z}$-agreements, and conversely, whenever the first two basis agreements are $\mathbb{Z}$-agreements, Alice and Bob end up with $\Theta = 110$.

More generally, it turns out that for $n = 1$ and for $k \in \mathbb{N}$ arbitrary, the iterative sifting protocol leads to

$$P_\Theta(1\ldots10) = g_z^k\,, \tag{5.33}$$

$$P_\Theta(\vartheta) = \frac{1 - g_z^k}{k} \quad \text{for all other } \vartheta \in \{0,1\}_k^l\,. \tag{5.34}$$

This is a uniform probability distribution if and only if $g_z = g_z^*$, where

$$g_z^* = \left(\frac{1}{k+1}\right)^{1/k}, \tag{5.35}$$

which is true iff $p_z = p_z^*$, where

$$p_z^* = \frac{g_z^* - \sqrt{g_z^*(1 - g_z^*)}}{2g_z^* - 1}\,. \tag{5.36}$$

Hence, we conclude that iterative sifting does not lead to uniformly random sampling, unless p_x and p_z are chosen in a very particular way. This particular choice does not seem to correspond to anything that has been considered in the literature so far.

5.4.2 Basis information leak

In iterative sifting, information about Alice's and Bob's basis choices reaches Eve in every round of the loop phase. In Step 3 of round r, Alice and Bob communicate their basis choice A_r, B_r of that round. They do so because they want to condition their upcoming action on the strings $A_1 \dots A_r$ and $B_1 \dots B_r$: if they have enough basis agreements, they quit the loop phase; otherwise they keep looping.

What seems to have remained unnoticed in the literature is that Eve can also condition her actions on the information previously communicated. More precisely, if there is a round $r+1$, Eve can condition her actions in that round on $A_1 \dots A_r$ and $B_1 \dots B_r$, thereby correlating the state of the qubit that Alice sends to Bob in round $r+1$ with $A_1 \dots A_r$ and $B_1 \dots B_r$. Hence, the state of the qubit that Bob measures is correlated with the classical register that keeps the information about the basis choice. Note that the basis information leak tells Eve how close Alice and Bob are to meeting their quotas for each basis. Eve can tailor her attack on future rounds based on this information. For example, if Alice and Bob have already met their $\mathbb{Z}$-quota, but not their $\mathbb{X}$-quota, then Eve can measure in the $\mathbb{X}$-basis, knowing that, if Alice and Bob happen to both measure $\mathbb{Z}$, the round may be discarded anyway.

We want to emphasize that the basis information leak is not resolved by using additional independent randomness for the choice of the sample. As we will discuss in Section 5.6, such additional randomness can ensure that the sampling is uniform, but it does not help against the basis information leak. Randomness injection for the sample is effectively equivalent to performing a random permutation on the qubits [Ren07]. This does not remove the correlation between the classical basis information register and the qubits.

We will see more concretely how the basis information leak is a problem when we present an eavesdropping attack in the next section and when we treat the problem more formally in Section 5.8.

5.5 Attack strategies exploiting the two security issues

A detailed analysis of the effect of non-uniform sampling and basis information leak on the key rate is beyond the scope of this thesis. It would involve developing a new security analysis for a whole protocol involving iterative sifting. Instead of attempting to find a modified analysis for iterative sifting, we will discuss alternative protocols in Section 5.6.

However, to give an intuitive idea of the effect, we will calculate another figure of merit: the error rate for an intercept-resend attack. We devise a strategy for Eve to attack the iterative sifting protocol during its loop phase and calculate the expected value of the error rate

$$E = \frac{1}{l} \sum_{i=1}^{l} S_i \oplus T_i \tag{5.37}$$

that results from this attack. One would typically expect an error rate no lower than 25% for an intercept-resend attack [HE94], which is why our results below are alarming.

5.5.1 Attack on non-uniform sampling

Let us first consider an attack on non-uniform sampling, i.e. on the fact that not every possible value of Θ is equally likely. It will be a particular kind of intercept-resend attack, i.e. Eve intercepts all the qubits that Alice sends to Bob during the loop phase, measures them in some basis and afterwards, prepares another qubit in the eigenstate associated with her outcome and sends it to Bob. Then we will show that the attack strategy leads to an error rate below 25%.

For the error rate calculation, we assume that the $\mathbb{X}$- and $\mathbb{Z}$-basis is the same for Alice, Bob and Eve, and that they are mutually unbiased. This way, if Alice and Bob measure in the same basis, but Eve measures in the other basis, then Eve introduces an error probability of 1/2 on this qubit (recall the discussion in section 3.1.3). Moreover, for simplicity, we make this calculation for the easiest possible choice of parameters. Consider the iterative sifting protocol with the parameters $k = n = 1$. From Equations (5.35) and (5.36), we get that the sampling probabilities in this case are

$$P_\Theta(01) = \frac{p_x^2}{p_x^2 + p_z^2}\,, \quad P_\Theta(10) = \frac{p_z^2}{p_x^2 + p_z^2}\,. \tag{5.38}$$

These sampling probabilities are uniform for the symmetric case $p_x = p_z$, but are non-uniform for all other values. In the following, we assume $p_x > 1/2$, which makes the sample $\Theta = 01$ more likely than the sample $\Theta = 10$. We choose the following attack: in the first round of the loop phase, she attacks in the $\mathbb{X}$-basis, and in all the other rounds, she attacks in the $\mathbb{Z}$-basis. We choose the attack this way because we know that the first non-discarded basis agreement is more likely to be an $\mathbb{X}$-agreement, whereas the second one is more likely to be a $\mathbb{Z}$-agreement.[6]

We calculate the expected error rate for this attack in Appendix A.1. The black curve in Figure 5.6 shows $\langle E \rangle$ as a function of p_x for this attack. Notice that $\langle E \rangle$ falls below 25% for $1/2 < p_x < 1$, and reaches a minimum of $\langle E \rangle \approx 22.8\%$ for $p_x \approx 0.73$.

The concerned reader might worry that the 25% error rate associated with the intercept-resend attack was derived under the assumption of equal weighting for the two bases $\mathbb{X}$ and $\mathbb{Z}$, whereas it seems here that we choose unequal weightings. However, for the protocol under consideration, the a priori probability distribution $\{p_x, p_z\}$ is not the relevant quantity. Rather, the fact that $n = k$ in our example ensures that the $\mathbb{X}$ and $\mathbb{Z}$ bases enter in with equal weighting.

[6] The attentive reader may point out that this attack could be improved by making Eve's basis choice dependent on the communication between Alice and Bob. This is correct, but we intentionally design the attack such that Eve ignores Alice and Bob's communication. That allows one to see the effect of non-uniform sampling alone and to compare it to attacks on basis information leak alone, see Sections 5.5.2 and 5.5.3.

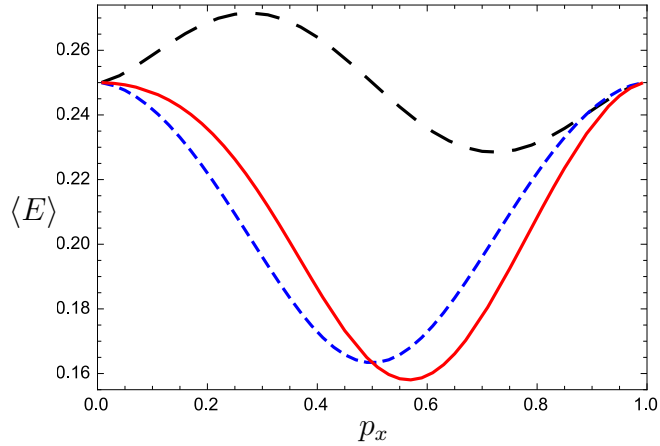


Figure 5.6: The error rate for three different eavesdropping attacks on iterative sifting: (1) attack on non-uniform sampling (long-dashed, black curve), (2) attack on basis-information leak (short-dashed, blue curve), (3) attack on both problems (solid, red curve).

5.5.2 Attack on basis information leak

We now give an eavesdropping strategy that exploits the basis information leak. It is an adaptive strategy, in which Eve's actions in round $r+1$ depend on the past communication of the strings $a_1 \dots a_r$ and $b_1 \dots b_r$. Again, we consider the simple case of $n = k = 1$. To make sure our attack is really exploiting the basis information leak and not the non-uniform sampling, we set $p_x = p_z = 1/2$. In this case, from Eq. (5.38), the sampling is uniform:

$$P_\Theta(01) = P_\Theta(10) = \frac{1}{2}. \tag{5.39}$$

Before we define Eve's strategy, we want to give some intuition. Suppose that during the protocol, Eve learns that Alice and Bob just had their first basis agreement. If this first agreement is a $\mathbb{Z}$-agreement, say, what does this mean for Eve? She knows that the protocol will now remain in the loop phase until they end up with an $\mathbb{X}$-agreement. Suppose that she now decides that she will measure all the remaining qubits in the $\mathbb{X}$-basis. Then, if the next basis agreement of Alice and Bob is an $\mathbb{X}$-agreement, Eve knows the raw key bit perfectly, and her measurement on that bit did not introduce an error. If the next basis agreement is a $\mathbb{Z}$-agreement, she may introduce an error on that test bit. However, there will be a chance that Alice and Bob discard this test bit, because they have a total of two (or more, in the end) $\mathbb{Z}$-agreements, and the protocol forces them to discard all $\mathbb{Z}$-agreements except $k = 1$ of them. Hence, learning that the first basis agreement was a $\mathbb{Z}$-agreement brings Eve into an favorable position: she knows that attacking in the $\mathbb{X}$-basis for the rest of the loop phase will necessarily tell her the raw key bit, while she has a high chance to remain undetected.

This intuition inspires the following intercept-resend attack. Before the first round of the loop phase, Eve flips a fair coin. Let F be the random variable of the coin flip outcome and let 0 and 1 be its possible values. If $F = 0$, then in the first round, Eve attacks in the $\mathbb{X}$ basis, and if $F = 1$, she attacks

in the $\mathbb{Z}$-basis. In the subsequent rounds, she keeps attacking in that basis until Alice and Bob first reached a basis agreement. If it is an $\mathbb{X}$-agreement (equivalent to $\Theta = 01$), Eve attacks in the $\mathbb{Z}$-basis in all remaining rounds, and if it is a $\mathbb{Z}$-agreement (equivalent to $\Theta = 10$), she attacks in the $\mathbb{X}$-basis in all remaining rounds.[7]

We calculate the expected error rate for this attack in the Appendix A.2. We find that

$$\langle E \rangle = \frac{2 - \ln 2}{8} \approx 16.3\% \,. \tag{5.40}$$

Hence, the basis information leak allows Eve to go far below the typical expected error rate of 25% for intercept-resend attacks [Sca+09]. The blue curve in Figure 5.6 shows, more generally, $\langle E \rangle$ as a function of p_x, for this attack.

5.5.3 Independence of the two problems

Are non-uniform sampling and basis information leak really two different problems, or is one a consequence of the other? We will argue now that the two problems are in fact independent. To this end, we describe a protocol that suffers from non-uniform sampling but not from basis information leak, and another protocol that suffers from basis information leak but not from non-uniform sampling.

We have already seen an instance of a protocol that suffers from basis information leak but not from non-uniform sampling: in section 5.5.2, we looked at the iterative sifting protocol with $n = k = 1$ and $p_x = p_z = 1/2$, in which case the sampling is uniform. Hence, there was no exploitation of non-uniform sampling, but the attack strategy exploited basis information leak.

What about the other way round? Can non-uniform sampling occur without basis information leak? A closer look at the attack on non-uniform sampling presented in Section 5.5.1 hints that this is possible: the attack strategy works, even though it completely ignores the communication between Alice and Bob, so it did not make any use of the basis information leak due to this communication.

A more dramatic example shows clearly that non-uniform sampling can occur without basis information leak. To this end, we forget about iterative sifting for a moment and look at a different protocol. Consider a sifting-protocol in which Alice and Bob agree in advance that they will measure the first $n = 100$ qubits in the $\mathbb{X}$-basis, and that they will measure the second $k = 100$ qubits in the $\mathbb{Z}$-basis, without any communication during the protocol. Of course, there is no hope for this protocol to be useful for QKD, but it serves well to demonstrate our point. It leads to a very dramatic form of non-uniform sampling, because $P_\Theta(0\ldots01\ldots1) = 1$ and $P_\Theta(\vartheta) = 0$ for all other $\vartheta \in \{0,1\}^l_k$. If Eve attacks the first 100 rounds in $\mathbb{X}$ and the second 100 rounds in $\mathbb{Z}$, then she knows the raw key perfectly, without introducing any error. At the same

[7] We let Eve flip a coin in order to make the attack symmetric between $\mathbb{X}$ and $\mathbb{Z}$. This allows for a more meaningful comparison with the attack on non-uniform sampling, as this attack here does not exploit non-uniform sampling even if $p_x \neq 1/2$, see Sections 5.5.1 and 5.5.3.

time, there is no communication between Alice and Bob during the protocol, so no information about the basis choice is *leaked during the protocol*. Instead, Eve (who is always assumed to know the protocol) already had this information before the first round.

Hence, we conclude that the problems of non-uniform sampling and basis information leak are independent. They just happen to occur simultaneously when iterative sifting is used together with SBPE, but they can occur separately in general. It is important to note that while non-uniform sampling can be avoided by using fresh randomness for the sample, the basis information leak cannot be avoided this way. Hence, iterative sifting is problematic, no matter which parameter estimation protocol follows. We will see the independence of the two problems more formally in Section 5.8.

5.5.4 Attack on both problems

Since the two problems are independent, it is interesting to devise an attack that exploits both of them. Let us again consider $k = n = 1$ and suppose $p_x > 1/2$ to ensure that we have non-uniform sampling. Suppose Eve begins in the same way as in the attack on non-uniform sampling, measuring in the $\mathbb{X}$-basis. However, as in the attack on the basis-information leak, she makes her attack adaptive by following the rule that she switches to the $\mathbb{Z}$-basis when Alice and Bob announce that they had an $\mathbb{X}$-agreement. If Alice and Bob announce a $\mathbb{Z}$-agreement, Eve keeps attacking in the $\mathbb{X}$-basis.

We give an expression for the error rate induced by this attack in Appendix A.3. The red curve in Figure 5.6 shows a plot of this error rate as a function of p_x. As one can see, the error rate attains its minimum of $\langle E \rangle \approx 15.8\%$ for $p_x \approx 0.57$. Hence, this combined attack on both problems performs much better than the one on non-uniform sampling alone (with a minimal error rate of $\sim 22.8\%$) and even better than the attack on the basis information leak alone (with a minimal error rate of $\sim 16.3\%$).

5.6 A secure yet efficient alternative

How can these problems be avoided? As we have seen, it is the communication in step 3 during the loop phase of iterative sifting which causes the basis information leak. An obvious fix to this problem is to take this communication out of the loop phase and to postpone it to the final phase, when all the quantum communication is over. Then there is no classical communication during the loop phase, and hence, there cannot be a termination condition that depends on classical communication. Instead, the number of rounds in the loop phase is set to a fixed number $m \in \mathbb{N}$. This number m then becomes a parameter of the protocol. In this case, there is no guarantee that the quota for the $\mathbb{X}$-agreements and the $\mathbb{Z}$-agreements will be met: the higher m is chosen, the more likely it is, but there is always a chance that they have not enough $\mathbb{X}$- and $\mathbb{Z}$-agreements. Thus, after Alice and Bob compared the basis choices, they may have to abort the protocol. We have already seen the resulting sifting protocol informally: it coincides with the sifting protocol of Lo, Chau and Ardehali [LCA05] that we have seen in section 5.2.

Since LCA sifting, together with SBPE, will form the raw key distribution protocol whose security we prove in the next subsection, it is worth choosing a notation that simplifies a formal proof. The resulting formal version of the LCA protocol is written out in protocol 5.3. Here, we shall go through the protocol and thereby explain the notation.

Steps 1 and 2 are the same as in iterative sifting: in every round r, they choose bases A_r, B_r and get measurement results Y_r, Y_r'. The only difference is that in LCA sifting, the two steps are repeated m times without any additional classical communication. In LCA sifting, the communication about the basis choices takes place in the final phase in step 3'. They communicate the basis choices of all the m rounds and determine the number of $\mathbb{X}$- and $\mathbb{Z}$-agreements. Formally, we say that they do so by determining the *comparison string* $C = C_1 \dots C_m$, defined as

$$C_r := \begin{cases} x & \text{if } A_r = B_r = 0\,, \\ z & \text{if } A_r = B_r = 1\,, \\ d & \text{if } A_r \neq B_r\,. \end{cases} \tag{5.42}$$

Then they determine the number of $\mathbb{X}$- and $\mathbb{Z}$-agreements by applying the functions $\mathcal{X}$ and $\mathcal{Z}$ to the comparison string C, defined as

$$\mathcal{X}(C) := \{r \in [m] \mid C_r = x\}\,, \tag{5.43}$$

$$\mathcal{Z}(C) := \{r \in [m] \mid C_r = z\}\,. \tag{5.44}$$

Alice and Bob abort if $|\mathcal{X}(C)| < n$ or $|\mathcal{Z}(C)| < k$. In that case we say formally that Alice and Bob output $S = T = \Theta = \perp$, where $\perp$ is just a flag indicating that they abort the protocol. Step 4 is the same as in protocol 5.1, i.e. they discard disagreements and surplus at random. The sets of all $\mathbb{X}$- and $\mathbb{Z}$-agreements are $\mathcal{X}(C)$ and $\mathcal{Z}(C)$, of which they choose subsets of size n and k, respectively. To denote the set of all subsets of a certain size, we use a notation which is common in combinatorics, namely

$$\binom{\mathcal{X}(C)}{n} := \{U \subseteq \mathcal{X}(C) \mid |U| = n\}\,. \tag{5.45}$$

Finally, steps 5 and 6 are exactly the same as in iterative sifting: they relabel the sifted outcome strings to S and T and the sifted basis choice string to Θ, and then output it.

LCA sifting trivially has no basis information leak, because there is no classical communication about the basis choices during the quantum communication. What about uniform sampling? Recall from section 5.2 that Lo, Chau and Ardehali, instead of using SBPE, proposed a parameter estimation where two error rates are determined, where one sample is formed by the sifted $\mathbb{Z}$-agreements and the other sample is chosen at random from the $\mathbb{X}$-agreements. We argued that it would be more efficient to use SBPE instead. In the case where SBPE is used, uniform sampling is equivalent to

$$P_\Theta(\vartheta) = P_\Theta(\vartheta') \quad \text{for all } \vartheta, \vartheta' \in \{0,1\}^l_k\,. \tag{5.46}$$

Checking condition equation (5.46) is non-trivial for LCA sifting. We will prove it in section 5.7. In section 5.8, we will prove that this condition implies

LCA Sifting

Parameters: $n, k, m \in \mathbb{N}_+$ with $m \geq n + k$, $p_x, p_z \in [0, 1]$ with $p_x + p_z = 1$.

Outputs:
- Alice: l-bit string $(S_i)_{i=1}^l \in \{0,1\}^l$ (sifted outcomes),
- Bob: l-bit string $(T_i)_{i=1}^l \in \{0,1\}^l$ (sifted outcomes),
- public: l-bit string $(\Theta_i)_{i=1}^l \in \{0,1\}_k^l$ (sifted basis choices)

The protocol

Loop phase: Steps 1 and 2 are repeated m times (round index $r = 1, \ldots, m$). In round r, Alice and Bob do the following:

Step 1: Alice prepares a qubit pair in a maximally entangled state and sends one half to Bob.

Step 2: Alice and Bob independently choose a basis $A_r, B_r \in \{0, 1\}$ with probability p_x and p_z, respectively, where 0 stands for the $\mathbb{X}$-basis and 1 stands for the $\mathbb{Z}$-basis. Then they measure their part of the qubit pair in that basis and get an outcome $Y_r, Y'_r \in \{0, 1\}$, respectively.

Final phase: The following steps are performed in a single run:

Step 3': Alice and Bob communicate their basis choice strings A and B over a public authenticated channel and determine the comparison string C as defined in equation equation (5.42). They check whether quota condition ($|\mathcal{X}(C)| \geq n$ and $|\mathcal{Z}(C)| \geq k$) holds, where $\mathcal{X}(C)$ and $\mathcal{Z}(C)$ count the occurrences of x and z in C, respectively (see equations (5.43) and (5.44)). If it holds, they proceed with Step 4. Otherwise, they abort and output $S = T = \Theta = \perp$ (abort flag).

Step 4: Alice and Bob choose subsets

$$U \in \binom{\mathcal{X}(C)}{n}, \quad V \in \binom{\mathcal{Z}(C)}{k} \tag{5.41}$$

fully at random (where the notation in equation (5.45) is used).

Step 5: Let R_i be the i-th element of $U \cup V$. Then Alice determines $(S_i)_{i=1}^l \in \{0,1\}^l$, Bob determines $(T_i)_{i=1}^l \in \{0,1\}^l$ and together they determine $(\Theta_i)_{i=1}^l \in \{0,1\}_k^l$, where for every $i \in [l]$,

$$S_i = Y_{R_i}\,, \quad T_i = Y'_{R_i}\,, \quad \Theta_i = A_{R_i}\,(= B_{R_i})\ .$$

Step 6: Alice locally outputs $(S_i)_{i=1}^l$, Bob locally outputs $(T_i)_{i=1}^l$, and they publicly output $(\Theta_i)_{i=1}^l$.

Protocol 5.3: The Lo-Chau-Ardehali (LCA) sifting protocol.

the security of the protocol on a formal level. As a preparation for the proof of equation (5.46), we will now formulate a probability space model for LCA sifting.

5.6.1 A probability space model for LCA sifting

We are looking for a probability space model for LCA sifting from which we can deduce the probability distribution of the random variable Θ. This means that we look for a probability space (Ω, P), where Ω is an appropriately chosen set of histories of the protocol and P gives the probability for each history. By "appropriately chosen", we mean that we only need to track those parts of the history of a protocol that are relevant for Θ. For example, the measurement outcomes Y, Y' of Alice and Bob are irrelevant for Θ, so they will not appear in the elements $\omega \in \Omega$ (c.f. the analogous discussion for iterative sifting on page 77). This will become more clear in the following.

In every run of the LCA sifting protocol, Alice and Bob produce a comparison string C. The sifted basis choice string Θ depends on that string C, but not on the basis choice strings A and B of Alice and Bob individually. We can distinguish between two main cases:

($\perp$) Alice and Bob do not have enough basis agreements and need to abort, i.e. $|\mathcal{X}(C)| < n$ or $|\mathcal{Z}(C)| < k$.

($\checkmark$) Alice and Bob have enough basis agreements, i.e. $|\mathcal{X}(C)| \geq n$ and $|\mathcal{Z}(C)| \geq k$,

In the case ($\perp$), we necessarily have that $\Theta = \perp$, so in that case, Θ does not depend on anything more than the comparison string. We set

$$\Omega^{\perp} = \{c \in \{x, z, d\}^m \mid |\mathcal{X}(c)| < n \text{ or } |\mathcal{Z}(c)| < k\}\,, \tag{5.47}$$

so $\Omega^{\perp}$ consists of all comparison strings that do not meet the quota condition.

In the case ($\checkmark$), the protocol continues, and Θ does not only depend on C but also on the choices of the subsets U and V. Thereby, only those U and V are possible that are subsets of $\mathcal{X}(C)$ and $\mathcal{Z}(C)$. We set

$$\Omega^{\checkmark} = \left\{(c, u, v) \in \{x, z, d\}^m \times \binom{[m]}{n} \times \binom{[m]}{k} \;\middle|\; u \subseteq \mathcal{X}(c) \text{ and } v \subseteq \mathcal{Z}(c)\right\}. \tag{5.48}$$

Note that if an n-element set u is a subset of $\mathcal{X}(c)$, then $|\mathcal{X}(c)| \geq n$, and similarly for v, so we do not need to explicitly require these inequalities to hold.

In every run of the protocol, either ($\perp$) or ($\checkmark$) occurs. That is,

$$\Omega = \Omega^{\perp} \uplus \Omega^{\checkmark}\,, \tag{5.49}$$

where the $+$ in the $\cup$ symbol means that the sets $\Omega^{\perp}$ and $\Omega^{\checkmark}$ are disjoint, but otherwise the meanings of $\cup$ and $\uplus$ are identical. Equations (5.47) ,(5.48) and (5.49) define the sample space of the probability space that we are looking for.

In order to determine the probability mass function P on Ω, it is useful to further partition $\Omega^{\perp}$ and $\Omega^{\checkmark}$ into subsets on which P is constant.

$$\Omega^{\perp} = \biguplus_{(n_x,n_z)\in\mathcal{N}^{\perp}} \Omega^{\perp}_{(n_x,n_z)} \,, \tag{5.50}$$

$$\Omega^{\checkmark} = \biguplus_{(n_x,n_z)\in\mathcal{N}^{\checkmark}} \Omega^{\checkmark}_{(n_x,n_z)} \,. \tag{5.51}$$

where

$$\Omega^{\perp}_{(n_x,n_z)} = \left\{ c \in \Omega^{\perp} \mid |\mathcal{X}(c)| = n_x \text{ and } |\mathcal{Z}(c)| = n_z \right\} \,, \tag{5.52}$$

$$\mathcal{N}^{\perp} = \left\{ (n_x,n_z) \in \{0,\dots,m\} \times \{0,\dots,m\} \;\middle|\; \begin{array}{l} n_x + n_z \;\leq\; m \text{ and} \\ (n_x < n \text{ or } n_z < k) \end{array} \right\} \,, \tag{5.53}$$

$$\Omega^{\checkmark}_{(n_x,n_z)} = \left\{ (c,u,v) \in \Omega^{\checkmark} \mid |\mathcal{X}(c)| = n_x \text{ and } |\mathcal{Z}(c)| = n_z \right\} \,, \tag{5.54}$$

$$\mathcal{N}^{\checkmark} = \left\{ (n_x,n_z) \in \{0,\dots,m\} \times \{0,\dots,m\} \;\middle|\; \begin{array}{l} n_x + n_z \;\leq\; m \text{ and} \\ n_x \geq n \text{ and } n_z \geq k \end{array} \right\} \,. \tag{5.55}$$

The set $\Omega^{\perp}_{(n_x,n_z)}$ is the set of all comparison strings $c \in \Omega^{\perp}$ which have n_x $\mathbb{X}$-agreements and n_z $\mathbb{Z}$-agreements, and analogously for triples $(c,u,v) \in \Omega^{\checkmark}_{(n_x,n_z)}$.

Now we are going to determine the probability mass function $P : \Omega \to [0,1]$. Let us first determine the probability of an element $\omega = c$ that only consists of a comparison string $c \in \Omega^{\perp}$. Note that in each round, the probability for an $\mathbb{X}$-agreement, $\mathbb{Z}$-agreement or disagreement is given by p_x^2, p_z^2 and $2p_xp_z$, respectively. Hence, what matters for the probability $P(\omega)$ is the number of $\mathbb{X}$-, $\mathbb{Z}$-agreements and disagreements of the comparison string $\omega = c$. For a string $\omega = c \in \Omega^{\perp}_{(n_x,n_z)}$ for some $(n_x,n_z) \in \mathcal{N}^{\perp}$, the probability is given by

$$P(\omega) = p_x^{2n_x} p_z^{2n_z} (2p_xp_z)^{m-n_x-n_z} \,. \tag{5.56}$$

Since $\Omega^{\perp}$ is the disjoint union of such sets $\Omega^{\perp}_{(n_x,n_z)}$, this uniquely determines $P(\omega)$ for all $\omega \in \Omega^{\perp}$.

We are left to determine the probability of a triple $\omega = (c,u,v) \in \Omega^{\checkmark}$. Again, the probability depends only on the number of $\mathbb{X}$-, $\mathbb{Z}$-agreements and disagreements. In the probability for an $\omega \in \Omega^{\checkmark}_{(n_x,n_z)}$ for some $(n_x,n_z) \in \mathcal{N}^{\checkmark}$, there is a factor $p_x^{2n_x} p_z^{2n_z} (2p_xp_z)^{m-n_x-n_z}$ as before. In addition, however, there are two factors for the probability of the choice of u and v. For $\omega = (c,u,v) \in \Omega^{\perp}_{(n_x,n_z)}$, u is a n-element subset of the n_x $\mathbb{X}$-agreements. There are $\binom{n_x}{n}$ such sets, and each of them has the same probability given by $\binom{n_x}{n}^{-1}$. Analogously, the set v is chosen with probability $\binom{n_z}{k}^{-1}$. Put together, this means that for $\omega \in \Omega^{\perp}_{(n_x,n_z)}$, the probability $P(\omega)$ is given by

$$P(\omega) = p_x^{2n_x} p_z^{2n_z} (2p_xp_z)^{m-n_x-n_z} \binom{n_x}{n}^{-1} \binom{n_z}{k}^{-1} \,. \tag{5.57}$$

Hence, the probability mass function $P : \Omega \to [0,1]$ that we are looking for is given by

$$\begin{aligned} P: \quad \Omega &\to [0,1] \\ \omega &\mapsto \begin{cases} p_x^{2n_x} p_z^{2n_z} (2p_x p_z)^{m-n_x-n_z} & \text{if } \omega \in \Omega^{\perp}_{(n_x,n_z)} \text{ for some } (n_x,n_z) \in \mathcal{N}^{\perp}, \\ p_x^{2n_x} p_z^{2n_z} (2p_x p_z)^{m-n_x-n_z} \binom{n_x}{n}^{-1} \binom{n_z}{k}^{-1} & \text{if } \omega \in \Omega^{\checkmark}_{(n_x,n_z)} \text{ for some } (n_x,n_z) \in \mathcal{N}^{\checkmark}. \end{cases} \end{aligned} \tag{5.58}$$

This determines the probability space (Ω, P).

Now we determine the random variable Θ. Recall from protocol 5.3 that either $\Theta = \perp$ or $\Theta \in \{0,1\}^l_k$. Therefore, the codomain Ω_Θ is given by

$$\Omega_\Theta = \{\perp\} \cup \{0,1\}^l_k \,. \tag{5.59}$$

We are looking for the map $\Theta : \Omega \to \Omega_\Theta$. We have two cases to distinguish: the case where $\omega = c \in \Omega^{\perp}$ and the case where $\omega = (c,u,v) \in \Omega^{\checkmark}$. In the case where $\omega \in \Omega^{\perp}$, Alice and Bob abort the protocol and output $\vartheta = \perp$, so $\Theta(\omega) = \perp$. In the case where $\omega = (c,u,v) \in \Omega^{\checkmark}_{(n_x,n_z)}$, Alice and Bob output a string $\vartheta \equiv \vartheta(u,v)$ which depends on the sets u and v. The value of the i-th element $\vartheta_i(u,v)$ of $\vartheta(u,v)$ depends on the i-th element of the set $u \cup v$: if it belongs to u, then $\vartheta_i(u,v) = 0$, and if it belongs to v, then $\vartheta_i(u,v) = 1$. Let us denote the i-th element of $u \cup v$ by $(u \cup v)_i$. Then, the random variable Θ that we are looking for is given by

$$\begin{aligned} \Theta: \quad \Omega &\to \Omega_\Theta \\ \omega &\mapsto \begin{cases} \perp & \text{if } \omega \in \Omega^{\perp}, \\ \vartheta(u,v) & \text{if } \omega \in \Omega^{\checkmark}, \end{cases} \end{aligned} \tag{5.60}$$

where

$$\vartheta_i(u,v) = \begin{cases} 0 & \text{if } (u \cup v)_i \in u\,, \\ 1 & \text{if } (u \cup v)_i \in v\,. \end{cases} \tag{5.61}$$

This completes our probability space model for LCA sifting: we determined a probability space (Ω, P) and a random variable Θ on that space. This will allow us to determine the distribution P_Θ in the next section.

5.7 Proof of uniform sampling for LCA sifting

Proposition 5.3 : *The LCA sifting protocol (see protocol 5.3), together with single-basis parameter estimation (protocol 5.2) samples uniformly. That is, for the random variable Θ on (Ω, P) as defined in the previous section, it holds that*

$$P_\Theta(\vartheta) = P_\Theta(\vartheta') \quad \text{for all } \vartheta, \vartheta' \in \{0,1\}^l_k \,. \tag{5.62}$$

The abort probability $p^{\text{sift}}_{\text{abort}} := P_\Theta(\perp)$ *of the protocol is given by*

$$P_\Theta(\perp) = 1 - \sum_{n_x=n}^{m-k} \sum_{n_z=k}^{m-n_x} \binom{m}{n_x} \binom{m-n_x}{n_z} p_x^{2n_x} p_z^{2n_z} (2p_x p_z)^{m-n_x-n_z} \,. \tag{5.63}$$

Proof. We first determine the probability of a sifted basis choice string $\vartheta \in \{0,1\}^l_k$. We will show that it does not depend on the choice of $\vartheta \in \{0,1\}^l_k$, which proves that the protocol samples uniformly. For $\vartheta \in \{0,1\}^l_k$,

$$P_\Theta(\vartheta) = \sum_{\omega \in \Theta^{-1}(\vartheta)} P(\omega) \,, \tag{5.64}$$

where

$$\Theta^{-1}(\vartheta) = \left\{ (c,u,v) \in \Omega^\checkmark \;\middle|\; (u \cup v)_i \in \begin{cases} u & \text{if } \vartheta_i = 0 \\ v & \text{if } \vartheta_i = 1 \end{cases} \right\} . \tag{5.65}$$

We can partition $\Theta^{-1}(\vartheta)$ as follows:

$$\Theta^{-1}(\vartheta) = \biguplus_{(n_x,n_z) \in \mathcal{N}^\checkmark} \underbrace{\Theta^{-1}(\vartheta) \cap \Omega^\checkmark_{(n_x,n_z)}}_{=:\Theta^{-1}_{(n_x,n_z)}(\vartheta)} \,. \tag{5.66}$$

In words, the set $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$ is the set of all triples (c,u,v) with n_x $\mathbb{X}$-agreements and n_z $\mathbb{Z}$-agreements that lead to the string ϑ. Since the union in (5.66) is a union of disjoint sets, we can write $P_\Theta(\vartheta)$ as the sum

$$P_\Theta(\vartheta) = \sum_{(n_x,n_z) \in \mathcal{N}^\checkmark} \sum_{\omega \in \Theta^{-1}_{(n_x,n_z)}} P(\omega) \,. \tag{5.67}$$

Recall from (5.58) that the probability mass function P is constant on the set $\Omega^\checkmark_{(n_x,n_z)}$. Therefore, P is also constant on $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$ with the same value, namely

$$P(\omega) = p_x^{2n_x} p_z^{2n_z} (2p_x p_z)^{m-n_x-n_z} \binom{n_x}{n}^{-1} \binom{n_z}{k}^{-1} \quad \text{for all } \omega \in \Theta^{-1}_{(n_x,n_z)}(\vartheta) \,. \tag{5.68}$$

Therefore, for every $\vartheta \in \{0,1\}^l_k$,

$$P_\Theta(\vartheta) = \sum_{(n_x,n_z) \in \mathcal{N}^\checkmark} \left| \Theta^{-1}_{(n_x,n_z)}(\vartheta) \right| p_x^{2n_x} p_z^{2n_z} (2p_x p_z)^{m-n_x-n_z} \binom{n_x}{n}^{-1} \binom{n_z}{k}^{-1} . \tag{5.69}$$

Thus, in order to show uniform sampling, it is sufficient to show that the size of $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$ is independent of the choice of $\vartheta \in \{0,1\}^l_k$. Not only are we going to show this independence, we also determine the size as a function of m, n, k, n_x, n_z (and $l := n + k$). More precisely, we are now going to show following equation:

$$\left| \Theta^{-1}_{(n_x,n_z)}(\vartheta) \right| = \binom{m}{l} \binom{m-l}{n_x-n} \binom{m-l-(n_x-n)}{n_z-k} . \tag{5.70}$$

We will arrive at this equation through combinatorial arguments.

In preparation for these combinatorial arguments, we want to gain some intuition for the set $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$. To this end, let us consider an example with the following parameters:

$$m = 10\,, n = k = 2\,, n_x = 3\,, n_z = 4\,. \tag{5.71}$$

The string $\vartheta \in \{0,1\}^l_k$ that we consider for this example shall be

$$\vartheta = 1001\,. \tag{5.72}$$

Consider an element of $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$ for this example:

$$(c,u,v) = (zxzdxdxzz, \{2,7\}, \{1,9\}) \in \Theta^{-1}_{(n_x,n_z)}(\vartheta)\,. \tag{5.73}$$

Let us convince ourselves of the fact that this is indeed an element of $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$. The string c has 3 x-entries and 4 z-entries, and $u \subseteq \mathcal{X}(c)$ and $v \subseteq \mathcal{Z}(c)$ are both true. Hence, $(c,u,v) \in \Omega^{\checkmark}_{(n_x,n_z)}$. Moreover, $(u \cup v)_1 \in u$, $(u \cup v)_2 \in v$, $(u \cup v)_3 \in v$, $(u \cup v)_4 \in u$, and thus $\Theta(c,u,v) = 1001$. Therefore, $(c,u,v) \in \Theta^{-1}(\vartheta)$ and thus $(c,u,v) \in \Theta^{-1}_{(n_x,n_z)}(\vartheta)$. Graphically, we can represent this example as follows:

first example element of $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$:

r :	1	2	3	4	5	6	7	8	9
c_r :	z	x	z	d	x	d	x	z	z
u :		2					7		
v :	1								9

(5.74)

Here, we colored the rounds that are chosen according to the set u in green and those that are chosen according to v in yellow. Let us consider another element of $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$, namely:

second example element of $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$:

r :	1	2	3	4	5	6	7	8	9
c_r :	x	z	d	x	x	d	z	z	z
u :				4	5				
v :		2						8	

(5.75)

Note that the relative order of the u-elements relative to the v-elements in the set $u \cup v$ is identical in the two examples: we see the colors in the order yellow, green, green, yellow. It has to be this way: $\vartheta = 1001$ requires the first and fourth element of $u \cup v$ to be elements of v and the second and third element to be elements of u. What differs between the two examples is the relative position of $u \cup v$ in $[m]$. In fact, *any* relative order of $u \cup v$ in $[m]$ is possible for a pre-image of ϑ. There are $\binom{m}{n+k} = \binom{m}{l}$ such relative orders. This is where the first factor in (5.70) comes from.

For each such order, there are $m - l$ remaining rounds in which the remaining $\mathbb{X}$-, $\mathbb{Z}$-agreements and disagreements need to happen. Let us first focus on the remaining $\mathbb{X}$-agreements. There is a total of n_x $\mathbb{X}$-agreements, n of which are already chosen through the choice of u. Hence, there are $n_x - n$ remaining $\mathbb{X}$-agreements that need to happen in any of the remaining $m - l$ rounds. Let us see in the two example elements of $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$ above where these remaining

$\mathbb{X}$-agreements are placed. In these examples, $m-l=5$ and $n_x-n=1$. Hence, one of the remaining five white rounds in (5.74) and (5.75) needs to have an $\mathbb{X}$-agreement, which we now color in blue:

first example element of $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$:

$$\begin{array}{lccccccccc} r: & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ c_r: & z & x & z & d & x & d & x & z & z \\ u: & & 2 & & & & & 7 & & \\ v: & 1 & & & & & & & & 9 \end{array} \tag{5.76}$$

second example element of $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$:

$$\begin{array}{lccccccccc} r: & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ c_r: & x & z & d & x & x & d & z & z & z \\ u: & & & & 4 & 5 & & & & \\ v: & & 2 & & & & & & 8 & \end{array} \tag{5.77}$$

In both examples, there are $\binom{m-l}{n_x-n}=5$ remaining white slots that could be filled with blue. More generally, for each relative order of $u\cup v$ in $[m]$, there are are $\binom{m-l}{n_x-n}$ remaining ways for positioning the remaining $\mathbb{X}$-agreements. This contributes the second factor in equation (5.70).

Given a relative order of $u\cup v$ in $[m]$ and a relative order of the remaining $\mathbb{X}$-agreements in the other $m-l$ rounds, there are $m-l-(n_x-n)$ remaining rounds in which the remaining n_z-k $\mathbb{Z}$-agreements take place. This contributes another factor $\binom{m-l-(n_x-n)}{n_z-k}$ to (5.70).

After these three choices (relative order of $u\cup v$ in $[m]$, remaining $\mathbb{Z}$-agreements in the remaining $m-l$ rounds, remaining $\mathbb{Z}$-agreements in the remaining $m-l-(n_x-n)$ rounds), the pre-image of ϑ is fixed, because the remaining rounds need to be disagreements. Hence, choosing a pre-image of ϑ means making these three choices, and therefore the size of $\Theta^{-1}_{(n_x,n_z)}(\vartheta)$ is given by equation (5.70). It is independent of the choice of $\vartheta\in\{0,1\}^l_k$, so by virtue of equation (5.69), we have proved uniform sampling.

Since P_Θ is a probability mass function on $\Omega_\Theta=\{0,1\}^l_k\cup\{\perp\}$, we have that

$$P_\Theta(\perp)=1-\sum_{\vartheta\in\{0,1\}^l_k}P_\Theta(\vartheta) \tag{5.78}$$

$$=1-\left|\{0,1\}^l_k\right|P_\Theta(\vartheta)\quad\text{with }\vartheta\in\{0,1\}^l_k \tag{5.79}$$

$$=1-\binom{l}{k}P_\Theta(\vartheta)\quad\text{with }\vartheta\in\{0,1\}^l_k\,. \tag{5.80}$$

Hence, in order to obtain the abort probability, we just need to finish our calculation of $P_\Theta(\vartheta)$ for $\vartheta\in\{0,1\}^l_k$. Inserting (5.70) into (5.69) yields a product of five binomial coefficients in the summand. An easy calculation using the definition of the binomial coefficient in terms of factorials and using $l=n+k$ shows that

$$\begin{aligned}&\binom{m}{l}\binom{m-l}{n_x-n}\binom{m-l-(n_x-n)}{n_z-k}\binom{n_x}{n}^{-1}\binom{n_z}{k}^{-1}\\ &=\binom{l}{k}^{-1}\binom{m}{n_x}\binom{m-n_x}{n_z}\,.\end{aligned} \tag{5.81}$$

Thus, for $\vartheta \in \{0,1\}^l_k$,

$$P_\Theta(\vartheta) = \binom{l}{k}^{-1} \sum_{(n_x,n_z)\in\mathcal{N}^\checkmark} \binom{m}{n_x}\binom{m-n_x}{n_z} p_x^{2n_x} p_z^{2n_z} (2p_x p_z)^{m-n_x-n_z} \tag{5.82}$$

$$= \binom{l}{k}^{-1} \sum_{n_x=n}^{m-k} \sum_{n_z=k}^{m-n_x} \binom{m}{n_x}\binom{m-n_x}{n_z} p_x^{2n_x} p_z^{2n_z} (2p_x p_z)^{m-n_x-n_z} . \tag{5.83}$$

Combining (5.80) and (5.83) yields

$$P_\Theta(\perp) = 1 - \sum_{n_x=n}^{m-k} \sum_{n_z=k}^{m-n_x} \binom{m}{n_x}\binom{m-n_x}{n_z} p_x^{2n_x} p_z^{2n_z} (2p_x p_z)^{m-n_x-n_z} . \tag{5.84}$$

This completes the proof. □

5.8 Formal security proof of raw key distribution protocols

In section 5.4, we have seen that iterative sifting leads to problems, which we call non-uniform sampling and basis information leak. In section 5.5, we have seen that these two problems allow attack strategies for Eve which induce a surprisingly low error rate. However, we have not formally understood yet why these two problems lead to a false estimation of the min-entropy $H^\varepsilon_{\min}(X|E)$.

In this section, we are going to show how the min-entropy estimate of a raw key distribution protocol can be proved formally. The strategy is as follows. First, we take LCA sifting and SBPE as an example to discuss our formal setup in which we will prove the min-entropy bound. Then we generalize the situation by considering *any* sifting protocol that satisfies two conditions. These conditions take the form of equalities (see equalities (5.99) and (5.100) below). They correspond precisely to the requirement that a sifting protocol must not exhibit non-uniform sampling or a basis information leak. (Hence, they are violated by iterative sifting but not by LCA sifting.) We show that any sifting protocol with these two properties, together with SBPE, leads to a correct bound on the min-entropy. This way, we can see at what point iterative sifting breaks the security proof by observing where the two conditions are used in the proof. At the same time, this proves the security of LCA sifting and SBPE as a raw key distribution protocol.

Let us consider the raw key distribution protocol composed of LCA sifting and SBPE. The diagram in figure 5.7 helps at understanding the following discussion. After the sifting protocol, Alice and Bob share a system in the state $\rho_{ST\Theta}$, where S and T denote Alice's and Bob's outcome string, respectively, and Θ is the (publicly known) string of sifted basis choices. It is of the form

$$\rho_{ST\Theta} = \left(\sum_{s,t,\vartheta\in\{0,1\}^l_k} P_{ST\Theta}(s,t,\vartheta)\ |s\rangle\langle s| \otimes |t\rangle\langle t| \otimes |\vartheta\rangle\langle\vartheta| \right) + \left(P_\Theta(\perp)|\perp\rangle\langle\perp|^{\otimes 3} \right) \tag{5.85}$$

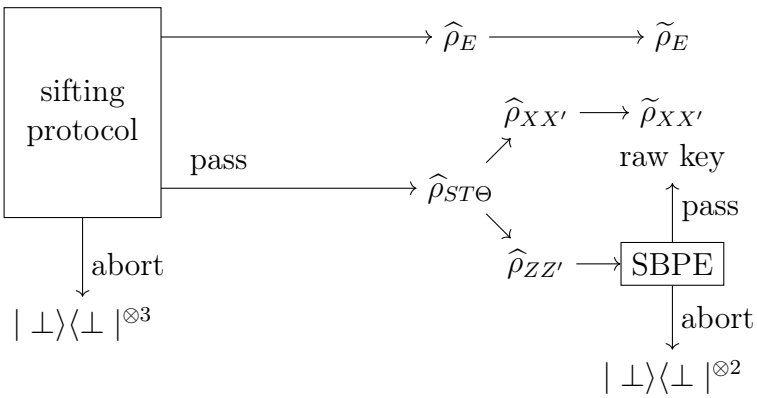


Figure 5.7: Diagram of a raw key distribution protocol. The protocol is composed of a sifting protocol (such as LCA sifting) and the single-basis parameter estimation protocol (SBPE). After sifting, they share a state $\widehat{\rho}_{ST\Theta}$ with the sifted measurement outcomes S and T and the sifted basis choice string Θ. For SBPE, Alice and Bob use the information in Θ to separate the outcomes X and X' in the $\mathbb{X}$-basis and the outcomes Z and Z' in the $\mathbb{Z}$-basis, and use Z and Z' for parameter estimation.

If Alice and Bob do not pass the quota test, i.e. if they do not have enough basis agreements, they abort the protocol and output the state $|\perp\rangle\langle\perp|^{\otimes 3}$ (see step 3' of protocol 5.3 on page 87). If Alice and Bob pass the quota test, they share the state

$$\widehat{\rho}_{ST\Theta} = \frac{\Pi_{\text{sift}}\rho_{ST\Theta}\Pi_{\text{sift}}}{\text{tr}(\Pi_{\text{sift}}\rho_{ST\Theta})}\,, \tag{5.86}$$

where

$$\Pi_{\text{sift}} = \mathbb{1}_A \otimes \mathbb{1}_B \otimes (\mathbb{1}_\Theta - |\perp\rangle\langle\perp|)\,. \tag{5.87}$$

We can rewrite this state as

$$\widehat{\rho}_{ST\Theta} = \sum_{s,t,\vartheta\in\{0,1\}_k^l} \widehat{P}_{ST\Theta}(s,t,\vartheta)|s\rangle\langle s| \otimes |t\rangle\langle t| \otimes |\vartheta\rangle\langle\vartheta|\,, \tag{5.88}$$

where

$$\widehat{P}_{ST\Theta}(s,t,\vartheta) = \frac{P_{ST\Theta}(s,t,\vartheta)}{1-P_\Theta(\perp)} \quad \forall\, s,t,\vartheta \in \{0,1\}_k^l\,. \tag{5.89}$$

Note that in particular,

$$\widehat{P}_\Theta(\vartheta) = \binom{l}{k}^{-1} \quad \forall\, \vartheta \in \{0,1\}_k^l\,. \tag{5.90}$$

In the next step, Alice and Bob use the information of the string Θ in order to split their outcome strings into strings of measurement outcomes in the $\mathbb{X}$-basis (which we denote by X and X') and strings of measurement outcomes in the $\mathbb{Z}$-basis (which we denote by Z and Z'). We can express this as

$$\sum_{\vartheta\in\{0,1\}_k^l} \Pi_\vartheta^\dagger\, \widehat{\rho}_{ST\Theta}\, \Pi_\vartheta \quad = \quad \widehat{\rho}_{ZZ'XX'}\,, \tag{5.91}$$

where Π_ϑ permutes the l bits of both Alice and Bob such that the first k bits are measured in $\mathbb{Z}$ and the last n bits are measured in $\mathbb{X}$, but otherwise unchanged in order. Then they use Z and Z' for SBPE. If they do not pass the correlation test (see step 2 of protocol 5.2), Alice and Bob abort the protocol and output $X = X' = \perp$. If they pass the correlation test, they end up with the raw keys X and X' in the state

$$\widetilde{\rho}_{XX'} = \frac{\Pi_{\mathrm{PE}}^\dagger \, \widehat{\rho}_{ZZ'XX'} \, \Pi_{\mathrm{PE}}}{\mathrm{tr}(\Pi_{\mathrm{PE}}^\dagger \, \widehat{\rho}_{ZZ'XX'} \, \Pi_{\mathrm{PE}})} \tag{5.92}$$

where

$$\Pi_{\mathrm{PE}}^\dagger = \left(\sum_{\frac{1}{k}\sum_{i=1}^k z_i \oplus z_i' \leq q_{\mathrm{tol}}} |z\rangle\langle z| \otimes |z'\rangle\langle z'| \right) \otimes \mathbb{1}_{XX'} \,. \tag{5.93}$$

This is the state for which we want to prove the min-entropy bound.

5.8.1 Construction of an equivalent protocol

Now we are going to modify the protocol to obtain an equivalent but easier-to-analyze protocol. Note that for each round r of the loop phase, the measurement performed in that round r commutes with all other actions performed in the protocol, except that the preparation and the channel use needs to precede the measurement. This means that the sifting protocol could be changed as follows: instead of measuring one qubit in each round of the loop phase, Alice and Bob store the qubits during the loop phase, implementing the identity channel on them. In this modified sifting protocol, Alice and Bob still make basis choices, compare them and discard rounds—they just do not actually perform the measurements. The output of this modified sifting protocol is a state $\rho_{AB\Theta}$, where A and B are l-qubit registers holding the stored qubits of Alice and Bob, respectively. This state is classical on Θ, that is, it is of the form

$$\rho_{AB\Theta} = \sum_\vartheta P_\Theta(\vartheta) \; \rho_{AB}^\vartheta \otimes |\vartheta\rangle\langle\vartheta| \,. \tag{5.94}$$

Again, we distinguish the case where Alice and Bob abort the sifting protocol, in which case they output the state $|\perp\rangle\langle\perp|^{\otimes 3}$, and the case where they pass the quota test, in which case they get the state conditioned on $\Theta \neq \perp$, given by

$$\widehat{\rho}_{AB\Theta} = \frac{\Pi_{\mathrm{sift}} \rho_{AB\Theta} \Pi_{\mathrm{sift}}}{\mathrm{tr}(\Pi_{\mathrm{sift}} \rho_{AB\Theta})} \,. \tag{5.95}$$

In the modified protocol, if the quota test is passed, then, *after* the sifting protocol, they measure all of the qubits at once with respect to Θ, just before the SBPE protocol is executed (see the lower part of figure 5.8). This produces a classical state

$$\widehat{\rho}_{ST\Theta} = \sum_{s,t,\vartheta} \widehat{P}_{ST\Theta}(s,t,\vartheta) \; |s\rangle\langle s| \otimes |t\rangle\langle t| \otimes |\vartheta\rangle\langle\vartheta| \tag{5.96}$$

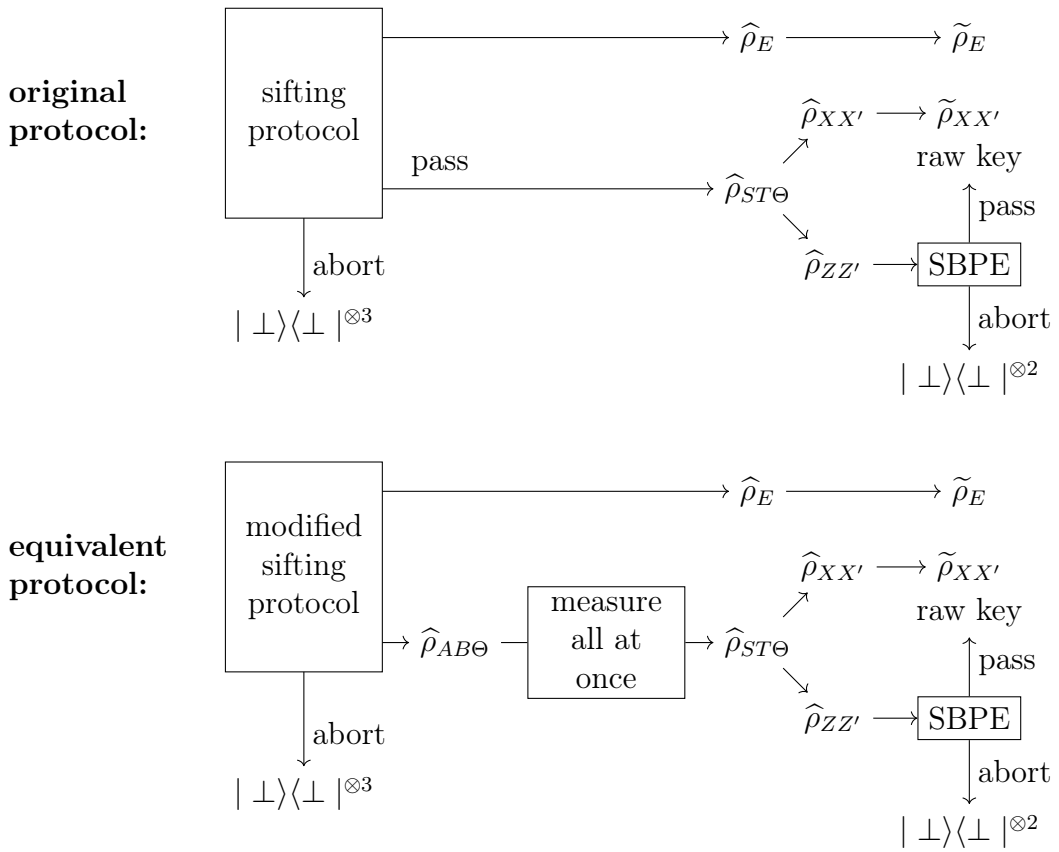


Figure 5.8: Construction of an equivalent protocol. For the security proof, we consider a modified but equivalent protocol. There, Alice and Bob choose and communicate bases and perform sifting, but they do not measure the qubits. Instead, they store them in quantum registers A and B. In a subsequent step, the qubits in A and B are measured all at once according to the bases given by Θ. Since these measurements commute with the other operations of the sifting protocol, the output state $\widehat{\rho}_{ST\Theta}$ is identical to the one in the original protocol. The rest of the protocol is identical to the original protocol.

with the probabilities

$$\widehat{P}_{ST\Theta}(s,t,\vartheta) = \mathrm{tr}(\Pi(s,t,\vartheta)\widehat{\rho}_{AB\Theta})\,, \tag{5.97}$$

where

$$\Pi(s,t,\vartheta) = \left(\bigotimes_{i=1}^{l} \mathbb{X}_{s_i}^{1-\vartheta_i}\mathbb{Z}_{s_i}^{\vartheta_i}\right) \otimes \left(\bigotimes_{i=1}^{l} \mathbb{X}_{t_i}^{1-\vartheta_i}\mathbb{Z}_{t_i}^{\vartheta_i}\right) \otimes \left(\bigotimes_{i=1}^{l} |\vartheta_i\rangle\langle\vartheta_i|\right)\,. \tag{5.98}$$

The rest of the modified protocol is identical to the original protocol (see figure 5.8).

Because of the commutation property explained above, the state $\widehat{\rho}_{ST\Theta}$ produced in this protocol, equation (5.96), is the same as the one produced in the original protocol, equations (5.86) and (5.88). Thus, the raw key output $\rho_{XX'}$ would be the same as in the original protocol, equation (5.92). This means that instead of analyzing $H_{\min}^{\varepsilon}(X|E)$ for LCA sifting with SBPE, we

can analyze it for this equivalent protocol. An experimental implementation of this equivalent protocol would be difficult, as reliable quantum storage is not available yet, but since this is only a theoretical construct, we shall not worry about that.

The modification that we have just considered can be made for any sifting protocol: one just skips all measurements and performs them all at once after the sifting protocol. This way, we can say that for every sifting protocol, there is a state $\rho_{AB\Theta}$ associated with the sifting protocol as in equation (5.94). In this picture, we can formally say what it means for a sifting protocol to sample uniformly and to have no basis information leak. In terms of the state $\rho_{AB\Theta}$, the conditions read:

$$P_\Theta(\vartheta) = P_\Theta(\vartheta') \quad \text{for all } \vartheta, \vartheta' \in \{0,1\}_k^l \quad \text{and} \tag{5.99}$$

$$\rho_{AB\Theta} = \rho_{AB} \otimes \rho_\Theta \,. \tag{5.100}$$

Condition (5.99) expresses uniform sampling, and it is exactly the same as condition (5.46) that we worked with before. The only difference is that now, we formulated it in terms of the state $\rho_{AB\Theta}$ associated with the sifting protocol. Condition (5.100) expresses the absence of a basis information leak. Formally, it says that the public basis information register Θ is uncorrelated with the quantum information that Alice and Bob hold, and it is equivalent to (c.f. equation (5.94) above)

$$\rho_{AB}^{\vartheta} = \rho_{AB}^{\vartheta'} \quad \forall\, \vartheta, \vartheta' \in \Omega_\Theta \,. \tag{5.101}$$

The independence of non-uniform sampling and basis information leak becomes obvious through the two conditions, as it is easy to see that one can find states for protocols such that one but not the other condition is satisfied.

We have seen in section 5.4.1 that iterative sifting violates condition (5.99). Moreover, from our discussion in section 5.4.2, we can see why iterative sifting violates condition (5.100). In round r of the loop phase, Eve knows the basis choices of the rounds $1, \ldots, r-1$. Therefore, she can modify the state that Bob receives in round r depending on the basis choices of those previous rounds (this is what happens in the attack described in section 5.5.1). Thus, in iterative sifting, the registers Θ and B are correlated, in general. For LCA sifting, we have proved condition (5.99) in section 5.7, and (5.100) follows trivially from the fact that Alice and Bob never communicate information about Θ as long as Eve can influence the quantum information sent through the channel.

For a protocol whose associated state $\rho_{AB\Theta}$ satisfies the two conditions (5.99) and (5.100) above, the state $\widehat{\rho}_{AB\Theta}$ conditioned on $\Theta \neq \perp$ is given by

$$\widehat{\rho}_{AB\Theta} = \rho_{AB} \otimes \left(\sum_{\vartheta \in \{0,1\}_k^l} \widehat{P}_\Theta(\vartheta)\, |\vartheta\rangle\langle\vartheta| \right) , \tag{5.102}$$

where $\widehat{P}_\Theta$ is the uniform distribution as in the original protocol,

$$\widehat{P}_\Theta(\vartheta) = \binom{l}{k}^{-1} \quad \forall\, \vartheta \in \{0,1\}_k^l \,. \tag{5.103}$$

5.8.2 The min-entropy bound and a Gedankenexperiment

Below, we are going to prove the following proposition.

Proposition 5.4 : *Consider a sifting protocol such that its associated state $\rho_{AB\Theta}$ satisfies the two conditions (5.99) and (5.100). If the protocol is followed by SBPE, then the state $\widetilde{\rho}_{XX'}$ conditioned on passing the quota test and the correlation test (see figure 5.8) satisfies*

$$H_{\min}^{\varepsilon'}(X|E) \geq n(q - h(q_{tol} + \mu(\varepsilon)))\,. \tag{5.104}$$

Here, E denotes Eve's information (the channel purification system), p_{pass}^{PE} is the probability that the correlation test passes, q is the preparation quality between the $\mathbb{X}$- and the $\mathbb{Z}$-basis (see equation (3.96) on page 45) and

$$\varepsilon' = \frac{\varepsilon}{\sqrt{p_{pass}^{PE}}}\,, \quad \mu(\varepsilon) = \sqrt{\frac{l}{nk}\frac{k+1}{k}\ln\frac{1}{\varepsilon}}\,. \tag{5.105}$$

The idea that leads to the proof of proposition 5.4 is to consider a *Gedankenexperiment*. It is shown as a diagram in figure 5.9. In this Gedankenexperiment, the measurement bases are not chosen according to Θ. Instead, *all* qubits are measured in the $\mathbb{Z}$-basis. We denote the resulting l-bit strings of $\mathbb{Z}$-measurement outcomes by Alice and Bob by bold letters $\mathbf{Z}$ and $\mathbf{Z}'$, respectively. The rest of the protocol is the same: the strings $\mathbf{Z}$ and $\mathbf{Z}'$ are split up according to Θ. This time, this yields strings Z and Z' on the one side as before, but on the other side, instead of getting strings X and X', they get strings $\overline{Z}$ and $\overline{Z}'$ of measurement outcomes in $\mathbb{Z}$. Conditioned on passing the correlation test of the SBPE, they get a "raw key" state $\widetilde{\rho}_{\overline{Z}\overline{Z}'}$.

The idea behind the proof of (5.4) is the following. When Alice and Bob pass the correlation test of the SBPE, then they know that they have a high correlation between the test bits. In the Gedankenexperiment, this means that they also know that the $\mathbb{Z}$-measurement outcomes of the key bits are likely to be correlated. This is because all bits are measurement outcomes in the same basis, and the test bits have been chosen at random according to Θ. (Below, we will make this mathematically precise.) A high correlation between $\mathbf{Z}$ and $\mathbf{Z}'$ means that the max-entropy $H_{\max}^{\varepsilon}(\overline{Z}|\overline{Z}')$ is low. This allows us to use the uncertainty relation for the smooth min- and max-entropy that we encountered in chapter 3 to connect the Gedankenexperiment to the protocol that we are actually analyzing. The uncertainty relation (corollary 3.32) reads

$$H_{\min}^{\varepsilon}(X|E) \geq nq - H_{\max}^{\varepsilon}(\overline{Z}|\overline{Z}')\,, \tag{5.106}$$

where q is the preparation quality between the bases $\mathbb{X}$ and $\mathbb{Z}$. Hence, if the max-entropy is low, then the min-entropy is high, which is what we want to prove.

Now we formalize the Gedankenexperiment. To this end, we consider the probability space $(\Omega_{\mathbf{ZZ}'\Theta}, P_{\mathbf{ZZ}'\Theta})$ of the outcomes of the $\mathbb{Z}$-measurements, together with the basis choices. The sample space is given by

$$\Omega_{\mathbf{ZZ}'\Theta} = \{0,1\}^l \times \{0,1\}^l \times \{0,1\}_k^l\,, \tag{5.107}$$

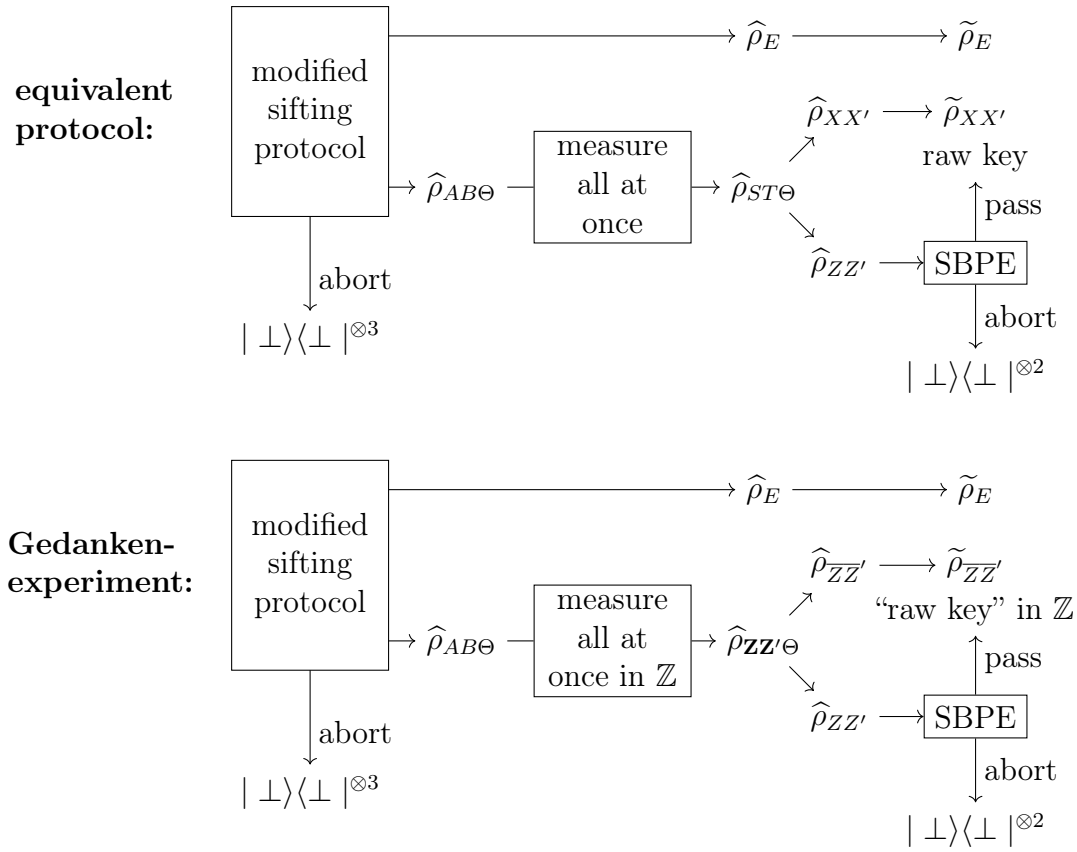


Figure 5.9: Diagram of the "Gedankenexperiment".

and the probability distribution $P_{\mathbf{ZZ}'\Theta}$ is given by

$$\begin{aligned} P_{\mathbf{ZZ}'\Theta}: \quad \Omega_{\mathbf{ZZ}'\Theta} &\to [0,1] \\ (\mathbf{z},\mathbf{z}',\vartheta) &\mapsto \mathrm{tr}(\Pi_G(\mathbf{z},\mathbf{z}',\vartheta)\widehat{\rho}_{AB\Theta}) \end{aligned} \tag{5.108}$$

with

$$\Pi_G(\mathbf{z},\mathbf{z}',\vartheta) = \left(\bigotimes_{i=1}^{l} \mathbb{Z}_{\mathbf{z}_i}\right) \otimes \left(\bigotimes_{i=1}^{l} \mathbb{Z}_{\mathbf{z}'_i}\right) \otimes \left(\bigotimes_{i=1}^{l} |\vartheta_i\rangle\langle\vartheta_i|\right) . \tag{5.109}$$

Note that we consider the case where the quota test is passed, so we consider the state $\widehat{\rho}_{\mathbf{ZZ}'\Theta}$ in equation (5.108). Nonetheless, we omit the hat in the classical probability space notation here, although we are in the case conditioned on passing the quota test.

We first introduce the random variable E_{key}, the number of errors on the key bits. Since the key bits are those bits where $\Theta_i = 0$, it is given by

$$\begin{aligned} E_{\text{key}}: \quad \Omega_{\mathbf{ZZ}'\Theta} &\to \{0,n\} \\ (\mathbf{z},\mathbf{z}',\vartheta) &\mapsto \sum_{i=1}^{N}(1-\vartheta_i)(\mathbf{z}\oplus\mathbf{z}') . \end{aligned} \tag{5.110}$$

The total number of errors is given by the random variable

$$\begin{aligned} E_{\text{tot}}: \quad \Omega_{\mathbf{ZZ}'\Theta} &\to \{0,l\} \\ (\mathbf{z},\mathbf{z}',\vartheta) &\mapsto \sum_{i=1}^{l}(\mathbf{z}\oplus\mathbf{z}') . \end{aligned} \tag{5.111}$$

Finally, the number of errors on the test bits is the random variable

$$E_{\text{test}} : \Omega_{\mathbf{ZZ}'\Theta} \to \{0, n\}\,, \tag{5.112}$$

given by

$$E_{\text{test}} = E_{\text{tot}} - E_{\text{key}}\,. \tag{5.113}$$

To get the error *rates* (rather than the number of errors), we divide by the number of bits and get the random variables

$$\Lambda_{\text{key}} = \frac{1}{n} E_{\text{key}}\,, \qquad \Lambda_{\text{test}} = \frac{1}{k} E_{\text{test}}\,, \qquad \Lambda_{\text{tot}} = \frac{1}{l} E_{\text{tot}}\,. \tag{5.114}$$

5.8.3 The proof

The proof of proposition 5.4 goes in two steps:

(1) First, we make the *tail probability estimate*. This means to prove the following: in the picture of the Gedankenexperiment, if Alice and Bob pass the quota test (which means $\Lambda_{\text{test}} \leq q_{\text{tol}}$), then the likelihood that the key bit error rate exceeds the test bit error rate by more than some number $\mu > 0$,

$$p_{\text{tail}}(\mu) := P[\Lambda_{\text{key}} \geq \Lambda_{\text{test}} + \mu \mid \Lambda_{\text{test}} \leq q_{\text{tol}}]\,. \tag{5.115}$$

is exponentially bounded. We will prove this in lemmata 5.5 to 5.7 below.

(2) Given the tail probability estimate, we derive an upper bound on the max-entropy $H^{\varepsilon}_{\max}(\overline{Z}|\overline{Z}')$. Together with inequality (5.106), which connects the Gedankenexperiment with the protocol that we actually analyze, the result follows.

To tackle the first step, let us start with some considerations. In the Gedankenexperiment, we can say that after the sifting protocol, the total number of errors, E_{tot}, is already fixed. They just do not know the number. Instead, when they perform the correlation test in the SBPE, they draw some of the bits at random without replacement, and see how many errors they have drawn. Eventually, we will be interested in bounding the quantity (5.115), but for now, let us consider the probability distribution $P_{E_{\text{key}}|E_{\text{tot}}}$, i.e. the probability that the key bits (which are also drawn at random from the total number of bits) have a certain number of errors, given that the total number of errors is fixed. If the sifting protocol really samples uniformly, then this is simply a situation of random sampling without replacement, where the characteristic of interest is binary (errors are already there, 1, or absent, 0). This gives rise to the *hypergeometric distribution*, as the following lemma shows.

Lemma 5.5 : *Let $\widehat{\rho}_{AB\Theta}$ be a state satisfying conditions (5.102) and (5.103). Then the conditional distribution $P_{E_{\text{key}}|E_{\text{tot}}}$ is a hypergeometric distribution, that is,*

$$P_{E_{\text{key}}|E_{\text{tot}}}(j|t) = \binom{l}{n}^{-1} \binom{t}{j} \binom{l-t}{n-j}\,, \tag{5.116}$$

where the random variables E_{key} and E_{tot} are as defined in equations (5.107) to (5.113).

Proof. By the definition of a conditional probability distribution (definition 2.11), we have that

$$P_{E_{\text{key}}|E_{\text{tot}}}(j|t) = \frac{P_{E_{\text{key}}E_{\text{tot}}}(j,t)}{P_{E_{\text{tot}}}(t)} \,. \tag{5.117}$$

The denominator is, by the definition of the distribution of a random variable (see definition 2.3), given by

$$P_{E_{\text{tot}}}(t) = \sum_{(z,z',\vartheta)\in E_{\text{tot}}^{-1}(t)} P_{ZZ'\Theta}(z,z',\vartheta) \,, \tag{5.118}$$

where

$$E_{\text{tot}}^{-1}(t) = \underbrace{\left\{ (z,z') \in \{0,1\}^l \times \{0,1\}^l \,\middle|\, \sum_{i=1}^{l} z_i \oplus z_i' = t \right\}}_{\Gamma_t} \times \{0,1\}_k^l \,. \tag{5.119}$$

Using equations (5.102) and (5.103), expression (5.118) reduces to

$$P_{E_{\text{tot}}}(t) = \binom{l}{k}^{-1} \sum_{(z,z')\in\Gamma_t} \sum_{\vartheta\in\{0,1\}_k^l} P_{ZZ'}(z,z') \tag{5.120}$$

$$= \binom{l}{k}^{-1} \binom{l}{k} \sum_{(z,z')\in\Gamma_t} P_{ZZ'}(z,z') \tag{5.121}$$

$$= \sum_{(z,z')\in\Gamma_t} P_{ZZ'}(z,z') \,. \tag{5.122}$$

For the numerator, we have

$$P_{E_{\text{key}}E_{\text{tot}}}(j,t) = \sum_{(z,z',\vartheta)\in E_{\text{key}}^{-1}(j)\cap E_{\text{tot}}^{-1}(t)} P_{ZZ'\Theta}(z,z',\vartheta) \tag{5.123}$$

$$= \sum_{(z,z',\vartheta)\in E_{\text{key}}^{-1}(j)\cap E_{\text{tot}}^{-1}(t)} \binom{l}{k}^{-1} P_{ZZ'}(z,z') \,, \tag{5.124}$$

where

$$E_{\text{key}}^{-1}(j) \cap E_{\text{tot}}^{-1}(t) = \biguplus_{(z,z')\in\Gamma_t} \{(z,z)\} \times \underbrace{\left\{ \vartheta \in \{0,1\}_k^l \,\middle|\, \sum_{i=1}^{l} (1-\vartheta_i)(z_i \oplus z_i') = j \right\}}_{\Gamma_j(z,z')} \,. \tag{5.125}$$

This gives us

$$P_{E_{\text{key}}E_{\text{tot}}}(j,t) = \binom{l}{k}^{-1} \sum_{(z,z')\in\Gamma_t} \sum_{\vartheta\in\Gamma_j(z,z')} P_{ZZ'}(z,z') \,. \tag{5.126}$$

Since $P_{ZZ'}(z, z')$ is independent of ϑ, we obtain

$$P_{E_{\text{key}}E_{\text{tot}}}(j, t) = \sum_{(z,z')\in\Gamma_t} |\Gamma_j(z, z')| P_{ZZ'}(z, z') \,. \tag{5.127}$$

A closer inspection of $\Gamma_j(z, z')$ and a simple combinatorial argument reveal that

$$|\Gamma_j(z, z')| = \binom{t}{j}\binom{l-t}{n-j} \quad \forall (z, z') \in \Gamma_t \,, \tag{5.128}$$

and thus

$$P_{E_{\text{key}}E_{\text{tot}}}(j, t) = \binom{l}{k}^{-1}\binom{t}{j}\binom{l-t}{n-j} \sum_{(z,z')\in\Gamma_t} P_{ZZ'}(z, z') \,. \tag{5.129}$$

Combining equations (5.117), (5.118) and (5.129) yields

$$P_{E_{\text{key}}|E_{\text{tot}}}(j|t) = \binom{l}{k}^{-1}\binom{t}{j}\binom{l-t}{n-j} \,. \tag{5.130}$$

Since $l = n + k$, it holds that

$$\binom{l}{k} = \binom{l}{n} \,. \tag{5.131}$$

Inserting equation (5.131) into (5.130) yields the claim. □

In the proof that we have just seen, it becomes apparent where iterative sifting fails in the security analysis: for the derivation of equation (5.118), we needed that the sifting protocol samples uniformly and has no basis information leak.

Lemma 5.5 shows that we are in the hypergeometric special case. This is an important special case which is, until today, a topic of intense research. An important result is *Serfling's bound*. For the hypergeometric case, it reads as follows.

Lemma 5.6 (Serfling's bound for the hypergeometric special case): *Let E_{key} and E_{tot} be random variables such that $P_{E_{\text{key}}|E_{\text{tot}}}$ is a hypergeometric distribution as in equation (5.116). Then, for the random variables Λ_{key} and Λ_{tot} as defined in equation (5.114) and for any $\nu > 0$, it holds that*

$$P\left[\sqrt{n}(\Lambda_{\text{key}} - \Lambda_{\text{tot}}) \geq \nu\right] \leq \exp\left(-2\nu^2 \frac{1}{1 - \frac{n-1}{l}}\right) \,. \tag{5.132}$$

A more general form of the bound was proved by Serfling [Ser74], and we will not repeat the proof here. The particular special case that we consider, inequality (5.132) corresponds exactly to inequality (1.3) in [GW15]. The last reference also discusses conjectured improvements of the bound.

Lemma 5.7 (Tail probability estimate): *For a state $\widehat{\rho}_{AB\Theta}$ satisfying conditions (5.102) and (5.103), it holds that*

$$p_{\text{tail}}(\mu) \leq \frac{\varepsilon^2}{p_{pass}^{PE}}\,, \tag{5.133}$$

where $p_{\text{tail}}(\mu)$ is defined in (5.115) and where

$$\varepsilon = \exp\left(-\frac{k^2 n}{l(k+1)}\mu^2\right)\,, \quad p_{pass}^{PE} = P[\Lambda_{\text{test}} \leq q_{tol}]\,. \tag{5.134}$$

Proof. According to lemmata 5.5 and 5.6, inequality (5.132) holds for all $\nu > 0$. The event on the left hand side of the inequality can be rewritten as follows:

$$\begin{aligned}
\sqrt{n}(\Lambda_{\text{key}} - \Lambda_{\text{tot}}) \geq \nu \iff & \frac{1}{n}E_{\text{key}} - \frac{1}{l}E_{\text{tot}} \geq \frac{\nu}{\sqrt{n}} && (5.135)\\
\iff & \frac{1}{n}E_{\text{key}} - \frac{1}{l}(E_{\text{test}} + E_{\text{key}}) \geq \frac{\nu}{\sqrt{n}} && (5.136)\\
\iff & \frac{l-n}{nl}E_{\text{key}} \geq \frac{1}{l}E_{\text{test}} + \frac{\nu}{\sqrt{n}} && (5.137)\\
\iff & \frac{1}{n}E_{\text{key}} \geq \frac{1}{k}E_{\text{test}} + \frac{l}{k\sqrt{n}}\nu && (5.138)\\
\iff & \Lambda_{\text{key}} \geq \Lambda_{\text{test}} + \frac{l}{k\sqrt{n}}\nu\,. && (5.139)
\end{aligned}$$

Inserting (5.139) in (5.132) and applying the variable transformation

$$\mu := \frac{l}{k\sqrt{n}}\nu\,, \quad \text{so that} \quad \nu = \frac{k\sqrt{n}}{l}\mu\,, \tag{5.140}$$

we find that for every $\mu > 0$,

$$\begin{aligned}
P\left[\Lambda_{\text{key}} \geq \Lambda_{\text{test}} + \mu\right] &\leq \exp\left(-2\left(\frac{k\sqrt{n}}{l}\mu\right)^2 \frac{1}{\frac{l-n+1}{l}}\right) && (5.141)\\
&= \exp\left(-2\frac{k^2 n}{l(k+1)}\mu^2\right) && (5.142)
\end{aligned}$$

Let us now get back to our original quantity of interest, $p_{\text{tail}}(\mu)$, as in equation (5.115). According to Bayes' theorem (see theorem 2.13), it holds that

$$\begin{aligned}
p_{\text{tail}}(\mu) &= P\left[\Lambda_{\text{key}} \geq \Lambda_{\text{test}} + \mu \middle| \Lambda_{\text{test}} \leq q_{\text{tol}}\right] && (5.143)\\
&= \frac{P[\Lambda_{\text{test}} \leq q_{\text{tol}} | \Lambda_{\text{key}} \geq \Lambda_{\text{test}} + \mu] P[\Lambda_{\text{key}} \geq \Lambda_{\text{test}} + \mu]}{P[\Lambda_{\text{test}} \leq q_{\text{tol}}]} && (5.144)\\
&\leq \frac{P[\Lambda_{\text{key}} \geq \Lambda_{\text{test}} + \mu]}{P[\Lambda_{\text{test}} \leq q_{\text{tol}}]}\,. && (5.145)
\end{aligned}$$

Combining inequalities (5.142) and (5.145) and using the abbreviation of equation (5.134), the claim follows. □

Now that we made the tail probability estimate, we are ready for the second step of the proof, namely bounding $H_{\max}^{\varepsilon}(\overline{Z}|\overline{Z}')$.

Lemma 5.8 : *Consider a sifting protocol such that in the Gedankenexperiment, the state $\widehat{\rho}_{AB\Theta}$ satisfies properties (5.102) and (5.103). If the protocol is followed by SBPE, then for any $\varepsilon > 0$, the resulting state $\widetilde{\rho}_{\overline{ZZ}'}$, which is conditioned on passing the correlation test, satisfies*

$$H^{\varepsilon'}_{\max}(\overline{Z}|\overline{Z}') \leq nh(q_{tol} + \mu)\,, \tag{5.146}$$

where

$$\varepsilon' = \frac{\varepsilon}{\sqrt{p^{PE}_{pass}}}\,, \quad \mu(\varepsilon) = \sqrt{\frac{l}{nk}\frac{k+1}{k}\ln\frac{1}{\varepsilon}}\,. \tag{5.147}$$

Proof. The proof that we present here is inspired by the proof in [Tom+12], but more direct and elementary.

The state $\widetilde{\rho}_{\overline{ZZ}'}$ is a classical state, i.e. it is of the form

$$\widetilde{\rho}_{\overline{ZZ}'} = \sum_{\overline{z},\overline{z}'} P_{\overline{ZZ}'|\Lambda_{\text{test}}\leq q_{\text{tol}}}(\overline{z},\overline{z}')\ |\overline{z}\rangle\langle\overline{z}| \otimes |\overline{z}'\rangle\langle\overline{z}'|\,. \tag{5.148}$$

Here, the probability distribution is conditioned on $\Lambda_{\text{test}} \leq q_{\text{tol}}$ because the state $\widetilde{\rho}_{\overline{ZZ}'}$ is conditioned on passing the correlation test. For inequality (5.146), it is sufficient to show that there is a state $\sigma_{\overline{ZZ}'}$ in the ε'-ball of $\widetilde{\rho}_{\overline{ZZ}'}$ such that

$$H_{\max}(\overline{Z}|\overline{Z}')_\sigma \leq nh(q_{\text{tol}} + \mu)\,. \tag{5.149}$$

We will choose a state $\sigma_{\overline{ZZ}'}$ which is diagonal in the same basis,

$$\sigma_{\overline{ZZ}'} = \sum_{\overline{z},\overline{z}'} Q_{\overline{ZZ}'}(\overline{z},\overline{z}')\ |\overline{z}\rangle\langle\overline{z}| \otimes |\overline{z}'\rangle\langle\overline{z}'| \tag{5.150}$$

for some probability distribution $Q_{\overline{ZZ}'}$ which is ε'-close to $P_{\overline{ZZ}'|\Lambda_{\text{test}}\leq q_{\text{tol}}}$. We want to choose a probability distribution for which

$$\Lambda_{\text{key}} \leq q_{\text{tol}} + \mu \tag{5.151}$$

holds with certainty. Note that in terms of the random variables $\overline{Z}$ and $\overline{Z}'$, Λ_{key} is given by

$$\Lambda_{\text{key}} = \frac{1}{n}\sum_{i=1}^{n} \overline{Z}_i \oplus \overline{Z}'_i\,. \tag{5.152}$$

According to lemma 5.7, we have that

$$P[\Lambda_{\text{key}} \leq q_{\text{tol}} + \mu \mid \Lambda_{\text{test}} \leq q_{\text{tol}}] = \sum_{(\overline{z},\overline{z}')\in\Lambda_{\text{key}}\leq q_{\text{tol}}+\mu} P_{\overline{ZZ}'|\Lambda_{\text{test}}\leq q_{\text{tol}}}(\overline{z},\overline{z}') < (\varepsilon')^2\,. \tag{5.153}$$

We construct $Q_{\overline{ZZ}'}$ by setting $Q_{\overline{ZZ}'}(\overline{z},\overline{z}') = 0$ for all $(\overline{z},\overline{z}') \in \Lambda_{\text{key}} \leq q_{\text{tol}} + \mu$ and by using the original distribution $P_{\overline{ZZ}'|\Lambda_{\text{test}}\leq q_{\text{tol}}}$, rescaled to a normalized probability distribution (see figure 5.10). More formally,

$$Q_{\overline{ZZ}'}(\overline{z},\overline{z}') = \begin{cases} 0 & \text{if } (\overline{z},\overline{z}') \in \Lambda_{\text{key}} \leq q_{\text{tol}} + \mu\,, \\ \dfrac{P_{\overline{ZZ}'|\Lambda_{\text{test}}\leq q_{\text{tol}}}(\overline{z},\overline{z}')}{1-(\varepsilon')^2} & \text{if } (\overline{z},\overline{z}') \notin \Lambda_{\text{key}} \leq q_{\text{tol}} + \mu\,. \end{cases} \tag{5.154}$$

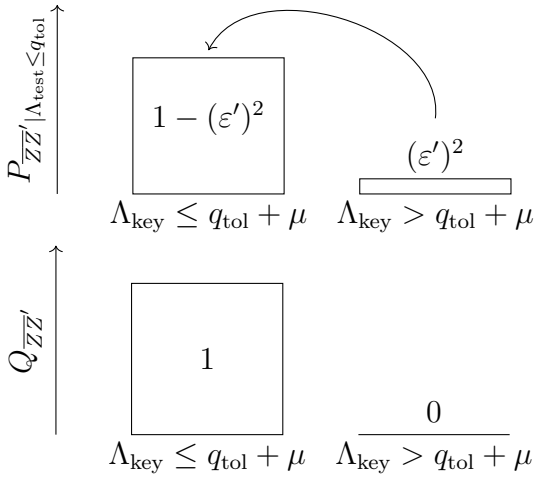


Figure 5.10: Construction of $Q_{\overline{ZZ}'}$.

This leads to a purified distance of (c.f. equation (3.64) in chapter 3)

$$P(P_{\overline{ZZ}'|\Lambda_{\text{test}}\leq q_{\text{tol}}}, Q_{\overline{Z},\overline{Z}'}) = \sqrt{1-\left(\sum_{\overline{z},\overline{z}'}\sqrt{P_{\overline{ZZ}'|\Lambda_{\text{test}}\leq q_{\text{tol}}}(\overline{z},\overline{z}')Q_{\overline{ZZ}'}(\overline{z},\overline{z}')}\right)^2} \tag{5.155}$$

$$= \sqrt{1-\left(\sum_{(\overline{z},\overline{z}')\notin\Lambda_{\text{key}}\leq q_{\text{tol}}+\mu}\frac{P_{\overline{ZZ}'|\Lambda_{\text{test}}\leq q_{\text{tol}}}(\overline{z},\overline{z}')}{\sqrt{1-(\varepsilon')^2}}\right)^2} \tag{5.156}$$

$$= \sqrt{1-(1-(\varepsilon')^2)} \tag{5.157}$$

$$= \varepsilon' . \tag{5.158}$$

Hence, $\sigma_{\overline{ZZ}'}$ lies in the ε'-ball around $\widetilde{\rho}_{\overline{ZZ}'}$ and thus,

$$H^{\varepsilon'}_{\max}(\overline{Z}|\overline{Z}')_{\widetilde{\rho}} \leq H_{\max}(\overline{Z}|\overline{Z}')_{\sigma} . \tag{5.159}$$

For the distribution $Q_{\overline{ZZ}'}$, it holds that $\Lambda_{\text{key}} \leq q_{\text{tol}}+\mu$ with certainty. According to equation (5.152), this means that the number of errors between $\overline{z}$ and $\overline{z}'$ is bounded, i.e.

$$Q_{\overline{ZZ}'}(\overline{z},\overline{z}') = 0 \quad \text{for all } (\overline{z},\overline{z}') \text{ with } \quad \sum_{i=1}^{n}\overline{z}_i \oplus \overline{z}'_i > \lfloor n(q_{\text{tol}}+\mu)\rfloor . \tag{5.160}$$

This is very useful for the calculation of $H_{\max}(\overline{Z}|\overline{Z}')$. To see why, let us express $H_{\max}(\overline{Z}|\overline{Z}')_{\sigma}$ in terms of the diagonal distribution $Q_{\overline{ZZ}'}$. We have seen in equation (3.88) in chapter 3 that this reads

$$H_{\max}(\overline{Z}|\overline{Z}')_{\sigma} = \log\sum_{\overline{z}'}Q_{\overline{Z}'}(\overline{z}')2^{H_{\max}(\overline{Z})_{Q^{\overline{z}'}}} , \tag{5.161}$$

where

$$H_{\max}(\overline{Z})_{Q^{\overline{z}'}} = 2\log \sum_{\overline{z}} \sqrt{Q_{\overline{Z}|\overline{Z}'=\overline{z}'}(\overline{z})}\,. \tag{5.162}$$

Hence,

$$H_{\max}(\overline{Z}|\overline{Z}')_\sigma = \log \sum_{\overline{z}'} Q_{\overline{Z}'}(\overline{z}') \left(\sum_{\overline{z}} \sqrt{Q_{\overline{Z}|\overline{Z}'=\overline{z}'}(\overline{z})} \right)^2 . \tag{5.163}$$

The square on the right hand side of this equality is the (1/2)-norm of the probability vector of $\overline{Z}$ conditioned on $\overline{Z}' = \overline{z}'$. Since the two-norm is bounded by the one-norm, we get

$$H_{\max}(\overline{Z}|\overline{Z}')_\sigma \leq \log \sum_{\overline{z}'} Q_{\overline{Z}'}(\overline{z}') \sum_{\overline{z}} Q_{\overline{Z}|\overline{Z}'=\overline{z}'}(\overline{z})\,. \tag{5.164}$$

Since the number of errors is bounded (equation (5.160)), the probability $Q_{\overline{Z}|\overline{Z}'=\overline{z}'}(\overline{z})$ in inequality (5.164) vanishes for every $\overline{z}$ that disagrees with $\overline{z}'$ in more than $\lfloor n(q_{\text{tol}} + \mu)\rfloor$ positions. Therefore, the sum can be restricted to those $\overline{z}$ which have at most $\lfloor n(q_{\text{tol}} + \mu)\rfloor$ disagreements with $\overline{z}'$, i.e.

$$H_{\max}(\overline{Z}|\overline{Z}')_\sigma \leq \log \sum_{\overline{z}'} Q_{\overline{Z}'}(\overline{z}') \sum_{\overline{z}\in S_{\overline{z}'}} Q_{\overline{Z}|\overline{Z}'=\overline{z}'}(\overline{z})\,, \tag{5.165}$$

where

$$S_{\overline{z}'} = \{\overline{z} \mid \textstyle\sum_i \overline{z}_i \oplus \overline{z}'_i \leq \lfloor n(q_{\text{tol}} + \mu)\rfloor\}\,. \tag{5.166}$$

For $\overline{z} \in S_{\overline{z}'}$, we can use the trivial bound

$$Q_{\overline{Z}|\overline{Z}'=\overline{z}'}(\overline{z}) \leq 1\,. \tag{5.167}$$

This gives us

$$H_{\max}(\overline{Z}|\overline{Z}')_\sigma \leq \log \sum_{\overline{z}'} Q_{\overline{Z}'}(\overline{z}')|S_{\overline{z}'}|\,. \tag{5.168}$$

Determining the size of $S_{\overline{z}'}$ is easy. For any fixed $\overline{z}'$, the number of strings $\overline{z}$ that disagree with $\overline{z}'$ in exactly e positions is given by $\binom{n}{e}$. Thus, for every $\overline{z}'$,

$$|S_{\overline{z}'}| = \sum_{e=0}^{\lfloor n(q_{\text{tol}}+\mu)\rfloor} \binom{n}{e} \tag{5.169}$$

and therefore

$$H_{\max}(\overline{Z}|\overline{Z}')_\sigma \leq \log \sum_{\overline{z}'} Q_{\overline{Z}'}(\overline{z}') \sum_{e=0}^{\lfloor n(q_{\text{tol}}+\mu)\rfloor} \binom{n}{e} \tag{5.170}$$

$$= \log \sum_{e=0}^{\lfloor n(q_{\text{tol}}+\mu)\rfloor} \binom{n}{e} \tag{5.171}$$

$$\leq nh(q_{\text{tol}} + \mu)\,, \tag{5.172}$$

where h denotes the binary entropy. The last inequality has been shown in [Lin99], section 1.4. Combining inequality (5.172) with inequality (5.159) completes the proof. □

Proposition 5.4 now follows as a corollary.

Proof of proposition 5.4. According to the uncertainty relation, it holds that

$$H_{\min}^{\varepsilon'}(X|E) \geq nq - H_{\max}^{\varepsilon'}(\overline{Z}|\overline{Z}')\,. \tag{5.173}$$

We have bounded the max-entropy in lemma 5.8, which gives us

$$\begin{aligned} H_{\min}^{\varepsilon'}(X|E) &\geq nq - nh(q_{\text{tol}} + \mu) && (5.174)\\ &= n(q - h(q_{\text{tol}} + \mu))\,. && (5.175) \end{aligned}$$

This completes the proof. □

Chapter 6

Privacy estimation of quantum information

6.1 Introduction

In this chapter, we will extend the ideas and concepts of the previous chapter and combine them with new ones. As a result, we will see a protocol which resembles quantum key distribution to some extent, but which allows to estimate an eavesdropper's uncertainty about *quantum* information rather than the uncertainty about a classical bit string (quantified by the min-entropy). As we have discussed in chapter 4, the min-entropy has many interesting characterizations, and thus, such a protocol is interesting for multiple reasons. For example, a simplified version of this protocol can be used for capacity tomography of quantum channels. We will discuss this in chapter 8. Further below in this chapter, we will see another motivation for the min-entropy estimation protocol in this chapter, namely its potential use in a protocol for entanglement distribution.

Devising protocols for the distribution of entanglement is not a new idea. In fact, some of the suggested schemes for QKD in the literature contain the distribution and distillation of entanglement as a subroutine [Deu+96]. For example, Lo and Chau presented a QKD protocol in which Alice and Bob first distribute and distill maximally entangled qubit pairs, before they extract the key by measuring the distilled pairs [LC99]. Lo and Chau's QKD protocol needs a fault-tolerant quantum computer on Alice's and Bob's side, but arguments by Shor and Preskill showed that the need for quantum computers can be eliminated to obtain a QKD protocol that works without distillation of entanglement [SP00]. Further arguments relate this protocol to quantum error correcting codes [Ben+96b; SP00] and to the BB84 protocol [BB84; NC00]. This proved the (asymptotic) security of the BB84 protocol against the most general attacks allowed by quantum theory, instead of attacks on individual qubits. Entanglement distillation protocols have also been considered outside of the QKD context, such as in work by Bennett et al. [Ben+96a; Ben+96a]; for an overview, see [DB07].

To see the connection of the results presented in this chapter with entanglement distribution, let us start with a high-level summary of what we have learned about raw key distribution, classical post-processing and quan-

tum state merging so far. In sections 4.2 and 4.3, we have seen that if two classical bit strings X and X' with an eavesdropper's quantum side information E are in a state $\rho_{XX'E}$ of high min-entropy $H_{\min}^{\varepsilon'}(X|E)$, then classical post-processing can transform them into smaller bit strings K and K' that are (almost certainly) identical, uniformly random and decoupled from the eavesdropper. In chapter 5, we studied raw key distribution protocols in detail. They are precisely designed to serve as an input source for classical post-processing protocols. For a class of raw key distribution protocols (which includes LCA sifting and SBPE), we proved that conditioned on passing the quota test and the correlation test, the bound

$$H_{\min}^{\varepsilon'}(X|E) \geq n(q - h(q_{\text{tol}} + \mu(\varepsilon)))\,, \tag{6.1}$$

holds, where μ and ε' are written out in equation (5.105) and where q_{tol} is a protocol parameter.

Somewhat analogously to QKD post-processing, we have seen in section 4.5 that if two quantum systems A and B with a purifying system E are in a state ρ_{ABE} of high min-entropy $H_{\min}^{\varepsilon'}(A|E)$, then there *exists* a protocol *for that state* which expands entanglement between Alice and Bob using the system AB as a resource.[1] We say that it *expands* entanglement because state merging, in general, needs some initial (pure) entanglement shared between Alice and Bob, which is then transformed to more entanglement in the case of states with a negative entanglement cost (see section 4.5). This is analogous to QKD, which requires Alice and Bob to have some initial shared key which they expand, in order to end up with a larger final key. Thus, in analogy to raw key distribution protocols as an input source for QKD post-processing protocols, it is an interesting question whether one can find a protocol that distributes quantum systems A and B of high min-entropy $H_{\min}^{\varepsilon'}(A|E)$ that could serve as a source for entanglement expansion protocols. We call such a protocol a *raw ebit distribution* (RED) protocol.

As the main result of this chapter, we will present such a protocol and prove a min-entropy bound for it. It distributes n-qubit systems A and B to Alice and Bob, respectively. As we will show in section 6.3, conditioned on passing the tests in the protocol, the state ρ_{ABE} of the protocol output satisfies

$$H_{\min}^{3\varepsilon+5\varepsilon'}(A|E)_\rho \geq n(q - 2h(q_{\text{tol}} + \mu)) - 2\log\frac{2}{\varepsilon^2}\,, \tag{6.2}$$

where the parameters in this inequality are analogous to the ones in the last chapter (we will see this in more detail in section 6.3). This can be seen as a fully quantum analogue of a raw key distribution protocol.

The proof of inequality (6.2) and the design of the protocol goes in two steps. In section 6.2 we show that for any state ρ_{ABE} of n-qubit systems A and B with quantum side information E, it holds that

$$H_{\min}^{3\varepsilon+5\varepsilon'}(A|E)_\rho \geq nq - (H_{\max}^{\varepsilon'}(X|B)_\rho + H_{\max}^{\varepsilon'}(Z|B)_\rho) - 2\log\frac{2}{\varepsilon^2}\,, \tag{6.3}$$

[1] However, remember from our discussion in section 4.5 that for practically applicable protocols, *universal* state merging protocols (or other universal protocols that can distill entanglement) are needed.

where X and Z arise from measuring the qubits in A in the $\mathbb{X}$- and $\mathbb{Z}$-basis, respectively (see proposition 6.6 below). This result reduces the estimation of an eavesdropper's uncertainty about quantum information A to the estimation of the uncertainty about classical bit strings. The two main tools used for proving inequality (6.3) are a *chain rule* theorem for the smooth min- and max-entropies proved by Vitanov et al. [Vit+13], and the *duality relation* between the smooth min- and the max-entropy, proved by Tomamichel et al. [TCR10].

In the second step, we construct a protocol that distributes n-qubit systems A and B to Alice and Bob, respectively, and prove that conditioned on passing the tests in the protocol, their state satisfies

$$H_{\max}^{\varepsilon'}(X|B) \leq nh(q_{\text{tol}} + \mu)\,, \tag{6.4}$$

$$H_{\max}^{\varepsilon'}(Z|B) \leq nh(q_{\text{tol}} + \mu)\,. \tag{6.5}$$

This looks very similar to what we have shown for raw key distribution protocols in chapter 5. Indeed, as we will see in sections 6.3 to 6.6, we can largely apply the same techniques that we used for raw key distribution protocols.

6.2 A privacy bound for qubits

Our goal in this section is to prove the validity of inequality (6.3). We will first cite a series of lemmas that we will need in section 6.2.1, before we carry out the proof in section 6.2.2.

6.2.1 A few lemmas

As mentioned above, the most important lemmas for the proof below are a chain rule theorem and the duality relation. The chain rule that we will use is actually just one out of a series of chain rule inequalities proved in [Vit+13]. The particular form that we use here can be found in [Tom12].

Lemma 6.1 (Chain rule for smooth max-entropy): *Let $\rho_{ABC} \in \mathcal{S}^{\leq}(\mathcal{H}_{ABC})$ be a tripartite state, let $\varepsilon > 0$, $\varepsilon' \geq 0$, $\varepsilon'' \geq 0$. Then*

$$H_{\max}^{\varepsilon+\varepsilon'+2\varepsilon''}(AB|C)_\rho \leq H_{\max}^{\varepsilon'}(A|BC)_\rho + H_{\max}^{\varepsilon''}(B|C)_\rho + \log\frac{2}{\varepsilon^2}\,. \tag{6.6}$$

The duality relation between the smooth min- and max-entropy, or *min-max duality*, for short, relates the smooth min-entropy of a state to the max-entropy of a purification of the state. It was first proved for the unsmoothed min- and max-entropy König, Renner and Schaffner in [KRS09]. The min-max duality for the smooth entropies is due to Tomamichel, Colbeck and Renner [TCR10].

Lemma 6.2 (Min-max duality): *Let $\rho_{ABE} \in \mathcal{S}(\mathcal{H}_{ABE})$ be a pure tripartite state, let $\varepsilon \geq 0$. Then*

$$H_{\min}(A|E)_\rho = -H_{\max}(A|B)_\rho \quad \text{and} \tag{6.7}$$

$$H_{\min}^{\varepsilon}(A|E)_\rho = -H_{\max}^{\varepsilon}(A|B)_\rho\,. \tag{6.8}$$

In section 3.4, we have seen that the min- and max-entropies are invariant under local unitaries. The following lemma generalizes this to the case of isometries [Tom12].

Lemma 6.3 (Invariance under isometries): *Let $\rho_{AB} \in \mathcal{S}^{\leq}(\mathcal{H}_{AB})$ be a bipartite state, let $\varepsilon \geq 0$. Then for all isometries $V : \mathcal{H}_A \to \mathcal{H}_{A'}$ and $W : \mathcal{H}_B \to \mathcal{H}_{B'}$, the embedded state $\sigma_{A'B'} = (V \otimes W)\rho_{AB}(V^\dagger \otimes W^\dagger)$ satisfies*

$$H^{\varepsilon}_{\min}(A|B)_\rho = H^{\varepsilon}_{\min}(A'|B')_\sigma \quad \text{and} \quad H^{\varepsilon}_{\max}(A|B)_\rho = H^{\varepsilon}_{\max}(A'|B')_\sigma \,. \tag{6.9}$$

In simple terms, the following lemma states that "forgetting" side information cannot decrease one's uncertainty. It is a special case of a more general theorem, called the *data processing inequality* [Tom12]. We only state the more special case that we are interested in.

Lemma 6.4 : *Let $\rho_{ABC} \in \mathcal{S}^{\leq}(\mathcal{H}_{ABC})$ be a tripartite state. Then*

$$H_{\max}(A|BC) \leq H_{\max}(A|B) \,. \tag{6.10}$$

Finally, the last lemma that we add to our list of tools shows how the (unsmoothed) max-entropy simplifies in the case where classical side information is given.

Lemma 6.5 : *Let $\rho_{ACX} \in \mathcal{S}^{\leq}(\mathcal{H}_{ACX})$ be a state of the form*

$$\rho_{ACX} = \sum_x p_x \; \rho^x_{AC} \otimes |x\rangle\langle x|_X \,, \quad \text{where} \quad \rho^x_{AC} \in \mathcal{S}^{\leq}(\mathcal{H}_{AC}) \,. \tag{6.11}$$

Then [Tom12]

$$H_{\max}(A|CX)_\rho = \log\left(\sum_x P_X(x)\; 2^{H_{\max}(A|C)_{\rho^x_{AC}}}\right) . \tag{6.12}$$

6.2.2 Formal statement and proof of the bound

Proposition 6.6 : *Let $\rho_{ABE} \in \mathcal{S}(\mathcal{H}_{ABE})$ be a pure tripartite state where A and B are each an n-qubit system, let $\mathbb{X} = \{\mathbb{X}_0, \mathbb{X}_1\}$ and $\mathbb{Z} = \{\mathbb{Z}_0, \mathbb{Z}_1\}$ be non-trivial projective measurements on a qubit (that is, both elements are one-dimensional projectors). Consider the states ρ_{XBE} and ρ_{ZBE} that arise from measuring all of the n qubits of system A with respect to $\mathbb{X}$ and $\mathbb{Z}$ and storing the outcomes in a classical register X and Z, respectively (c.f. section 3.1.3),*

$$\rho_{XBE} = \sum_{x\in\{0,1\}^n} P_X(x)\; |x\rangle\langle x| \otimes \rho^x_{BE} \,, \tag{6.13}$$

$$\rho_{ZBE} = \sum_{z\in\{0,1\}^n} P_Z(z)\; |z\rangle\langle z| \otimes \rho^z_{BE} \,. \tag{6.14}$$

Then, for $\varepsilon > 0$ and $\varepsilon' \geq 0$, it holds that

$$H^{3\varepsilon+5\varepsilon'}_{min}(A|E)_\rho \geq nq - (H^{\varepsilon'}_{\max}(X|B)_\rho + H^{\varepsilon'}_{\max}(Z|B)_\rho) - 2\log\frac{2}{\varepsilon^2} \,, \tag{6.15}$$

where q is the preparation quality as in theorem 3.30,

$$q = -\log \max_{i,j\in\{0,1\}} \left\| \sqrt{\mathbb{X}_i}\sqrt{\mathbb{Z}_j} \right\|_\infty^2 . \tag{6.16}$$

In this case (where the $\mathbb{X}_i$, $\mathbb{Z}_j$ are one-dimensional projectors),

$$q = -\log \max \left| \langle \psi_x^i | \psi_z^j \rangle \right| , \tag{6.17}$$

where ψ_x^i and ψ_z^j are eigenstates of $\mathbb{X}_i$ and $\mathbb{Z}_j$, respectively.

Proof. Starting from ρ_{ABE}, we construct a purification $\sigma_{AXX'BE}$ of ρ_{XBE}. Further below, we will expand the smooth max-entropy of this state using the chain rule (lemma 6.1). Reformulating the terms in that expansion will lead us to the desired result.

Consider the product POVM elements

$$\Pi_X(x) = \bigotimes_{i=1}^{n} \mathbb{X}_{x_i} \quad \text{for } x = (x_i)_{i=1}^n \in \{0,1\}^n . \tag{6.18}$$

We construct $\sigma_{AXX'BE}$ from ρ_{ABE} by performing a coherent measurement on the A system with respect to the POVM formed by the elements (6.18). The outcome of this measurement is stored in two copies X and X' of a classical register. For $x \in \{0,1\}^n$, let V_x be the map

$$\begin{array}{rccc} V_x : & \mathcal{H}_A & \to & \mathcal{H}_{AXX'} \\ & |\psi\rangle & \mapsto & \Pi_X(x)|\psi\rangle \otimes |x\rangle_X \otimes |x\rangle_{X'} . \end{array} \tag{6.19}$$

We define the state $\sigma_{AXX'BE} := V(\rho_{ABE})$, where

$$\begin{array}{rccc} V : & \mathrm{End}(\mathcal{H}_{ABE}) & \to & \mathrm{End}(\mathcal{H}_{AXX'BE}) \\ & \rho_{ABE} & \mapsto & \sum_x (V_x \otimes \mathbb{1}_{BE})\rho_{ABE}(V_x^\dagger \otimes \mathbb{1}_{BE}) . \end{array} \tag{6.20}$$

The map V is an isometry that maps the pure state ρ_{ABE} to the pure state $\sigma_{AXX'BE}$. Thus, by virtue of lemma 6.2, it holds that

$$H_{\min}^{\varepsilon'}(X|E)_\sigma = -H_{\max}^{\varepsilon'}(X|AX'B)_\sigma . \tag{6.21}$$

In addition, $\sigma_{AXX'BE}$ purifies ρ_{XBE}, i.e. $\mathrm{tr}_{AX'}(\sigma_{AXX'BE}) = \rho_{XBE}$ and thus (note the subscripts)

$$H_{\min}^{\varepsilon'}(X|E)_\sigma = H_{\min}^{\varepsilon'}(X|E)_\rho . \tag{6.22}$$

Combining equations equation (6.21) and equation (6.22) gives us

$$H_{\min}^{\varepsilon'}(X|E)_\rho = -H_{\max}^{\varepsilon'}(X|AX'B)_\sigma . \tag{6.23}$$

We will use equation (6.23) further below.

Now we expand the max-entropy of $\sigma_{AXX'BE}$ using the chain rule, lemma 6.1:

$$H_{\max}^{\varepsilon+\varepsilon'+2(\varepsilon+2\varepsilon')}(AXX'|B)_\sigma \leq H_{\max}^{\varepsilon'}(X|AX'B)_\sigma + H_{\max}^{\varepsilon+2\varepsilon'}(AX'|B)_\sigma + \log\frac{2}{\varepsilon^2} . \tag{6.24}$$

The states ρ_{AB} and $\sigma_{AXX'B}$ only differ by an isometry, so by lemma 6.3, we have

$$H_{\max}^{\varepsilon+\varepsilon'+2(\varepsilon+2\varepsilon')}(AXX'|B)_\sigma = H_{\max}^{3\varepsilon+5\varepsilon'}(A|B)_\rho\,. \tag{6.25}$$

(It will become clear further below why we choose the smoothing parameter on the left hand side this way.) Moreover, the marginals $\sigma_{AX'B}$ and σ_{AXB} only differ by a unitary $\mathcal{H}_X \to \mathcal{H}_{X'}$ and therefore

$$H_{\max}^{\varepsilon+2\varepsilon'}(AX'|B)_\sigma = H_{\max}^{\varepsilon+2\varepsilon'}(AX|B)_\sigma \tag{6.26}$$

Combining equations (6.24) to (6.26) yields

$$H_{\max}^{\varepsilon'}(X|AX'B)_\sigma \geq H_{\max}^{3\varepsilon+5\varepsilon'}(A|B)_\rho - H_{\max}^{\varepsilon+2\varepsilon'}(AX|B)_\sigma - \log\frac{2}{\varepsilon^2}\,. \tag{6.27}$$

Now we expand the term $H_{\max}^{\varepsilon+2\varepsilon'}(AX|B)$ using the chain rule:

$$H_{\max}^{\varepsilon+2\varepsilon'}(AX|B)_\sigma \leq \underbrace{H_{\max}^{0}(A|XB)_\sigma}_{H_{\max}(A|XB)_\sigma} + H_{\max}^{\varepsilon'}(X|B)_\sigma + \log\frac{2}{\varepsilon^2} \tag{6.28}$$

$$= H_{\max}(A|XB)_\sigma + H_{\max}^{\varepsilon'}(X|B)_\rho + \log\frac{2}{\varepsilon^2}\,, \tag{6.29}$$

where the equality follows from the fact that $\sigma_{AXX'BE}$ purifies ρ_{ABE}. Combining (6.27) with (6.29) allows us to infer

$$H_{\max}^{\varepsilon'}(X|AX'B)_\sigma \geq H_{\max}^{3\varepsilon+5\varepsilon'}(A|B)_\rho - H_{\max}(A|XB)_\sigma - H_{\max}^{\varepsilon'}(X|B)_\rho - 2\log\frac{2}{\varepsilon^2}\,. \tag{6.30}$$

Now we use equation (6.23) that we derived above to rewrite inequality (6.30) as

$$H_{\min}^{\varepsilon'}(X|E)_\rho \leq -H_{\max}^{3\varepsilon+5\varepsilon'}(A|B)_\rho + H_{\max}(A|XB)_\sigma + H_{\max}^{\varepsilon'}(X|B)_\rho + 2\log\frac{2}{\varepsilon^2}\,. \tag{6.31}$$

Reordering terms and using lemma 6.4 and the uncertainty relation for the smooth min- and max-entropy (theorem 3.30), we get

$$H_{\max}^{3\varepsilon+5\varepsilon'}(A|B)_\rho \leq \underbrace{H_{\max}(A|XB)_\sigma}_{\leq H_{\max}(A|X)_\sigma} + H_{\max}^{\varepsilon'}(X|B)_\rho \underbrace{- H_{\min}^{\varepsilon'}(X|E)_\rho}_{\leq H_{\max}^{\varepsilon'}(Z|B)_\rho - nq} + 2\log\frac{2}{\varepsilon^2} \tag{6.32}$$

$$\leq H_{\max}(A|X)_\sigma + H_{\max}^{\varepsilon'}(X|B)_\rho + H_{\max}^{\varepsilon'}(Z|B)_\rho - nq + 2\log\frac{2}{\varepsilon^2}\,, \tag{6.33}$$

where q is as in (6.16). Applying the duality relation (lemma 6.2) to the left hand side of equation (6.33), we get

$$H_{\min}^{3\varepsilon+5\varepsilon'}(A|E)_\rho \geq nq - H_{\max}(A|X)_\sigma - \left(H_{\max}^{\varepsilon'}(X|B)_\rho + H_{\max}^{\varepsilon'}(Z|B)_\rho\right) + 2\log\frac{2}{\varepsilon^2}\,. \tag{6.34}$$

We are left to show that $H_{\max}(A|X)_\sigma$ is upper bounded by 0. We show, more precisely, that $H_{\max}(A|X)_\sigma = 0$. This goes as follows.

$$\begin{aligned}
\sigma_{AX} &= \mathrm{tr}_{X'BE}(\sigma_{AXX'BE}) && (6.35)\\
&= \mathrm{tr}_{X'BE}\left(\sum_x (V_x \otimes \mathbb{1}_{BE})\rho_{ABE}(V_x^\dagger \otimes \mathbb{1}_{BE})\right) && (6.36)\\
&= \mathrm{tr}_{X'}\left(\sum_x V_x \rho_A V_x^\dagger\right) && (6.37)\\
&= \sum_x \Pi_X(x)\rho_A \Pi_X(x) \otimes |x\rangle\langle x|_X && (6.38)\\
&= \sum_x P_X(x)\ \rho_A^x \otimes |x\rangle\langle x|_X\,, && (6.39)
\end{aligned}$$

where

$$\begin{aligned}
P_X(x) &= \mathrm{tr}(\Pi_X(x)\rho_A)\,, && (6.40)\\
\rho_A^x &= \frac{\Pi_X(x)\rho_A\Pi_X(x)}{P_X(x)}\,. && (6.41)
\end{aligned}$$

Now we can apply lemma 6.5 to equation (6.39): By setting the system C in the lemma to a trivial system ($\mathcal{H}_C \simeq \mathbb{C}$), we can deduce that

$$H_{\max}(A|X)_\sigma = \log\left(\sum_x P_X(x)\ 2^{H_{\max}(A)_{\rho_A^x}}\right)\,, \tag{6.42}$$

where $H_{\max}(A)_{\rho_A^x}$ reduces to the unconditional form of the max-entropy,

$$H_{\max}(A)_{\rho_A^x} = \log\left\|\sqrt{\rho_A^x}\right\|_1^2 = \log\left(\mathrm{tr}\left(\sqrt{\rho_A^x}\right)\right)^2\,. \tag{6.43}$$

Since the $\Pi_X(x)$ are one-dimensional projectors, we have that

$$H_{\max}(A)_{\rho_A^x} = 0 \quad \text{for all } x \in \{0,1\}^n \tag{6.44}$$

and therefore $H_{\max}(A|X)_\sigma = 0$, as claimed. Thus, we have proved that

$$H_{\min}^{3\varepsilon+5\varepsilon'}(A|E)_\rho \geq nq - \left(H_{\max}^{\varepsilon'}(X|B)_\rho + H_{\max}^{\varepsilon'}(Z|B)_\rho\right) - 2\log\frac{2}{\varepsilon^2}\,, \tag{6.45}$$

which is what we wanted to show. □

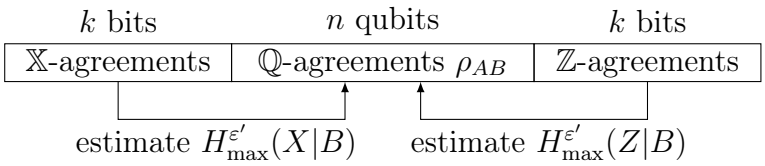
6.3 A raw ebit distribution protocol

In the last section, we have seen that the estimation of the smooth min-entropy $H_{\min}^{3\varepsilon+5\varepsilon'}(A|E)$ of a state ρ_{ABE} of n-qubit systems A and B can be reduced to the estimation of $H_{\max}^{\varepsilon'}(X|B)$ and $H_{\max}^{\varepsilon'}(Z|B)$, where X and Z are measurement results on A. This is very promising, because we have learned in chapter 5 how to estimate such quantities. Using ideas that we developed there, we will now construct a protocol that distributes qubits for which these two max-entropies

are upper-bounded. Recall that we call such a protocol a raw ebit distribution (RED) protocol. Just like a raw key distribution protocol, the protocol consists of a sifting part and a parameter estimation part. We will first give a rough overview and then explain the RED sifting protocol and the RED parameter estimation protocol in detail.

The idea is to modify a raw key distribution protocol (like LCA sifting and SBPE) in the following way. In the loop phase of the sifting protocol, Alice and Bob not only measure some of the qubits in $\mathbb{X}$ and $\mathbb{Z}$, but they also store some of the qubits without measuring them. After the loop phase, they determine their $\mathbb{X}$-, $\mathbb{Z}$- and $\mathbb{Q}$-agreements, where a $\mathbb{Q}$-agreement is a round in which both of them did not measure their qubit and stored it instead. The stored qubits form n-qubit systems A and B in a joint state ρ_{AB}, while the outcome bit strings in the $\mathbb{X}$- and $\mathbb{Z}$-basis are each k bits long. In the parameter estimation protocol, Alice and Bob communicate their measurement outcomes for the $\mathbb{X}$-agreements and $\mathbb{Z}$-agreements, and determine the error rate for the two blocks separately. This allows them to estimate both $H_{\max}^{\varepsilon'}(X|B)$ and $H_{\max}^{\varepsilon'}(Z|B)$ of the state ρ_{AB}: the error rate on the $\mathbb{X}$-agreements is used to bound $H_{\max}^{\varepsilon'}(X|B)$, and the error rate on the $\mathbb{Z}$-agreements is used to bound $H_{\max}^{\varepsilon'}(Z|B)$, as illustrated in the following diagram:

$$l := 2k + n$$



(6.46)

The proof that the two max-entropies of the protocol output are bounded is analogous to the proof for raw key distribution protocols that we saw in chapter 5. We will again consider the completely unmeasured state $\rho_{\mathbf{AB}\Theta}$ that arises in an equivalent protocol where all measurements are postponed. (In this chapter, we denote the hypothetical unmeasured l-qubit systems by bold letters $\mathbf{A}$ and $\mathbf{B}$ to distinguish them from the unmeasured n-qubit systems A and B of the actual protocol output.) Here, Θ is a bit string of length $l = 2k + n$, containing entries 0, 1 and 2, standing for an $\mathbb{X}$-, $\mathbb{Z}$- and $\mathbb{Q}$-agreement in the corresponding round. We will show the uniform sampling property and the absence of a basis information leak,

$$P_\Theta(\vartheta) = P_\Theta(\vartheta') \quad \forall\, \vartheta, \vartheta' \in \{0,1,2\}^l_{k,k}\,, \tag{6.47}$$

$$\rho_{\mathbf{AB}\Theta} = \rho_{\mathbf{AB}} \otimes \rho_\Theta\,, \tag{6.48}$$

where

$$\{0,1,2\}^l_{k,k} := \{\vartheta \in \{0,1,2\}^l \mid \vartheta \text{ contains exactly } k \text{ zeros and } k \text{ ones}\}\,. \tag{6.49}$$

The proof of uniform sampling will be analogous to the proof for LCA sifting: we will construct a probability space model for the sifting protocol and use similar arguments as in the proof of proposition 5.3. Just as for LCA sifting, equation (6.48) is trivial since the protocol has no classical communication during the quantum communication phase.

The validity of equations equations (6.47) and (6.48) implies all that we need. In particular, as we will illustrate in section 6.6, the analogous equations hold for the reduced systems where the $\mathbb{X}$-agreements or the $\mathbb{Z}$-agreements are discarded. Thus, if the error rate on the remaining system is low enough, the corresponding max-entropy bound is implied by what we have shown in section 5.8. Thus, the only actual proof that we need to carry out in is the proof of (6.47). We will prove it in section 6.5.

6.3.1 RED sifting

The sifting protocol, which we call RED sifting, is largely analogous to LCA sifting. We have written it out in detail below (see protocol 6.1). It also consist of a loop phase and a final phase. As in LCA sifting, the loop phase consists of m rounds in which Alice prepares two-qubit system in a maximally entangled state and sends one half to Bob. The main difference is that instead of measuring in either the $\mathbb{X}$-basis or in the $\mathbb{Z}$-basis, Alice and Bob measure in the $\mathbb{X}$-basis, in the $\mathbb{Z}$-basis, or they simply store the unmeasured qubit. The probabilities for measuring in the $\mathbb{X}$- or the $\mathbb{Z}$-basis are identical,

$$p_x = p_z =: p \in [0, 1/2]\,, \tag{6.50}$$

and the probability for storing the qubit is given by

$$\overline{p} := 1 - 2p\,. \tag{6.51}$$

In the first step of the final phase of RED sifting, Alice and Bob communicate over an authenticated channel to find out in which round the other party has measured the qubit in $\mathbb{X}$, in $\mathbb{Z}$ or not at all. Below, we will prove the uniform sampling property of RED sifting, analogously to chapter 5. To this end, it is again convenient to formulate the protocol in terms of a comparison string $C = C_1 \dots C_m$ that Alice and Bob determine. This time, the comparison string needs to distinguish between a few more cases. As before, we write $C_r = x$ if Alice and Bob had an $\mathbb{X}$-agreement in round r and $C_r = z$ if they had a $\mathbb{X}$-agreement. If they both did not measure their qubit, we say that they had a $\mathbb{Q}$-agreement, and write $C_r = \emptyset$. In contrast to LCA sifting, we need to distinguish between two different kinds of disagreements, because they do not have the same probability. The first kind of disagreement is the case where one party measures in $\mathbb{X}$ and the other party measures in $\mathbb{Z}$. In this case, which occurs with probability $2p^2$, we write $C_r = d$. The other kind of disagreement is the case where one party measures the qubit (in $\mathbb{X}$ or $\mathbb{Z}$), and the other party does not measure but store the qubit. In this case, which occurs with probability $4p\overline{p}$, we write $C_r = e$. Formally, we can summarize this as

$$C_r := \begin{cases} x & \text{if } A_r = B_r = 0\,, \\ z & \text{if } A_r = B_r = 1\,, \\ \emptyset & \text{if } A_r = B_r = 2\,, \\ d & \text{if } (A_r = 0 \text{ and } B_r = 1) \text{ or } (A_r = 1 \text{ and } B_r = 0)\,, \\ e & \text{if } (A_r \in \{0,1\} \text{ and } B_r = 2) \text{ or } (A_r = 2 \text{ and } B_r \in \{0,1\})\,. \end{cases} \tag{6.53}$$

RED Sifting

Parameters:
- $n, k, m \in \mathbb{N}_+$ with $m \geq n + 2k$ (define $l := n + 2k$),
- $p \in [0, 1/2]$ (define $\overline{p} := 1 - 2p$)

Outputs:
- Alice: l-bit string $(S_i)_{i=1}^l \in \{0,1\}^l$, n-qubit system A,
- Bob: l-bit string $(T_i)_{i=1}^l \in \{0,1\}^l$, n-qubit system B,
- public: l-bit string $(\Theta_i)_{i=1}^l \in \{0,1,2\}_{k,k}^l$

The protocol

Loop phase: Steps 1 and 2 are repeated m times (round index $r = 1, \ldots, m$). In round r, Alice and Bob do the following:

Step 1: Alice prepares a qubit pair in a maximally entangled state and sends one half to Bob.

Step 2: Alice and Bob independently choose $A_r, B_r \in \{0,1,2\}$ with probability p, p and $\overline{p}$, respectively, where 0 stands for the $\mathbb{X}$-basis, 1 stands for the $\mathbb{Z}$-basis and 2 stands for no measurement at all. Then they (do not) measure their part of the qubit pair according to A_r, B_r and store the outcome $Y_r, Y_r' \in \{0,1\}$, respectively (they store 0 in the case of no measurement).

Final phase: The following steps are performed in a single run:

Step 3: Alice and Bob communicate their choices A_r and B_r for $r \in [m]$ over a public authenticated channel and determine the comparison string C as defined in equation equation (6.53). They check whether quota condition ($|\mathcal{X}(C)| \geq k$ and $|\mathcal{Z}(C)| \geq k$ and $|\mathcal{Q}(C)| \geq n$) holds, where $\mathcal{X}(C)$, $\mathcal{Z}(C)$ and $\mathcal{Q}(C)$ count the occurrences of x, z and $\emptyset$ in C, respectively (see equations (6.54) to (6.56)). If it holds, they proceed with Step 4'. Otherwise, they abort and output $S = T = \Theta = \perp$ (abort flag).

Step 4: Alice and Bob choose subsets

$$U \in \binom{\mathcal{X}(C)}{k}, \quad V \in \binom{\mathcal{Z}(C)}{k}, \quad W \in \binom{\mathcal{Q}(C)}{n}, \tag{6.52}$$

at random and discard the unmeasured qubits of rounds r with $r \notin W$.

Step 5: Let R_i be the i-th element of $U \cup V \cup W$. Then Alice determines $(S_i)_{i=1}^l \in \{0,1\}^l$, Bob determines $(T_i)_{i=1}^l \in \{0,1\}^l$ and together they determine $(\Theta_i)_{i=1}^l \in \{0,1\}_k^l$, where for every $i \in [l]$,

$$S_i = Y_{R_i}\,, \quad T_i = Y'_{R_i}\,, \quad \Theta_i = A_{R_i}\,(= B_{R_i})\,.$$

The n non-discarded qubits form system A and B, respectively.

Step 6: Alice locally outputs $(S_i)_{i=1}^l$, Bob locally outputs $(T_i)_{i=1}^l$, and they publicly output $(\Theta_i)_{i=1}^l$.

Protocol 6.1: The RED sifting protocol.

Then they check in which rounds they had $\mathbb{X}$-, $\mathbb{Z}$- and $\mathbb{Q}$-agreements in order to check the quota condition. In analogy to LCA sifting, we write this formally as

$$\mathcal{X}(C) := \{r \in [m] \mid C_r = x\}\,, \tag{6.54}$$
$$\mathcal{Z}(C) := \{r \in [m] \mid C_r = z\}\,. \tag{6.55}$$
$$\mathcal{Q}(C) := \{r \in [m] \mid C_r = \emptyset\}\,. \tag{6.56}$$

We choose identical quota for the $\mathbb{X}$- and $\mathbb{Z}$-agreements and set it as a protocol parameter k. The quota for the $\mathbb{Q}$-agreements is denoted by n. Hence, the quota condition reads

$$|\mathcal{X}(C)| \geq k \text{ and } |\mathcal{Z}(C)| \geq k \text{ and } |\mathcal{Q}(C)| \geq n\,. \tag{6.57}$$

If the quota condition is met, they continue with the next step; otherwise they abort.

In the next step, Alice and Bob choose a random subset U of size k from their $\mathbb{X}$-agreements, a random subset V of size k from their $\mathbb{Z}$-agreements and a random subset W of of size n their $\mathbb{Q}$-agreements. Just like in the LCA sifting protocol, the outcome strings and the basis choice string is then constructed from this choice: the bits that have not been chosen are discarded, and the rest is left in order. This produces the output strings S, T and Θ.

6.3.2 RED parameter estimation

The parameter estimation protocol is very simple. It is written out in protocol 6.2. It can be thought of as the joint execution of two SBPE correlation tests, where the correlation test of RED PE is only passed if both the SBPE correlation tests are passed. One of the SBPE correlation tests is carried out on the sifted $\mathbb{X}$-agreements, and the other one is carried out on the sifted $\mathbb{Z}$-agreements. For both correlation tests, we choose the same tolerated error rate $q_{\text{tol}} \in [0, 1]$.

6.4 A probability space model for RED sifting

In this section, we develop a probability space model for RED sifting, in analogy to the probability space model that we developed for LCA sifting in section 5.6.1. This means that we construct a probability space (Ω, P), where the elements of Ω represent "histories" of the protocol, and a random variable

$$\Theta : \Omega \to \Omega_\Theta = \{\perp\} \cup \{0, 1, 2\}^l_{k,k} \tag{6.58}$$

that maps a history ω to the output basis choice string Θ for that history.

Again, we partition the set Ω of histories into two subsets $\Omega^\perp$ and $\Omega^\checkmark$, corresponding to those histories that do not pass the quota test and those histories that do pass the correlation test, respectively,

$$\Omega = \Omega^\perp \uplus \Omega^\checkmark\,. \tag{6.59}$$

RED Parameter Estimation

Parameters: $n, k \in \mathbb{N}$, $q_{\text{tol}} \in [0,1]$.

Inputs:
- Alice: l-bit string $S = (S_i)_{i=1}^l \in \{0,1\}^l$, n-qubit system A,
- Bob: l-bit string $T = (T_i)_{i=1}^l \in \{0,1\}^l$, n-qubit system B,
- public: l-bit string $\Theta = (\Theta_i)_{i=1}^l \in \{0,1,2\}_{k,k}^l$

Outputs:
- Alice: n-qubit system A,
- Bob: n-qubit system B.

The protocol

Step 1: Alice and Bob communicate their test bits, i.e. the bits S_i and T_i with i for which $\Theta_i \in \{0,1\}$, over a public authenticated channel.

Step 2: Alice and Bob determine the error rates

$$\Lambda_{\text{test}}^x := \frac{1}{k} \sum_{i\in[l]:\Theta_i=0} S_i \oplus T_i\,, \quad \Lambda_{\text{test}}^z := \frac{1}{k} \sum_{i\in[l]:\Theta_i=1} S_i \oplus T_i\,,$$

and perform the *correlation test*: if ($\Lambda_{\text{test}}^x \leq q_{\text{tol}}$ and $\Lambda_{\text{test}}^z \leq q_{\text{tol}}$), they continue the protocol and move on to Step 3. Otherwise, they abort and output an abort flag $\perp$.

Step 3: Alice outputs the n-qubit system A, Bob outputs the n-qubit system B.

Protocol 6.2: The RED parameter estimation protocol.

When Alice and Bob abort (that is, they do not meet the quota condition (6.57)), a comparison string C is generated, but no subsets U, V and W are chosen. The set of all comparison strings not meeting the quota condition is given by

$$\Omega^{\perp} = \{c \in \{x, z, \emptyset, d, e\}^m \mid |\mathcal{X}(c)| < k \text{ or } |\mathcal{Z}(c)| < k \text{ or } |\mathcal{Q}(c)| < n\}\,. \tag{6.60}$$

In the case where they pass the quota test, Alice and Bob choose subsets U, V and W, so the partition $\Omega^{\checkmark}$ consists of quadruples (c, u, v, w). In analogy to (5.48), we have that

$$\Omega^{\checkmark} = \left\{ (c,u,v,w) \in \{x,z,\emptyset,d,e\}^m \times \binom{[m]}{k} \times \binom{[m]}{k} \times \binom{[m]}{n} \,\middle|\, \begin{array}{l} u \subseteq \mathcal{X}(c), \\ v \subseteq \mathcal{Z}(c), \\ w \subseteq \mathcal{Q}(c) \end{array} \right\}. \tag{6.61}$$

Again, we further partition these sets into subsets of constant probability. Note that the probability of a comparison string c depends on the number of occurrences of x, z, $\emptyset$, d and e. In addition to the counting functions $\mathcal{X}$, $\mathcal{Z}$

and $\mathcal{Q}$ in equations (6.54) to (6.56),

$$\mathcal{D}(C) := \{r \in [m] \mid C_r = d\}\,, \tag{6.62}$$
$$\mathcal{E}(C) := \{r \in [m] \mid C_r = e\}\,. \tag{6.63}$$

This way, we can write the probability of a comparison string c as

$$P(c) = (p^2)^{\mathcal{X}(c)}(p^2)^{\mathcal{Z}(c)}(\overline{p}^2)^{\mathcal{Q}(c)}(2p^2)^{\mathcal{D}(c)}(4p\overline{p})^{\mathcal{E}(c)}\,. \tag{6.64}$$

Note that the five counting functions are not independent: for every comparison string c, it holds that

$$\mathcal{X}(c) + \mathcal{Z}(c) + \mathcal{Q}(c) + \mathcal{D}(c) + \mathcal{E}(c) = m\,. \tag{6.65}$$

Thus, when we determine the subsets of $\Omega^{\perp}$ and $\Omega^{\checkmark}$ where these functions are constant, we only need to set four of them to a constant, and the remaining one is eliminated by equation (6.65). We choose to eliminate $\mathcal{D}$ and partition $\Omega^{\perp}$ and $\Omega^{\checkmark}$ as follows:

$$\Omega^{\perp} = \biguplus_{(n_x,n_z,n_\emptyset,n_e)\in\mathcal{N}^{\perp}} \Omega^{\perp}_{(n_x,n_z,n_\emptyset,n_e)}\,, \tag{6.66}$$
$$\Omega^{\checkmark} = \biguplus_{(n_x,n_z,n_\emptyset,n_e)\in\mathcal{N}^{\perp}} \Omega^{\checkmark}_{(n_x,n_z,n_\emptyset,n_e)}\,, \tag{6.67}$$

where

$$\Omega^{\perp}_{(n_x,n_z,n_\emptyset,n_e)} = \{c \in \Omega^{\perp} \mid |\mathcal{X}(c)| = n_x, \ldots, |\mathcal{E}(c)| = n_e\}\,, \tag{6.68}$$
$$\mathcal{N}^{\perp} = \left\{(n_x,n_z,n_\emptyset,n_e) \in \{0,\ldots,m\}^4 \;\middle|\; \begin{array}{l} n_x + n_z + n_\emptyset + n_e \leq m \text{ and} \\ (n_x < k \text{ or } n_z < k \text{ or } n_\emptyset < n) \end{array}\right\} \tag{6.69}$$
$$\Omega^{\checkmark}_{(n_x,n_z,n_\emptyset,n_e)} = \{(c,u,v,w) \in \Omega^{\perp} \mid |\mathcal{X}(c)| = n_x, \ldots, |\mathcal{E}(c)| = n_e\}\,, \tag{6.70}$$
$$\mathcal{N}^{\checkmark} = \left\{(n_x,n_z,n_\emptyset,n_e) \in \{0,\ldots,m\}^4 \;\middle|\; \begin{array}{l} n_x + n_z + n_\emptyset + n_e \leq m \text{ and} \\ n_x \geq k \text{ and } n_z \geq k \text{ and } n_\emptyset \geq n \end{array}\right\} \tag{6.71}$$

For $\omega \in \Omega^{\perp}_{(n_x,n_z,n_\emptyset,n_e)}$ for some $(n_x,n_z,n_\emptyset,n_e) \in \mathcal{N}^{\checkmark}$, it holds that

$$P(\omega) = (p^2)^{n_x}(p^2)^{n_z}(\overline{p}^2)^{n_\emptyset}(2p^2)^{m-n_x-n_z-n_\emptyset-n_e}(4p\overline{p})^{n_e} \tag{6.72}$$
$$= 2^{m-n_x-n_z-n_\emptyset+n_e}p^{2(m-n_\emptyset)-n_e}\overline{p}^{2n_\emptyset+n_e} \tag{6.73}$$
$$=: f(n_x,n_z,n_\emptyset,n_e)\,, \tag{6.74}$$

where f is just a notational abbreviation. For $\omega = (c,u,v,w) \in \Omega^{\checkmark}_{(n_x,n_z,n_\emptyset,n_e)}$, we need to incorporate the choice probabilities for U, V and W to get the correct probability,

$$P(\omega) = f(n_x,n_z,n_\emptyset,n_e)\binom{n_x}{k}^{-1}\binom{n_z}{k}^{-1}\binom{n_\emptyset}{n}^{-1}\,. \tag{6.75}$$

Thus, to summarize, we have

$$
\begin{aligned}
P: \quad \Omega &\to [0,1] \\
\omega &\mapsto \begin{cases} f(n_x, n_z, n_\emptyset, n_e) & \text{if } \omega \in \Omega^{\perp}_{(n_x,n_z,n_\emptyset,n_e)} \text{ for some } (n_x, n_z, n_\emptyset, n_e) \in \mathcal{N}^{\perp} \\ f(n_x, n_z, n_\emptyset, n_e)\binom{n_x}{k}^{-1}\binom{n_z}{k}^{-1}\binom{n_\emptyset}{n}^{-1} & \text{if } \omega \in \Omega^{\checkmark}_{(n_x,n_z,n_\emptyset,n_e)} \text{ for some } (n_x, n_z, n_\emptyset, n_e) \in \mathcal{N}^{\checkmark} \end{cases}
\end{aligned}
\tag{6.76}
$$

where

$$
f(n_x, n_z, n_\emptyset, n_e) := 2^{m-n_x-n_z-n_\emptyset+n_e} p^{2(m-n_\emptyset)-n_e} \overline{p}^{2n_\emptyset+n_e} \,. \tag{6.77}
$$

Now we are left to construct the random variable Θ. This is perfectly analogous to equations (5.60) and (5.61): we set

$$
\begin{aligned}
\Theta: \quad \Omega &\to \Omega_\Theta \\
\omega &\mapsto \begin{cases} \perp & \text{if } \omega \in \Omega^{\perp}\,, \\ \vartheta(u,v,w) & \text{if } \omega \in \Omega^{\checkmark}\,, \end{cases}
\end{aligned}
\tag{6.78}
$$

where

$$
\vartheta_i(u,v,w) = \begin{cases} 0 & \text{if } (u \cup v \cup w)_i \in u\,, \\ 1 & \text{if } (u \cup v \cup w)_i \in v\,, \\ 2 & \text{if } (u \cup v \cup w)_i \in w\,. \end{cases} \tag{6.79}
$$

6.5 Proof of uniform sampling for RED sifting

Now we are ready to show the uniform sampling property of RED sifting, equation (6.47). We will use this property in the next section to conclude the analysis of the protocol. We are going to use the notation for multinomial coefficients (see the general conventions on page 17).

Proposition 6.7 : *The RED sifting protocol (see protocol 6.1), together with RED parameter estimation (protocol 6.2) samples uniformly. That is, for the random variable Θ on (Ω, P) defined in the previous section, it holds that*

$$
P_\Theta(\vartheta) = P_\Theta(\vartheta') \quad \text{for all } \vartheta, \vartheta' \in \{0,1,2\}^l_{k,k}\,. \tag{6.80}
$$

The abort probability of PE sifting, $p^{\text{sift}}_{\text{abort}} := P_\Theta(\perp)$, is given by

$$
P_\Theta(\vartheta) = 1 - \sum_{(n_x,n_z,n_\emptyset,n_e)\in\mathcal{N}^{\checkmark}} \binom{m}{n_x, n_z, n_\emptyset, n_e, m-n_x-n_z-n_\emptyset-n_e} f(n_x, n_z, n_\emptyset, n_e)\,, \tag{6.81}
$$

where

$$
\sum_{(n_x,n_z,n_\emptyset,n_e)\in\mathcal{N}^{\checkmark}} = \sum_{n_x=k}^{m-k-n} \sum_{n_z=k}^{m-n_x-n} \sum_{n_\emptyset=n}^{m-n_x-n_z} \sum_{n_e=0}^{m-n_x-n_z-n_\emptyset}\,, \tag{6.82}
$$

and where the function f is as defined in (6.77).

Proof. We are going to employ the same ideas as in the proof of proposition 5.3. The only difference is that we have comparison strings with five different entries (instead of three) and a quota condition with three quota (instead of two). This results in slightly more complicated expressions. Apart from that, the proofs are identical. Therefore, we assume that the reader understands the proof of proposition 5.3 and only give a summarized version of the proof here. We start with the calculation of $P_\Theta(\vartheta)$ for $\vartheta \in \{0,1,2\}^l_{k,k}$. It will turn out to be independent of the choice of $\vartheta \in \{0,1,2\}^l_{k,k}$, which implies uniform sampling.

Let $\vartheta \in \{0,1,2\}^l_{k,k}$. By definition, it holds that

$$P_\Theta(\vartheta) = \sum_{\omega \in \Theta^{-1}(\vartheta)} P(\omega)\,. \tag{6.83}$$

We partition the set $\Theta^{-1}(\vartheta)$ into subsets with a constant number of the five types of agreements and disagreements (x, z, $\emptyset$, d and e),

$$\Theta^{-1}(\vartheta) = \biguplus_{(n_x,n_z,n_\emptyset,n_e)\in\mathcal{N}^\checkmark} \underbrace{\Theta^{-1}(\vartheta) \cap \Omega^\checkmark_{(n_x,n_z,n_\emptyset,n_e)}}_{=:\Theta^{-1}_{(n_x,n_z,n_\emptyset,n_e)}(\vartheta)}\,. \tag{6.84}$$

Since the probability mass function P is constant on $\Theta^{-1}_{(n_x,n_z,n_\emptyset,n_e)}(\vartheta)$ (see equation (6.76)), this allows us to rewrite $P_\Theta(\vartheta)$ as

$$P_\Theta(\vartheta) = \sum_{(n_x,n_z,n_\emptyset,n_e)\in\mathcal{N}^\checkmark} \sum_{\omega\in\Theta^{-1}_{(n_x,n_z,n_\emptyset,n_e)}(\vartheta)} P(\omega) \tag{6.85}$$

$$= \sum_{(n_x,n_z,n_\emptyset,n_e)\in\mathcal{N}^\checkmark} \left|\Theta^{-1}_{(n_x,n_z,n_\emptyset,n_e)}(\vartheta)\right| f(n_x,n_z,n_\emptyset,n_e) \binom{n_x}{k}^{-1}\binom{n_z}{k}^{-1}\binom{n_\emptyset}{n}^{-1}. \tag{6.86}$$

The proof of non-uniform sampling reduces to showing that the size of the set $\Theta^{-1}_{(n_x,n_z,n_\emptyset,n_e)}(\vartheta)$ is independent of the choice of $\vartheta \in \{0,1,2\}^l_{k,k}$. The arguments for this independence are perfectly analogous to the ones in the proof of proposition 5.3. We will not repeat them here. It turns out that

$$\left|\Theta^{-1}_{(n_x,n_z,n_\emptyset,n_e)}(\vartheta)\right| = \binom{m}{l, n_x-k, n_z-k, n_\emptyset-n, n_e, m-n_x-n_z-n_\emptyset-n_e}, \tag{6.87}$$

where the right hand side is a multinomial coefficient. It corresponds to choosing the following rounds within the total m rounds: l rounds that are kept during sifting (within which the order of the agreements is fixed, c.f. figure 5.5), $n_x - k$ discarded $\mathbb{X}$-agreements, $n_z - k$ $\mathbb{Z}$-agreements, $n_\emptyset - n$ discarded $\emptyset$-agreements, n_e disagreements of type e (see equation (6.53)) and $n_d = m - n_x - n_z - n_\emptyset - n_e$ disagreements of type d. A simple calculation shows that

$$\left|\Theta^{-1}_{(n_x,n_z,n_\emptyset,n_e)}(\vartheta)\right| = \binom{l}{k,k,n}^{-1}\binom{m}{n_x,n_z,n_n,n_e,m-n_x-n_z-n_\emptyset-n_e}\binom{n_x}{k}\binom{n_z}{k}\binom{n_\emptyset}{n}. \tag{6.88}$$

Since the probabilities $P_\Theta(\vartheta)$ (including $P_\Theta(\perp)$) sum up to one, we get that

$$P_\Theta(\perp) = 1 - \sum_{\vartheta \in \{0,1,2\}^l_{k,k}} P_\Theta(\vartheta) \tag{6.89}$$

$$= 1 - \left|\{0,1,2\}^l_{k,k}\right| P_\Theta(\vartheta) \quad \text{with } \vartheta \in \{0,1,2\}^l_{k,k} \tag{6.90}$$

$$= 1 - \binom{l}{k,k,n} P_\Theta(\vartheta) \quad \text{with } \vartheta \in \{0,1,2\}^l_{k,k}\,. \tag{6.91}$$

Combining equations (6.86), (6.88) and (6.91), we get that

$$P_\Theta(\perp) = 1 - \sum_{(n_x,n_z,n_\emptyset,n_e)\in\mathcal{N}^\checkmark} \binom{m}{n_x, n_z, n_n, n_e, m - n_x - n_z - n_\emptyset - n_e} f(n_x, n_z, n_\emptyset, n_e)\,, \tag{6.92}$$

as claimed. Equation (6.82) is just a parametrization of the set $\mathcal{N}^\checkmark$. □

6.6 Conclusion of the protocol's analysis

In this section, we complete the analysis of the raw ebit distribution protocol and show that the output satisfies inequality (6.2), which we repeat here for the readers convenience:

$$H_{\min}^{3\varepsilon+5\varepsilon'}(A|E)_\rho \geq n(q - 2h(q_{\text{tol}} + \mu)) - 2\log\frac{2}{\varepsilon^2}\,. \tag{6.93}$$

To analyze the RED protocol, we consider the equivalent protocol in which all measurements are postponed to after the sifting protocol, in analogy to our analysis in section 5.8. We denote the output state of this hypothetical sifting protocol by $\rho_{\mathbf{AB}\Theta}$, where $\mathbf{A}$ and $\mathbf{B}$ are each an l-qubit system. In the last section, we have shown that the state $\rho_{\mathbf{AB}\Theta}$ satisfies

$$P_\Theta(\vartheta) = P_\Theta(\vartheta') \quad \forall\, \vartheta, \vartheta' \in \{0,1,2\}^l_{k,k}\,. \tag{6.94}$$

Since there is no classical communication during the quantum communication phase of the RED sifting protocol, it also satisfies

$$\rho_{\mathbf{AB}\Theta} = \rho_{\mathbf{AB}} \otimes \rho_\Theta\,. \tag{6.95}$$

If we denote by $\rho_{\mathbf{AB}\Theta}$ the state conditioned on passing the quota test, then equations (6.94) and (6.95) taken together can be written as

$$\rho_{\mathbf{AB}\Theta} = \rho_{\mathbf{AB}} \otimes \binom{l}{k,k,n}^{-1} \sum_{\vartheta \in \{0,1,2\}^l_{k,k}} |\vartheta\rangle\langle\vartheta|\,. \tag{6.96}$$

In the equivalent protocol, the parameter estimation of the RED protocol can be seen as a parallel execution of two SBPE protocols, namely one for the error rate in the $\mathbb{X}$-bits and one for the error rate in the $\mathbb{Z}$-bits (see figure 6.1).

In the SBPE protocol for the error rate in the $\mathbb{X}$-bits, all the $\mathbb{Z}$-bits are ignored. This can be seen as Alice and Bob tracing out those positions i in

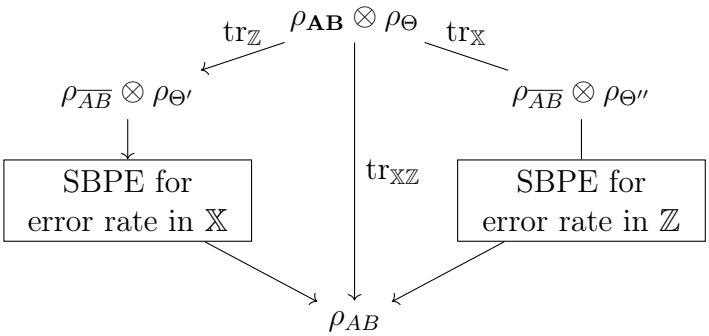


Figure 6.1: The RED PE protocol as a parallel execution of two SBPE protocols.

the (qu)bit strings $\mathbf{A}$, $\mathbf{B}$ and Θ where $\Theta_i = 1$. To see what this means, let us consider a simple example. Let $k = n = 1$. In this case, the strings are of length three, that is, $\mathbf{A} = A_1A_2A_3$, $\mathbf{B} = B_1B_2B_3$ and $\Theta = \Theta_1\Theta_2\Theta_3$. The state $\rho_{\mathbf{AB}\Theta}$ can be written out as

$$\begin{aligned}\rho_{\mathbf{AB}} \otimes \rho_\Theta = \rho_{A_1A_2A_3B_1B_2B_3} \otimes \frac{1}{6}\Big(&\underbrace{|102\rangle\langle 102| + |120\rangle\langle 120|}_{\mathbb{Z}\text{-bit at position 1}} + \\ &\underbrace{|012\rangle\langle 012| + |210\rangle\langle 210|}_{\mathbb{Z}\text{-bit at position 2}} + \\ &\underbrace{|021\rangle\langle 021| + |201\rangle\langle 201|}_{\mathbb{Z}\text{-bit at position 3}}\Big)\end{aligned} \tag{6.97}$$

Thus, tracing out the $\mathbb{Z}$-bits, i.e. the (qu)bit i where $\Theta_i = 1$, yields

$$\begin{aligned}\mathrm{tr}_{\mathbb{Z}}(\rho_{\mathbf{AB}} \otimes \rho_\Theta) &= \mathrm{tr}_{A_1B_1}(\rho_{\mathbf{AB}}) \otimes \frac{1}{6}(|02\rangle\langle 02| + |20\rangle\langle 20|) \\ &\quad + \mathrm{tr}_{A_2B_2}(\rho_{\mathbf{AB}}) \otimes \frac{1}{6}(|02\rangle\langle 02| + |20\rangle\langle 20|) \qquad (6.98) \\ &\quad + \mathrm{tr}_{A_3B_3}(\rho_{\mathbf{AB}}) \otimes \frac{1}{6}(|02\rangle\langle 02| + |20\rangle\langle 20|) \\ &= \rho_{\overline{AB}} \otimes \rho_{\Theta'}\,, \qquad (6.99)\end{aligned}$$

where

$$\rho_{\overline{AB}} = \frac{1}{3}\Big(\mathrm{tr}_{A_1B_1}(\rho_{\mathbf{AB}}) + \mathrm{tr}_{A_2B_2}(\rho_{\mathbf{AB}}) + \mathrm{tr}_{A_3B_3}(\rho_{\mathbf{AB}})\Big)\,, \tag{6.100}$$

$$\rho_{\Theta'} = \frac{1}{2}\Big(|02\rangle\langle 02| + |20\rangle\langle 20|\Big)\,. \tag{6.101}$$

Equations (6.99) and (6.101) express that the SBPE determining the error rate in $\mathbb{X}$ is carried out under the same requirements as the SBPE for QKD that we saw in chapter 5, namely uniform sampling and the absence of a basis information leak. Thus, if the correlation test in the $\mathbb{X}$-basis is passed, then the output's max-entropy $H^\varepsilon_{\max}(X|B)$ is bounded,

$$H^\varepsilon_{\max}(X|B)_\rho \leq nh(q_{\mathrm{tol}} + \mu)\,, \tag{6.102}$$

where

$$\varepsilon' = \frac{\varepsilon}{\sqrt{p_{\text{pass}}^{\text{PE}}}}\,, \quad \mu(\varepsilon) = \sqrt{\frac{l}{nk}\frac{k+1}{k}\ln\frac{1}{\varepsilon}}\,. \tag{6.103}$$

These are the same parameters as in the case of QKD (in fact, we have chosen the parameters of the RED protocol such that this is the case).

Analogously, the parameter estimation for the error rate in the $\mathbb{Z}$-basis is performed on the state

$$\text{tr}_{\mathbb{X}}(\rho_{\mathbf{AB}} \otimes \rho_{\Theta}) = \rho_{\overline{AB}} \otimes \rho_{\Theta''}\,, \tag{6.104}$$

where $\rho_{\overline{AB}}$ is the same state as in (6.100) and where

$$\rho_{\Theta''} = \frac{1}{2}\Big(|12\rangle\langle 12| + |21\rangle\langle 21|\Big)\,. \tag{6.105}$$

Thus, conditioned on passing the correlation test, we have that

$$H_{\max}^{\varepsilon}(Z|B)_{\rho} \leq nh(q_{\text{tol}} + \mu)\,, \tag{6.106}$$

where ε' and $\mu(\varepsilon)$ are as in (6.103). The bounds (6.102) and (6.106) are about the same system in the same state. To see this, note that the output state ρ_{AB} of the system undergoing the SBPE in $\mathbb{X}$ is obtained by tracing out the $\mathbb{X}$-bits in (6.99), i.e. the (qu)-bits with $\Theta_i = 0$,

$$\rho_{AB} = (\text{tr}_{A_1B_1A_2B_2} + \text{tr}_{A_1B_1A_3B_3} + \text{tr}_{A_2B_2A_3B_3})(\rho_{\mathbf{AB}})\,. \tag{6.107}$$

As one can easily see through a comparison of equations (6.101) and (6.105), this is the same output state as for the other SBPE (where the bits with $\Theta_i = 1$ get traced out). Thus, the bounds (6.102) and (6.106) apply jointly. Inserting these bounds into inequality equation (6.15) that we proved in section 6.2.1 yields the desired result of inequality (6.93).

For the sake of simplicity, our analysis here was restricted to the case where $k = n = 1$, but it is not hard to see that this analysis generalizes to arbitrary choices of $n, k \in \mathbb{N}$. For all such choices, the uniform sampling property and the absence of a basis information leak of the RED sifting protocol (equations (6.94) and (6.95)) imply the analogous properties of the reduced states undergoing SBPE. The uniform sampling property (equation (6.101)) follows trivially. The product form of the state in equation (6.99) follows from the fact that in (6.98), all the terms on the right hands side are identical. It is not difficult to see that this always follows from equation (6.94).

Chapter 7

Theory-independent decoherence estimation

7.1 Introduction

7.1.1 Overview

In the last two chapters, we developed a min-entropy estimation formalism that was tailored for the extraction of a resource. In chapter 5, this resource was a raw shared key, while in chapter 6, the resource were highly correlated systems that we called raw ebits. The potential noise on the channel that connects Alice and Bob in the protocols that extract these resources was seen as an adversary's interference that prevents them from the extraction of the resource. When such an interference is detected, the protocol aborts. In this case, our only concern was that an interaction between the transmitted system and some environment took place. This interaction was personified as the action of Eve, who behaves maliciously and who might employ sophisticated strategies to prevent Alice and Bob from extracting the resource. It was an *adversarial scenario*, in which Eve may adjust her actions in every round to the given situation, rather than behaving the same way in every round. The *threat model* was a very strong one: Eve was allowed to do whatever quantum mechanics allows her to do. Our goal was to devise a test whose outcome can rule out any interaction by Eve. However, the implications of such a test on the particular *kind* of interaction that might occur was not of our interest.

The present chapter is also devoted to the estimation of the min-entropy (and a generalization thereof), but the spirit is different from the resource-oriented approach that we followed before. We no longer aim at the extraction of a resource. Instead, we develop a decoherence estimation formalism that can be extended to the framework of *generalized probabilistic theories* (GPTs). This is a very general class of probabilistic theories that contains quantum theory as a special case (we will explain this in more detail in section 7.3). Such a generalized decoherence estimation formalism could be useful for experiments that investigate decoherence processes that might not be correctly described by quantum theory. An interesting candidate for such a process is the postulated effect of *gravitational decoherence*. Since we have no consistent theory of quantum gravitation, a generalized decoherence estimation formalism that

covers a wide range of probabilistic theories might turn out to be very useful for the investigation of gravitational decoherence. Many models for gravitational decoherence have been proposed [Pen96; Dió89; Dio11; Dio84; Dio87; KTM14; Sta12; AH13; Hu14; AH07; Kay98; BGL07; WBM06]. To show potential applications of our framework, we will develop a test for a proposed model for gravitational decoherence by Diósi [Dió89] in section 7.4. Although gravitational decoherence is a prime candidate for the application of our framework, our decoherence estimation formalism is not specific to gravitational decoherence and could, in principle, be applied to any process of decoherence.

We will take our inspiration from the characterization of the min-entropy that we have seen in section 4.6. There, we have seen that the min-entropy of a quantum state ρ_{AE} can be expressed as

$$H_{\min}(A|E)_\rho = -\log d_A \max_{\mathcal{R}_{E\to A'}} F^2(|\Phi\rangle\langle\Phi|_{AA'}, \mathbb{1}_A \otimes \mathcal{R}_{E\to A'}(\rho_{AE}))\,. \tag{7.1}$$

Based on this expression, we define

$$\mathrm{Dec}(A|E)_\rho = \max_{\mathcal{R}_{E\to A'}} F^2(|\Phi\rangle\langle\Phi|_{AA'}, \mathbb{1}_A \otimes \mathcal{R}_{E\to A'}(\rho_{AE}))\,. \tag{7.2}$$

We call it the *decoherence quantity* . This might seem like a trivial redefinition of the min-entropy, since

$$H_{\min}(A|E) = -\log d_A \mathrm{Dec}(A|E)\,. \tag{7.3}$$

However, the quantity (7.2) has a great advantage: as we will see in section 7.3, we can generalize this quantity to the GPT framework. There, it reads

$$\mathrm{Dec}(A|E)_\omega := \sup_{T_E\in\mathcal{T}_E} \sup_{\psi\in\Psi_{AE}} F^2(\psi, T_E(\omega))\,. \tag{7.4}$$

We will explain the specifics of this quantity in section 7.3. Our technical contribution in this section is the proof that this quantity $\mathrm{Dec}(A|E)$ can be estimated by performing a *CHSH test* [Cla+69], not only for quantum theory but for GPTs in general. Now we continue by explaining the general idea behind this test for the case of quantum theory.

7.1.2 Decoherence estimation through CHSH tests

The general idea behind our decoherence estimation test is to probe an unknown decoherence process. Assume that in our lab, we have a system A' that interacts with another system.[1] Unfortunately, we do not know much about this interaction, so we think of it as a black box (see figure 7.1). When system A' enters the black box, it encounters another system and interacts with it. These systems together evolve as a closed system. During this interaction, we have no control over the systems and cannot monitor their evolution. After the interaction took place, we have access to a subsystem B of the whole system that evolved as a closed system, while the complementary subsystem E is not under our control.

[1] It will become clear below why we prefer to denote this sytem by A' rather than by A (see figure 7.3).

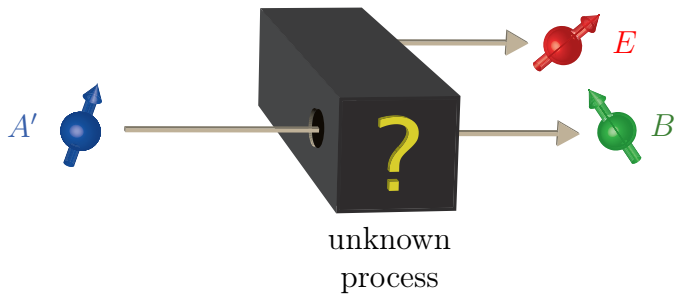


Figure 7.1: An unknown decoherence process. System A' undergoes some evolution that whose details we do not understand. It interacts with another system, and may thereby decohere. The systems together evolve as a closed system, but after the interaction, we only see a subsystem B, while we do not have acces to the complementary subsystem E.

In many cases of interest (such as in an elastic scattering experiment), system B is identical to system A'. In general, however, these systems might be completely different. For example, one may consider the case where A' is a neutron that enters the black box, where it is absorbed by an atom which in turn emits a photon B. In this case, we may be able to perform measurements on the photon B, while having no access to the atom E with the absorbed neutron (we may not know its location within a material). Speaking in the language of quantum information theory, the black box implements a channel from system A' to a system B, and the system E is the purifying system of the Stinespring dilation of the channel (see section 3.3).

From what we discussed so far, nothing is really different from what we considered in chapters 5 and 6. We only changed our language, now speaking of physical systems interacting naturally, rather than of a malicious party Eve with intentions and strategies. It was merely a change in spirit rather than a change in our technical assumptions. Now we are going to introduce an assumption that accounts for this change of spirit. In this chapter, we assume that the black box shows no adversarial behavior. We assume that each time the system A' enters the black box, its output state is the same, provided that the input state was the same in each run. We assume that the box has no strategy but simply behaves the same way in each run of the experiment. Technically speaking, we assume that repeating the experiment results in an *independent and identically distributed* sequence of channel uses. This assumption is usually referred to as the *i.i.d. assumption*. In short, we assume that the black box implements an unknown but constant channel from A' to B that we can use as many times as we wish.

This assumption makes us more powerful as an experimenter. Instead of just getting individual measurement outcomes, we can now experimentally determine outcome *probabilities*. This allows us to perform tests on the unknown channel that would otherwise be impossible. The general setup of our test is shown in figure 7.2. The tested channel takes a system A' as its input and outputs a system B. As such, it is a single-system channel: it takes one system as its input and outputs one system. The idea behind the test is to lift this single-system setting to a setting with two systems. To this end, not only

one system A' is prepared, but a pair of systems A and A' is prepared in a maximally entangled state. System A then remains unchanged, while system A' undergoes the evolution of the channel and transforms into the output B of the channel. In this regard, the setting is very similar to the settings that we considered in the last two chapters. This way, we have not just one but two systems at hand that we can use to probe the channel.

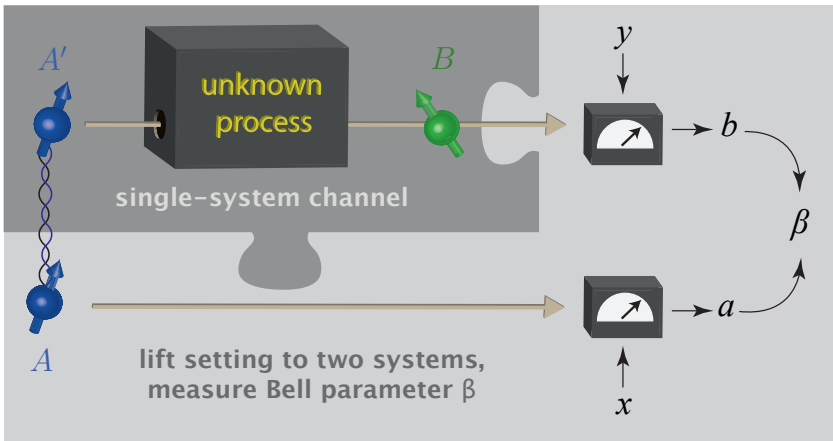


Figure 7.2: Probing an unknown decoherence process through CHSH tests. The subsystem A' of a maximally entangled pair AA' of systems is used as the input for the unknown channel from A' to B. This results in a bipartite system AB, on which we can perform CHSH tests. Since we make the i.i.d. assumption, we can perform measurements on the same state many times and thus estimate the CHSH parameter β_{AB}.

The parameter that is measured in this test is the CHSH parameter β_{AB} [Cla+69]. It is defined in a setting where bipartite measurements are performed on a state ρ_{AB}, just as in our case (see figure 7.2). It assumes that Alice and Bob, who control system A and B, can perform one out of two measurements on their system, each of which has two possible outcomes. In the most common formulation of the parameter β_{AB}, this is described by *observables* (i.e. Hermitian operators) $\mathbb{A}_0$, $\mathbb{A}_1$ for Alice and $\mathbb{B}_0$, $\mathbb{B}_1$ for Bob, each of which have the possible outcomes (i.e. eigenvalues) 1 and -1. We write their spectral decomposition as

$$\mathbb{A}_0 = \mathbb{A}_{1|0} - \mathbb{A}_{-1|0}\,, \qquad \mathbb{B}_0 = \mathbb{B}_{1|0} - \mathbb{A}_{-1|0}\,, \tag{7.5}$$

$$\mathbb{A}_1 = \mathbb{A}_{1|1} - \mathbb{A}_{-1|1}\,, \qquad \mathbb{B}_1 = \mathbb{B}_{1|1} - \mathbb{B}_{-1|1}\,, \tag{7.6}$$

where for every $x, y \in \{0, 1\}$, $\mathbb{A}_{1|x}$, $\mathbb{A}_{-1|x}$ and $\mathbb{B}_{1|y}$, $\mathbb{B}_{-1|y}$ are pairs of mutually orthogonal projectors. If Alice measures with respect to $\mathbb{A}_x$ and Bob with respect to $\mathbb{B}_y$, then the expectation value $\langle ab|x, y\rangle$ of the product ab of their outcomes a and b is given by

$$\langle ab|x, y\rangle = \operatorname{tr}\big((\mathbb{A}_x \otimes \mathbb{B}_y)\rho_{AB}\big)\,. \tag{7.7}$$

In these terms, the CHSH parameter of a state ρ_{AB} is defined as

$$\beta_{AB} = \langle ab|0, 0\rangle + \langle ab|0, 1\rangle + \langle ab|1, 0\rangle - \langle ab|1, 1\rangle \tag{7.8}$$

$$= \operatorname{tr}\big(\mathbb{C}_{AB}\rho_{AB}\big)\,, \tag{7.9}$$

where $\mathbb{C}_{AB}$ is the "CHSH correlator"

$$\mathbb{C}_{AB} = (\mathbb{A}_0 \otimes \mathbb{B}_0 + \mathbb{A}_0 \otimes \mathbb{B}_1 + \mathbb{A}_1 \otimes \mathbb{B}_0 - \mathbb{A}_1 \otimes \mathbb{B}_1)\,. \tag{7.10}$$

The parameter β_{AB} appears in the *CHSH inequality* [Cla+69], which famously states that if the experiment is described by a local hidden variable theory, then the parameter β_{AB} as in equation (7.8) satisfies

$$\beta_{AB} \leq 2\,. \tag{7.11}$$

In quantum theory, where β_{AB} can be written as in equation (7.9), a maximal value of $\beta_{AB} = 2\sqrt{2}$ can be achieved. This is the famous proof of the *nonlocality* of quantum mechanics. Such a proof was first presented in a seminal paper by John Bell [Bel64]. The form that we presented here, which is experimentally more accessible than Bell's original formulation, was derived by Clauser, Horne, Shimony and Holt [Cla+69]. While the term "CHSH inequality" is technically more correct, inequality (7.11) it is often called "Bell's inequality", honoring Bell for his original idea. We shall use the terms "Bell" and "CHSH" interchangeably. We assume that the reader has some familiarity with Bell's inequality and the nonlocality of quantum mechanics, and do not give further background on these topics here. For a review article on the subject, see [Bru+14].

In our test, many copies of a system AA' in a maximally entangled state $|\Phi\rangle\langle\Phi|_{AA'}$ are prepared and measured in the setting shown in figure 7.2. By measuring many times in the four possible settings where Alice and Bob vary their choice of the measurement $x, y = 0, 1$, the parameter β_{AB} can be estimated. For our purposes, we are not interested in testing whether the experiment can be described by a local hidden variable theory. Therefore, in our experiment, no measures need to be taken to close Bell test loopholes as in the recent loophole-free Bell test [Hen+15]. We make the i.i.d. assumption and assume no malicious behavior by the black box.

7.1.3 Implications of high CHSH values in quantum theory

We measure the parameter β_{AB} in order to learn something about the correlations between the systems A, B and the purifying system E (see figure 7.3). The intuition is as follows. If Alice and Bob measure a CHSH parameter $\beta_{AB} = 2\sqrt{2}$, then they know that the state ρ_{AB} must be a maximally entangled state.[2] In that case, they know that system E is necessarily decoupled from AB, that is, $\rho_{ABE} = \rho_{AB} \otimes \rho_E$ (see proposition 3.22). Thus, all the initial entanglement between A and A' is preserved in the system AB, and there is no entanglement between A and E.

This principle—that a system A that is strongly entangled with B cannot, at the same time, be entangled with another system E—is called the *monogamy of entanglement* [Ter04]. The argument that we just made is for

[2] This is shown using a technique called *self-testing*. The first results of this form were given in [PR92]. For further reading, we refer to [Wu+15], [MM11b].

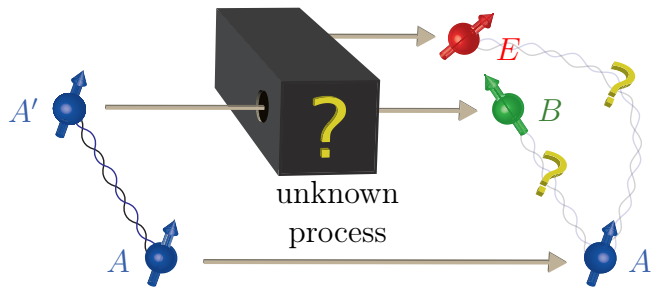


Figure 7.3: Monogamy of entanglement and correlations. If A and B are strongly entangled, as expressed by a high CHSH value β_{AB}, then the systems A and E are necessarily uncorrelated. In other words, system A cannot be strongly correlated with both systems B and E at the same time.

the most extreme case, where A and B are maximally entangled. Such monotonicity statements can also be made in a quantitative way, thereby including a range of non-extreme cases. The question that arises in this case is how to quantify the entanglement—or correlation—between the different parties. In a work by Toner and Verstraete [TV06], this is solved as follows. They consider a tripartite quantum state ρ_{ABE}, together with a pair of observables for each party ($\mathbb{A}_0$ and $\mathbb{A}_1$ for Alice, $\mathbb{B}_0$ and $\mathbb{B}_1$ for Bob, $\mathbb{E}_0$ and $\mathbb{E}_1$ for Eve). They show that

$$\beta_{AB}^2 + \beta_{AE}^2 \leq 8\,, \tag{7.12}$$

where β_{AB} is as in equations (7.9) and (7.10), and where β_{AE} is the corresponding quantity for A and E,

$$\beta_{AE} = \mathrm{tr}(\mathbb{C}_{AE}\rho_{AE})\,, \quad \text{where} \tag{7.13}$$

$$\mathbb{C}_{AE} = (\mathbb{A}_0 \otimes \mathbb{E}_0 + \mathbb{A}_0 \otimes \mathbb{E}_1 + \mathbb{A}_1 \otimes \mathbb{E}_0 - \mathbb{A}_1 \otimes \mathbb{E}_1)\,. \tag{7.14}$$

Inequality (7.12) shows that if the CHSH correlation between A and B is maximal (with $\beta_{AB} = 2\sqrt{2}$), then A and E are necessarily uncorrelated ($\beta_{AE} = 0$), and therefore reproduces the argument above. In addition to that, it provides a bound for the intermediate cases where none of the two correlations is maximal. This provides a robust monotonicity statement for CHSH correlations.

Inequality (7.12) shows that high values of β_{AB} restrict the β_{AE}. An interesting question is whether high values of β_{AB} can also be shown to restrict other quantities of correlation between A and E. We will show that this is indeed the case. As one of our main results of this chapter, we will prove that non-classical values of β_{AB} (that is, $\beta_{AB} > 2$) restrict the min-entropy $H_{\min}(A|E)$. Figure 7.4 shows a lower bound on $H_{\min}(A|E)$ for a given value of β_{AB} that we will derive in section 7.2. This lower bound on the min-entropy translates into an upper bound on the decoherence quantity $\mathrm{Dec}(A|E)_\rho$ as defined in equation (7.2). The resulting feasible region is shown in figure 7.5 in dark green.

This bound can be used, for example, to test existing models of gravitational decoherence. For a quantum-mechanical model that describes such a process, one can calculate the predicted value for the decoherence quantity

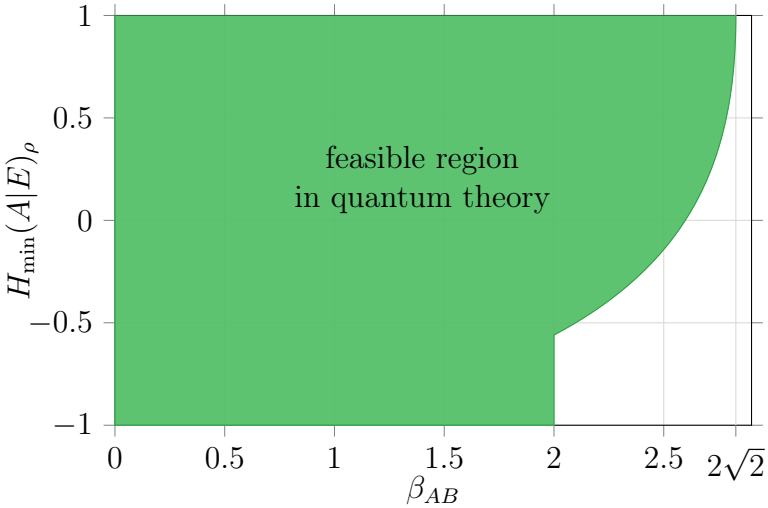


Figure 7.4: Min-entropy bound for a given CHSH value β_{AB}. A point $(\beta_{AB}, H^{\varepsilon}_{\min}(A|E)_\rho)$ in this figure is colored in green if and only if there exists a state ρ_{AB} such that a purification ρ_{ABE} of it has a min-entropy of $H^{\varepsilon}_{\min}(A|E)$ and if there exist measurements for Alice and Bob such that its CHSH value is β_{AB}. We call the set of all such points the *feasible region*. The part of the feasible region with $\beta_{AB} \geq 2$ is drawn in figure 7.5, converted to an upper bound on the decoherence quantity $\mathrm{Dec}(A|E)$.

$\mathrm{Dec}(A|E)$ under this model and see whether it is compatible with the experimental data and the bound. This gives us a falsification tool for testing models for unknown decoherence processes.

7.1.4 Implications of high CHSH values beyond quantum theory

It turns out that the ideas of the last subsection can be extended beyond quantum theory. Indeed, it has already been noted by Toner [Ton09] that a result similar to inequality (7.12) can be found for all theories that satisfy the *no-signalling principle*. The idea is as follows. The experiment may not be correctly described by quantum theory, but there may be another theory that predicts the correct outcome probabilities. We denote the probability of Alice, Bob and Eve getting an outcome a, b, c when performing a measurement indexed by $x, y, z \in \{0, 1\}$ by $P[a, b, c|x, y, z]$. While the experiment may not follow the laws of quantum mechanics, we assume that it respects the no-signalling principle. It states that the probabilities $P[a, b, c|x, y, z]$ are such that any party cannot influence the marginal distribution of the other parties by choosing a particular measurement. More precisely, it says that for all a, b, x and y,

$$\sum_c P[a, b, c|x, y, 0] = \sum_c P[a, b, c|x, y, 1]\,, \tag{7.15}$$

and the analogous statements for the other two parties. If equation (7.15) was violated, then Eve could influence Alice's and Bob's outcome probability

by choosing either $z = 0$ or $z = 1$. This could be interpreted as signalling a message, and the no-signalling principle states that this is impossible (for a formal definition, see definition 7.25). Note that the no-signalling principle holds in quantum theory.

In such a non-signalling theory, the CHSH parameters β_{AB} and β_{AE} can be defined in analogy to the quantum case. According to equation (7.8), we just need to express the expectation value $\langle ab|x,y\rangle$ as a function of the AB-marginal

$$P[a,b|x,y] = \sum_c P[a,b,c|x,y,z]\,. \tag{7.16}$$

(The choice of c is irrelevant by the no-signalling principle.) It simply reads

$$\langle ab|x,y\rangle = P[1,1|x,y] + P[-1,-1|x,y] - P[1,-1|x,y] - P[-1,1|xy]\,, \tag{7.17}$$

and the analogous can be done for the AE-marginal.

Ben Toner [Ton09] showed that for non-signalling theories, a statement similar to inequality (7.12) can be made. He proved that

$$\beta_{AB} + \beta_{AE} \leq 4\,. \tag{7.18}$$

This implies that non-classical CHSH values for Alice and Bob ($\beta_{AB} > 2$) restrict the CHSH value for Alice and Eve to classical values ($\beta_{AE} < 2$). In analogy to the quantum case of the previous subsection, we may now ask whether it holds that in non-signalling theories, high values of β_{AB} also restrict some quantity analogous to the min-entropy $H_{\min}(A|E)$ or the decoherence quantity $\mathrm{Dec}(A|E)$ that we defined in equation (7.2).

As a main result of this chapter, we will show in section 7.3 that this is indeed the case. In a first step, we will formulate a decoherence quantity $\mathrm{Dec}(A|E)$ for GPTs. This requires a lot of effort to be formalized. This can be seen from our quantum definition of $\mathrm{Dec}(A|E)$ in equation (7.2), which we shall repeat here:

$$\mathrm{Dec}(A|E)_\rho = \max_{\mathcal{R}_{E\to A'}} F^2(|\Phi\rangle\langle\Phi|_{AA'}, \mathbb{1}_A \otimes \mathcal{R}_{E\to A'}(\rho_{AE}))\,. \tag{7.19}$$

For this equation to be translated to GPTs, one needs to formalize the notion of parties, maximally entangled states, recovery maps and the fidelity for GPTs. We discuss how to do this in detail in section 7.3. In a second step, we show that high values of β_{AB} restrict the value of $\mathrm{Dec}(A|E)$. To do this, we will use linear programming techniques, inspired by the proof of inequality (7.18) by Ben Toner. The red region in figure 7.5 shows the pairs $(\beta_{AB}, \mathrm{Dec}(A|E))$ that are ruled out by our bound for *all* non-signalling theories.

Numerically, the GPT bound in figure 7.5 may seem weak. However, this should be seen less as a ready-to-use bound than as a proof of concept. Note that the red region is excluded for *all* non-signalling theories. For a particular candidate theory that one wants to test in an experiment, one typically wants to add additional linear constraints in the theory that push the bound down to experimentally more accessible values. For example, one may want to test whether a certain decoherence process can be described in a non-signalling

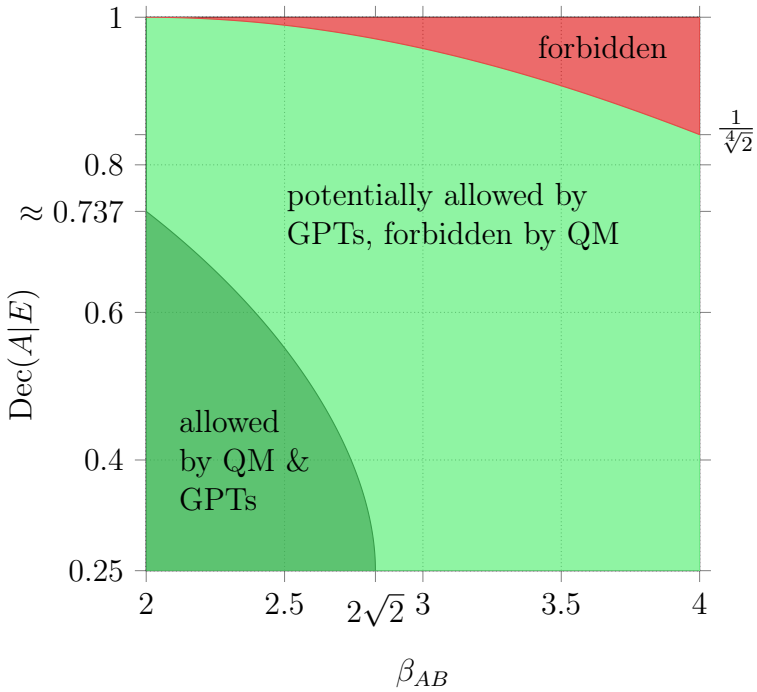


Figure 7.5: Allowed values of the decoherence quantity for measured CHSH values. This figure shows what values of the decoherence quantity are compatible with some measured CHSH value β_{AB}, assuming either quantum theory or any other probabilistic theory. The dark green region consists of all points $(\beta_{AB}, \mathrm{Dec}(A|E)_\rho)$ for which there exists a state ρ_{AB} and two pairs $(\mathbb{A}_0, \mathbb{A}_1)$ and $(\mathbb{B}_0, \mathbb{B}_1)$ of observables with the according values, i.e. the bound is tight. The red region shows pairs $(\beta_{AB}, \mathrm{Dec}(A|E)_\omega)$ that cannot be realized in any non-signalling probabilistic theory. The curve between the light green area and the red area is a bound on $\mathrm{Dec}(A|E)_\omega$ which is valid for all non-signalling probabilistic theories. A bound for any specific non-signalling probabilistic theory runs below the red region.

theory with uncertainty relations. Since uncertainty relations may be formulated as linear constraints, these would lead to a new linear program that can be solved in the very same way as the linear program that produced the red region in figure 7.5.

Thus, our decoherence estimation formalism allows us to devise tests to measure CHSH values β_{AB} that do not only tell us something about the tested channel as a quantum channel. If quantum models for the decoherence process are ruled out, the same experimental data can be used to be tested against more general classes of probabilistic theories. By varying the constraints that define the linear program that produces the bound, one can see what properties of nature are compatible with the observed data.

7.1.5 Outline of the chapter

Section 7.2 is devoted to proving the min-entropy bound for given CHSH values β_{AB} in quantum theory. In other words, we derive the shape of the boundary

between the dark green region and the light green region in figure 7.5. We will also show that this bound is tight. In section 7.3, we will prove the GPT bound, i.e. the boundary between the dark green region and the red region in figure 7.5. In contrast to the quantum bound, this bound is unlikely to be tight. As we will discuss in the outlook in chapter 8, we have strong indications that this bound may be improved significantly by using alternative techniques of optimization. Finally, in section 7.4, we give an example application of our framework. We show how a specific model for gravitational decoherence by Diosi [Dió89] can be tested experimentally using our framework. The bounds on the value β_{AB} that needs to be measured in order to rule out the model are derived with the quantum mechanical bound. Should this bound be violated, then our formalism can be used to test the data against other models of nature that might describe the experiment in place of quantum theory.

7.2 Decoherence estimation through CHSH tests in quantum theory

Our goal is to show that Alice and Bob can estimate the decoherence quantity $\mathrm{Dec}(A|E)$ as defined in (7.2)—or equivalently, the min-entropy $H_{\min}(A|E)$—by performing a Bell experiment. We pose it as a feasibility problem: is it possible to observe certain statistics in a Bell experiment given a certain level of decoherence? Solving this problem allows us to determine and plot the *feasible region* in the space of suitably chosen parameters. Since the range of values that the min-entropy takes depends on the dimension of Alice's system (denoted by d_A), it is only meaningful to compare scenarios in which d_A is fixed. For simplicity, we consider the simplest non-trivial scenario in which the subsystems held by Alice and Bob are qubits, $d_A = d_B = 2$.

We define the feasible region $\mathcal{S}$ as follows. A pair of real numbers (u, v), where $u \in [-1, 1]$ and $v \in [0, 2\sqrt{2}]$ belongs to $\mathcal{S}$ if there exists a tripartite state ρ_{ABE} and binary observables A_0, A_1 on $\mathcal{H}_A$ and B_0, B_1 on $\mathcal{H}_B$ such that

- Subsystems A and B are qubits: $\dim \mathcal{H}_A = \dim \mathcal{H}_B = 2$,
- The conditional min-entropy of A given E equals u: $H_{\min}(A|E) = u$,
- The CHSH value given by Eq. (7.9) equals v: $\beta_{AB} = v$.

First note that a CHSH value of $v \leq 2$ can be achieved using trivial measurements (namely $\{\mathbb{1}, 0\}$) acting on an arbitrary state. Therefore, for $v \leq 2$ all values of $u \in [-1, 1]$ are allowed. For the remainder of the argument we implicitly assume that $v > 2$ and the following intuitive argument shows why certain pairs (u, v) must indeed be forbidden. Consider a point $u \approx -1$ and $v > 2$. According to the operational meaning of the min-entropy, $u \approx -1$ means that Eve can recover the maximally entangled state with Alice with fidelity close to unity, which clearly allows Alice and Eve to violate the CHSH inequality. On the other hand, since $v > 2$ Alice also observes a CHSH violation with Bob. This violates the monogamy relation for tripartite three-qubit states proved in [SG01], which states that Alice can violate the CHSH inequality with at

most one party (even if she is allowed to use different measurements for different scenarios). This simple argument leads to the conclusion that the region $u \approx -1$ and $v > 2$ is forbidden. In the remainder of this section we show that the non-trivial part of the feasible region $\mathcal{S}$ can be fully characterized by a single inequality.

Theorem 7.1 : *A pair of real numbers (u, v) where $u \in [-1, 1]$ and $v \in (2, 2\sqrt{2}]$ belongs to the feasible region $\mathcal{S}$ if and only if*

$$u \geq f(v), \tag{7.20}$$

where

$$f(v) := 3 - 2 \log \max_{c_z} \left(2\sqrt{1 + c_z} + \sqrt{1 - c_z + \frac{v}{\sqrt{2}}} + \sqrt{1 - c_z - \frac{v}{\sqrt{2}}} \right), \tag{7.21}$$

where the maximization is taken over

$$-1 \leq c_z \leq 1 - \frac{v}{\sqrt{2}}. \tag{7.22}$$

While the definition of f might seem complicated, it is straightforward to see that f is monotonically increasing in v and evaluating $f(v)$ numerically for a particular value of v is straightforward since the function to be maximized is concave. The feasible region $\mathcal{S}$ is plotted in figure 7.4.

The proof of theorem 7.1 is conceptually simple, but it requires a wide array of technical tools, which we present in section 7.2.1. In sections 7.2.2 and 7.2.3 we prove the direct and converse parts of theorem 7.1, respectively.

7.2.1 Preliminaries

Definition 7.2 : *Let $\mathcal{H}_A$, $\mathcal{H}_B$ be Hilbert spaces of dimension d. A* ***generalized Bell basis*** *for $\mathcal{H}_A \otimes \mathcal{H}_B$ is a set $\{|\Phi_j\rangle\langle\Phi_j|\}_{j=1}^{d^2}$ of d^2 pure states on $\mathcal{H}_A \otimes \mathcal{H}_B$ which satisfy*

$$\mathrm{tr}_A|\Phi_j\rangle\langle\Phi_j| = \frac{\mathbb{1}_B}{d}, \quad \mathrm{tr}_B|\Phi_j\rangle\langle\Phi_j| = \frac{\mathbb{1}_A}{d} \quad \text{for } j = 1, \ldots, d^2 \text{ and} \tag{7.23}$$

$$\sum_{j=1}^{d^2} |\Phi_j\rangle\langle\Phi_j| = \mathbb{1}_A \otimes \mathbb{1}_B. \tag{7.24}$$

A state $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ is called ***Bell-diagonal*** *if it is diagonal in some generalized Bell basis, i.e. if there exists a probability distribution $\{p_j\}_{j=1}^{d^2}$ such that*

$$\rho_{AB} = \sum_{j=1}^{d^2} p_j |\Phi_j\rangle\langle\Phi_j|. \tag{7.25}$$

Lemma 7.3 : *Let $A \geq 0$ be a positive semi-definite operator, let Π_A be the projector on its support and let $|b\rangle$ be a normalized vector. Then $A \geq |b\rangle\langle b|$ iff*

$$\Pi_A|b\rangle = |b\rangle \quad \text{and} \quad \langle b|A^{-1}|b\rangle \leq 1. \tag{7.26}$$

Note that since A might not be invertible, A^{-1} is only defined on the support of A.

Two-qubit states

A two-qubit state written in the Pauli basis takes the form

$$\rho_{AB} = \frac{1}{4}\big(\mathbb{1}_A \otimes \mathbb{1}_B + \sum_j a_j\sigma_j \otimes \mathbb{1}_B + \mathbb{1}_A \otimes \sum_j b_j\sigma_j + \sum_{j,k} T_{jk}\sigma_j \otimes \sigma_k\big), \quad (7.27)$$

where all the summations go over $\{x, y, z\}$. It is known that for every state there exists a local unitary $U_A \otimes U_B$ which diagonalizes the correlation tensor (i.e. ensures that $T_{jk} = 0$ for $j \neq k$) and since all the properties we consider are invariant under local unitaries we can make this assumption without loss of generality. We denote these diagonal entries T_{xx}, T_{yy} and T_{zz} by c_x, c_y and c_z, respectively, which simplifies the expression to

$$\rho_{AB} = \frac{1}{4}\big(\mathbb{1}_A \otimes \mathbb{1}_B + \sum_j a_j\sigma_j \otimes \mathbb{1}_B + \mathbb{1}_A \otimes \sum_j b_j\sigma_j + \sum_j c_j\sigma_j \otimes \sigma_j\big). \quad (7.28)$$

Without loss of generality, we assume that $|c_x| \geq |c_y| \geq |c_z|$ and $c_x, c_y \geq 0$. As shown in Ref. [HH96] every Bell-diagonal state of two qubits (up to local unitaries which, again, we can safely ignore) can be written as

$$\rho_{AB} = \sum_{j=1}^{4} p_j |\Phi_j\rangle\langle\Phi_j|, \quad (7.29)$$

where $\{p_j\}_{j=1}^4$ is a probability distribution and

$$|\Phi_{1,2}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \qquad |\Phi_{3,4}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}. \quad (7.30)$$

It is easy to verify that

$$\rho_{AB} = \frac{1}{4}\big(\mathbb{1}_A \otimes \mathbb{1}_B + \sum_j c_j\sigma_j \otimes \sigma_j\big), \quad (7.31)$$

where

$$\begin{aligned} c_x &= p_1 - p_2 + p_3 - p_4\,, \\ c_y &= -p_1 + p_2 + p_3 - p_4\,, \\ c_z &= p_1 + p_2 - p_3 - p_4\,. \end{aligned} \quad (7.32)$$

Non-locality

Definition 7.4 : *For a bipartite quantum state ρ_{AB} the maximum CHSH value is defined as*

$$\beta_{\max}(\rho_{AB}) := \max_{\mathbb{A}_0,\mathbb{A}_1,\mathbb{B}_0,\mathbb{B}_1} \operatorname{tr}\Big((\mathbb{A}_0\otimes\mathbb{B}_0 + \mathbb{A}_0\otimes\mathbb{B}_1 + \mathbb{A}_1\otimes\mathbb{B}_0 - \mathbb{A}_1\otimes\mathbb{B}_1)\rho_{AB}\Big), \quad (7.33)$$

where the maximization is taken over all Hermitian, binary observables with eigenvalues 1 and -1.

Note that for all states $\beta_{\max} \geq 2$ and we say that the state violates the CHSH inequality if $\beta_{\max} > 2$. It was shown in Ref. [HHH95a] that if ρ_{AB} is a state of two qubits then the value of $\beta_{\max}$ is fully determined by the correlation tensor. Adopting the convention $|c_x| \geq |c_y| \geq |c_z|$ we have

$$\beta_{\max}(\rho_{AB}) = \begin{cases} 2 & \text{if } \; c_x^2 + c_y^2 \leq 1, \\ 2\sqrt{c_x^2 + c_y^2} & \text{otherwise.} \end{cases} \quad (7.34)$$

Max-entropy for Bell-diagonal states

To derive a bound on the min-entropy $H_{\min}(A|E)_\rho$, we will make use of the min-max duality (lemma 6.2) and an alternative expression for the max-entropy (that is, different from the one in definition 3.26). Namely, as shown in [Tom12], the max-entropy can be written as

$$H_{\max}(A|B) = \max_{\sigma_B} \log d_A F^2(\rho_{AB}, \pi_A \otimes \sigma_B)\,, \tag{7.35}$$

where π_A is the maximally mixed state on A and the maximization is taken over all states on B. We need an explicit expression for the max-entropy of a Bell-diagonal state. Note that by assumption $d_A = d_B = d$.

Lemma 7.5 : *Let ρ_{AB} be a Bell-diagonal state of form (7.25). Then the conditional max-entropy equals*

$$H_{\max}(A|B) = -\log d + 2\log\Big(\sum_j \sqrt{p_j}\Big). \tag{7.36}$$

To prove lemma 7.5, we use the fact that the optimization problem which appears in the definition of the max-entropy (7.35) can be written as a semidefinite program (SDP) [Vit+13]. More specifically, given ρ_{AB} we have $H_{\max}(A|B) = \log\lambda$, where λ is the value of the following SDP for ρ_{ABE} being an arbitrary purification of ρ_{AB}

$$\begin{array}{lll} \texttt{PRIMAL}: & \text{minimize} & \mu \\ & \text{subject to} & \mu\mathbb{1}_B \geq \mathrm{tr}_A(Z_{AB}) \\ & & Z_{AB}\otimes\mathbb{1}_E \geq \rho_{ABE} \\ & & Z_{AB} \in \mathrm{Pos}(\mathcal{H}_{AB}) \\ & & \mu \geq 0 \end{array} \tag{7.37}$$

$$\begin{array}{lll} \texttt{DUAL}: & \text{maximize} & \mathrm{tr}(\rho_{ABE}Y_{ABE}) \\ & \text{subject to} & \mathrm{tr}_E(Y_{ABE}) \leq \mathbb{1}_A\otimes\sigma_B \\ & & \mathrm{tr}\sigma_B \leq 1 \\ & & Y_{ABE} \in \mathrm{Pos}(\mathcal{H}_{ABE}) \\ & & \sigma_B \in \mathrm{Pos}(\mathcal{H}_B) \end{array} \tag{7.38}$$

where $\mathrm{Pos}(\mathcal{H})$ denotes the set of positive semi-definite operators acting on $\mathcal{H}$. By providing feasible solutions for the `PRIMAL` and the `DUAL` we show that for Bell-diagonal states

$$\lambda = \frac{1}{d}\Big(\sum_j \sqrt{p_j}\Big)^2 \tag{7.39}$$

which is precisely the statement of lemma 7.5.

Proof. Let $\rho_{ABE} = |\psi_{ABE}\rangle\langle\psi_{ABE}|$ be a purification of ρ_{AB}, e.g.

$$|\psi_{ABE}\rangle = \sum_j \sqrt{p_j}|\Phi_j\rangle\otimes|j\rangle. \tag{7.40}$$

For the PRIMAL consider

$$Z_{AB} = \Big(\sum_j \sqrt{p_j}\Big) \sum_k \sqrt{p_k} |\Phi_k\rangle\langle\Phi_k|, \tag{7.41}$$

$$\mu = \frac{1}{d}\Big(\sum_j \sqrt{p_j}\Big)^2. \tag{7.42}$$

Clearly, $Z_{AB} \geq 0$, $\mu \geq 0$ and since $\mathrm{tr}_A(Z_{AB}) = \frac{1}{d}\big(\sum_j \sqrt{p_j}\big)^2 \mathbb{1}_B$ the first constraint is easy to check. The last inequality we need to check is

$$\Big(\sum_j \sqrt{p_j}\Big) \sum_k \sqrt{p_k} |\Phi_k\rangle\langle\Phi_k| \otimes \mathbb{1}_E \geq \rho_{ABE}. \tag{7.43}$$

We apply lemma 7.3 to $A = Z_{AB} \otimes \mathbb{1}_E$ and $|b\rangle = |\psi_{ABE}\rangle$. The projector on the support of $Z_{AB} \otimes \mathbb{1}_E$ equals

$$\Pi = \sum_{j:p_j>0} |\Phi_j\rangle\langle\Phi_j| \otimes \mathbb{1}_E \tag{7.44}$$

and it is easy to verify that $\Pi|\psi_{ABE}\rangle = |\psi_{ABE}\rangle$. Moreover, since

$$(Z_{ABE})^{-1} = (Z_{AB})^{-1} \otimes \mathbb{1}_E\,, \tag{7.45}$$

we have that

$$\begin{aligned}
&\Big(\sum_m \sqrt{p_m}\langle\Phi_m| \otimes \langle m|\Big)\Big(\Big(\sum_j \sqrt{p_j}\Big)^{-1} \sum_{k:p_k>0} \frac{1}{\sqrt{p_k}} |\Phi_k\rangle\langle\Phi_k| \otimes \mathbb{1}_E\Big) \cdot \\
&\qquad \cdot \Big(\sum_n \sqrt{p_n}|\Phi_n\rangle \otimes |n\rangle\Big) \\
&= \Big(\sum_j \sqrt{p_j}\Big)^{-1} \Big(\sum_m \sqrt{p_m}\langle\Phi_m| \otimes \langle m|\Big)\Big(\sum_{n:p_n>0} |\Phi_n\rangle \otimes |n\rangle\Big) && (7.46)\\
&= 1. && (7.47)
\end{aligned}$$

Showing that Z_{AB} and μ constitute a valid solution to the PRIMAL implies that $\lambda \leq \frac{1}{d}\big(\sum_j \sqrt{p_j}\big)^2$.
For the DUAL consider

$$Y_{ABE} = \frac{1}{d} \sum_{jk} |\Phi_j\rangle\langle\Phi_k| \otimes |j\rangle\langle k|, \tag{7.48}$$

$$\sigma_B = \frac{\mathbb{1}_B}{d}. \tag{7.49}$$

Note that Y_{ABE} is proportional to a rank-1 projector. The first constraint gives

$$\mathrm{tr}_E(Y_{ABE}) = \frac{1}{d} \sum_j |\Phi_j\rangle\langle\Phi_j| = \frac{1}{d}\, \mathbb{1}_A \otimes \mathbb{1}_B = \mathbb{1}_A \otimes \sigma_B \tag{7.50}$$

and the remaining ones are easily verified to be true. The value of this solution equals $\mathrm{tr}(\rho_{ABE} Y_{ABE}) = \frac{1}{d}\big(\sum_j \sqrt{p_j}\big)^2$ which implies that $\lambda \geq \frac{1}{d}\big(\sum_j \sqrt{p_j}\big)^2$. $\square$

Sufficiency of considering Bell-diagonal states

To prove the converse part of theorem 7.1, we will use the following argument, which is similar in spirit and inspired by the symmetrization argument presented in Ref. [Ací+07].

Lemma 7.6 : *Let ρ_{AB} be an arbitrary state of two qubits. Then, there exists a Bell-diagonal state σ_{AB} which satisfies*

$$\beta_{\max}(\rho_{AB}) = \beta_{\max}(\sigma_{AB}) \quad \text{and} \quad H_{max}(A|B)_\sigma \geq H_{max}(A|B)_\rho. \tag{7.51}$$

Proof. We present an explicit construction of σ_{AB} which meets the requirements. According to Eq. (7.28), ρ_{AB} can be written as

$$\rho_{AB} = \frac{1}{4}\big(\mathbb{1}_A \otimes \mathbb{1}_B + \sum_j a_j \sigma_j \otimes \mathbb{1}_B + \mathbb{1}_A \otimes \sum_j b_j \sigma_j + \sum_j c_j \sigma_j \otimes \sigma_j\big). \tag{7.52}$$

Moreover, consider the following random unitary channel

$$\Lambda(\rho_{AB}) = \frac{1}{4}\sum_{j=1}^{4}(U_j \otimes U_j)\rho_{AB}(U_j^\dagger \otimes U_j^\dagger), \tag{7.53}$$

where $U_1 = \mathbb{1}$, $U_2 = \sigma_x$, $U_3 = \sigma_y$ and $U_4 = \sigma_z$. It is easy to verify that for $j \in \{x, y, z\}$

$$\Lambda(\sigma_j \otimes \mathbb{1}_B) = \Lambda(\mathbb{1}_A \otimes \sigma_j) = 0 \tag{7.54}$$

because each Pauli operator commutes with identity and itself but anticommutes with the other two unitaries. This implies that $\sigma_{AB} = \Lambda(\rho_{AB})$ is Bell-diagonal. Moreover, one can check that the map preserves the correlation tensor, i.e. for $j \in \{x, y, z\}$

$$\Lambda(\sigma_j \otimes \sigma_j) = \sigma_j \otimes \sigma_j, \tag{7.55}$$

which implies that $\beta_{\max}(\rho_{AB}) = \beta_{\max}(\sigma_{AB})$. To check the last property consider the following state

$$\sigma_{ABK} = \frac{1}{4}\sum_{j=1}^{4}(U_j \otimes U_j)\rho_{AB}(U_j^\dagger \otimes U_j^\dagger) \otimes |j\rangle\langle j|. \tag{7.56}$$

By the data processing inequality, we have $H_{\max}(A|B)_\sigma \geq H_{\max}(A|BK)_\sigma$ and by conditioning on classical information we have

$$H_{\max}(A|BK)_\sigma = \log\Big(\sum_{j=1}^{4}\frac{1}{4}\cdot 2^{H_{\max}(A|B)_{\tau^j}}\Big), \tag{7.57}$$

$$\text{where} \quad \tau_{AB}^j = (U_j \otimes U_j)\rho_{AB}(U_j^\dagger \otimes U_j^\dagger). \tag{7.58}$$

Since the max-entropy is invariant under local unitaries we have

$$H_{\max}(A|B)_{\tau^j} = H_{\max}(A|B)_\rho \quad \forall\, j \in \{x, y, z\}\,, \tag{7.59}$$

which implies that

$$H_{\max}(A|B)_\sigma \geq H_{\max}(A|BK)_\sigma = H_{\max}(A|B)_\rho. \tag{7.60}$$

This completes the proof. □

The final technical lemma concerns the problem of maximizing the max-entropy of a Bell-diagonal state of two qubits whose maximal CHSH violation is fixed.

Lemma 7.7 : *Let ρ_{AB} be a Bell-diagonal state of two qubits, whose maximal CHSH violation equals $\beta \in (2, 2\sqrt{2}]$. Then, the max-entropy of ρ_{AB} satisfies the following inequality*

$$H_{\max}(A|B) \leq -f(\beta) \tag{7.61}$$

for function f defined in Eq. (7.21). Moreover, there exists a state which saturates this inequality.

Proof. According to lemma 7.5 the max-entropy of a Bell-diagonal state of two qubits equals

$$H_{\max}(A|B) = -1 + 2\log\Big(\sum_{j=1}^{4}\sqrt{p_j}\Big). \tag{7.62}$$

Here, it is convenient to express the probabilities through the correlation coefficients c_x, c_y, c_z. Inverting Eqs. (7.32) gives

$$p_1 = \frac{1}{4}(1 + c_x - c_y + c_z), \quad p_2 = \frac{1}{4}(1 - c_x + c_y + c_z), \tag{7.63}$$

$$p_3 = \frac{1}{4}(1 + c_x + c_y - c_z), \quad p_4 = \frac{1}{4}(1 - c_x - c_y - c_z), \tag{7.64}$$

which allows us to write

$$H_{\max}(A|B) = -3 + 2\log g(c_x, c_y, c_z), \tag{7.65}$$

where

$$g(c_x, c_y, c_z) = \sqrt{1 + c_x - c_y + c_z} + \sqrt{1 - c_x + c_y + c_z} \tag{7.66}$$

$$+ \sqrt{1 + c_x + c_y - c_z} + \sqrt{1 - c_x - c_y - c_z}. \tag{7.67}$$

In the space of correlation coefficients the feasible set are the triples (c_x, c_y, c_z) for which the function $g(c_x, c_y, c_z)$ is well-defined (the expressions under the roots must be non-negative). As before, we assume without loss of generality that $|c_x| \geq |c_y| \geq |c_z|$ and $c_x, c_y \geq 0$. Then, the maximal CHSH violation (we are only interested in states that violate the CHSH inequality) is given by Eq. (7.34)

$$\beta = 2\sqrt{c_x^2 + c_y^2}.$$

Since in our case β_{AB} is fixed, the angular parametrization takes the form

$$c_x = \frac{q}{\sqrt{2}}\sin\Big(\phi + \frac{\pi}{4}\Big) \quad \text{and} \quad c_y = \frac{q}{\sqrt{2}}\cos\Big(\phi + \frac{\pi}{4}\Big),$$

where $q = \frac{\beta}{\sqrt{2}}$ and $\phi \in [0, \pi/4]$ (which ensures $c_x \geq c_y \geq 0$). Note that

$$c_x + c_y = q\cos\phi,$$
$$c_x - c_y = q\sin\phi.$$

It is easy to check that the allowed range of c_z is

$$q\sin\phi - 1 \leq c_z \leq 1 - q\cos\phi.$$

Note that we should also impose the condition $|c_z| \leq |c_y|$ but as it turns out the optimal solution will satisfy it even if we do not include it explicitly. To maximize the max-entropy it is sufficient to maximize function g defined in Eq. (7.66), which in the angular parametrization equals

$$g(\phi, c_z) = \sqrt{1 + c_z + q\sin\phi} + \sqrt{1 + c_z - q\sin\phi} \tag{7.68}$$

$$+ \sqrt{1 - c_z + q\cos\phi} + \sqrt{1 - c_z - q\cos\phi}, \tag{7.69}$$

over

$$\mathcal{R} = \big\{(\phi, c_z) : \phi \in [0, \pi/4],\ q\sin\phi - 1 \leq c_z \leq 1 - q\cos\phi\big\}. \tag{7.70}$$

The maximum is achieved either in the interior (denoted by $\mathcal{R}_{\text{int}}$) or at the boundary. Let us start by ruling out the first option. Function g is differentiable everywhere in $\mathcal{R}_{\text{int}}$ and the partial derivatives are

$$\frac{\partial g}{\partial c_z} = \frac{1}{2\sqrt{1 + c_z + q\sin\phi}} + \frac{1}{2\sqrt{1 + c_z - q\sin\phi}} \tag{7.71}$$

$$+ \frac{-1}{2\sqrt{1 - c_z + q\cos\phi}} + \frac{-1}{2\sqrt{1 - c_z - q\cos\phi}}, \tag{7.72}$$

$$\frac{\partial g}{\partial \phi} = \frac{q\cos\phi}{2\sqrt{1 + c_z + q\sin\phi}} + \frac{-q\cos\phi}{2\sqrt{1 + c_z - q\sin\phi}} \tag{7.73}$$

$$+ \frac{-q\sin\phi}{2\sqrt{1 - c_z + q\cos\phi}} + \frac{q\sin\phi}{2\sqrt{1 - c_z - q\cos\phi}}. \tag{7.74}$$

To prove that there is no maximum in the interior, it suffices to show that there is no $(\phi, c_z) \in \mathcal{R}_{\text{int}}$ such that both derivatives vanish $\frac{\partial g}{\partial c_z} = \frac{\partial g}{\partial \phi} = 0$. To do this we consider the following linear combination

$$s(\phi, c_z) = 2\sin\phi\frac{\partial g}{\partial c_z} + \frac{2}{q}\frac{\partial g}{\partial \phi} \tag{7.75}$$

$$= \frac{\sin\phi + \cos\phi}{\sqrt{1 + c_z + q\sin\phi}} + \frac{\sin\phi - \cos\phi}{\sqrt{1 + c_z - q\sin\phi}} + \frac{-2\sin\phi}{\sqrt{1 - c_z + q\cos\phi}} \tag{7.76}$$

and show that $s(\phi, c_z) = 0$ has no solution in $\mathcal{R}_{\text{int}}$. Since the last term of $s(\phi, c_z)$ is negative, a necessary condition for $s(\phi, c_z) = 0$ is that the sum of the first two terms is non-negative, which is equivalent to

$$\frac{\sin\phi + \cos\phi}{\sqrt{1 + c_z + q\sin\phi}} \geq \frac{\cos\phi - \sin\phi}{\sqrt{1 + c_z - q\sin\phi}}.$$

This can be rearranged to give

$$c_z \geq \frac{q}{2\cos\phi} - 1,$$

which contradicts the second inequality in the definition of $\mathcal{R}_{\text{int}}$ as shown below.

$$c_z \geq \frac{q}{2\cos\phi} - 1 \quad \text{and} \quad 1 - q\cos\phi > c_z \tag{7.77}$$

$$\implies 1 - q\cos\phi > \frac{q}{2\cos\phi} - 1 \iff \frac{1}{2\cos\phi} + \cos\phi < \frac{2}{q}. \tag{7.78}$$

It is easy to check that the left-hand side of the final inequality is always at least $\sqrt{2}$, while the right hand side is always at most $\sqrt{2}$. This proves that the final (strict) inequality is always false, which implies that $s(\phi, c_z) = 0$ has no solutions in $\mathcal{R}_{\text{int}}$ and that $g(\phi, c_z)$ has no maximum in $\mathcal{R}_{\text{int}}$.

The boundaries $c_z = q\sin\phi - 1$ and $c_z = 1 - q\cos\phi$ correspond to one of the expression under the roots being zero. Since the square root function has infinite slope at 0, such solutions cannot be optimal. Therefore, the maximum must be achieved at the boundary $\phi = 0$. Combining Equations (7.65) and (7.68) and setting $\phi = 0$ leads directly to the statement of the lemma.

To show that the solution of the optimization problem satisfies $|c_z| \leq |c_y|$, it is sufficient to show that for $\phi = 0$ and $c_z = -c_y = -q/2$ the partial derivative $\partial g/\partial c_z$ is strictly positive. □

7.2.2 The direct part

Here, we show (by an explicit construction) that points described by $v \in (2, 2\sqrt{2}]$ and $f(v) \leq u \leq 1$ are allowed. lemma 7.7 shows that for $v \in (2, 2\sqrt{2}]$ there exists a Bell-diagonal state of two qubits whose max-entropy equals

$$H_{\max}(A|B) = -f(v). \tag{7.79}$$

By duality (lemma 6.2), if ρ_{ABE} is an arbitrary purification, the conditional min-entropy equals

$$H_{\min}(A|E) = f(v). \tag{7.80}$$

In this example $u = f(v)$, which corresponds to a point lying precisely on the boundary defined in theorem 7.1. In order to obtain higher values of u (all the way up to 1), it suffices to apply noise of appropriate strength to subsystem E.

7.2.3 The converse part

Here, we show that every feasible point (u, v) must satisfy $u \geq f(v)$. Consider a state ρ_{ABE} for which $H_{\min}(A|E)_\rho = u$ and which for some measurements achieves the CHSH value of v. Clearly, $\beta_{\max}(\rho_{AB}) \geq v$ and by lemma 6.2 $H_{\max}(A|B)_\rho \geq -u$. Applying the symmetrization argument (lemma 7.6) gives rise to a Bell-diagonal state σ_{AB} such that $H_{\max}(A|B)_\sigma \geq -u$ and $\beta_{\max}(\sigma_{AB}) \geq v$. By lemma 7.7 these quantities must satisfy

$$H_{\max}(A|B)_\sigma \leq -f\big(\beta_{\max}(\sigma_{AB})\big), \tag{7.81}$$

which implies that

$$u \geq -H_{\max}(A|B)_\sigma \geq f\big(\beta_{\max}(\sigma_{AB})\big) \geq f(v), \tag{7.82}$$

where the last inequality follows from the fact that f is monotonically increasing.

7.3 Decoherence estimation through CHSH tests in GPTs

In this section, we are going to develop a framework for decoherence analysis in analogy to the last section, but without assuming that nature is correctly described by quantum theory. Instead, we will work in a framework that makes only minimal assumptions about the probabilistic structure of measurements. This allows to make statements in cases where quantum theory might not be a correct description of nature.

In section 7.3.1, we define a framework for probabilistic theories that has become a standard one in the literature. Besides defining the core structure in, we explain how we extend this framework to make it suitable for analyzing tripartite states, in a way that allows us to make a decoherence analysis that is analogous to the quantum case.

In section 7.3.2, we will define a decoherence quantity $\mathrm{Dec}(A|E)_\omega$ for GPTs as an analogue of the quantum min-entropy $H_{\min}(A|E)_\rho$. This will be our quantity of interest for the decoherence analysis for GPTs. We will first motivate an expression for $\mathrm{Dec}(A|E)_\omega$, analogous to equation (7.2) for quantum theory. This expression will require us to define what a maximally entangled state in a GPT is.

Section 7.3.3 is devoted to finding a bound on our decoherence quantity in terms of the CHSH winning probability for Alice and Bob (which is a quantity directly related to the CHSH parameter β_{AB}). This bound allows us to infer non-trivial statements about decoherence from measured data when, apart from the iid assumption, we assume only very little about the behavior of nature. We approach our bound by first bounding our fidelity-based decoherence quantity by a trace distance-based quantity. We will then bound this trace distance-based quantity in terms of the CHSH winning probability for Alice and Bob by a quantity that can be expressed as a linear program.

Finally, in section 7.3.4, we show how our bound can be expressed as a linear program and present the numerical results. This is followed by a discussion of the physical interpretation of our numerical findings.

7.3.1 The framework

A basic framework for GPTs

Frameworks for probabilistic theories in which quantum theory and classical theory can be formulated as special cases have already been considered some decades ago [Mac93; Edw70; DL70]. After some period of oblivion, a seminal paper by Hardy [Har01] caused a revival in the interest in such frameworks (see, for example, [MM11a; Mas+12; CDP11; DB11; Udu12; PW13] and references therein). Today, they are generally referred to as frameworks for *generalized probabilistic theories* [Bar07].

We formalize our decoherence analysis for GPTs in the *abstract state space* framework [BW09; Bar+08; BGW09; BW11]. It is one rigorous formalization of what a generalized probabilistic theory is, amongst a few equivalent or closely related ones that can be found in the literature (see the references cited

above). We prefer it for its concise and precise formulation. For the sake of brevity, we will not go far beyond the mere mathematical definitions related to abstract state spaces here. For a detailed introduction to abstract state spaces, see [Pfi12].

Definition 7.8 : *An* ***abstract state space*** *is a triple* (V, V^+, u)*, where* V *is a finite- dimensional real vector space,* V^+ *is a cone*[3] *in* V *which is closed*[4] *and generating*[5] *and* $u \in V^*$ *is a linear functional*[6] *on* V *such that* $u(\omega) > 0$ *for all* $\omega \in V^+ \setminus \{0\}$*. The functional* u *is called the* ***unit effect****.*

Definition 7.9 : *For an abstract state space* (V, V^+, u)*, we define the following induced structure (see figure 7.6):*
The ***normalized states*** *are the elements of the set*[7]

$$\Omega := \{\omega \in V^+ \mid u(\omega) = 1\}\,. \tag{7.83}$$

The ***subnormalized states*** *are the elements of the set*

$$\Omega^{\leq} := \{\omega \in V^+ \mid u(\omega) \leq 1\}\,. \tag{7.84}$$

The ***effects*** *are the elements of the set*

$$\mathcal{E} := \{e \in V^* \mid 0 \leq e(\omega) \leq 1 \ \forall \omega \in \Omega\}\,. \tag{7.85}$$

The ***measurements*** *are the elements of the set*

$$\mathcal{M} := \left\{ M \subseteq \mathcal{E} \text{ finite} \,\middle|\, \sum_{e \in M} e = u \right\}\,. \tag{7.86}$$

An effect represents a measurement outcome. If a system in a state ω is measured with respect to a measurement $M = \{e_1, \ldots, e_n\}$, then $e_k(\omega)$ is the probability that the measurement yields the outcome associated with e_k.

Example 7.10 (Quantum theory): *The probabilistic structure of measurements on a (finite-dimensional) quantum system can be formulated as an abstract state space. For a quantum system with an associated Hilbert space* $\mathcal{H}$*, consider the abstract state space*

$$(V, V^+, u) = (\mathrm{Herm}(\mathcal{H}), \mathrm{Pos}(\mathcal{H}), \mathrm{tr})\,, \tag{7.87}$$

[3] A subset $V^+ \subseteq V$ is a *cone* in V if

(C1) $V^+ + V^+ \subseteq V^+$,

(C2) $\alpha V^+ \subseteq V^+$ for all $\alpha \geq 0$,

(C3) $V^+ \cap (-V^+) = \{0\}$,

[4] We assume the standard topology on V, i.e. the only linear Hausdorff topology on V.

[5] A cone $V^+ \subseteq V$ is *generating* if $V^+ - V^+ = V$.

[6] For a finite-dimensional vector space V, we denote by V^* the dual space of V, i.e. the vector space of linear functionals on V.

[7] Unfortunately, using the letter Ω here produces a notation clash: we have already used this symbol to denote sample spaces of probability spaces (see chapter 2). However, in both cases, the use of the letter Ω is a strongly established standard that we want to comply with. In this chapter, Ω will always refer to the set of states of an abstract state space, so there should not be any confusion.

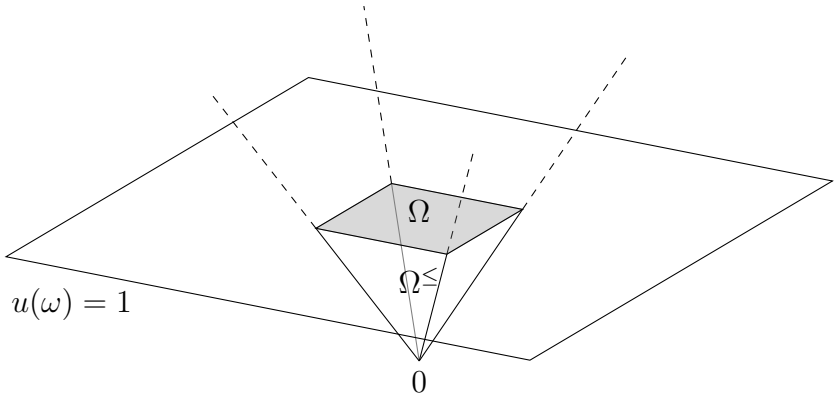


Figure 7.6: Visualization of an abstract state space. The set V^+ is a cone in a vector space V, here shown as a cone with a square base. The normalized states Ω are given by the intersection of V^+ with the plane on which the functional u takes the value 1. The set $\Omega^{\leq}$ consists of those elements of V^+ on which the functional u takes values between 0 and 1.

where $V = \mathrm{Herm}(\mathcal{H})$ is the real vector space of Hermitian operators on $\mathcal{H}$, $V^+ = \mathrm{Pos}(\mathcal{H})$ is the cone of positive operators on $\mathcal{H}$ and $u = \mathrm{tr}$ is the trace on $\mathcal{H}$. According to definition 7.9, this yields the states

$$\Omega = \{\rho \in \mathrm{Pos}(\mathcal{H}) \mid \mathrm{tr}(\rho) = 1\}\,, \tag{7.88}$$

which are precisely the density operators on $\mathcal{H}$. Analogously, $\Omega^{\leq}$ are the subnormalized density operators. The effects are the functionals induced by POVM elements via the trace,

$$\mathcal{E} = \{\mathrm{tr}(P\,\cdot\,) \mid P \in \mathrm{Pos}(\mathcal{H}), P \leq \mathbb{1}_{\mathcal{H}}\}k,\,. \tag{7.89}$$

Accordingly, the measurements are the sets of functionals that are induced by POVMs,

$$\mathcal{M} = \Big\{\{\mathrm{tr}(P_k\,\cdot\,) \mid P_k \in \{P_k\}_k\} \mid \{P_k\}_k \text{ is a POVM}\Big\}\,. \tag{7.90}$$

This precisely reproduces the structure of measurement statistics in quantum theory. For further details, see [Pfi12]. ■

By our definition, $\mathcal{E}$ is the set of *all* linear functionals e such that $0 \leq e(\omega) \leq 1$ for all $\omega \in \Omega$. The underlying assumption that every such linear functional represents a physical measurement outcome has been called the *no-restriction hypothesis* [Udu12]. A priori, there seems to be no immediate physical reason for this assumption, and some authors have argued about how to weaken this assumption [JL13]. For our purposes here, it is not relevant whether the no-restriction hypothesis holds, and weakening the assumption complicates the definitions. Thus, we assume it for simplicity.

In section 7.3.2, we will define a decoherence quantity $\mathrm{Dec}(A|E)_\omega$ analogous to the corresponding quantity in quantum theory, expression (7.2). It involves the fidelity as a measure of closeness of quantum states. Therefore, it is desirable to have a generalization of the fidelity to states in abstract state

spaces. Looking at the expression definition 3.14, there seems to be no obvious generalization. However, as we have seen in proposition 3.16, the fidelity can be expressed as the classical fidelity of the probability distribution over the outcomes of a measurement, minimized over all measurements. This motivates us to define the fidelity for abstract state spaces as follows.

Definition 7.11 : *Let (V, V^+, u) be an abstract state space with normalized states Ω and measurements $\mathcal{M}$. For states $\omega, \tau \in \Omega$, we define the* ***fidelity*** *of ω and τ as*

$$F(\omega, \tau) := \inf_{M \in \mathcal{M}} b(\omega, \tau | M)\,, \quad \text{where} \quad b(\omega, \tau | M) = \sum_{e \in M} \sqrt{e(\omega)}\sqrt{e(\tau)}\,. \tag{7.91}$$

The quantity $b(\omega, \tau|M)$ is the ***Bhattacharyya coefficient*** *(or sometimes called the classical fidelity) of the probability distributions that the measurement M induces on the states ω and τ.*

The fidelity as defined in definition 7.11 precisely reduces to the quantum fidelity in the case where the abstract state space is a quantum state space.

In addition to the fidelity, in section 7.3.3 we will also consider a generalization of the quantum trace distance $D(\rho, \sigma) = \frac{1}{2}\mathrm{tr}|\rho - \sigma|$ in order to formulate a bound on $\mathrm{Dec}(A|E)_\omega$. Again, proposition 3.16 tells us how to generalize it to abstract state spaces, motivating the following definition.

Definition 7.12 : *Let (V, V^+, u) be an abstract state space with normalized states Ω and measurements $\mathcal{M}$. For states $\omega, \tau \in \Omega$, the* ***trace distance*** *between ω and τ is given by*

$$D(\omega, \tau) := \sup_{M \in \mathcal{M}} d(\omega, \tau | M)\,, \quad \text{where} \quad d(\omega, \tau | M) = \frac{1}{2} \sum_{e \in M} |e(\omega) - e(\tau)| \tag{7.92}$$

The quantity $d(\omega, \tau|M)$ is the ***total variation distance*** *(or sometimes called the classical trace distance) between the probability distributions that the measurement M induces on the states ω and τ.*

Note that the fidelity and the trace distance take values between 0 and 1 for all states. For squares of the quantities F, b, D and d, we will write the square sign right after the letter, e.g. we will write $F^2(\omega, \tau)$ instead of $(F(\omega, \tau))^2$.

A tripartite framework for GPTs

In section 7.3.2, we will consider a tripartite situation for the decoherence analysis. This requires us to model a tripartite scenario mathematically since such a structure is not induced by an abstract state space (V, V^+, u) alone. We need to specify it as additional structure. Our goal here is to do this with the weakest possible assumptions, resulting in a very general validity of the bounds we derive.

Instead of assuming individual state spaces for every party, we only consider their overall combined state space, modeled by an abstract state space (V, V^+, u) and all its induced structure as in definitions 7.8 and 7.9. This has the advantage that we do not have to make assumptions about how individual state spaces combine to multipartite state spaces, keeping our assumptions

weak. For our purposes, the only structure that we need to add to an abstract state space (V, V^+, u) to make it suitable for the description of a tripartite scenario are the local transformations that each individual party can perform. The local measurements of the three parties are then induced by these local transformations.

We consider three parties, which we call Alice (A), Bob (B) and Eve (E) as before. We begin our considerations by assuming that there are three sets $\mathcal{T}_A$, $\mathcal{T}_B$ and $\mathcal{T}_E$, containing all the transformations that Alice, Bob and Eve can perform, respectively. By a transformation, we mean a linear map $T : V \to V$ which maps states to subnormalized states, i.e. $T(\Omega) \subseteq \Omega^{\leq}$ (or, equivalently, $T(V^+) \subseteq V^+$ and $(u \circ T)(\omega) \leq u(\omega)$ for all $\omega \in V^+$). We can consider the case where several transformations are applied because compositions of transformations are transformations again: If T, T' are linear maps $V \to V$ which map Ω inside $\Omega^{\leq}$, then the same is true for the composition $T \circ T'$ (we denote the composition of maps by a $\circ$ symbol).

We assume that the three parties act individually at spatially separated locations. Relativistic considerations lead to the consistency requirement that transformations performed by different parties must commute, e.g. if Alice performs a transformation $T_A \in \mathcal{T}_A$ and Bob performs a transformation $T_B \in \mathcal{T}_B$, then the total transformation must satisfy $T_A \circ T_B = T_B \circ T_A$.

For our purposes, we do not need to specify the sets $\mathcal{T}_A$, $\mathcal{T}_B$ and $\mathcal{T}_E$ any further; the only requirement is that transformations of distinct parties commute. The sets $\mathcal{T}_A$, $\mathcal{T}_B$ and $\mathcal{T}_E$ *define* the systems A, B and E, i.e. we define the individual parties via the transformations that they can perform. This leads us to the following definition.

Definition 7.13 : *A **tripartite scenario** is a quadruplet*

$$S_{ABE} = ((V, V^+, u), \mathcal{T}_A, \mathcal{T}_B, \mathcal{T}_E)\,, \tag{7.93}$$

where (V, V^+, u) is an abstract state space, and where

$$\mathcal{T}_A, \mathcal{T}_B, \mathcal{T}_E \subseteq \left\{ T : V \to V \text{ linear} \;\middle|\; T(\Omega) \subseteq \Omega^{\leq} \right\} \tag{7.94}$$

*are such that for all $P, P' \in \{A, B, E\}$ with $P \neq P'$, it holds that $T_P \circ T_{P'} = T_{P'} \circ T_P$ for all $T_P \in \mathcal{T}_P$ and for all $T_{P'} \in \mathcal{T}_{P'}$. We call the elements of $\mathcal{T}_A$, $\mathcal{T}_B$ and $\mathcal{T}_E$ the **local transformations** of A, B and E, respectively.*

It is absolutely natural to define tripartite scenarios via commuting transformations rather than via a tensor product structure. In quantum theory, the two approaches are equivalent in finite dimensions (we will talk about this below). In more general infinite-dimensional cases, where it is not known whether the two approaches are equivalent, things are usually formalized in a commutative way rather than via tensor products (see [SW87], for example). Knowing about the equivalence in finite dimensions, we will formulate some quantum examples in the tensor product structure below.

Example 7.14 (A tripartite quantum scenario): *One can formulate a tripartite situation in quantum theory as a* tripartite scenario. *Based on*

example 7.10, consider the tripartite scenario

$$((\mathrm{Herm}(\mathcal{H}), \mathrm{Pos}(\mathcal{H}), \mathrm{tr}), \mathcal{T}_A, \mathcal{T}_B, \mathcal{T}_E)\,, \quad \textit{where} \tag{7.95}$$

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E\,, \tag{7.96}$$

$$\mathcal{T}_A = \{\mathcal{R}_A \otimes \mathbb{1}_B \otimes \mathbb{1}_E \mid \mathcal{R}_A \textit{ is a trace non-increasing CPM on } \mathrm{Herm}(\mathcal{H}_A)\}\,, \tag{7.97}$$

$$\mathcal{T}_B = \{\mathbb{1}_A \otimes \mathcal{R}_B \otimes \mathbb{1}_E \mid \mathcal{R}_B \textit{ is a trace non-increasing CPM on } \mathrm{Herm}(\mathcal{H}_B)\}\,, \tag{7.98}$$

$$\mathcal{T}_E = \{\mathbb{1}_A \otimes \mathbb{1}_B \otimes \mathcal{R}_E \mid \mathcal{R}_E \textit{ is a trace non-increasing CPM on } \mathrm{Herm}(\mathcal{H}_E)\}\,, \tag{7.99}$$

where CPM stands for completely positive map*. Having tensor product form, the local transformations of different parties commute.* ■

For our purposes, definition 7.13 is all the structure one needs to specify. The local measurements are induced by the local transformations. We formalize this via the notion of a local *instrument* [DL70]. To get an intuition for what an instrument is, consider a Stern-Gerlach experiment. A spin-1/2 particle enters a magnet and undergoes one of two transformations: It either gets deflected upwards or downwards. Which of the two transformations it undergoes is determined probabilistically. Then it hits a screen, which reveals which of the two transformations the particle has undergone. This way, a measurement has been performed in two stages: a probabilistic application of a transformation and a detection. The sum of the probabilities of detecting the particle at the top or the bottom of the screen is one. If the state of the particle is described by a state $\omega \in \Omega$ of an abstract state space, we may model this by a set of two transformations $\{T_{\mathrm{up}}, T_{\mathrm{down}}\}$. Such a set is an instrument. The norm $u(T_{\mathrm{up}}(\omega))$ is the probability that the particle is deflected upwards, and likewise for $u(T_{\mathrm{down}}(\omega))$. Thus, u can be seen to play the role of the screen, detecting the particle. The requirement that the particle must undergo one of the two deflections reads $u \circ T_{\mathrm{up}} + u \circ T_{\mathrm{down}} = u$. The transformation T_{up} is the analogue of the transformation $\rho \mapsto P_{\mathrm{up}} \rho P_{\mathrm{up}}$ in quantum theory, where P_{up} is the projector onto the spin-up state. Since u is given by the trace in quantum theory, the probability for the upward-deflection to occur is given by $\mathrm{tr}(P_{\mathrm{up}} \rho P_{\mathrm{up}}) = \mathrm{tr}(P_{\mathrm{up}} \rho)$, which is precisely the Born rule.

A *local* instrument is such a set of transformations where all the transformations are the *local* transformations of one party. This motivates the following definition.

Definition 7.15 (Local instruments): *For a tripartite scenario*

$$S_{ABE} = ((V, V^+, u), \mathcal{T}_A, \mathcal{T}_B, \mathcal{T}_E) \tag{7.100}$$

with Ω as defined in definition 7.9, we define the ***local instruments*** *as the elements of*

$$\mathcal{I}_P := \left\{ I_P \subseteq \mathcal{T}_P \ \textit{finite} \;\middle|\; \sum_{T_P \in I_P} u \circ T_P = u \right\} \quad \textit{for } P \in \{A, B, E\}\,. \tag{7.101}$$

Example 7.16 (Local instruments in a tripartite quantum scenario): *Considering the tripartite scenario of example 7.14, we get that the local instruments are given by*

$$\mathcal{I}_P = \left\{ I_P \subseteq \mathcal{T}_P \;\middle|\; \sum_{T_P \in I_P} T_P \text{ is a TPCPM} \right\} \quad \text{for } P \in \{A, B, E\}\,. \qquad \blacksquare$$

Remark 7.17 (Local measurements)**:** The definition of local instruments gives us a notion of local measurements as well. Consider a tripartite scenario $S_{ABE} = ((V, V^+, u), \mathcal{T}_A, \mathcal{T}_B, \mathcal{T}_E)$ with its set of measurements $\mathcal{M}$. It is easily verified that for a local transformation $T_A \in \mathcal{T}_A$, the map $u \circ T_A$ is an effect (as defined in definition 7.9). Likewise, for a local instrument $I_A \in \mathcal{I}_A$, the set $\{u \circ T_A \mid T_A \in I_A\}$ is a measurement. We interpret it as a measurement performed by Alice. We can also consider composite measurements where several parties locally perform measurements. For local instruments $I_A \in \mathcal{I}_A$ and $I_B \in \mathcal{I}_B$, for example, the set $\{u \circ T_A \circ T_B \mid T_A \in I_A, T_B \in I_B\}$ is a measurement. We interpret it as a composite measurement where Alice and Bob each perform local measurements, described by I_A and I_B. The analogous holds for other parties and combinations thereof.

Example 7.18 (Local measurements in a tripartite quantum scenario): *Based on examples 7.14 and 7.16, we can say how local measurements look like in a tripartite quantum scenario. A local effect of Alice is of the form*

$$\rho_{ABE} \mapsto \operatorname{tr}(\mathcal{R}_A \otimes \mathbb{1}_B \otimes \mathbb{1}_E(\rho_{ABE})) \tag{7.102}$$

for a trace non-increasing CPM $\mathcal{R}_A$ on $\operatorname{Herm}(\mathcal{H}_A)$. However, for every such CPM, there is a POVM element P_A on $\mathcal{H}_A$ such that[8]

$$\operatorname{tr}((P_A \otimes \mathbb{1}_B \otimes \mathbb{1}_E)\rho_{ABE}) = \operatorname{tr}(\mathcal{R}_A \otimes \mathbb{1}_B \otimes \mathbb{1}_E(\rho_{ABE}))\,. \tag{7.103}$$

This recovers the Born rule. Analogously, a composite measurement where Alice and Bob each perform local measurements consists of local effects of the form

$$\rho_{ABE} \mapsto \operatorname{tr}(\mathcal{R}_A \otimes \mathcal{R}_B \otimes \mathbb{1}_E(\rho_{ABE})) = \operatorname{tr}((P_A \otimes P_B \otimes \mathbb{1}_E)\rho_{ABE}) \tag{7.104}$$

for POVM elements P_A, P_B on $\mathcal{H}_A$, $\mathcal{H}_B$. Thus, in our tripartite quantum example, local measurements reduce to POVM measurements of product form. $\blacksquare$

In examples 7.14, 7.16 and 7.18, instead of choosing a tensor factorization for $\mathcal{H}$ and setting the local transformations to be acting non-trivially on one tensor factor, we could have chosen sets of transformations that merely commute, without a tensor product structure. The question of whether the resulting measurement statistics in that case would be different from the case with the tensor factor structure is known as *Tsirelson's problem* [SW08; Doh+08]. More precisely, the question is the following. Let $\mathcal{H}$ be a Hilbert space, let ρ be a density operator on $\mathcal{H}$, let $\{P_k\}_k$, $\{Q_l\}_l$ be POVMs on $\mathcal{H}$ such that

[8] This can be seen from the Kraus representation of $\mathcal{R}_A$: $\operatorname{tr}(\mathcal{R}_A(\rho_A)) = \operatorname{tr}(\sum_k F_k \rho_A F_k^\dagger) = \operatorname{tr}(\sum_k F_k^\dagger F_k \rho_A) = \operatorname{tr}(P_A \rho_A)$ for $P_A = \sum_k F_k^\dagger F_k$. (We omitted the other tensor factors for brevity.)

$P_k Q_l = Q_l P_k$ for all k, l. Tsirelson's problem is: Does there necessarily exist Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$, a density operator σ on $\mathcal{H}_A \otimes \mathcal{H}_B$ and POVMs $\{R_k\}_k$ on $\mathcal{H}_A$ and $\{S_l\}_l$ on $\mathcal{H}_B$ such that $\mathrm{tr}(P_k Q_l \rho) = \mathrm{tr}((R_k \otimes S_l)\sigma)$ for all k, l? In the case where $\mathcal{H}$ is finite-dimensional, the answer is known to be affirmative. For infinite-dimensional Hilbert spaces, the answer is still unknown.

Thus, for finite-dimensional quantum systems, we can restrict ourselves to the case with the tensor product structure without loss of generality. For abstract state spaces, however, an analogous restriction might cause a loss of generality. The advantage of our weak definition of a tripartite scenario is that we do not need to know the answer to an equivalent of Tsirelson's problem for generalized probabilistic theories. The downside is that it makes defining an equivalent of the min-entropy more difficult. We will deal with this issue in the next subsection.

Notation : *From now on, whenever we speak of a tripartite scenario S_{ABE}, we implicitly assume that all its parts and induced structures are denoted as in definitions 7.8, 7.9, 7.13 and 7.15 without restating it, i.e. instead of writing "Let $S_{ABE} = ((V, V^+, u), \mathcal{T}_A, \mathcal{T}_B, \mathcal{T}_E)$ be a tripartite scenario, let Ω be its set of normalized states, ...", we will only write "Let S_{ABE} be a tripartite scenario".*

7.3.2 A decoherence quantity for GPTs

Motivation of an expression that quantifies decoherence

We are now going to motivate an expression for the central quantity $\mathrm{Dec}(A|E)_\omega$ for our decoherence analysis for GPTs. We take our inspiration from equation (7.2) for the quantum version of the quantity, which we repeat here for the reader's convenience:

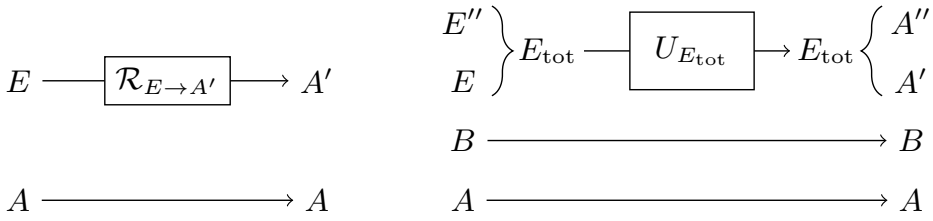
$$\mathrm{Dec}(A|E)_\rho = \max_{\mathcal{R}_{E\to A'}} F^2(|\Phi\rangle\langle\Phi|_{AA'}, \mathbb{1}_A \otimes \mathcal{R}_{E\to A'}(\rho_{AE}))\,. \tag{7.105}$$

There are two issues that prevent us from directly translating expression (7.105) into our framework. The first issue is that in section 7.3.1, to keep our framework as general as possible, we have defined a tripartite scenario with an overall state space (V, V^+, u) with tripartite states Ω. We do not have notions of individual state spaces at hand. Thus, we do not have an analogue of a reduced state ρ_{AE} or of a transformation $\mathcal{R}_{E\to A'}$ from one state space to another.

The second issue is that we do not know what the analogue of a maximally entangled state $\Phi_{AA'}$ in our framework is. We resolve the first issue here, arriving at an expression for $\mathrm{Dec}(A|E)_\omega$. In the next subsection we will then define what a maximally entangled state is in our framework.

Expression (7.105), which involves the state ρ_{AE} and TPCPMs $\mathcal{R}_{E\to A'}$, can be transformed to an expression in which both the state and the TPCPMs are purified (see figure 7.7). This expression will be our motivation for the expression for $\mathrm{Dec}(A|E)_\omega$. The maximization over TPCPMs from E to A' is replaced by a maximization over unitaries from EE'' to $A'A''$, where E'' and A'' are ancilla systems extending system E and A', respectively. This is precisely the purification (or Stinespring dilation) of a channel. Since systems EE'' and

$A'A''$ have the same dimension, we can identify their Hilbert spaces and regard the resulting Hilbert space as the Hilbert space of a system E_{tot}. This system involves all subsystems that the third party needs to control in order to bring itself as close as possible to maximal entanglement with Alice. Since $U_{E_{\text{tot}}}$ is a transformation on system E_{tot} alone, we can translate it into our generalized framework.



(a) Unpurified situation (b) Purified situation

Figure 7.7: Purification of equation (7.105). Part (a) shows the system and maps involved in expression (7.105) for the quantum min-entropy. In expression (7.106), we purify this situation, as shown in (b), to arrive at a situation with three parties A, B and E_{tot}, and with a map $U_{E_{\text{tot}}}$ which acts on one system E_{tot} alone rather than mapping from one system to another.

The state ρ_{AE} is replaced by a purification ρ_{ABE}. We choose the purifying system B to be the channel's output system, which gives us the overall picture of our decoherence analysis as shown in figure 7.8.

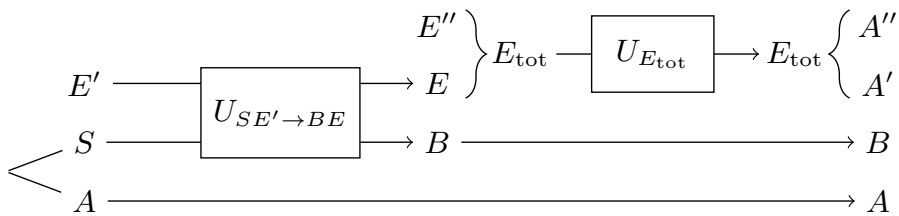


Figure 7.8: Overall picture of our decoherence analysis for GPTs. Since the purifying system B in expression (7.106) is not specified, we can choose it such that it fits our situation for the decoherence analysis.

The following lemma gives a precise formulation of the purification of expression (7.105). It can be proved using purification and Stinespring dilation.

Lemma 7.19 : *Let $\mathcal{H}_A$, $\mathcal{H}_E$ be finite-dimensional Hilbert spaces of dimensions d_A, d_E, respectively, let $\rho_{AE} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_E)$. Then, for any purification $\rho_{ABE} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$ of ρ_{AE}, any Hilbert spaces $\mathcal{H}_{A'}$, $\mathcal{H}_{A''}$ and $\mathcal{H}_{E''}$ of dimension $d_{A'} = d_A$, $d_{A''} = d_A d_E$ and $d_{E''} = d_A^2$, respectively, any maximally entangled state $\Phi_{AA'} \in \Gamma_{AA'}$ and any pure state $|0\rangle\langle 0|_{E''} \in \mathcal{S}(\mathcal{H}_{E''})$, it holds that*

$$\begin{aligned} &H_{\min}(A|E)_\rho \\ &\quad = -\log d_A \max_{U_{E_{tot}}} \max_{\sigma_{BA''}} F^2(\Phi_{AA'} \otimes \sigma_{BA''}, (\mathbb{1}_{AB} \otimes U_{E_{tot}})\rho_{ABE_{tot}}(\mathbb{1}_{AB} \otimes U_{E_{tot}}^\dagger)) \,, \end{aligned} \tag{7.106}$$

where $\rho_{ABE_{\text{tot}}} = \rho_{ABE} \otimes |0\rangle\langle 0|_{E''}$ *and where the first maximization ranges over unitaries*

$$U_{E_{\text{tot}}} : \mathcal{H}_E \otimes \mathcal{H}_{E''} \to \mathcal{H}_{A'} \otimes \mathcal{H}_{A''}\,, \quad \text{where } \mathcal{H}_{A'} \otimes \mathcal{H}_{A''} \simeq \mathcal{H}_E \otimes \mathcal{H}_{E''} =: \mathcal{H}_{E_{\text{tot}}} \tag{7.107}$$

and the second maximization ranges over pure states $\sigma_{BA''} \in \mathcal{S}(\mathcal{H}_B \otimes \mathcal{H}_{A''})$.

Now we translate expression (7.106) into our generalized framework. We interpret the system E_{tot} as the system controlled by Eve, and therefore rename $E_{\text{tot}} \to E$.

- We replace the maximization over all unitaries $U_{E_{\text{tot}}}$ acting on system E_{tot} by a supremum[9] over all local transformations $T_E \in \mathcal{T}_E$.[10]

- We generalize the quantum fidelity to the fidelity in abstract state spaces as defined in definition 7.11.

- We replace the state $\rho_{ABE_{\text{tot}}} = \rho_{ABE} \otimes |0\rangle\langle 0|_{E''}$ by a state $\omega \in \Omega$.

- If we look at the state $\Phi_{AA'} \otimes \sigma_{BA''}$, we see that it is a state of maximal entanglement between Alice (A) and Eve ($A'A''$) in the sense that by performing measurements with elements of the form $P_A \otimes P_{A'} \otimes \mathbb{1}_B \otimes \mathbb{1}_{A''}$, they can get any statistics that two parties A and A' would be able to get by performing local measurements on the maximally entangled state $\Phi_{AA'}$. We translate this into our framework by assuming that there is a set Ψ_{AE} of "states with maximal correlation between Alice and Eve". Instead of minimizing over states $\Phi_{AA'} \otimes \sigma_{BA''}$, we then minimize over the set Ψ_{AE}.

We postpone the discussion of how such a set Ψ_{AE} looks like. We will give a definition of such a set in the next subsection. For now, we write down an expression for our decoherence quantity $\text{Dec}(A|E)_\omega$ that depends on the choice of such a set $\Psi_{AE} \subseteq \Omega$. According to what we have just discussed, the expression is

$$\sup_{T_E \in \mathcal{T}_E} \sup_{\psi \in \Psi_{AE}} F^2(\psi, T_E(\omega))\,. \tag{7.108}$$

We interpret the decoherence to be high when this quantity is high and vice versa, which is the opposite of $H_{\min}(A|E)_\rho$. Before we can define $\text{Dec}(A|E)_\omega$, however, we need to specify what a maximally entangled state in a GPT is.

[9] We do not assume enough about $\mathcal{T}_E$ to guarantee that the maximum is achieved, so we replace it by a supremum.

[10] One might raise the objection that in the quantum case, example 7.14, the unitaries only correspond to those elements of $\mathcal{T}_E$ which bijectively map the space of density operators onto itself. It would be possible to include this restriction, but we decide not to do so, for two reason: We want to keep things simple, and we want to avoid the assumption that actions that the third party can perform can be purified as in the quantum case.

Definition of maximal correlation in GPTs

The expression (7.108) for our decoherence quantity $\mathrm{Dec}(A|E)_\omega$ contains a maximization over a set $\Psi_{AE} \subseteq \Omega$ which we interpret to be the set of states with maximal correlation between Alice and Eve. We now define this set.

Definition 7.20 : *For a tripartite scenario S_{ABE}, we define the set Ψ_{AE} of* ***states with maximal correlation*** *between Alice and Eve by*

$$\Psi_{AE} := \left\{ \psi \in \Omega \;\middle|\; \begin{array}{l} \text{For every binary local instrument } I_A = \{T_A^0, T_A^1\} \in \mathcal{I}_A, \\ \text{there is a binary local instrument } I_E = \{T_E^0, T_E^1\} \in \mathcal{I}_E \\ \text{such that } (u \circ T_A^0 \circ T_E^0)(\psi) + (u \circ T_A^1 \circ T_E^1)(\psi) = 1. \end{array} \right\} . \tag{7.109}$$

Definition 7.20 can be read as follows. The superscripts 0 and 1 of the elements of the instruments I_A and I_E stand for measurement outcomes, so $(u \circ T_A^0 \circ T_E^0)(\psi)$ or $(u \circ T_A^1 \circ T_E^1)(\psi)$ is the probability that Alice and Eve both get outcome 0 or both get outcome 1, respectively, when they measure with respect to I_A, I_E, respectively. Thus, the sum of these probabilities is the probability that Alice's and Eve's measurement outcomes are perfectly correlated. This means that for a state $\psi \in \Psi_{AE}$, it holds that for every binary measurement of Alice, there is a binary measurement for Eve such that their measurement outcomes are perfectly correlated.

A closer look at some subtleties is advisable here, both to avoid confusion and to see the advantages of the weak assumptions that define our framework. With reference to example 7.18, one may point out that the set

$$\left\{ \sigma \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E) \;\middle|\; \begin{array}{l} \text{For every binary POVM } \{P_A^0, P_A^1\} \text{ on } \mathcal{H}_A, \text{ there} \\ \text{is a binary POVM } \{P_E^0, P_E^1\} \text{ on } \mathcal{H}_E \text{ such that} \\ \\ \mathrm{tr}((P_A^0 \otimes \mathbb{1}_B \otimes P_E^0)\sigma) + \mathrm{tr}((P_A^1 \otimes \mathbb{1}_B \otimes P_E^1)\sigma) = 1 . \end{array} \right\} \tag{7.110}$$

is empty. This may seem to make our definition of Ψ_{AE} incompatible with quantum theory. Note, however, that the set

$$\left\{ \sigma \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E) \;\middle|\; \begin{array}{l} \text{For every binary projective measurement} \\ \{P_A^0, P_A^1\} \text{ on } \mathcal{H}_A, \text{ there is a binary projective} \\ \text{measurement } \{P_E^0, P_E^1\} \text{ on } \mathcal{H}_E \text{ such that} \\ \\ \mathrm{tr}((P_A^0 \otimes \mathbb{1}_B \otimes P_E^0)\sigma) + \mathrm{tr}((P_A^1 \otimes \mathbb{1}_B \otimes P_E^1)\sigma) = 1 . \end{array} \right\} \tag{7.111}$$

is not empty as long as $\dim \mathcal{H}_E \geq \dim \mathcal{H}_A$. If, as above, $\mathcal{H}_E = \mathcal{H}_{A'} \otimes \mathcal{H}_{A''}$ with $\mathcal{H}_{A'} \simeq \mathcal{H}_A$, then this set contains all the states of the form $\Phi_{AA'} \otimes \sigma_{BA''}$ with $\Phi_{AA'} \in \Gamma_{AA'}$ as in (7.106). The advantage of our weak definition of the local transformations is that it does not force to see $\mathcal{T}_A$ as the analogue of the set of *all* CPMs of the form $\mathcal{R}_A \otimes \mathbb{1}_B \otimes \mathbb{1}_E$, but that it can be considered to be the analogue of all such CPMs which induce a functional of the form $\sigma \mapsto \mathrm{tr}(P\sigma)$, where P is a projector. example 7.18 can be modified accordingly

(see example 7.22 below). This makes our definition of Ψ_{AE} compatible with quantum theory.

With definition 7.20 at hand, we are finally ready to define the decoherence quantity.

Definition 7.21 : *Let S_{ABE} be a tripartite scenario, let $\omega \in \Omega$. We define the* ***decoherence quantity*** *of ω by*

$$\mathrm{Dec}(A|E)_\omega := \sup_{T_E \in \mathcal{T}_E} \sup_{\psi \in \Psi_{AE}} F^2(\psi, T_E(\omega)) \tag{7.112}$$

Example 7.22 : *We consider a special case of a tripartite scenario in quantum theory. Consider*

$$((\mathrm{Herm}(\mathcal{H}), \mathrm{Pos}(\mathcal{H}), \mathrm{tr}), \mathcal{T}_A, \mathcal{T}_B, \mathcal{T}_E)\,, \quad \textit{where} \tag{7.113}$$

$$\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E \tag{7.114}$$

$$\mathcal{T}_A = \left\{ \mathcal{R}_A \otimes \mathbb{1}_B \otimes \mathbb{1}_E \;\middle|\; \begin{array}{l} \mathcal{R}_A \text{ is a trace non-increasing CPM on} \\ \mathrm{Herm}(\mathcal{H}_A) \text{ such that there is a projector } P_A \\ \text{on } \mathcal{H}_A \text{ with } \mathrm{tr}(P_A\rho_A) = \mathrm{tr}(\mathcal{R}_A(\rho_A)) \text{ for all} \\ \rho_A \in \mathcal{S}(\mathcal{H}_A) \end{array} \right\}, \tag{7.115}$$

and analogously for $\mathcal{T}_B$ and $\mathcal{T}_E$. In addition, we assume for simplicity that $\mathcal{H}_A \simeq \mathcal{H}_E$. In this case,

$$\Psi_{AE} = \left\{ \sigma \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E) \;\middle|\; \begin{array}{l} \text{For every binary projective measure-} \\ \text{ment } \{P_A^0, P_A^1\} \text{ on } \mathcal{H}_A, \text{ there is a bi-} \\ \text{nary projective measurement } \{P_E^0, P_E^1\} \\ \text{on } \mathcal{H}_E \text{ such that} \\ \qquad \mathrm{tr}((P_A^0 \otimes \mathbb{1}_B \otimes P_E^0)\sigma) \\ \qquad + \mathrm{tr}((P_A^1 \otimes \mathbb{1}_B \otimes P_E^1)\sigma) = 1\,. \end{array} \right\} \tag{7.116}$$

$$= \{\Phi_{AE} \otimes \sigma_B \mid \Phi_{AE} \in \Gamma_{AE}\,,\ \sigma_B \in \mathcal{S}(\mathcal{H}_B)\}\,, \tag{7.117}$$

where Γ_{AE} is the set of maximally entangled states on $\mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_E)$. For a pure state $\rho_{ABE} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E)$, this gives us

$$\mathrm{Dec}(A|E)_\rho = \max_{\mathcal{R}_E} \max_{\Phi_{AE}} \max_{\sigma_B} F^2(\Phi_{AE} \otimes \rho_B, \mathbb{1}_A \otimes \mathbb{1}_B \otimes \mathcal{R}_E(\rho_{ABE})) \tag{7.118}$$

$$= \max_{\mathcal{R}_E} F^2(\Phi_{AE}, \mathbb{1}_A \otimes \mathcal{R}_E(\rho_{AE})) \tag{7.119}$$

$$= \frac{1}{d_A} 2^{-H_{\min}(A|E)_\rho}\,. \tag{7.120}$$

Hence, $H_{\min}(A|E)_\rho = -\log d_A \mathrm{Dec}(A|E)_\rho$. ■

7.3.3 Bounds on the decoherence quantity for GPTs

The goal of this subsection is to derive an upper bound on $\mathrm{Dec}(A|E)_\omega$ in terms of the CHSH winning probability p_{AB}^{CHSH} of Alice and Bob. This probability is

a function of β_{AB}, given by [Bru+14]

$$p_{AB}^{\text{CHSH}} = \frac{1}{2}\left(1 + \frac{\beta_{AB}}{4}\right) . \tag{7.121}$$

It corresponds to a game in which Alice and Bob are given *question* $x, y \in \{0,1\}$ and try to give *answers* $a, b \in \{0,1\}$ such that $a \oplus b = xy$. We assume that this connection is clear to the reader. For further information, see [Bru+14].

We formulate the bound as a minimization problem which we solve and interpret in section 7.3.4. In the following, we derive a lower bound on $-\log \mathrm{Dec}(A|E)_\omega$. We make the convention that $-\log 0 = \infty$, where ∞ is a symbol for which we accept the inequality $\infty \geq r$ for every real number r. This lower bound on $-\log \mathrm{Dec}(A|E)_\omega$ then gives us an upper bound on $\mathrm{Dec}(A|E)_\omega$. In a first step, we bound the fidelity-based quantity $-\log \mathrm{Dec}(A|E)_\omega$ by a trace distance-based quantity. This has the advantage that the resulting optimization problem which gives us the bound can be solved using linear programming.

Proposition 7.23 : *Let S_{ABE} be a tripartite scenario, let $\omega \in \Omega$. Then*

$$-\log \mathrm{Dec}(A|E)_\omega \geq \inf_{T_E \in \mathcal{T}_E} \inf_{\psi \in \Psi_{AE}} D^2(\psi, T_E(\omega)) . \tag{7.122}$$

The following lemma is useful for the proof of proposition 7.23 below.

Lemma 7.24 : *For all $x \in (0,1]$, it holds that $-\log(x^2) \geq 2(1-x)$.*

Proof. We have that $-\log(x^2) = -2\log(x)$, so the claim is equivalent to

$$(x-1) - \log(x) \geq 0 \quad \text{for all } x \in (0,1] . \tag{7.123}$$

The functions $F(x) = \log(x)$ and $G(x) = x-1$ are differentiable on $\mathbb{R}_{>0}$. Thus, by the fundamental theorem of calculus, it holds that for all $x \in \mathbb{R}_{>0}$,

$$F(x) = F(1) + \int_1^x f(y)dy , \quad G(x) = G(1) + \int_1^x g(y)dy , \quad \text{where} \tag{7.124}$$

$$f(y) = \frac{d}{dy}F(y) , \quad g(y) = \frac{d}{dy}G(y) , \tag{7.125}$$

so for all $x \in (0,1]$, we have that

$$\begin{aligned}
(x-1) - \log(x) &= G(x) - F(x) && (7.126)\\
&= \int_1^x g(y) - f(y)dy && (7.127)\\
&= -\int_x^1 \underbrace{1 - \frac{1}{\ln(2)y}}_{<0 \text{ for all } y \in (0,1]} dy \geq 0 . && (7.128)
\end{aligned}$$

This proves the claim. □

Proof of proposition 7.23. Since the right hand side of (7.122) is a finite real number, the inequality trivially holds if $\mathrm{Dec}(A|E)_\omega = 0$ by the above convention. Thus, we assume in the following that $\mathrm{Dec}(A|E)_\omega > 0$. We have

that

$$-\log \mathrm{Dec}(A|E)_\omega = -\log \sup_{T_E \in \mathcal{T}_E} \sup_{\psi \in \Psi_{AE}} F^2(\psi, T_E(\omega)) \tag{7.129}$$

$$= -\log \left(\sup_{T_E \in \mathcal{T}_E} \sup_{\psi \in \Psi_{AE}} F(\psi, T_E(\omega)) \right)^2 \tag{7.130}$$

For $x \in (0,1]$, it holds that $-\log x^2 \geq 2(1-x)$ (see lemma 7.24). Thus, since

$$\sup_{T_E \in \mathcal{T}_E} \sup_{\psi \in \Psi_{AE}} F(\psi, T_E(\omega)) \in (0,1]\,, \tag{7.131}$$

we get that

$$-\log \mathrm{Dec}(A|E)_\omega \geq 2 \left(1 - \sup_{T_E \in \mathcal{T}_E} \sup_{\psi \in \Psi_{AE}} F(\psi, T_E(\omega)) \right) \tag{7.132}$$

$$= \inf_{T_E \in \mathcal{T}_E} \inf_{\psi \in \Psi_{AE}} 2(1 - F(\psi, T_E(\omega))) \tag{7.133}$$

$$= \inf_{T_E \in \mathcal{T}_E} \inf_{\psi \in \Psi_{AE}} \sup_{M \in \mathcal{M}} 2(1 - b(\psi, T_E(\omega)|M))\,. \tag{7.134}$$

For the Bhattacharyya coefficient b and the total variation distance d, it has been shown [Kra55] that for any two probability distributions distributions, it holds that $2(1-b) \geq d^2$. Since this is true in particular for the two probability distributions that the measurement M induces on the states ψ and $T_E(\omega)$, we get that

$$-\log \mathrm{Dec}(A|E)_\omega \geq \inf_{T_E \in \mathcal{T}_E} \inf_{\psi \in \Psi_{AE}} \sup_{M \in \mathcal{M}} d^2(\psi, T_E(\omega)|M) \tag{7.135}$$

$$= \inf_{T_E \in \mathcal{T}_E} \inf_{\psi \in \Psi_{AE}} D^2(\psi, T_E(\omega))\,, \tag{7.136}$$

as claimed. □

The idea that the fidelity and the trace distance are related is not new. In quantum theory, the *Fuchs-van de Graaf inequalities* (FvdG) relate the two quantities [FG99]. Inequality (7.122) is not completely analogous to the FvdG inequalities: It makes use of the logarithm in (7.122), which allows to apply classical relations that lead to a stronger bound than with the application of the FvdG inequalities.

For the bounds that we are going to derive, the notion of a *non-signalling distribution* is central. Our bounds are essentially minimizations of functions over sets of non-signalling distributions $P[a,b,c|x,y,z]_\omega$ and $P[a,c|x,z]_\psi$ with certain additional properties.

Definition 7.25 : *A set of numbers $P[a,b,c|x,y,z]_\omega \in [0,1]$, indexed by numbers $a,b,c \in \{0,1\}$ which we call* ***outcomes****, and numbers $x,y,z \in \{0,1\}$*

which we call ***settings****, is a* ***non-signalling distribution*** *if*

normalization:

$$\sum_{a,b,c} P[a,b,c|x,y,z]_\omega = 1 \quad \text{for all } x,y,z \in \{0,1\}\,, \tag{7.137}$$

no-signalling:

$$\sum_a P[a,b,c|0,y,z]_\omega = \sum_a P[a,b,c|1,y,z]_\omega \quad \forall\, b,c,y,z \in \{0,1\}\,, \tag{7.138}$$

$$\sum_b P[a,b,c|x,0,z]_\omega = \sum_b P[a,b,c|x,1,z]_\omega \quad \forall\, a,b,x,y \in \{0,1\}\,, \tag{7.139}$$

$$\sum_b P[a,b,c|x,y,0]_\omega = \sum_b P[a,b,c|x,y,1]_\omega \quad \forall\, a,b,x,y \in \{0,1\}\,. \tag{7.140}$$

Similarly, a set of numbers $P[a,c|x,z]_\psi \in [0,1]$*, indexed by outcomes* $a,c \in \{0,1\}$ *and settings* $x,z \in \{0,1\}$ *is a non-signalling distribution if*

normalization:

$$\sum_{a,c} P[a,c|x,z]_\psi = 1 \quad \forall\, x,z \in \{0,1\}\,, \tag{7.141}$$

no-signalling:

$$\sum_a P[a,c|0,z]_\psi = \sum_a P[a,c|1,z]_\psi \quad \forall\, c,z \in \{0,1\}\,, \tag{7.142}$$

$$\sum_c P[a,c|x,0]_\psi = \sum_c P[a,c|x,1]_\psi \quad \forall\, a,x \in \{0,1\}\,. \tag{7.143}$$

The interpretation of equations (7.138) to (7.140) is that it is impossible for each of the three parties to *signal* to the other two parties by influencing their measurement statistics with the choice of the measurement setting. These one-party no-signalling constraints imply all the multi-party no-signalling constraints, saying that no collection of parties can signal to the remaining parties [Bar+05], so we do not need to require these constraints separately.

Now we are going to formulate the bound on $-\log \mathrm{Dec}(A|E)_\omega$ in terms of the CHSH winning probability of Alice and Bob. Assume that Alice, Bob and Eve are in a situation described by a tripartite scenario S_{ABE}. Suppose that Alice and Bob have estimated that for the state $\omega \in \Omega$ that they are analyzing, their CHSH winning probability is at least λ for some $\lambda \in [0,1]$. Formulated in our tripartite scenario language, this means that they have found out that for local instruments

$$I_A^0 = \{T_A^{0|0}, T_A^{1|0}\} \in \mathcal{I}_A, \qquad I_B^0 = \{T_B^{0|0}, T_B^{1|0}\} \in \mathcal{I}_B, \tag{7.144}$$

$$I_A^1 = \{T_A^{0|1}, T_A^{1|1}\} \in \mathcal{I}_A, \qquad I_B^1 = \{T_B^{0|1}, T_B^{1|1}\} \in \mathcal{I}_B\,, \tag{7.145}$$

it holds that

$$\frac{1}{4}\sum_{x,y}\sum_{\substack{a,b\\ a\oplus b = xy}} \left(u \circ T_A^{a|x} \circ T_B^{b|y}\right)(\omega) \geq \lambda\,. \tag{7.146}$$

In that case, what can Alice and Bob infer about $-\log \mathrm{Dec}(A|E)_\omega$? We have seen in proposition 7.23 that this quantity is lower bounded by the infimum

over the squared trace distance. Alice's and Bob's estimate on their CHSH winning probability can be translated into a bound on this quantity. This is shown by the following proposition.

Proposition 7.26 : *Let S_{ABE} be a tripartite scenario, let $\omega \in \Omega$ be a state. If the CHSH winning probability of Alice and Bob is at least λ, i.e. if there are local instruments I_A^0, I_A^1, I_B^0 and I_B^1 as in (7.144) and (7.145) and a $\lambda \in [0,1]$ such that (7.146) is satisfied, then*

$$\begin{aligned} &\inf_{T_E \in \mathcal{T}_E} \inf_{\psi \in \Psi_{AE}} D(\psi, T_E(\omega)) \\ &\geq \min_{\substack{x,z \in \{0,1\} \\ P[a,b,c|x,y,z]_\omega \in \mathcal{D}_\omega(\lambda) \\ P[a,c|x,z]_\psi \in \mathcal{D}_\psi}} \frac{1}{2} \sum_{a,c} \left| P[a,c|x,z]_\psi - \sum_b P[a,b,c|x,y,z]_\omega \right| , \end{aligned} \tag{7.147}$$

where $\mathcal{D}_\omega(\lambda)$ is the set of non-signalling distributions for Alice, Bob and Eve such that Alice and Bob have a CHSH winning probability of at least λ, i.e.

$$\mathcal{D}_\omega(\lambda) = \left\{ P[a,b,c|x,y,z]_\omega \;\middle|\; \begin{array}{l} P[a,b,c|x,y,z]_\omega \text{ is a non-signalling distribution such that} \\ \frac{1}{4} \sum_{x,y} \sum_{\substack{a,b \\ a \oplus b = xy}} \sum_c P[a,b,c|x,y,z]_\omega \geq \lambda , \end{array} \right\} . \tag{7.148}$$

and where $\mathcal{D}_\psi$ is the set of non-signalling distributions for Alice and Eve such that their measurement outcomes are perfectly correlated when they choose the same measurement setting, i.e.

$$\mathcal{D}_\psi = \left\{ P[a,c|x,z]_\psi \;\middle|\; \begin{array}{l} P[a,c|x,z]_\psi \text{ is a non-signalling distribution such that } P[a=c|x=z]_\psi = 1. \end{array} \right\} . \tag{7.149}$$

Proposition 7.26 reduces our problem of lower bounding the decoherence quantity for GPTs to an optimization over non-signalling distributions. This allows us to use linear programming techniques, which in similar ways have been used in [Ton09] to answer questions about non-signalling distributions.

We need the following lemma for the proof of proposition 7.26 below.

Lemma 7.27 : *Let S_{ABE} be a tripartite scenario, let $\omega, \psi \in \Omega$. Then, for all local instruments $(I_A, I_B, I_E) \in \mathcal{I}_A \times \mathcal{I}_B \times \mathcal{I}_E$, it holds that*

$$\begin{aligned} &\inf_{T_E \in \mathcal{T}_E} D(\psi, T_E(\omega)) \\ &\geq \frac{1}{2} \inf_{T_E \in \mathcal{T}_E} \sum_{\substack{T_A \in I_A \\ U_E \in I_E}} \left| (u \circ T_A \circ U_E)(\psi) - \sum_{T_B \in I_B} (u \circ T_A \circ T_B \circ U_E \circ T_E)(\omega) \right| . \end{aligned} \tag{7.150}$$

Proof. It is sufficient to show that for all $\omega, \psi \in \Omega$, for all $T_E \in \mathcal{T}_E$ and for all

$(I_A, I_B, I_E) \in \mathcal{I}_A \times \mathcal{I}_B \times \mathcal{I}_E$,

$$D(\psi, T_E(\omega)) \geq \frac{1}{2} \sum_{\substack{T_A \in I_A \\ U_E \in I_E}} \left| (u \circ T_A \circ U_E)(\psi) - \sum_{T_B \in I_B} (u \circ T_A \circ T_B \circ U_E \circ T_E)(\omega) \right| . \tag{7.151}$$

This is what we are going to show now. Let $\omega, \psi \in \Omega$, let $T_E \in \mathcal{T}_E$, let $(I_A, I_B, I_E) \in \mathcal{I}_A \times \mathcal{I}_B \times \mathcal{I}_E$. Then

$$D(\psi, T_E(\omega)) = \sup_{M \in \mathcal{M}} d(\psi, T_E(\omega)|M) = \frac{1}{2} \sup_{M \in \mathcal{M}} \sum_{e \in M} |e(\psi) - e(T_E(\omega))| . \tag{7.152}$$

If instead of taking the supremum over $\mathcal{M}$, we only evaluate the expression for a particular element of $\mathcal{M}$, we get a lower bound on (7.152). We choose the element (c.f. remark 7.17)

$$\{u \circ T_A \circ U_E \mid T_A \in \mathcal{I}_A, U_E \in \mathcal{I}_E\} \in \mathcal{M} . \tag{7.153}$$

Hence,

$$D(\psi, T_E(\omega)) \geq \frac{1}{2} \sum_{\substack{T_A \in \mathcal{I}_A \\ U_E \in \mathcal{I}_E}} |(u \circ T_A \circ U_E)(\psi) - (u \circ T_A \circ U_E \circ T_E)(\omega)| . \tag{7.154}$$

By the definition of a local instrument, $u = \sum_{T_B \in I_B} u \circ T_B$. Thus,

$$D(\psi, T_E(\omega)) \geq \frac{1}{2} \sum_{\substack{T_A \in \mathcal{I}_A \\ U_E \in \mathcal{I}_E}} \left| (u \circ T_A \circ U_E)(\psi) - \sum_{T_B \in I_B} (u \circ T_B \circ T_A \circ U_E \circ T_E)(\omega) \right| \tag{7.155}$$

$$= \frac{1}{2} \sum_{\substack{T_A \in \mathcal{I}_A \\ U_E \in \mathcal{I}_E}} \left| (u \circ T_A \circ U_E)(\psi) - \sum_{T_B \in I_B} (u \circ T_A \circ T_B \circ U_E \circ T_E)(\omega) \right| , \tag{7.156}$$

where in the last equality, we made use of the fact that transformations of different parties commute. □

Proof of proposition 7.26. It is sufficient to show that for every $\psi \in \Psi_{AE}$, the claimed inequality holds without the minimization over Ψ_{AE}, i.e.

$$\inf_{T_E \in \mathcal{T}_E} D(\psi, T_E(\omega)) \geq \min_{\substack{x,z \in \{0,1\} \\ P[a,b,c|x,y,z]_\omega \in \mathcal{D}_\omega(\lambda) \\ P[a,c|x,z]_\psi \in \mathcal{D}_\psi(\Psi_{AE},\lambda)}} \frac{1}{2} \sum_{a,c} \left| P[a,c|x,z]_\psi - \sum_b P[a,b,c|x,y,z]_\omega \right| . \tag{7.157}$$

By means of lemma 7.27, we know that for all $x, y \in \{0,1\}$ and every $I_E \in \mathcal{I}_E$,

$$\inf_{T_E \in \mathcal{T}_E} D(\psi, T_E(\omega)) \geq \frac{1}{2} \inf_{T_E \in \mathcal{T}_E} \sum_{\substack{a \in \{0,1\} \\ U_E \in I_E}} \left| (u \circ T_A^{a|x} \circ U_E)(\psi) - \sum_{b \in \{0,1\}} (u \circ T_A^{a|x} \circ T_B^{b|y} \circ U_E \circ T_E)(\omega) \right| . \tag{7.158}$$

Let $\psi \in \Psi_{AE}$, let $I_E^0 = \{U_E^{0|0}, U_E^{1|0}\}$, $I_E^1 = \{U_E^{0|1}, U_E^{1|1}\} \in \mathcal{I}_E$ be local instruments for Eve such that

$$(u \circ T_A^{0|0} \circ U_E^{0|0})(\psi) + (u \circ T_A^{1|0} \circ U_E^{1|0})(\psi) = 1 , \tag{7.159}$$

$$(u \circ T_A^{0|1} \circ U_E^{0|1})(\psi) + (u \circ T_A^{1|1} \circ U_E^{1|1})(\psi) = 1 , \tag{7.160}$$

which exist according to the definition of Ψ_{AE} (definition 7.20). It holds that for every $x, y, z \in \{0,1\}$,

$$\inf_{T_E \in \mathcal{T}_E} D(\psi, T_E(\omega)) \geq \frac{1}{2} \inf_{T_E \in \mathcal{T}_E} \sum_{a,c \in \{0,1\}} \left| (u \circ T_A^{a|x} \circ U_E^{c|z})(\psi) - \sum_{b \in \{0,1\}} (u \circ T_A^{a|x} \circ T_B^{b|y} \circ U_E^{c|z} \circ T_E)(\omega) \right| \tag{7.161}$$

$$= \frac{1}{2} \inf_{T_E \in \mathcal{T}_E} \sum_{a,c \in \{0,1\}} \left| P[a,c|x,z]_\psi - \sum_{b \in \{0,1\}} P[a,b,c|x,y,z]_\omega \right| , \tag{7.162}$$

where

$$P[a,c|x,z]_\psi = (u \circ T_A^{a|x} \circ U_E^{c|z})(\psi) , \tag{7.163}$$

$$P[a,b,c|x,y,z]_\omega = (u \circ T_A^{a|x} \circ T_B^{b|y} \circ U_E^{c|z} \circ T_E)(\omega) . \tag{7.164}$$

Hence,

$$\inf_{T_E \in \mathcal{T}_E} D(\psi, T_E(\omega)) \geq \frac{1}{2} \min_{x,y,z} \inf_{T_E \in \mathcal{T}_E} \sum_{a,c \in \{0,1\}} \left| P[a,c|x,z]_\psi - \sum_{b \in \{0,1\}} P[a,b,c|x,y,z]_\omega \right| . \tag{7.165}$$

$P[a,c|x,z]_\psi$ forms a non-signalling distribution: For the normalization, note

that for all $x, z \in \{0,1\}$, we have that

$$\sum_{a,c} P[a,c|x,z]_\psi = \sum_{a,c} (u \circ T_A^{a|x} \circ U_E^{c|z})(\psi) \tag{7.166}$$

$$= \underbrace{\left(\sum_a u \circ T_A^{a|x}\right)}_{u} \circ \left(\sum_c U_E^{c|z}\right)(\psi) \tag{7.167}$$

$$= \left(\sum_c u \circ U_E^{c|z}\right)(\psi) \tag{7.168}$$

$$= u(\psi) \tag{7.169}$$

$$= 1\,. \tag{7.170}$$

For the no-signalling condition, note that for all $c, z \in \{0,1\}$, it holds that

$$\sum_a P[a,c|0,z]_\psi = \left(\left(\sum_a u \circ T_A^{a|0}\right) \circ U_E^{c|z}\right)(\psi) \tag{7.171}$$

$$= (u \circ U_E^{c|z})(\psi) \tag{7.172}$$

$$= \left(\left(\sum_a u \circ T_A^{a|1}\right) \circ U_E^{c|z}\right)(\psi) \tag{7.173}$$

$$= \sum_a P[a,c|1,z]_\psi\,, \tag{7.174}$$

and that for all $a, x \in \{0,1\}$, it holds that

$$\sum_c P[a,c|x,0]_\psi = \sum_c (u \circ T_A^{a|x} \circ U_E^{c|0})(\psi) \tag{7.175}$$

$$= \sum_c (u \circ U_E^{c|0} \circ T_A^{a|x})(\psi) \tag{7.176}$$

$$= \left(\left(\sum_c u \circ U_E^{c|0}\right) \circ T_A^{a|x}\right)(\psi) \tag{7.177}$$

$$= (u \circ T_A^{a|x})(\psi) \tag{7.178}$$

$$= \left(\left(\sum_c u \circ U_E^{c|1}\right) \circ T_A^{a|x}\right)(\psi) \tag{7.179}$$

$$= \sum_c P[a,c|x,1]_\psi\,, \tag{7.180}$$

where in the second equality, we made use of the fact that local transformations of different parties commute. Analogously, for every $T_E \in \mathcal{T}_E$, $P[a,b,c|x,y,z]_\omega$

is a non-signalling distribution. Moreover, $P[a,b,c|x,y,z]_\omega$ satisfies

$$\begin{aligned}
&\frac{1}{4}\sum_{x,y}\sum_{\substack{a,b\\a\oplus b=xy}}\sum_{c} P[a,b,c|x,y,z]_\omega \\
&\quad= \frac{1}{4}\sum_{x,y}\sum_{\substack{a,b\\a\oplus b=xy}}\sum_{c}(u\circ T_A^{a|x}\circ T_B^{b|y}\circ U_E^{c|z}\circ T_E)(\omega) && (7.181)\\
&\quad= \frac{1}{4}\sum_{x,y}\sum_{\substack{a,b\\a\oplus b=xy}}\underbrace{\left(\sum_{c}(u\circ U_E^{c|z}\circ T_E\right)}_{u}\circ T_A^{a|x}\circ T_B^{b|y})(\omega) && (7.182)\\
&\quad\geq \lambda\,, && (7.183)
\end{aligned}$$

where the inequality is one of the assumptions of the proposition. Furthermore, $P[a,c|x,1]_\psi$ satisfies

$$P[0,0|0,0]_\psi + P[1,1|0,0]_\psi = (u\circ T_A^{0|0}\circ U_E^{0|0})(\psi) + (u\circ T_A^{1|0}\circ U_E^{1|0})(\psi) = 1\,, \tag{7.184}$$

$$P[0,0|1,1]_\psi + P[1,1|1,1]_\psi = (u\circ T_A^{0|1}\circ T^{0|1})(\psi) + (u\circ T_A^{1|1}\circ U_E^{1|1})(\psi) = 1 \tag{7.185}$$

(where we made use of (7.159) and (7.160)), which we may abbreviate as $P[a=c|x=z]_\psi = 1$. Thus, for every $T_E\in\mathcal{T}_E$, we have that $P[a,b,c|x,y,z]_\omega \in \mathcal{D}_\omega(\lambda)$ and $P[a,c|x,z]_\psi\in\mathcal{D}_\psi$. Thus,

$$\begin{aligned}
&\inf_{T_E\in\mathcal{T}_E} D(\psi, T_E(\omega))\\
&\geq \frac{1}{2}\min_{x,y,z}\inf_{\substack{P[a,b,c|x,y,z]_\omega\in\mathcal{D}_\omega(\lambda)\\ P[a,c|x,z]_\psi\in\mathcal{D}_\psi(\Psi_{AE},\lambda)}}\sum_{a,c\in\{0,1\}}\left|P[a,c|x,z]_\psi - \sum_{b\in\{0,1\}}P[a,b,c|x,y,z]_\omega\right|\,.
\end{aligned} \tag{7.186}$$

Since $P[a,b,c|x,y,z]_\omega$ satisfies the no-signalling property, the right hand side of (7.186) is independent of y, so the minimization only needs to be performed over x and z. Moreover, the infimum over the sets $\mathcal{D}_\omega(\lambda)$ and $\mathcal{D}_\psi$ is a minimum because it is the infimum of a continuous function over a convex polytope, which is always attained (see section 7.3.4 for more details). This completes the proof. □

Corollary 7.28 (The bound): *Let S_{ABE} be a tripartite scenario, let $\omega\in\Omega$ be a state. If the CHSH winning probability of Alice and Bob is at least λ (in the above sense), then*

$$\mathrm{Dec}(A|E)_\omega \leq 2^{-\delta^2(\lambda)}\,, \tag{7.187}$$

where

$$\delta(\lambda) = \min_{\substack{x,z\in\{0,1\}\\ P[a,b,c|x,y,z]_\omega\in\mathcal{D}_\omega(\lambda)\\ P[a,c|x,z]_\psi\in\mathcal{D}_\psi}}\frac{1}{2}\sum_{a,c}\left|P[a,c|x,z]_\psi - \sum_{b}P[a,b,c|x,y,z]_\omega\right|\,, \tag{7.188}$$

Proof. This is a direct consequence of propositions 7.23 and 7.26. □

7.3.4 Evaluation of the bound and results

Formulation of the bound as a linear program

In this subsection, we evaluate the bound (7.187). To this end, we rewrite (7.188) in terms of linear programs.

Linear Program : *The bound $\delta(\lambda)$, which is a function $\delta : [0,1] \to [0,1]$, is given as follows. For all $\lambda \in [0,1]$, the value $\delta(\lambda)$ is the solution of the linear program*

$$\begin{aligned} &\textit{minimize} && \delta(\lambda) \\ &\textit{subject to} && P[a,b,c|x,y,z]_\omega \in \mathcal{D}_\omega(\lambda) \\ &&& P[a,c|x,z]_\psi \in \mathcal{D}_\psi \\ &&& \delta(\lambda) \geq \textstyle\sum_{a,c} \delta_{ac}^{xz} \ \forall x,z \in \{0,1\} \\ &&& \delta_{ac}^{xz} \geq \tfrac{1}{2}(P[a,c|x,z]_\psi - \textstyle\sum_b P[a,b,c|x,0,z]_\omega) \\ &&& \qquad \geq -\delta_{ac}^{xz} \ \forall a,c,x,z \in \{0,1\} \end{aligned} \tag{7.189}$$

This is a linear program in 97 variables:

$\left\{P[a,b,c\|x,y,z]_\omega\right\}_{a,b,c,x,y,z\in\{0,1\}}$	64 variables
$\left\{P[a,c\|x,z]_\psi\right\}_{a,c,x,z\in\{0,1\}}$	+ 16 variables
$\left\{\delta_{ac}^{xz}\right\}_{a,c,x,z\in\{0,1\}}$	+ 16 variables
$\delta(\lambda)$	+ 1 variable
	= 97 variables

We have already written out the constraints for these 97 variables as inequalities. The third and fourth line are already written as such in the program description, and for the first two lines, we refer to the following:

constraint	(in)equalities
$P[a,b,c\|x,y,z]_\omega \in \mathcal{D}_\omega(\lambda)$	(7.137) to (7.140) and inequality in (7.148)
$P[a,c\|x,z]_\psi \in \mathcal{D}_\psi(\lambda)$	(7.141) to (7.143) and equation in (7.149)

The inequalities define a convex polytope over which the convex function $\delta(\lambda)$ is minimized, so the minimum is attained. It is straightforward to bring these inequalities into the standard form of linear programming. We solved the resulting linear program using standard linear programming routines in Mathematica and Octave.

Solution of the linear program and discussion of the results

We plot the result in figure 7.9. The bound $2^{-\delta^2(\lambda)}$ is non-trivial for values $\lambda \in (3/4, 1]$. This is a very satisfactory result as one cannot expect the bound to be non-trivial for $\lambda \in [0, 3/4]$: A CHSH winning probability of at least $\lambda \in [0, 3/4]$ for Alice and Bob is always compatible with $\mathrm{Dec}(A|E)_\omega = 1$. To see this, note that the requirement for a state to yield a CHSH winning probability for Alice and Bob of at least $\lambda \in [0, 3/4]$ is trivial: Alice and Bob can choose trivial measurements that always yields 1 as an outcome, independently of the state. More precisely, in our tripartite scenario language,

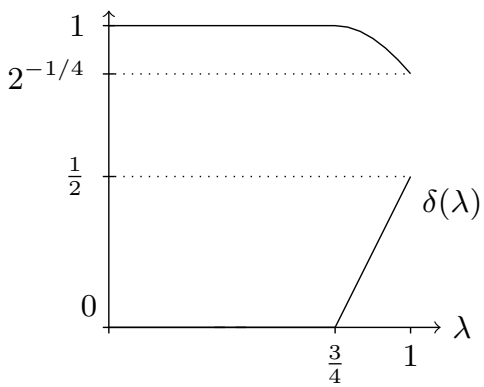


Figure 7.9: Plot of the result. The bound $2^{-\delta^2(\lambda)}$ is non-trivial precisely when the CHSH winning probability for Alice and Bob is non-classical, i.e. $\lambda > 3/4$.

we can express this as follows. Certainly, there are tripartite scenarios in which the identity map $\mathbb{1}_V$ and the zero map 0_V are in $\mathcal{T}_A$, $\mathcal{T}_B$ and $\mathcal{T}_E$.[11] For such tripartite scenarios, the condition (c.f. (7.144) to (7.146) in section 7.3.3)

$$\frac{1}{4}\sum_{x,y}\sum_{\substack{a,b\\ a\oplus b=xy}}\left(u\circ T_A^{a|x}\circ T_B^{b|y}\right)(\omega)\geq\lambda\in[0,3/4]$$
$$\text{for some}\quad \begin{matrix}\{T_A^{0|0},T_A^{1|0}\},\{T_A^{0|1},T_A^{1|1}\}\in\mathcal{I}_A,\\ \{T_B^{0|0},T_B^{1|0}\},\{T_B^{0|1},T_B^{1|1}\}\in\mathcal{I}_B\end{matrix} \tag{7.190}$$

is always satisfied because for all $\omega\in\Omega$,

$$\frac{1}{4}\sum_{x,y}\sum_{\substack{a,b\\ a\oplus b=xy}}\left(u\circ T_A^{a|x}\circ T_B^{b|y}\right)(\omega)=\frac{3}{4}\quad\text{for}\quad \begin{matrix}T_A^{0|0}=T_A^{0|1}=T_B^{0|0}=T_B^{0|1}=0_V\,,\\ T_A^{1|0}=T_A^{1|1}=T_B^{1|0}=T_B^{1|1}=\mathbb{1}_V\,.\end{matrix} \tag{7.191}$$

This means that the requirement that the CHSH winning probability for Alice and Bob is at least $\lambda\in[0,3/4]$ does not exclude the case $\omega\in\Psi_{AE}$. In that case, $\mathrm{Dec}(A|E)_\omega=\sup_{T_E\in\mathcal{T}_E}\sup_{\psi\in\Psi_{AE}}F^2(\psi,T_E(\omega))=1$.

7.4 An example test for gravitational decoherence

In sections 7.2 and 7.3, we have derived bounds on the decoherence quantity in terms of the CHSH parameter β_{AB} for quantum theory and for more general probabilistic theories. In this section, we will apply the quantum bound derived in section 7.2 to derive a test for a particular model for gravitational

[11] Every tripartite scenario can be turned into such by adding $\mathbb{1}_V$ and 0_V to the sets of local transformations. In fact, it would be physical to assume that each set of local transformations contains $\mathbb{1}_V$ and 0_V.

decoherence. By what we explained in section 7.1, the CHSH parameter β_{AB} that is measured in this test can then be tested against non-quantum theories as well. For example, it can be tested against the weak bound that we derived in the last section, or it can be tested against more specific non-quantum theories by adding additional constraints to the linear program that derives the bound. For the numerical calculations in this section, we use the quantum bound of section 7.2.

As we mentioned in section 7.1, gravitational decoherence is a prime candidate for the application of our generalized decoherence estimation formalism. This is because we have no consistent theory of quantum gravity. It seems that correct descriptions of experiments involving gravitational effects are likely to fall outside the regime of quantum theory. Therefore, it is useful to have experimental tests at hand whose outcomes can be interpreted without relying on quantum mechanics.

Candidate systems for the observation of gravitational decoherence are not easy to find. On the one hand, the system needs to be massive enough to exhibit detectable gravitational effects. At the same time, however, they should be small enough to interact coherently with other systems over a time period that is long enough for an experiment. If these two conditions are satisfied simultaneously, we may hope to see a gravitationally induced decoherence of a system that is originally in a coherent superposition. Such systems are, in some sense, neither macroscopic nor microscopic, and some people refer to such systems as *mesoscopic systems*.

A particularly promising candidate for such a mesoscopic system that may be used for probing gravitational decoherence is an *optomechanical cavity*. This is an optical cavity where one of the bounding mirrors is movable, forming a mechanical oscillator (see the lower part of figure 7.10). The physics of optomechanical cavities is an open research field, and different models for potentially occurring effects of gravitational decoherence exist [Pen96; Dió89; Dio11; Dio84; Dio87; KTM14; Sta12; AH13; Hu14; AH07; Kay98; BGL07; WBM06].

Here, we derive a test for Diosi's model of gravitational decoherence [Dió89]. For the explanations in this section to be understood, some basic familiarity with optomechanics is useful, but not strictly required.

7.4.1 An optomechanical setting and its model for gravitational decoherence

The objective here is to create two entangled photonic qubits in which one photon is prepared in an opto-mechanical system that is itself subject to gravitational decoherence—if there is any—and the other photon is prepared in an identical cavity except the mirrors are fixed and cannot move. This model is a modification of the model first proposed by Bouwmeester [Mar+03] in which an itinerant single photon pulse is injected into a cavity rather than created intra-cavity as here. Our modification avoids the problem that the time over which the photons interact with the mechanical element is stochastic and determined by the random times at which the photons enter and exit the cavity through an end mirror. In the new scheme, the cavities are assumed to have

almost perfect mirrors — very narrow line width (see for example[Kes+12]).

The intracavity single photon Raman source is described in Nisbet-Jones, et al. [NJ+11]. In this scheme (see Fig. 7.10) a control pulse can quickly and efficiently prepare a cavity mode in a single photon state by driving a Raman transition between two hyperfine levels we label as $|g\rangle, |e\rangle$. In our scheme there are two optical cavities otherwise identical except in one of the cavities a mechanical element can respond to the radiation pressure force of light.

We will assume that we can prepare the atomic sources in an arbitrary entangled state $|g, e\rangle + |e, g\rangle$, for example, using the trapped ion schemes of Monroe [DM10]. In addition we will assume that we can make arbitrary rotations in the g, e subspace of each source and also make fast efficient single shot readout of the state of each source, for example using fluorescence shelving. This means we can readout the atomic qubit in each cavity in any basis.

The write laser implements the Hamiltonian

$$H_w = i\hbar\Omega(t)\frac{a^\dagger|e\rangle\langle g| - a|g\rangle\langle e|}{2}\,. \tag{7.192}$$

This is a rotation in the state space $\{|g\rangle|0\rangle, |e\rangle|1\rangle\}$. We can thus prepare arbitrary states of the form $\cos\vartheta/2|g\rangle|0\rangle + \sin\vartheta/2|e\rangle|1\rangle$, where ϑ is determined by the pulse area. We will refer to the case of $\vartheta = \pi$ as a π-pulse. Note that if the source is in the excited state $|e\rangle$ and the cavity is in the vacuum, no photon is excited.

Starting with the cavities in the vacuum state the protocol proceeds as follows:

1. Prepare the source atoms in the state $|g, e\rangle + |e, g\rangle$,
2. Apply the write laser with a π-pulse,
3. Free evolution of the OM systems for a time T,
4. Apply the write laser with a π-pulse,
5. Readout the atomic state in each cavity.

At the end of Step 2, the state of the sources and the cavities is $|\psi_2\rangle = |e, e\rangle \otimes (|1, 0\rangle + |0, 1\rangle)$ where $|n, m\rangle = |n\rangle \otimes |m\rangle$ with each factor being a photon number eigenstate.

Gravitational decoherence.

We will use Diosi's theory of gravitational decoherence[Dió89]. This is equivalent to the decoherence model introduced in Kafri et al. [KTM14]. One mirror of the opto-mechanical cavity is free to move in a harmonic potential with frequency ω_m. The master equation for a massive particle moving in a harmonic potential, including gravitational decoherence is

$$\frac{d\rho}{dt} = -i\omega_m[b^\dagger b, \rho] - \Lambda_{\text{grav}}[b + b^\dagger, [b + b^\dagger, \rho]] \tag{7.193}$$

where

$$b = \sqrt{\frac{m\omega_m}{2\hbar}}\hat{x} + i\frac{1}{\sqrt{2\hbar m\omega_m}}\hat{p} \tag{7.194}$$

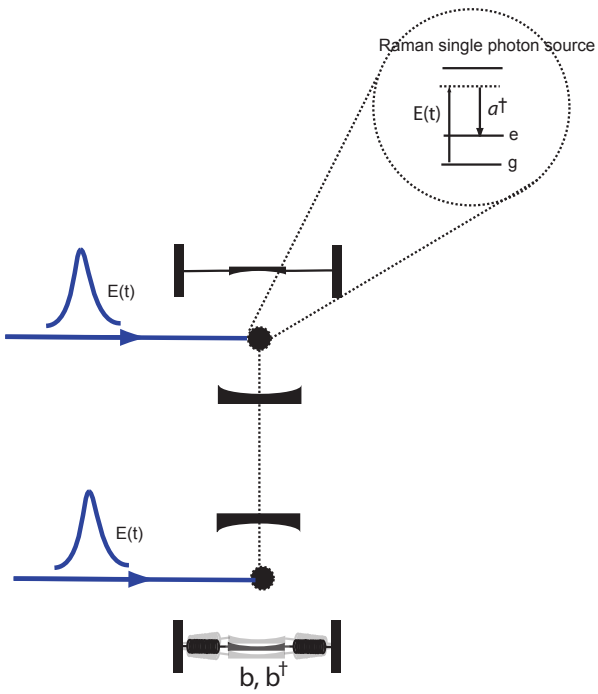


Figure 7.10: Two cavities each contain a Raman single photon source controlled by an external laser 'write field' $E(t)$. The Raman sources are first prepared in an entangled state. Only one cavity contains a mechanical element coupled by radiation rouser to the cavity field.

with $\hat{x}, \hat{p}$ the usual canonical position and momentum operators. The gravitational decoherence rate Λ_{grav} is given by

$$\Lambda_{\text{grav}} = \frac{2\pi}{3}\frac{G\Delta}{\omega_m} \tag{7.195}$$

with G the Newton gravitational constant and Δ the density of the mechanical element. As one might expect Λ_{grav} is quite small, of the order of 10^{-8} s^{-1} for suspended mirrors (as in LIGO) with $\omega_m \sim 1$.

Form a phenomenological perspective the effect of gravitational decoherence is analogous to a Browning heating effect. To see this we note that the average vibrational quantum number increases diffusively

$$\frac{d\langle b^\dagger b\rangle}{dt} = 2\Lambda_{\text{grav}} \tag{7.196}$$

Indeed, one could simulate this effect by adding a stochastic driving force to the mechanical element via the stochastic Hamiltonian

$$H_s = \frac{dI}{dt}(b + b^\dagger) \tag{7.197}$$

where $I(t)$ satisfies an Ito stochastic differential equation,

$$dI(t) = \sqrt{4\Lambda_{\text{grav}}}\, dW(t) \tag{7.198}$$

where $dW(t)$ is the Weiner increment. Averaging over all histories of the stochastic driving force gives the final term in Eq. 7.193.

In the absence of mechanical dissipation, there is no steady state. In reality the mechanical quality factor, $Q = \omega_m/\gamma_m$, is finite leading to a steady state with mean phonon number given by

$$\langle b^\dagger b\rangle_{ss} = \frac{2\Lambda_{\rm grav}}{\gamma_m} \tag{7.199}$$

This of course assumes that there is no additional mechanical heating (regular thermodynamic kind): hardly a realistic assumption. This adds a large (comparatively) additional term to $\Lambda_{\rm grav}$ so that we find (for $k_BT >> \hbar\omega_m$),

$$\Lambda_{\rm grav} \to \Lambda_{\rm grav} + \Lambda_{\rm heat}\,, \quad \text{where } \Lambda_{\rm heat} = \frac{k_BT}{\hbar Q}\,. \tag{7.200}$$

Given the incredibly large quality factor of $Q = 10^{10}$, one would need to cool the mechanical element to nano-Kelvin for the thermodynamical heating to be of the order of the gravitational heating.

Optomechanical probe of gravitational decoherence.

The optomechanical Hamiltonian in cavity-one is

$$H_{\rm om} = \hbar\omega_m b^\dagger b + \hbar g_0(b + b^\dagger) \tag{7.201}$$

g_0 is the single photon optomechanical coupling rate. Typically $g_0 \sim 1$ s^{-1} for the sorts of cavities we are considering here. This is about the same order of magnitude as ω_m. In new field OM cavity technologies, g_0 can be as high as 10^3 s^{-1} however in such cases the mechanical frequency is also typically much higher $\sim$ tens of MHz. The interaction time is T which is short compared to the cavity decay time (which we neglect). We will assume that the mechanics starts in a thermal state, the steady state of the system subject to gravitational decoherence, heating and dissipation. This is given by

$$\rho_{\rm om} = \frac{1}{\pi\bar{n}}\int d^2\alpha\; e^{-\frac{|\alpha|^2}{\bar{n}}}\; |\alpha\rangle_b\langle\alpha| \tag{7.202}$$

where $\bar{n} = \langle b^\dagger b\rangle_{ss}$ is the steady state mean phonon number given in Eq. 7.199.

It is simplest to work in an interaction picture defined by the mechanical free dynamics,

$$H_{\rm om,I} = \hbar g_0(be^{-i\omega_m t} + b^\dagger e^{i\omega_m t}) \tag{7.203}$$

The corresponding unitary evolution operator is

$$U(t) = e^{\beta(t)b^\dagger - \beta^*(t)b} \tag{7.204}$$

where

$$\beta(t) = \frac{g_0}{\omega_m}(e^{-i\omega_m t} - 1) \tag{7.205}$$

The initial state for the OM interaction is the state at the end of Step 2

$$\rho_{\rm om}(0) = \frac{1}{2}\left(|1,0\rangle\langle 1,0| + |0,1\rangle\langle 0,1| + |1,0\rangle\langle 0,1| + |0,1\rangle\langle 1,0|\right) \otimes \rho_m \tag{7.206}$$

where ρ_m is the state of the mechanical element at the start of the protocol, a thermal state. We can ignore the state of the atomic sources at this stage as they do not participate in the OM interaction.

The state of the optomechanical system after an interaction time T is given by

$$\rho_{\rm om}(t) = \frac{1}{2}\Big(|1,0\rangle\langle 1,0|\rho_m + |0,1\rangle\langle 0,1|U(t)\rho_m U^\dagger(t) \\ +|1,0\rangle\langle 0,1|\rho_m U^\dagger(t) + |0,1\rangle\langle 1,0|U(t)\rho_m\Big) \tag{7.207}$$

The reduced state of the cavity fields is given by tracing out the mechanical degree of freedom,

$$\rho_f(t) = \frac{1}{2}\left(|1,0\rangle\langle 1,0| + |0,1\rangle\langle 0,1| + R^*|1,0\rangle\langle 0,1| + R|0,1\rangle\langle 1,0|\right) \tag{7.208}$$

where

$$R = e^{-(1+2\bar{n})|\beta(t)|^2/2} \tag{7.209}$$

where

$$\bar{n} = \overline{n}_{\rm grav} + \overline{n}_{\rm heat} \tag{7.210}$$

$$:= \frac{2\Lambda_{\rm grav}}{\gamma_m} + \frac{2\Lambda_{\rm heat}}{\gamma_m} \tag{7.211}$$

with (as above)

$$\Lambda_{\rm grav} = \frac{2\pi}{3}\frac{G\Delta}{\omega_m}, \quad \Lambda_{\rm heat} = \frac{k_B T}{\hbar Q} \tag{7.212}$$

and

$$|\beta(t)|^2 = \frac{4g_0^2}{\omega_m^2}\sin^2(\omega_m t/2) \tag{7.213}$$

Continuing with the protocol from Step 4, now results in the state of the atom-field system

$$\rho_{af}(t) = \rho_a(t) \otimes |00\rangle\langle 00| \tag{7.214}$$

where

$$\rho_a(t) = \frac{1}{2}(|ge\rangle\langle ge| + |eg\rangle\langle eg| + R^*|eg\rangle\langle ge| + R|ge\rangle\langle eg|) \tag{7.215}$$

The suppression of coherence due to the thermal state of the mechanics has been transferred to a reduction of entanglement in the atomic sources. A readout of the atomic sources will reveal this through either state tomography or via a reduction in a CHSH correlation for a Bell-type experiment.

The function $R(t)$ is a periodic function of time. At each period of the motion it returns to its initial value of zero and the cavity field state would return to the fully entangled state it was in after Step 2. If we chose $T = 2\pi/\omega_m$ then the protocol will return the atomic system to the same entangled state in which it began. This is because we have ignored the heating of the mechanics over the period T so the only way decoherence enters is through the initial thermal excitation of the mechanics. In effect the protocol is a thermometer. We thus see that for maximum effect we need to ensure $g_0 \gg \omega_m$. On the other

hand, gravitational heating requires a small value of ω_m and typically such OM systems have $g_0/\omega_m \ll 1$. Perhaps technical advances will enable OM systems with long mechanical periods and large single photon coupling. Of course this will also require sub hertz cavity line widths. In the (exceptionally) optimistic case we can take $T \sim 1$ nK, $\omega_m \sim 1$ s^{-1}, $\gamma_m \sim 10^{-10}$ s^{-1} so that $Q \sim 10^{10}$.

7.4.2 An experimental test of the model

In section 7.4.1 above, an optomechanical setting has been described. Making some assumptions about how gravitational decoherence influences the optomechanical system, a model has been given that describes how the state of the optomechanical system changes over time. In this section, we consider this model for the state of the optomechanical system as given and analyze it using our decoherence test formalism. We calculate the amount of decoherence that would be introduced to the optomechanical system if the model was correct. We compare this to the amount of decoherence that one would observe if there was no such gravitational decoherence, determining the difference between the two predictions. We devise an experiment that aims at estimating the actual amount of decoherence at a point in time when this difference is maximal. This turns the optomechanical experiment into a test that allows to falsify the above model for gravitational decoherence if it was wrong. This shows that the decoherence testing formalism presented in this work can be applied in situations where the physical process is unknown. It allows to subject proposed models of the process to a consistency check.

We first present the predicted values of $\mathrm{Dec}(A|E)_\rho$ of the optomechanical system for the two cases where gravitational decoherence is present or absent, respectively, for some example parameters of the experiment. We then calculate the CHSH value β_{AB} that one would have to measure in order to falsify the model for gravitational decoherence.

The main quantity of interest in our analysis is the decoherence quantity $\mathrm{Dec}(A|E)_\rho$ for the state $\rho_{AB} = \rho_f(t)$ described in equation (7.208). This can be calculated using lemma 7.5. It turns out to be

$$\mathrm{Dec}(A|E)_\rho = \frac{1}{4}\left(1+\sqrt{1-R^2}\right) \tag{7.216}$$

$$= \frac{1}{4}\left(1+\sqrt{1-\exp\left(-4(1+2\overline{n})\frac{g_0^2}{\omega_m^2}\sin^2\left(\frac{\omega_m t}{2}\right)\right)}\right) . \tag{7.217}$$

If the above model is correct and gravitational decoherence occurs, both the gravitational interaction and the mechanical heating contribute to the average vibrational quantum number, i.e. we have

$$\overline{n} = \overline{n}_{\mathrm{grav}} + \overline{n}_{\mathrm{heat}} \tag{7.218}$$

$$= \frac{4\pi G}{3}\frac{1}{\gamma_m\omega_m}\Delta + \frac{2k_B}{\hbar}\frac{1}{\omega_m}T \tag{7.219}$$

and thus

$$\mathrm{Dec}(A|E)_\rho = \frac{1}{4}\Bigg(1+ \tag{7.220}$$

$$\sqrt{1-\exp\left(-4\left(1+2\left(\frac{4\pi G}{3}\frac{1}{\gamma_m\omega_m}\Delta+\frac{2k_B}{\hbar}\frac{1}{\omega_m}T\right)\right)\frac{g_0^2}{\omega_m^2}\sin^2\left(\frac{\omega_m t}{2}\right)\right)}\Bigg). \tag{7.221}$$

If gravitational decoherence is absent, then only the mechanical heating contributes to the average vibrational quantum number, i.e. we have

$$\overline{n} = \overline{n}_{\mathrm{heat}} \tag{7.222}$$

$$= \frac{2k_B}{\hbar}\frac{1}{\omega_m}T \tag{7.223}$$

and thus

$$\mathrm{Dec}(A|E)_\rho = \frac{1}{4}\left(1+\sqrt{1-\exp\left(-4\left(1+2\left(\frac{2k_B}{\hbar}\frac{1}{\omega_m}T\right)\right)\frac{g_0^2}{\omega_m^2}\sin^2\left(\frac{\omega_m t}{2}\right)\right)}\right). \tag{7.224}$$

Figure 7.11 shows how the decoherence quantity in equation (7.220) as a function of time varies for different materials of the mechanical element and different temperatures, compared to the case where there is no gravitational decoherence as in equation (7.224).

In order to rule out the model for gravitational decoherence, one needs to measure a CHSH value β_{AB} which is incompatible with the value of $\mathrm{Dec}(A|E)_\rho$ given in (7.220). The minimal value β_{fals} of β_{AB} that needs to be measured for this falsification can be calculated using theorem 7.1: Using MATLAB, we numerically evaluated the quantum bound on $\mathrm{Dec}(A|E)_\rho$, which is given as a point-wise maximization problem in theorem 7.1. We inverted the resulting set of data points and interpolated a function from the resulting data using Mathematica. The resulting function takes a value of $\mathrm{Dec}(A|E)_\rho$ as its input and outputs the minimal β_{AB} that needs to be exceeded in a measurement in order to rule out the given value of $\mathrm{Dec}(A|E)_\rho$. Thus, applying this function to the curves of the $\mathrm{Dec}(A|E)_\rho$ values of the gravitational decoherence model in Figure 7.11 yields the curves for β_{fals}. The results are plotted in figure 7.12 for the same materials and temperatures as above.

In order to determine whether it is promising to measure a value of β_{AB} that lies above β_{fals}, we need to determine the value β_{mech} of β_{AB} which is predicted in the case where gravitational decoherence is absent, i.e. where we only have mechanical heating. We can do that exactly: Equation (7.208) gives us an expression for the state, which we consider for the value of R given in the case of mechanical heating only, $\overline{n} = \overline{n}_{\mathrm{mech}}$. Then we calculate the value of β_{mech} for the case where the measurements are taken to be the standard CHSH measurements

$$A_0 = \sigma_x\,, \qquad A_1 = \sigma_z\,,$$

$$B_0 = \frac{\sigma_x - \sigma_z}{\sqrt{2}}\,, \qquad B_1 = \frac{\sigma_x + \sigma_z}{\sqrt{2}}\,,$$

where σ_x, σ_z are the Pauli x- and z-operator, respectively. The resulting curves are shown in figure 7.12 as solid curves. It turns out that for the relevant time interval (where β_{mech} is larger than either of the β_{fals}), the curve of β_{mech} for the standard CHSH measurements is almost identical to the curve one would get for the optimal measurements for each time t. The latter can be calculated using a formula presented in [HHH95b]. This is an experimentally desirable fact: Using a fixed measurement independent of the measurement time is almost optimal.

The most promising measurement time for a falsification of the gravitational decoherence model is given by the time when β_{mech} (that one may hope to actually measure) is high but β_{fals} (which one needs to exceed) is low. Thus, the optimal measurement time can be calculated as the time t_{max} that maximizes the gap function

$$g(t) := \beta_{\text{mech}}(t) - \beta_{\text{fals}}(t)\,. \tag{7.225}$$

This gap function is depends on the density Δ of the mechanical element and its temperature T. One can see that temperatures that look promising for a falsification measurement when looking at the $\text{Dec}(A|E)_\rho$ values in Figure 7.11 turn out to be too warm when looking at the experimentally relevant analysis of the β_{AB} values in figure 7.12. As an example, we have calculated the optimal measurement times for $T = 1$ nK for the densities of aluminum and rhenium. They are visualized in figure 7.13. If there is no gravitational decoherence, one needs to measure values of β_{AB} that are ~ 0.1 close (aluminum) or ~ 0.2 close (rhenium) to the value that one can maximally measure using the standard CHSH measurements, in order to exclude gravitational decoherence.

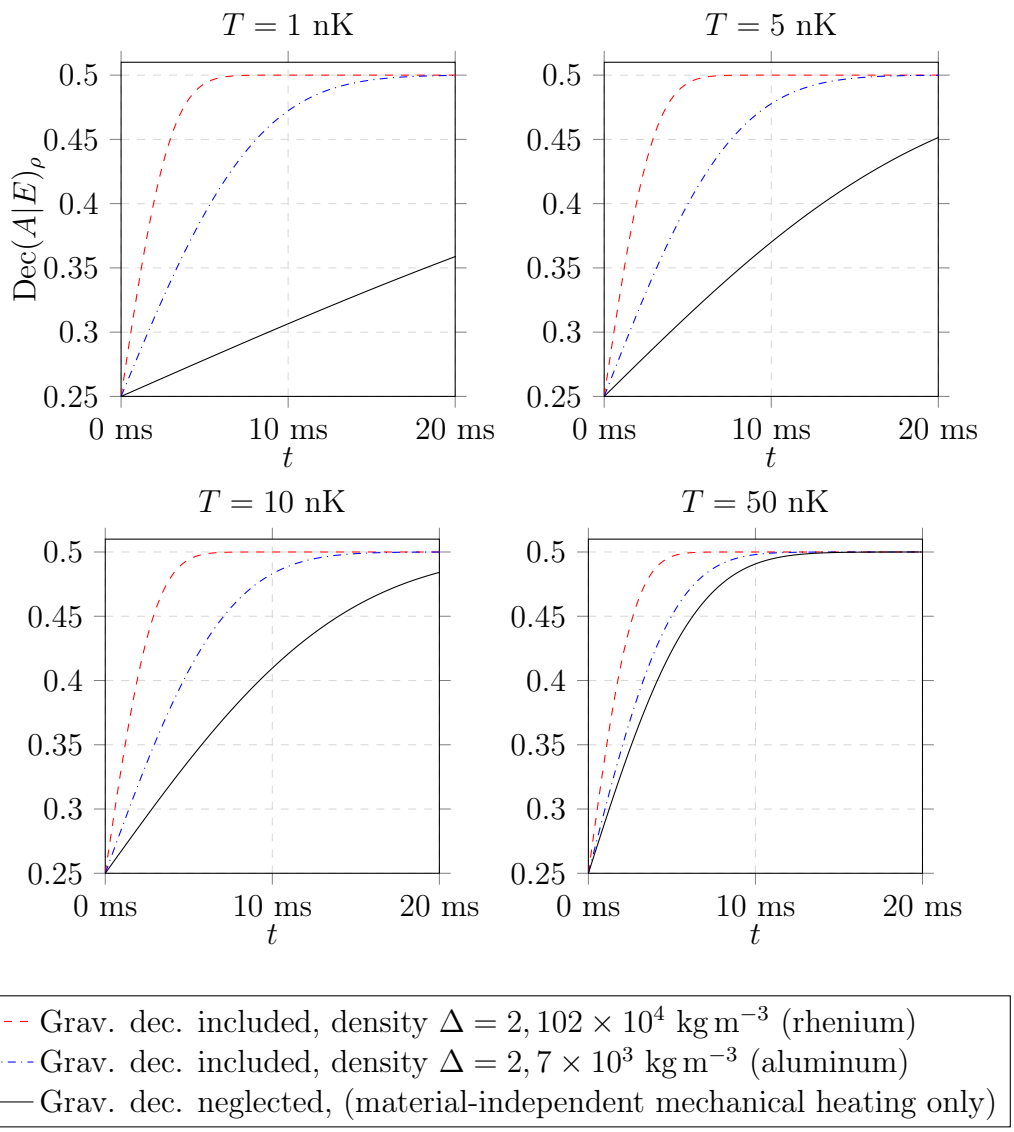


Figure 7.11: Predicted values of the decoherence quantity in the optomechanical experiment. The decoherence quantity $\mathrm{Dec}(A|E)_\rho$ as in Equation (7.220) is plotted as a function of time for different temperatures and two different materials of the mechanical element. In addition, $\mathrm{Dec}(A|E)_\rho$ is plotted for the case where there is no gravitational decoherence, Equation (7.224). The calculations have been made for the experimental parameters $g_0 = 1$ s^{-1}, $\omega_m = 1$ s^{-1} and $\gamma_m = 10^{-10}$ s^{-1}.

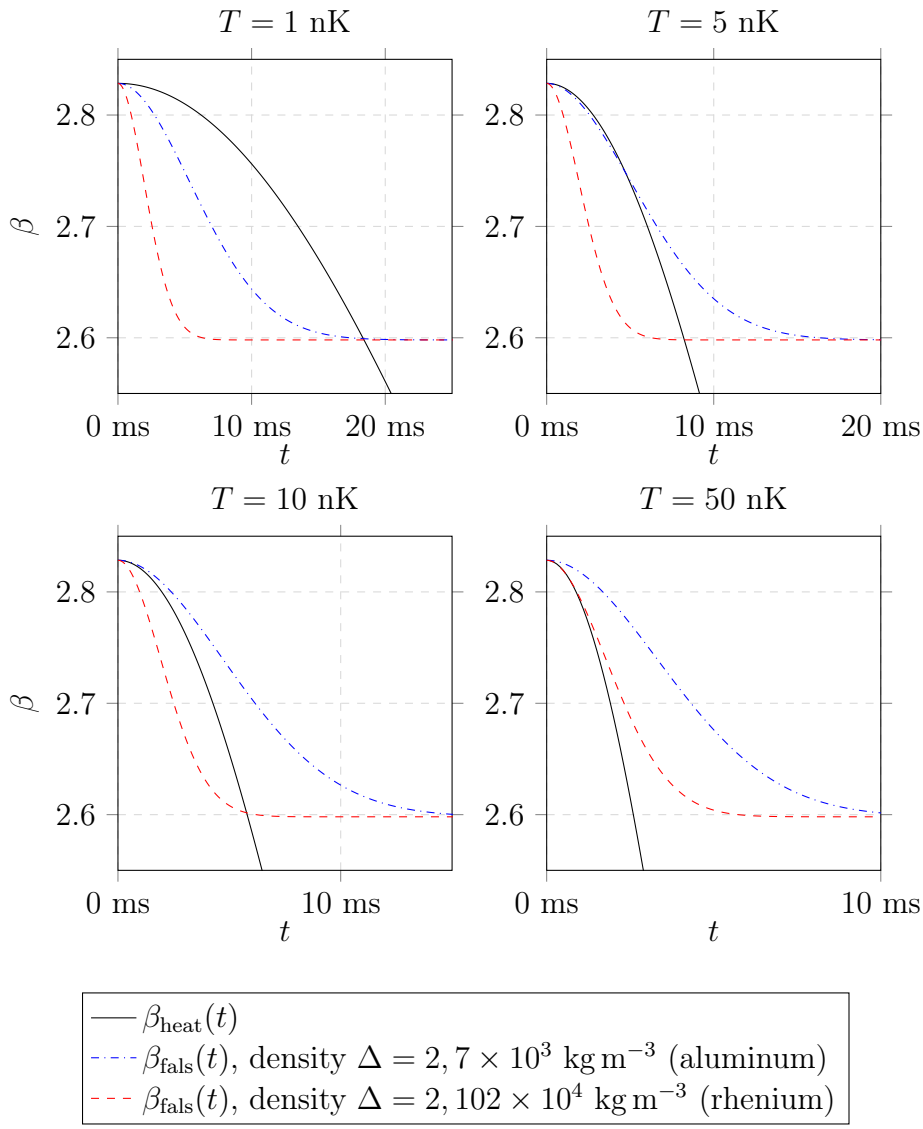


Figure 7.12: Minimal CHSH values for the falsification of the gravitational decoherence model. The quantity β_{fals}, which is the minimal value that needs to be exceeded in the measurement of the CHSH value β_{AB} in order to rule out the gravitational decoherence model, is plotted as a function of time for the same materials and temperatures as above. In addition, the value β_{mech} is plotted, which is the CHSH value that can actually be measured using the standard CHSH measurement in the case where gravitational decoherence is absent and only mechanical heating contributes to the decoherence.

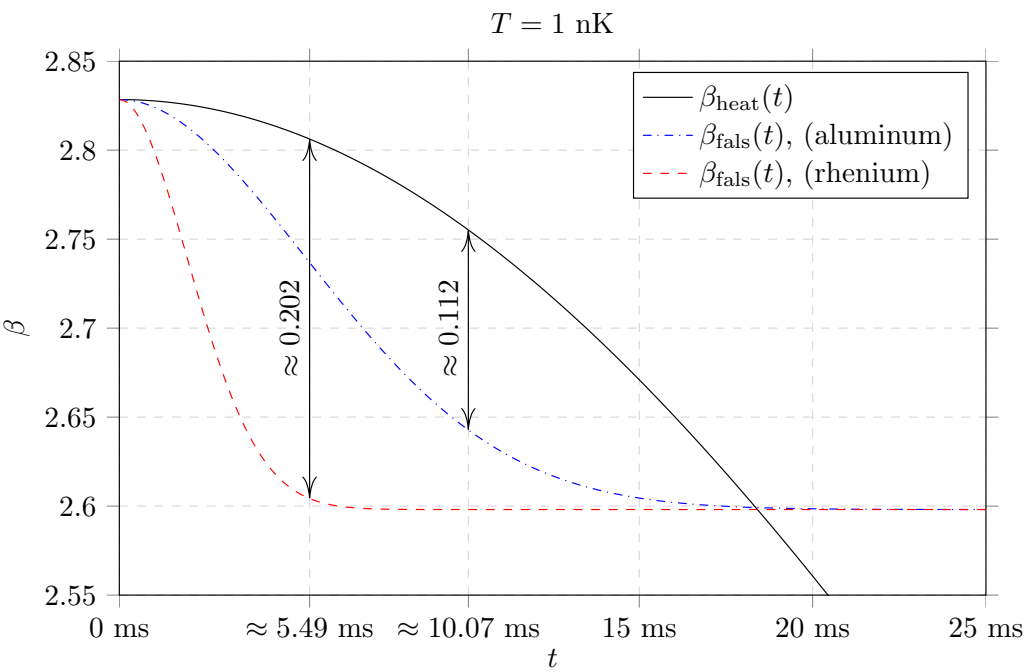


Figure 7.13: Optimal measurement times for ruling out the gravitational decoherence model. The three plots are identical to the ones in the leftmost box in figure 7.12, i.e. for $T = 1$ nK. In addition, the time $t_{\max}$ at which the gap $g(t)$ between β_{mech} and β_{fals} is maximal is indicated for the two cases where the material of the mechanical element has the density of aluminum or rhenium.

Chapter 8

Conclusions and outlook

In this thesis, we have seen a series of results on the estimation of the min-entropy and a generalization thereof as an operational quantification of decoherence. In chapter 5, we analyzed in detail the min-entropy estimate in QKD protocols. We found that the specifics of the sifting subroutine, which is largely ignored in some well-known works in the literature, are crucial for the security of the protocol. We found that some protocols in the literature have a security loophole related to sifting and presented attacks that exploit them. We suggested an alternative protocol that maintains much of the efficiency of the problematic protocols, but which is not subject to the problems that we identified. Our security analysis of the protocol incorporates the sifting stage of the protocol, which not only helps to avoid security loopholes but also allows to develop a more thorough understanding of the QKD security analysis. We hope that this work inspires more complete security proofs of efficient QKD protocols that take sifting-related issues into account.

In chapter 6, we saw that ideas from QKD can be extended to a protocol that allows to estimate an eavesdropper's uncertainty about *quantum* information. We proved that the min-max duality and a chain rule for smooth entropies can be used to show that high amount of uncertainty about information encoded in the $\mathbb{X}$ and $\mathbb{Z}$-basis of a qubit implies high uncertainty about the quantum information encoded in the qubit. We presented a protocol that makes use of this result. It is designed as a distributed protocol for an adversarial scenario: it distributes qubits about which an adversary has a high uncertainty. As we explained, such a protocol may be used as a source for a protocol that extracts entanglement from this source. More precisely, it may be used as part of a protocol that expands a small initial amount of entanglement into a larger final amount of entanglement, akin to QKD protocols which expand a small initial shared key into a large final key.

However, this entanglement distribution perspective is not the only interesting aspect of our result, which is in fact a more general result on min-entropy estimation. For example, another interesting aspect are the implications of our result on channel capacity tomography [Pfi+]. This concerns a non-adversarial scenario, in which a channel that is implemented in the laboratory is tested for its usability for some tasks. Quantum process tomography [CN97] is a method that allows for such tests. However, since it aims at a complete description of the channel in question, it requires a high amount of data that is collected us-

ing a high number of different measurement settings. Moreover, such schemes typically operate under the i.i.d. assumption, which reduces their generality. In contrast, our results can be applied to devise a test that collects data in only two bases to estimate the min-entropy. In this non-adversarial case, our protocol can be simplified such that Alice and Bob have random but perfectly correlated basis choices (that is, they have no basis disagreements). The basis choices still being random, this allows to test quantum channels with correlated errors (i.e. no i.i.d. assumption is necessary). Instead of a full description of the channel, this only yields an estimate of the min-entropy, but since the min-entropy characterizes many practical tasks, this can serve as a relevant figure of merit.

In chapter 7, we found a generalization of the min-entropy estimation to a generalized class of probabilistic theories which, essentially, are only constrained by the no-signalling principle. One may raise the objection that quantitatively, the bound on our decoherence quantity that we found for these general constraints is weak (see the red region in figure 7.5). One reason for the weakness of the bound is that it has been derived using a rather rough estimate of the fidelity that bounds it by the trace distance (see proposition 7.23). As it turns out in a follow-up work on this topic [HPW], this resort to the fidelity is unnecessary, and a significantly improved bound can be derived by bounding the fidelity directly. Apart from that, the strength of our result should not be seen in the quantitative bound that we derived, but in the general concept that it demonstrates. Instead of testing the measured data against the no-signalling principle alone, further properties of nature can be used to further constrain the optimization problem, such as fine-grained uncertainty relations [OW10; HPW]. This way, the influence of such properties on decoherence can be studied, and the measured data can be tested for compatibility with these properties of nature.

Part IV

Appendix

Appendix A

Error rate calculations for the attacks on iterative sifting

A.1 Attack that exploits non-uniform sampling

Here, we calculate the expected error rate for the attack on iterative sifting which exploits non-uniform sampling, as explained in Section 5.5.1. We first recall the relevant conventions that we made. The iterative sifting protocol is described in Protocol 5.1. Eve performs an intercept-resend attack during the loop phase of the protocol. In the first round, she attacks in the $\mathbb{X}$-basis, and in all the other rounds of the loop phase, she attacks in the $\mathbb{Z}$-basis. We defined the error rate in Equation (5.37), namely

$$E = \frac{1}{l}\sum_{i=1}^{l} S_i \oplus T_i \,. \tag{A.1}$$

Moreover, recall that we assume that the $\mathbb{X}$- and $\mathbb{Z}$-basis is the same for Alice, Bob and Eve, and that they are mutually unbiased. This way, if Alice and Bob measure in the same basis, but Eve measures in the other basis, then Eve introduces an error probability of 1/2 on this qubit.

The calculation of $\langle E\rangle$ for this attack goes as follows. We first make a split:

$$\langle E\rangle = \sum_{\vartheta} P[\Theta=\vartheta]\langle E|\Theta=\vartheta\rangle \tag{A.2}$$

$$= \underbrace{P[\Theta=01]\langle E|\Theta=01\rangle}_{\Delta_x} + \underbrace{P[\Theta=10]\langle E|\Theta=10\rangle}_{\Delta_z} \,. \tag{A.3}$$

Writing commas instead of logical conjunction symbols ($\wedge$) for the next equation, we can write Δ_x as

$$\begin{aligned}\Delta_x = \sum_{n_x=1}^{\infty}\Big(& \\ & P[\Theta=01, N_x=n_x, A_1=B_1=0] \quad \langle E|\Theta=01, N_x=n_x, A_1=B_1=0\rangle \\ &+P[\Theta=01, N_x=n_x, A_1\neq B_1] \quad \langle E|\Theta=01, N_x=n_x, A_1\neq B_1\rangle \\ &+\underbrace{P[\Theta=01, N_x=n_x, A_1=B_1=1]}_{0} \quad \langle E|\Theta=01, N_x=n_x, A_1=B_1=1\rangle\Big)\,.\end{aligned} \tag{A.4}$$

The third summand on the right hand side of Equation (A.4) vanishes because $\Theta = 01$ is impossible if Alice and Bob have a $\mathbb{Z}$-agreement in the first round of the loop phase. The event

$$\Theta = 01 \wedge N_x = n_x \wedge A_1 = B_1 = 0 \tag{A.5}$$

consists of all histories of the protocol in which Alice and Bob have an $\mathbb{X}$-agreement in the first round and n_x $\mathbb{X}$-agreements in total. Infinitely many such histories are possible because an arbitrary number of disagreements is possible. We express the probability of the event (A.5) as the marginal of the probability of the event

$$\Theta = 01 \wedge N_x = n_x \wedge A_1 = B_1 = 0 \wedge N_d = n_d\,. \tag{A.6}$$

The event (A.6) consists of $\binom{n_x+n_d+1}{n_d}$ histories of the protocol, and each history has the probability $(p_x^2)^{n_x} p_z^2 (2p_x p_z)^{n_d}$. Therefore,

$$\begin{aligned} &P[\Theta = 01 \wedge N_x = n_x \wedge A_1 = B_1 = 0] && \text{(A.7)}\\ &= \sum_{n_d=0}^{\infty} P[\Theta = 01 \wedge N_x = n_x \wedge A_1 = B_1 = 0 \wedge N_d = n_d] && \text{(A.8)}\\ &= \sum_{n_d=0}^{\infty} (p_x^2)^{n_x} p_z^2 (2p_x p_z)^{n_d} \binom{n_x + n_d - 1}{n_d} && \text{(A.9)} \end{aligned}$$

Moreover, we have that

$$\langle E | \Theta = 01 \wedge N_x = n_x \wedge A_1 = B_1 = 0 \rangle = \frac{1}{4}\left(1 - \frac{1}{n_x}\right)\,. \tag{A.10}$$

The validity of equation (A.10) can be seen as follows. On the second bit of S and T, there is no error because it comes from a round in which all parties have measured in the $\mathbb{Z}$-basis. Hence, the left hand side of (A.10) is the probability of getting an error on the first bit of S and T, divided by the total number of bits, 2. Hence, we need to determine the error probability of the first bit. If $N_x = 1$, then the first bit comes from the first round of the loop phase, in which Alice, Bob and Eve have measured in the $\mathbb{X}$-basis and hence, there is no error. However, for $N_x = n_x$, the first bit of S and T is chosen at random from one of the n_x $\mathbb{X}$-agreements. In only one of these n_x rounds, Eve has measured in the $\mathbb{X}$-basis, and in $n_x - 1$ rounds, she measured in the $\mathbb{Z}$-basis. Hence, the probability that Eve measured in the wrong basis on the first bit of S and T is $(n_x - 1)/n_x$, and therefore the error probability of the first bit is $1/2 \cdot (n_x - 1)/n_x$. Thus,

$$\begin{aligned} \langle E | \Theta = 01 \wedge N_x = n_x \wedge A_1 = B_1 = 0 \rangle &= \frac{1}{2} \cdot \frac{1}{2}\left(\frac{n_x}{n_x - 1}\right) && \text{(A.11)}\\ &= \frac{1}{4}\left(1 - \frac{1}{n_x}\right)\,. && \text{(A.12)} \end{aligned}$$

Similarly, we get

$$P[\Theta = 01 \wedge N_x = n_x \wedge A_1 \neq B_1] = \sum_{n_d=0}^{\infty} (p_x^2)^{n_x} p_z^2 (2p_x p_z)^{n_d} \binom{n_x + n_d - 1}{n_x} \tag{A.13}$$

and

$$\langle E|\Theta = 01 \wedge N_x = n_x \wedge A_1 \neq B_1\rangle = \frac{1}{4}\,. \tag{A.14}$$

Taking Equations (A.9), (A.10), (A.13) and (A.14) together, we get that

$$\Delta_x = \frac{1}{4}\sum_{n_x=1}^{\infty}\sum_{n_d=0}^{\infty}(p_x^2)^{n_x}p_z^2(2p_xp_z)^{n_d}\left(\binom{n_x+n_d-1}{n_d}\left(1-\frac{1}{n_x}\right) + \binom{n_x+n_d-1}{n_x}\right). \tag{A.15}$$

In a similar way, we get

$$\Delta_z = \frac{1}{4}\sum_{n_z=1}^{\infty}\sum_{n_d=0}^{\infty}p_x^2(p_z^2)^{n_z}(2p_xp_z)^{n_d}\left(\binom{n_z+n_d-1}{n_d} + \binom{n_z+n_d-1}{n_d}\left(1+\frac{1}{n_x}\right)\right). \tag{A.16}$$

Equations (A.3), (A.15) and (A.16) taken together result in

$$\langle E\rangle = \sum_{n_d=0}^{\infty}(2p_xp_z)^{n_d}\Bigg[\tag{A.17}$$

$$\sum_{n_x=1}^{\infty}(p_x^2)^{n_x}p_x^2\left(\binom{n_x+n_d-1}{n_d}\left(1-\frac{1}{n_x}\right)+\binom{n_x+n_d-1}{n_x}\right) + \sum_{n_z=1}^{\infty}p_x^2(p_z^2)^{n_z}\left(\binom{n_z+n_d-1}{n_z}+\binom{n_z+n_d-1}{n_d}\left(1+\frac{1}{n_z}\right)\right)\Bigg]. \tag{A.18}$$

Figure 5.6 shows a plot of $\langle E\rangle$ as in (A.17) as a function of p_x. As one can see, $\langle E\rangle$ achieves a minimum of $\langle E\rangle \approx 22.8\%$ for $p_x \approx 0.73$.

A.2 Attack that exploits basis-information leak

Now we calculate the expected error rate of iterative sifting for the attack which exploits basis-information leak as described in Section 5.5.2. As before, let $\langle E\rangle$ be the expected value of the error rate as defined in Equation (5.37). Again, we assume that the $\mathbb{X}$- and $\mathbb{Z}$-basis are the same for Alice, Bob and Eve and that they are mutually unbiased. Recall the strategy of Eve's intercept-resend attack: Before the first round of the loop phase, Eve flips a fair coin. Let F be the random variable of the coin flip outcome and let 0 and 1 be its possible values. If $F = 0$, then in the first round, Eve attacks in the $\mathbb{X}$ basis, and if $F = 1$, she attacks in the $\mathbb{Z}$-basis. In the subsequent rounds, she keeps attacking in that basis until Alice and Bob first reach a basis agreement. If it is an $\mathbb{X}$-agreement (equivalent to $\Theta = 01$), Eve attacks in the $\mathbb{Z}$-basis in

all remaining rounds, and if it is a $\mathbb{Z}$-agreement (equivalent to $\Theta = 10$), she attacks in the $\mathbb{X}$-basis in all remaining rounds.

The calculation of $\langle E \rangle$ goes as follows:

$$\begin{aligned}
\langle E \rangle &= P_F(0)\langle E|F=0\rangle + P_F(1)\langle E|F=1\rangle && \text{(A.19)}\\
&= \langle E|F=0\rangle && \text{(A.20)}\\
&= \underbrace{P_\Theta(01)}_{1/2}\langle E|F=0\wedge\Theta=01\rangle + \underbrace{P_\Theta(10)}_{1/2}\underbrace{\langle E|F=0\wedge\Theta=10\rangle}_{1/4}\,. && \text{(A.21)}
\end{aligned}$$

Equality (A.19) is just a decomposition of $\langle E \rangle$ into conditional expectations. Equality (A.20) follows from the fact that the problem is symmetric under the exchange of $\mathbb{X}$ and $\mathbb{Z}$, i.e. under the exchange of 0 and 1. The only quantity that is not trivial to calculate in Equation (A.21) is the expected value of the error rate, given that Eve first measures in $\mathbb{X}$ and that the first basis agreement is an $\mathbb{X}$-agreement. It is calculated as follows:

$$\begin{aligned}
&\langle E|F=0\wedge\Theta=01\rangle && \text{(A.22)}\\
&= \sum_{n_x=1}^{\infty}\langle E|F=0\wedge\Theta=01\wedge N_x=n_x\rangle\,\underbrace{P_{N_x|\Theta F}(n_x|01,0)}_{P_{N_x|\Theta}(n_x|01)} && \text{(A.23)}\\
&= \sum_{n_x=1}^{\infty}\underbrace{\langle E|F=0\wedge\Theta=01\wedge N_x=n_x\rangle}_{\frac{n_x-1}{4n_x}}\underbrace{P_{N_x\Theta}(n_x,01)}_{\sum_{n_d=0}^{\infty}(p_x^2)^{n_x}p_z^2(2p_xp_z)^{n_d}\binom{n_x+n_d}{n_d}}\underbrace{\frac{1}{P_\Theta(01)}}_{2} && \text{(A.24)}\\
&= \sum_{n_x=1}^{\infty}\frac{n_x-1}{2n_x}\sum_{n_d=0}^{\infty}(p_x^2)^{n_x}p_z^2(2p_xp_z)^{n_d}\binom{n_x+n_d}{n_d} && \text{(A.25)}\\
&= \frac{1}{4}(1-\ln 2)\,, && \text{(A.26)}
\end{aligned}$$

Therefore,

$$\begin{aligned}
\langle E \rangle &= \frac{1}{2}\frac{1}{4}(1-\ln 2) + \frac{1}{2}\frac{1}{4} && \text{(A.27)}\\
&= \frac{2-\ln 2}{8} && \text{(A.28)}\\
&\approx 16.3\%\,. && \text{(A.29)}
\end{aligned}$$

A.3 Attack that exploits both problems

Here we present the error rate induced by the intercept-resend attack presented in Section 5.5.4, which exploits both non-uniform sampling and basis information leak. Let us recall the attack strategy. In the first round of the loop phase of the iterative sifting protocol, she attacks in the $\mathbb{X}$-basis. She keeps doing that in subsequent rounds until Alice and Bob announce a basis-agreement. If they announce an $\mathbb{X}$-agreement, Eve attacks in the $\mathbb{Z}$-basis in all the following rounds. Otherwise, she keeps attacking in the $\mathbb{X}$-basis.

The calculation of the error rate is similar to the calculations done in Appendices A.1 and A.2. We only show the result here:

$$\langle E \rangle = \sum_{n_z=1}^{\infty} \sum_{n_d=0}^{\infty} p_x^2 p_z^{2n_z} (2p_x p_z)^{n_d} \binom{n_z + n_d}{n_d} \frac{1}{4} + \sum_{n_x=1}^{\infty} \sum_{n_d=0}^{\infty} p_x^{2n_x} p_z^2 (2p_x p_z)^{n_d} \binom{n_x + n_d}{n_d} \frac{n_x - 1}{4n_x} . \tag{A.30}$$

A plot of (A.30) is shown in Figure 5.6 as a function of p_x. As one can see, the expected error rate has a minimum of $\langle E \rangle \approx 15.8\%$ for $p_x \approx 0.57$. Hence, this combined attack on both problems performs much better than the one on non-uniform sampling alone (with a minimal expected error rate of $\approx 22.8\%$, see Section 5.5.1) and even better than the attack on the basis information leak alone (with a minimal expected error rate of $\approx 16.3\%$, see Section 5.5.2).

Bibliography

[Abe+09] Anura Abeyesinghe et al. "The mother of all protocols: restructuring quantum information's family tree". In: *Proc. R. Soc. A* **465**(2108) (2009), pp. 2537–2563. DOI: 10.1098/rspa.2009.0202 (cited on page 56).

[Ací+07] Antonio Acín et al. "Device-Independent Security of Quantum Cryptography against Collective Attacks". In: *Phys. Rev. Lett.* **98**(23) (2007), p. 230501 (cited on page 141).

[AH07] C. Anastopoulous and B. L. Hu. "Decoherence in quantum gravity: issues and critiques". In: *Journal of Physics: Conference Series* **67** (2007), p. 012012 (cited on pages 128, 167).

[AH13] C. Anastopoulous and B. L. Hu. "A Master equation for gravitational decoherence: Probing the textures of spacetime". In: *Class. Quant. Grav.* **30** (2013), p. 165007 (cited on pages 128, 167).

[Ass06] Gilles van Assche. *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, 2006 (cited on pages 3, 65, 71).

[Bac+13] Davide Bacco et al. "Experimental quantum key distribution with finite-key security analysis for noisy channels". In: *Nat. Commun.* **4** (2013). DOI: 10.1038/ncomms3363 (cited on pages 68, 71, 72, 75).

[Bar+05] Jonathan Barrett et al. "Nonlocal correlations as an information-theoretic resource". In: *Phys. Rev. A* **71**(2) (2005), p. 022101 (cited on page 159).

[Bar+08] Howard Barnum et al. "Teleportation in General Probabilistic Theories". In: (2008). arXiv: 0805.3553 [quant-ph] (cited on page 145).

[Bar07] Jonathan Barrett. "Information processing in generalized probabilistic theories". In: *Phys. Rev. A* **75** (3 2007), p. 032304. DOI: 10.1103/PhysRevA.75.032304. eprint: quant-ph/0508211. URL: http://link.aps.org/doi/10.1103/PhysRevA.75.032304 (cited on page 145).

[BB84] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.* (1984), pp. 175–179 (cited on pages 10, 109).

[BBJ13] I. Bjelaković, H. Boche, and G. Janßen. "Universal quantum state merging". In: *Journal of Mathematical Physics* **54**(3) (2013). DOI: 10.1063/1.4795243 (cited on page 60).

[BBR88] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. "Privacy Amplification by Public Discussion". In: *SIAM J. Comput.* **17**(2) (1988), pp. 210–229 (cited on pages 48, 52).

[Bel64] John S. Bell. "On the Einstein Podolsky Rosen Paradox". In: *Physics* **1**(3) (1964), pp. 195–290 (cited on page 131).

[Ben+92] Charles H. Bennett et al. "Experimental quantum cryptography". In: *Journal of Cryptology* **5**(1) (1992), pp. 3–28. DOI: 10.1007/BF00191318 (cited on pages 48, 52).

[Ben+95] C. H. Bennett et al. "Generalized privacy amplification". In: *IEEE Trans. Inf. Theory* **41**(6) (1995), pp. 1915–1923. DOI: 10.1109/18.476316 (cited on page 48).

[Ben+96a] Charles H. Bennett et al. "Concentrating partial entanglement by local operations". In: *Phys. Rev. A* **53** (4 1996), pp. 2046–2052. DOI: 10.1103/PhysRevA.53.2046 (cited on page 109).

[Ben+96b] Charles H. Bennett et al. "Mixed-state entanglement and quantum error correction". In: *Phys. Rev. A* **54** (5 1996), pp. 3824–3851. DOI: 10.1103/PhysRevA.54.3824 (cited on page 109).

[Ber08] Mario Berta. "Single-shot Quantum State Merging". Diploma thesis. ETH Zürich, 2008. arXiv: 0912.4495 [quant-ph] (cited on pages 56, 58).

[BGL07] H. P. Breuer, E. Göklü, and C. Lämmerzah. In: *Class. Quant. Grav.* **26** (2007), p. 105012 (cited on pages 128, 167).

[BGW09] Howard Barnum, Carl Philipp Gaebler, and Alexander Wilce. "Ensemble Steering, Weak Self-Duality, and the Structure of Probabilistic Theories". In: (2009). arXiv: 0912.5532 [quant-ph] (cited on page 145).

[Bru+14] Nicolas Brunner et al. "Bell nonlocality". In: *Rev. Mod. Phys.* **86** (2 2014), pp. 419–478. DOI: 10.1103/RevModPhys.86.419 (cited on pages 131, 157).

[BS94] Gilles Brassard and Louis Salvail. "Advances in Cryptology—EUROCRYPT '93". In: ed. by Tor Helleseth. Springer Berlin Heidelberg, 1994. Chap. Secret-Key Reconciliation by Public Discussion, pp. 410–423. DOI: 10.1007/3-540-48285-7_35 (cited on page 52).

[BW09] Howard Barnum and Alexander Wilce. "Ordered linear spaces and categories as frameworks for information-processing characterizations of quantum and classical theory". In: (2009). arXiv: 0908.2354 [quant-ph] (cited on page 145).

[BW11] Howard Barnum and Alexander Wilce. "Information Processing in Convex Operational Theories". In: *Electron. Notes Theor. Comput. Sci.* **270**(1) (2011), pp. 3–15. ISSN: 1571-0661. DOI: 10.1016/j.entcs.2011.01.002. arXiv: 0908.2352 [quant-ph]. URL: http://www.sciencedirect.com/science/article/pii/S157106611100003X (cited on page 145).

[Cac97] Christian Cachin. "Advances in Cryptology — EUROCRYPT '97". In: ed. by Walter Fumy. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997. Chap. Smooth Entropy and Rényi Entropy, pp. 193–208. DOI: 10.1007/3-540-69053-0_14 (cited on page 43).

[CDP11] Giulio Chiribella, Giacomo Mauro D'Ariano, and Paolo Perinotti. "Informational derivation of quantum theory". In: *Phys. Rev. A* **84** (1 2011), p. 012311. DOI: 10.1103/PhysRevA.84.012311. arXiv: 1011.6451 [quant-ph]. URL: http://link.aps.org/doi/10.1103/PhysRevA.84.012311 (cited on page 145).

[Cho75] Man-Duen Choi. "Completely Positive Linear Maps on Complex Matrices". In: *Linear Algebra and its Applications* **10**(3) (1975), pp. 285–290. DOI: 10.1016/0024-3795(75)90075-0 (cited on page 41).

[Cla+69] John F. Clauser et al. "Proposed Experiment to Test Local Hidden-Variable Theories". In: *Phys. Rev. Lett.* **23**(15) (1969), pp. 880–884 (cited on pages 128, 130, 131).

[CM97] Christian Cachin and Ueli Maurer. "Smoothing probability distributions and smooth entropy". In: *Proceedings of IEEE International Symposium on Information Theory 1997*. 1997, pp. 91–. DOI: 10.1109/ISIT.1997.613006 (cited on page 43).

[CN97] Isaac L. Chuang and M. A. Nielsen. "Prescription for experimental determination of the dynamics of a quantum black box". In: *J. Mod. Opt.* **44**(11–12) (1997), pp. 2455–2467. DOI: 10.1080/09500349708231894 (cited on page 179).

[Cur+14] Marcos Curty et al. "Finite-key analysis for measurement-device-independent quantum key distribution". In: *Nat. Commun.* **5** (2014). DOI: 10.1038/ncomms4732 (cited on pages 68, 71, 72, 75).

[DB07] W. Dür and H. J. Briegel. "Entanglement purification and quantum error correction". In: *Reports on Progress in Physics* **70**(8) (2007), p. 1381 (cited on page 109).

[DB11] Borivoje Dakic and Caslav Brukner. "Quantum Theory and Beyond: Is Entanglement Special?" In: *Deep Beauty: Understanding the Quantum World through Mathematical Innovation*. Ed. by Hans Halvorson. Cambridge University Press, 2011, pp. 365–392. DOI: 10.1017/CBO9780511976971.011 (cited on page 145).

[Deu+96] David Deutsch et al. "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels". In: *Phys. Rev. Lett.* **77** (13 1996), pp. 2818–2821. DOI: 10.1103/PhysRevLett.77.2818 (cited on page 109).

[Dev05] Igor Devetak. "The private classical capacity and quantum capacity of a quantum channel". In: *IEEE Trans. Inf. Theory* **51**(1) (2005), pp. 44–55 (cited on page 9).

[Dio11] L. Diosi. "The gravity-related decoherence master equation from hybrid dynamics". In: *J. Phys.: Conf. Ser.* **306** (2011), p. 012006 (cited on pages 128, 167).

[Dio84] L. Diosi. In: *Phys. Lett. A* **105** (1984), p. 199 (cited on pages 128, 167).

[Dio87] L. Diosi. In: *Phys. Lett.* **120** (1987), p. 377 (cited on pages 128, 167).

[Dió89] L. Diósi. "Models for universal reduction of macroscopic quantum fluctuations". In: *Phys. Rev. A* **40**(3) (1989), pp. 1165–1174 (cited on pages 128, 136, 167, 168).

[DL70] E. B. Davies and J. T. Lewis. "An Operational Approach to Quantum Probability". In: *Commun. Math. Phys.* **17**(3) (1970), pp. 239–260 (cited on pages 145, 150).

[DM10] L.-M. Duan and C. Monroe. "Colloquium: Quantum networks with trapped ions". In: *Rev. Mod. Phys.* **82**(2) (2010), pp. 1209–1224 (cited on page 168).

[Doh+08] Andrew C. Doherty et al. "The quantum moment problem and bounds on entangled multi-prover games". In: *Proc. 23rd IEEE Conf. on Computational Complexity (CCC'08)* (2008), pp. 199–210 (cited on page 151).

[Dup+10] Frédéric Dupuis et al. "One-shot decoupling". In: *Commun. Math. Phys.* **328**(1) (2010), pp. 251–284. DOI: 10.1007/s00220-014-1990-4 (cited on pages 47, 56–58, 60).

[Dup09] Frédéric Dupuis. "The decoupling approach to quantum information theory". PhD thesis. Université de Montréal, 2009 (cited on page 56).

[Edw70] C.M. Edwards. "The operational approach to algeraic quantum theory I". In: *Comm. Math. Phys.* **16**(3) (1970), pp. 207–230 (cited on page 145).

[Eke91] Artur K. Ekert. "Quantum cryptography based on Bell's theorem". In: *Phys. Rev. Lett.* **67**(6) (1991), pp. 661–663 (cited on page 10).

[FG99] Christopher A. Fuchs and Jeroen van de Graaf. "Cryptographic distinguishability measures for quantum-mechanical states". In: *IEEE Trans. Inf. Theory* **45**(4) (1999), pp. 1216–1227 (cited on page 158).

[Fuc95] Christopher A. Fuchs. "Distinguishability and accessible information in quantum theory". PhD thesis. University of New Mexico, 1995. arXiv: quant-ph/9601020 [quant-ph] (cited on page 35).

[GW15] Evan Greene and Jon A. Wellner. *Exponential Bounds for the Hypergeometric Distribution*. 2015. arXiv: 1507.08298v2 [math.ST] (cited on page 103).

[Har01] Lucien Hardy. "Quantum Theory From Five Reasonable Axioms". In: (2001). eprint: quant-ph/0101012 (cited on page 145).

[Hay+08] Patrick Hayden et al. "A Decoupling Approach to the Quantum Capacity". In: *Open Systems & Information Dynamics* **15**(01) (2008), pp. 7–19. DOI: 10.1142/S1230161208000043 (cited on page 56).

[HE94] Bruno Huttner and Artur K. Ekert. "Information gain in eavesdropping". In: *J. Mod. Opt.* **41**(12) (1994), pp. 2455–2466. DOI: 10.1080/09500349414552301 (cited on page 82).

[Hen+15] B. Hensen et al. "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". In: *Nature* **526**(7575) (2015), pp. 682–686 (cited on page 131).

[HH96] Ryszard Horodecki and Michal Horodecki. "Information-theoretic aspects of inseparability of mixed states". In: *Phys. Rev. A* **54**(3) (Sept. 1996), pp. 1838–1843. ISSN: 1050-2947. DOI: 10.1103/PhysRevA.54.1838. URL: http://link.aps.org/doi/10.1103/PhysRevA.54.1838 (cited on page 138).

[HHH95a] Ryszard Horodecki, Pawel Horodecki, and Michal Horodecki. "Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition". In: *Phys. Lett. A* **200**(5) (1995), pp. 340–344. DOI: 10.1016/0375-9601(95)00214-N (cited on page 138).

[HHH95b] Ryszard Horodecki, Pawel Horodecki, and Michal Horodecki. "Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition". In: *Phys. Lett. A* **200**(5) (1995), pp. 340–344. DOI: 10.1016/0375-9601(95)00214-N (cited on page 174).

[Hor+09] Ryszard Horodecki et al. "Quantum entanglement". In: *Rev. Mod. Phys.* **81** (2 2009), pp. 865–942. DOI: 10.1103/RevModPhys.81.865 (cited on page 59).

[HOW05] Michal Horodecki, Jonathan Oppenheim, and Andreas Winter. "Partial quantum information". In: *Nature* **436**(7051) (2005), pp. 673–676. DOI: 10.1038/nature03909 (cited on page 58).

[HOW06] Michal Horodecki, Jonathan Oppenheim, and Andreas Winter. "Quantum State Merging and Negative Information". In: *Comm. Math. Phys.* **269**(1) (2006), pp. 107–136 (cited on page 58).

[HP07] Patrick Hayden and John Preskill. "Black holes as mirrors: quantum information in random subsystems". In: *Journal of High Energy Physics* **2007**(09) (2007), p. 120. DOI: 10.1088/1126-6708/2007/09/120 (cited on page 58).

[HP10] W. Cary Huffman and Vera Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 2010 (cited on page 53).

[HPW] Willem Hekman, Corsin Pfister, and Stephanie Wehner. In preparation (cited on page 180).

[HT16] Masahito Hayashi and Toyohiro Tsurumaru. "More Efficient Privacy Amplification With Less Random Seeds via Dual Universal Hash Function". In: *IEEE Trans. Inf. Theory* **62**(4) (2016), pp. 2213–2232. DOI: 10.1109/TIT.2016.2526018 (cited on page 48).

[Hu14] B. L. Hu. "Gravitational decoherence, alternative theories, and semiclassical gravity". In: *Journal of Physics: Conference Series* **504** (2014), p. 012021 (cited on pages 128, 167).

[ILL89] Russell Impagliazzo, Leonid A. Levin, and Michael Luby. "Pseudorandom Generation from One-way Functions". In: *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*. STOC '89. New York, NY, USA: ACM, 1989, pp. 12–24. DOI: 10.1145/73007.73009 (cited on page 48).

[Jam72] Andrzej Jamiolkowski. "Linear transformations which preserve trace and positive semidefiniteness of operators". In: *Rep. Math. Phys.* **3**(4) (1972), pp. 275–278. DOI: 10.1016/0034-4877(72)90011-0 (cited on page 41).

[JL13] Peter Janotta and Raymond Lal. "Generalized probabilistic theories without the no-restriction hypothesis". In: *Phys. Rev. A* **87**(5) (2013), p. 052131. DOI: 10.1103/PhysRevA.87.052131 (cited on page 147).

[Joo+03] Erich Joos et al. *Decoherence and the Appearance of a Classical World in Quantum Theory*. Springer-Verlag Berlin Heidelberg, 2003 (cited on page 4).

[Kay98] B. Kay. In: *Class. Quant. Grav.* **15** (1998), p. L89 (cited on pages 128, 167).

[Kes+12] T. Kessler et al. "A sub-40-mHz-linewidth laser based on a silicon single-crystal optical cavity". In: *Nature Photonics* **6** (2012), p. 687 (cited on page 168).

[KMR05] Robert Konig, Ueli Maurer, and Renato Renner. "On the power of quantum memory". In: *IEEE Trans. Inf. Theory* **51**(7) (2005), pp. 2391–2401. DOI: 10.1109/TIT.2005.850087 (cited on page 48).

[KR11] Robert König and Renato Renner. "Sampling of Min-Entroy Relative to Quantum Knowledge". In: *IEEE Trans. Inf. Theory* **57**(7) (2011). DOI: 10.1109/TIT.2011.2146730 (cited on page 33).

[Kra55] Charles H. Kraft. "Some conditions for consistency and uniform consistency of statistical procedures". In: *University of California Publications in Statistics, Vol. 1*. University of California Press, 1955, pp. 125–142 (cited on page 158).

[Kra83] Karl Kraus. *States, Effects, and Operations*. Springer-Verlag Berlin Heidelberg, 1983 (cited on page 25).

[KRS09] Robert König, Renato Renner, and Christian Schaffner. "The operational meaning of min- and max-entropy". In: *IEEE Trans. Inf. Theory* **55**(9) (2009), pp. 4337–4347 (cited on pages 12, 47, 58, 61, 111).

[KTM14] D. Kafri, J. M. Taylor, and G. J. Milburn. "A classical channel model for gravitational decoherence". In: *New J. Phys.* **16**(6) (2014), p. 065020 (cited on pages 128, 167, 168).

[LC99] Hoi-Kwong Lo and H.F. Chau. "Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances". In: *Science* **283**(5410) (1999), pp. 2050–2056. DOI: 10.1126/science.283.5410.2050 (cited on page 109).

[LCA05] Hoi-Kwong Lo, H. F. Chau, and M. Ardehali. "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security". In: *J. Cryptol.* **18**(2) (2005), pp. 133–165. DOI: 10.1007/s00145-004-0142-y (cited on pages 69, 85).

[Lim+13] Charles Ci Wen Lim et al. "Device-Independent Quantum Key Distribution with Local Bell Test". In: *Phys. Rev. X* **3**(3) (2013), p. 031006. DOI: 10.1103/PhysRevX.3.031006 (cited on pages 68, 71, 72, 75).

[Lim+14] Charles Ci Wen Lim et al. "Concise security bounds for practical decoy-state quantum key distribution". In: *Phys. Rev. A* **89**(2) (2014), p. 022307. DOI: 10.1103/PhysRevA.89.022307 (cited on pages 68, 71, 72, 75).

[Lin99] J.H. van Lint. *Introduction to Coding Theory*. Springer-Verlag Berlin Heidel Heidelberg, 1999 (cited on page 107).

[Llo97] Seth Lloyd. "Capacity of the noisy quantum channel". In: *Phys. Rev. A* **55**(3) (1997), pp. 1613–1622 (cited on page 9).

[Mac92] Ludwig Mach. "Über einen Interferenzrefraktor". In: *Zeitschrift für Instrumentenkunde* **12** (1892), pp. 89–93 (cited on page 5).

[Mac93] George Whitelaw Mackey. *The mathematical foundations of quantum mechanics*. W.A. Benjamin, 1093 (cited on page 145).

[Mar+03] W. Marshall et al. "Towards quantum superpositions of a mirror". In: *Phys. Rev. Lett.* **91** (2003), p. 130401 (cited on page 167).

[Mas+12] Lluís Masanes et al. "A digital approach to quantum theory". In: (2012). arXiv: 1208.0493 [quant-ph] (cited on page 145).

[MM11a] Lluís Masanes and Markus P. Müller. "A derivation of quantum theory from physical requirements". In: *New J. Phys.* **13**(6) (2011), p. 063001. DOI: 10.1088/1367-2630/13/6/063001. arXiv: 1004.1483 [quant-ph]. URL: http://stacks.iop.org/1367-2630/13/i=6/a=063001 (cited on page 145).

[MM11b] Matthew McKague and Michele Mosca. "Theory of Quantum Computation, Communication, and Cryptography: 5th Conference, TQC 2010, Leeds, UK, April 13-15, 2010, Revised Selected Papers". In: ed. by Wim Dam, Vivien M. Kendon, and Simone Severini. Springer Berlin Heidelberg, 2011. Chap. Generalized Self-testing and the Security of the 6-State Protocol, pp. 113–130. DOI: 10.1007/978-3-642-18073-6_10 (cited on page 131).

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000 (cited on pages 4, 6, 9, 25–28, 32, 35, 37–39, 109).

[Neu27] John von Neumann. "Thermodynamik quantenmechanischer Gesamtheiten". In: *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* **1927** (1927), pp. 273–291 (cited on page 43).

[NJ+11] B. R. Nisbet-Jones et al. "Highly efficient source for indistinguishable single photons of controlled shape". In: *New J. Phys.* **13**(10) (2011), p. 103036 (cited on page 168).

[OW10] Jonathan Oppenheim and Stephanie Wehner. "The Uncertainty Principle Determines the Nonlocality of Quantum Mechanics". In: *Science* **330**(6007) (2010), pp. 1072–1074. DOI: 10.1126/science.1192065 (cited on page 180).

[Pau03] Vern Paulsen. *Completely Bounded Maps and Operator Algebras*. Cambridge University Press, 2003 (cited on page 41).

[Pen96] R. Penrose. "On Gravity's role in Quantum State Reduction". In: *General Relativity and Gravitation* **28** (1996), p. 581 (cited on pages 128, 167).

[Pfi+] Corsin Pfister et al. "Capacity tomography of quantum channels with correlated errors". In preparation (cited on pages vii, 179).

[Pfi+15] Corsin Pfister et al. "Understanding nature from experimental observations: a theory independent test for gravitational decoherence". In: (2015). arXiv: 1503.00577 [quant-ph] (cited on page vii).

[Pfi+16] Corsin Pfister et al. "Sifting attacks in finite-size quantum key distribution". In: *New J. Phys.* **18**(5) (2016), p. 053001. DOI: 10.1088/1367-2630/18/5/053001 (cited on page vii).

[Pfi12] Corsin Pfister. "One simple postulate implies that every polytopic state space is classical". In: (2012). arXiv: 1203.5622 [quant-ph] (cited on pages 146, 147).

[Pil67] John Emanuel de Pillis. "Linear Transformations Which Preserve Hermitian and Positive Semidefinite Operators". In: *Pacific J. Math.* **23**(1) (1967), pp. 129–137. DOI: 10.2140/pjm.1967.23.129 (cited on page 41).

[PR92] Sandu Popescu and Daniel Rohrlich. "Which states violate Bell's inequality maximall?" In: *Phys. Rev. A.* **169**(6) (1992), pp. 411–414. DOI: 10.1016/0375-9601(92)90819-8 (cited on page 131).

[PW13] Corsin Pfister and Stephanie Wehner. "An information-theoretic principle implies that any discrete physical theory is classical". In: *Nat. Commun.* **4**(1851) (2013). DOI: 10.1038/ncomms2821. arXiv: 1210.0194 [quant-ph] (cited on pages vii, 145).

[Ren05] Renato Renner. "Security of Quantum Key Distribution". PhD thesis. ETH Zürich, 2005. arXiv: 0512258 [quant-ph] (cited on pages 12, 37, 43).

[Ren07] Renato Renner. "Symmetry of large physical systems implies independence of subsystems". In: *Nature Phys.* **3**(9) (2007), pp. 645–649 (cited on page 81).

[RK05] Renato Renner and Robert König. "Universally Composable Privacy Amplification Against Quantum Adversaries". In: *Proceedings of the Second International Conference on Theory of Cryptography*. TCC'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 407–425. DOI: 10.1007/978-3-540-30576-7_22 (cited on page 48).

[Rob85] Jean-Marc Robert. "Détection et Correction d'Erreurs en Cryptographie". Master thesis. Université de Montréal, 1985 (cited on page 52).

[Rén60] Alfréd Rényi. "On measures of information and entropy". In: *Proceedings of the fourth Berkeley Symposium on Mathematics, Statistics and Probability* (1960), pp. 547–561 (cited on page 43).

[Sca+09] Valerio Scarani et al. "The security of practical quantum key distribution". In: *Rev. Mod. Phys.* **81**(3) (2009), pp. 1301–1350. DOI: 10.1103/RevModPhys.81.1301 (cited on page 84).

[Sch05] Maximilian Schlosshauer. "Decoherence, the measurement problem, and interpretations of quantum mechanics". In: *Rev. Mod. Phys.* **76** (4 2005), pp. 1267–1305. DOI: 10.1103/RevModPhys.76.1267. URL: http://link.aps.org/doi/10.1103/RevModPhys.76.1267 (cited on pages 3, 4).

[Ser74] Robert J. Serfling. "Probability Inequalities for the Sum in Sampling without Replacement". In: *Ann. Stat.* **2**(1) (1974), pp. 39–48. DOI: 10.1214/aos/1176342611 (cited on page 103).

[SG01] Valerio Scarani and Nicolas Gisin. "Quantum Communication between N Partners and Bell's Inequalities". In: *Phys. Rev. Lett.* **87** (11 2001), p. 117901. DOI: 10.1103/PhysRevLett.87.117901. URL: http://link.aps.org/doi/10.1103/PhysRevLett.87.117901 (cited on page 136).

[Sha48] Claude E. Shannon. "A Mathematical Theory of Communication". In: *Bell System Technical Journal* **27**(3) (1948). DOI: 10.1002/j.1538-7305.1948.tb01338.x (cited on page 43).

[Sho02] Peter Shor. *The quantum channel capacity and coherent information*. 2002. URL: http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/ (cited on page 9).

[SN96] Benjamin Schumacher and Michael Aaron Nielsen. "Quantum data processing and error correction". In: *Phys. Rev. A* **54**(4) (1996), pp. 2629–2635 (cited on page 9).

[SP00] Peter W. Shor and John Preskill. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol". In: *Phys. Rev. Lett.* **85**(2) (2000), pp. 441–444. DOI: 10.1103/PhysRevLett.85.441 (cited on pages 67, 109).

[Sta12] P. C. E. Stamp. "Environmental decoherence vs. intrinsic decoherence". In: *Phil. Trans. Roy. Soc. A* **370** (2012), p. 4429 (cited on pages 128, 167).

[Sti02] Douglas Robert Stinson. "Universal Hash Families and the Leftover Hash Lemma, and Applications to Cryptography and Computing". In: *Journal of Combinatorial Mathematics and Combinatorial Computing* **42** (2002), pp. 3–32 (cited on page 48).

[Sti05] Douglas Robert Stinson. *Cryptography: Theory and Practice*. 3rd ed. Discrete Mathematics and Its Applications. Taylor & Francis, 2005 (cited on page 10).

[Sti55] W. Forrest Stinespring. "Positive Functions on C*-algebras". In: *Proc. Amer. Math. Soc.* **6**(2) (1955) (cited on pages 8, 40).

[SW08] Volkher B. Scholz and Reinhard F. Werner. "Tsirelson's Problem". In: (2008). arXiv: 0812.4305 [quant-ph] (cited on page 151).

[SW87] Stephen J. Summers and Reinhard Werner. "Bell's inequalities and quantum field theory. I. General setting". In: *J. Math. Phys.* **28**(10) (1987), p. 2440 (cited on page 149).

[Sze+13] Oleg Szehr et al. "Decoupling with unitary approximate two-designs". In: *New J. Phys.* **15**(5) (2013), p. 053022. DOI: 10.1088/1367-2630/15/5/053022 (cited on page 58).

[TCR10] Marco Tomamichel, Roger Colbeck, and Renato Renner. "Duality Between Smooth Min- and Max-Entropies". In: *IEEE Trans. Inf. Theory* **56**(9) (2010), pp. 4674–4681. DOI: 10.1109/TIT.2010.2054130 (cited on page 111).

[Ter04] B. Terhal. "Is entanglement monogamous?" In: *IBM Journal of Research and Development* **48**(1) (2004), pp. 71–78 (cited on page 131).

[Tom+11] Marco Tomamichel et al. "Leftover Hashing Against Quantum Side Information". In: *IEEE Trans. Inf. Theory* **57**(8) (2011), pp. 5524–5535 (cited on pages 12, 47–50).

[Tom+12] Marco Tomamichel et al. "Tight finite-key analysis for quantum cryptography". In: *Nat. Commun.* **3**(634) (2012). DOI: 10.1038/ncomms1631. arXiv: 1103.4130 [quant-ph] (cited on pages 47, 51, 68, 71, 72, 75, 80, 105).

[Tom+14] M. Tomamichel et al. "Fundamental finite key limits for information reconciliation in quantum key distribution". In: *2014 IEEE International Symposium on Information Theory*. 2014, pp. 1469–1473. DOI: 10.1109/ISIT.2014.6875077 (cited on page 52).

[Tom12] Marco Tomamichel. "A Framework for Non-Asymptotic Quantum Information Theory". PhD thesis. ETH Zürich, 2012. arXiv: 1203.2142 [quant-ph] (cited on pages 27, 35, 37, 44–46, 111, 112, 139).

[Ton09] Ben Toner. "Monogamy of non-local quantum correlations". In: *Proc. R. Soc. A* **465**(2101) (2009), pp. 59–69 (cited on pages 133, 134, 160).

[TR11] Marco Tomamichel and Renato Renner. "Uncertainty Relation for Smooth Entropies". In: *Phys. Rev. Lett.* **106**(11) (2011), p. 110506. DOI: 10.1103/PhysRevLett.106.110506 (cited on page 45).

[TV06] Benjamin F. Toner and Frank Verstraete. *Monogamy of Bell correlations and Tsirelson's bound*. 2006. arXiv: quant-ph/0611001 [quant-ph] (cited on page 132).

[Udu12] Cozmin Ududec. "Perspectives on the Formalism of Quantum Theory". PhD thesis. University of Waterloo, 2012 (cited on pages 145, 147).

[Vit+13] Alexander Vitanov et al. "Chain Rules for Smooth Min- and Max-Entropies". In: *IEEE Trans. Inf. Theory* **59**(5) (2013), pp. 2603–2612. DOI: 10.1109/TIT.2013.2238656 (cited on pages 111, 139).

[WBM06] C.H.T. Wang, R. Bingham, and J. T. Mendoca. In: *Class. Quant. Grav.* **23** (2006), p. L59 (cited on pages 128, 167).

[Wil13] Mark Wilde. *Quantum Information Theory*. Cambridge University Press, 2013 (cited on pages 10, 25–27, 39).

[Wu+15] Xingyao Wu et al. *Device-independent parallel self-testing of two singlets*. 2015. arXiv: 1512.02074 [quant-ph] (cited on page 131).

[Zeh91] Ludwig Zehnder. "Ein neuer Interferenzrefraktor". In: *Zeitschrift für Instrumentenkunde* **11** (1891), pp. 275–285 (cited on page 5).

[Zur03] Wojciech Hubert Zurek. "Decoherence, einselection, and the quantum origins of the classical". In: *Rev. Mod. Phys.* **75** (3 2003), pp. 715–775. DOI: 10.1103/RevModPhys.75.715. URL: http://link.aps.org/doi/10.1103/RevModPhys.75.715 (cited on page 3).

[Zur91] Wojciech Hubert Zurek. "Decoherence and the Transition from Quantum to Classical". In: *Physics Today* **44** (10 1991), p. 36 (cited on page 4).