Entanglement and Non Local Correlations:
Quantum Resources for Information Processing

Ph.D. Thesis

Ph.D. Candidate:
Giuseppe Prettico

Thesis Supervisor:
Dr. Antonio Acín

ICFO - Institut de Ciènces Fotòniques

A zia Rita e zio Mimino, per averci insegnato
che l'umiltà e la semplicità possono rendere
immortale l'essere umano.

Acknowledgements

This work represents a great achievement of my life that could not have been possible without the help of many of you. I believe it is fundamental to start with the person who offered me the chance of a PhD in his group five years ago. Muchisima gracias Toni! Beloved boss, available person, and fun friend. Thank you for the amount of patience you have had in these years with me, for the interesting Physics I've learnt with you... for having showed me that success and modesty can coexists only in special people.

Special thanks go to my collaborators, Dani, Remik, Junu, Chirag and Gonzalo with which I learnt many interesting aspects of the Quantum Information World.

A big thank goes also to the whole QIT group which I've seen changing and expanding in these years: Ale, Stefano, Artur, Dani, Mafi, Mario (Leandro), Augusto, Planeta, Chirag, Jonatan, Anthony, Tobias, Gonzalo, Rodrigo, Lars, Belen, Elsa, Ariel ...

Thank you for all kind of interesting discussions we had...I guess in the future will be very hard to have colleagues so open-minded like you. I want to add that I'll never forget the nice conferences, barbecues, and other events that we have enjoyed together in these years. Thanks.

Thanks to the HR and KTT staff of Icfo for the intense work that they do to give us a better life (without boring bureaucracy, through nice events...) in particular to Mery and Marta.

It is a pleasure to say thank you to the people at the Dipartimento di Energetica in Rome, in particular to A. Belardini and F. Michelotti which gave me through their teachings a great stimulus to start a PhD programme.

Per terminare, vorrei ringraziare i miei genitori per essere stati un supporto fondamentale in questi anni... nonostante i chilometri che ci separano e gli occhi lucidi che sempre appaiono ogni volta che ci si dice $\ll$ *A presto*! $\gg$ Grazie, per darmi quelle possibilità che a voi non sono state date. Siete voi i veri Dottori!

Y un fuerte agradecimiento va a la señora Encarna, el señor Antonio, a Celeste, Jordi y Albert para acogerme tan calurosamente en su bella familia.

Y *dulcis in fundo*, gracias a ti mi querida Noelia. Tu, que me has acompañado en este largo y maravilloso camino juntos. Tu, que eres el resultado mas deseado que un italiano cabezón del sur podria obtener en su doctorado. Gracias por ser tan preciosa.

List of Publications

- Chirag Dhara, Giuseppe Prettico and Antonio Acín.
  Maximal randomness in Bell tests,
  arXiv:1211.0650 , submitted to Physical Review Letters;

- Giuseppe Prettico and Antonio Acín.
  Can bipartite classical information resources be activated?,
  arXiv:1203.1445, accepted in QIC;

- Giuseppe Prettico and Joonwoo Bae.
  Superactivation, unlockability, and secrecy distribution of bound information,
  arXiv:1011.2120, Phys. Rev. A 83, 042336 (2011);

- Remigiusz Augusiak, Daniel Cavalcanti, Giuseppe Prettico and Antonio Acín.
  Perfect Quantum Privacy Implies Nonlocality,
  arXiv:0911.3274, Physical Review Letters 104, 230401 (2010).

Contents

Abstract

Quantum Information Theory studies how information can be processed and transmitted when encoded on quantum states. New information applications become possible when resorting to intrinsically quantum properties. Here we focus on the relations among some of these quantum properties. More precisely, we establish connections between entanglement distillation and secret-key extraction, quantum privacy and non-locality and, finally, between non-locality and certified quantum randomness.

The connection between information-theoretic key agreement and quantum entanglement purification has led to several analogies between the two scenarios. The most intriguing open question is the conjectured existence of *bound information*, a classical analog of *bound entanglement*. It refers to classical correlations that, despite containing some intrinsic secrecy, do not allow its extraction by means of any protocol based on local operations and public communication between two honest parties. Despite some evidence of its existence in the bipartite scenario, a proof is still missing. By exploiting the analogies between the quantum and classical scenario, we provide two probability distributions that are not key-distillable by two-way communication protocols and therefore may have bound information. Then, we show that the combination of these two distributions leads to a positive secret-key rate. This result thus supports the idea that the secret-key rate, a fully classical information concept, may be a non-additive quantity.

Moving to the multipartite scenario, the freedom offered by consider different bipartitions of the honest parties considerably simplifies the problem and allows showing that bound information indeed exists. We have shown

that several properties of bound entanglement, such as superactivation or unlockability, can be translated to bound information. We also provide another common feature of both resources. Although non-distillable, they can help to distribute pure state entanglement and multipartite secret correlations, respectively, when a new party is added to the considered scenario.

We move later to deepen the connection between privacy and non-locality. With this aim, we consider the *private states*, that is, those quantum states from which two or more honest parties can extract a secret key. We show that all private states are non local, in the sense that they always violate the CHSH inequality. The proof is completely general since it applies for any dimension and any number of parties.

Finally, we study the relation between non-locality and randomness certification. It is well known that non-local correlations must have random outcomes to be compatible with the no-signalling principle. Thus, within a no-signalling theory, the violation of a Bell's inequality can be considered a certificate of randomness. Still, it is not known under which circumstances one can certify maximal randomness. We show that the symmetry of a Bell's inequality plus the uniqueness of the probability distribution maximally violating it can be used to certify maximal randomness. The advantage of our method relies on the fact that simple analytical considerations can bring insightful results on randomness certification via quantum non-locality without the need of any heavy numerical computation.

The dissertation ends up with an overview of the obtained results and possible follow-up research directions.

Chapter 1

Introduction

This chapter presents the context and main results obtained during the PhD Thesis. While the formal treatment will be given in the next chapters, we give here the questions and the motivations that have led to the work that we report in this thesis. Finally, a graphical scheme is sketched representing the connections analysed in this dissertation.

1.1 Introduction

Quantum Information Theory (QIT) can be understood as the effort to generalise Classical Information Theory to the quantum world. The fact that very-small scale Physics differs considerably from that of macroscopic objects implies a richer structure of the new theory. Although its formulation lacks the intuition common to the old theories of Nature, the accurate predictions of quantum phenomena do of Quantum Mechanics a fundamental tool of investigation.

Among others, phenomena as entanglement and the existence of non-local correlations make this theory very special, since these effects are not possible for classical systems. Although intrinsically non-intuitive, these strange effects have been shown to lead to intriguing applications with no classical analogue. In particular, the comparison of the same task based

on classical and quantum technology has almost always seen a significant advantage of the latter over the former. To cite only few, the possibility of sharing a secret key [BB84, Eke91], to teleport the unknown state of a quantum particle [BBC$^+$93] and to factorise huge numbers in a polynomial time [Sho94] is something possible at a quantum level. But this is just a small sample of the new range of possibilities offered by the introduction of Quantum Physics in the Information world.

Despite the vast amount of successes achieved by QIT in these years, many interesting fundamental questions are left unanswered. Being a field under current development, many powerful resources appear whose relations are still not completely understood. At a more foundational level, and despite the great effort by the scientific community, simple questions remain unanswered, leaving the feeling that very novel ideas are required.

1.2 Motivations and Results

Quantum Information Theory, like Classical Information Theory, is mostly a theory about resources: quantum effects are seen as resources for information processing. But the new theory is richer than its classical counterpart and new resources appear in the formalism, such as quantum bits, entangled qubits, private quantum bits, non-local correlations or intrinsic randomness. The main scope of this thesis is to establish qualitative and quantitative connections among these different quantum information resources. In what follows, we introduce the questions addressed in this work.

Q1. Is the secret key rate an additive quantity?
Among the many weird effects that quantum systems present, the non-additivity concept plays an important role. In the quantum realm, the joint processing of two quantum resources is often better than the sum of the two resources. Activation is the strongest manifestation of non-additivity. Such a process can be understood as the capability of two objects to achieve a given task that is impossible for each of them when considered individually.

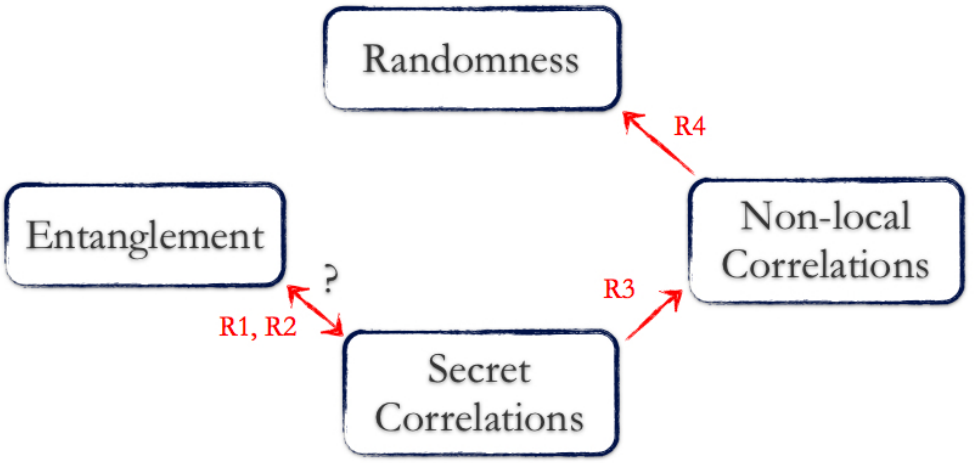

Figure 1.1: **Scheme of the thesis.** The drawing above shows the connections analysed in this dissertation. In chapters 3 and 4 the likely correspondence between entanglement and secret-key agreement is discussed providing some evidence among bound entanglement and bound information (R1, R2). In chapters 5 a general proof is given that states which provide secret correlations are non-local (R3). Finally in chapter 6, the non-locality of quantum distribution is used to certify the presence of genuine randomness (R4).

Many examples are known nowadays of activation of quantum resources: the entanglement of formation, the distillable entanglement and the classical and private capacities of a quantum channel can be activated. From a classical point of view, while additivity is known to hold for the capacity of classical channels, it is unknown whether there may be classical information resources that can be activated. Here we study whether the classical secret-key rate can be activated. That is, is it possible to combine classical resources obtaining a positive secret-key rate, despite no secrecy can be extracted from them individually?

R1
We provide two probability distributions conjectured to have bound information, hence from which it is conjectured that no secret key can be extracted (even by two-way communication protocols), when taken individually, but that lead to a positive secret-key rate when combined. In order to prove this result we exploit the close connection between the information-theoretic key agreement and the quantum entanglement scenario.

Q2. Can bound information be super-activated and unlocked?
Entanglement is one of the key resources that distinguishes Quantum Information Theory from its classical counterpart. The impossibility for remote parties to create an entangled state between particles that never interacted in the past, makes this feature really unique for communication purposes. The presence of pure entanglement constitutes the main ingredient for devising protocols that allow distant users to share secrecy. In the key-agreement scenario, several parties, including a possible adversary, share partially correlated classical information. The goal of the honest parties is to share secret correlations from the given initial ones, in such a way that no information is known to the malicious party. The two scenarios share thereby many interesting similarities. Despite the natural expectation that all noisy entangled states can be brought to a pure form, the existence of non-distillable (bound) entangled states was shown. From the analogy between the entanglement and key-agreement scenario, Gisin and Wolf gave

evidence for the existence of a classical analog of bound entanglement, the so-called *bound information*. Bound information refers to classical correlations that do contain some intrinsic secrecy but that cannot be distilled into a pure secret key by means of any protocol. It is known that bound entanglement can be super-activated and unlocked. Given the existing connections between the two scenarios, do the same properties also hold for bound information?

R2
We present the analogs of finite copy super activation and unlockability of bound entanglement for classical secret correlations. In order to do so, we provide examples of multipartite classical probability distributions with bound information and prove that they can be super-activated and unlocked. Additionally, we provide a new property that is shared by bound entanglement and information. Bound entanglement (information) can be used for distributing pure state entanglement (secret correlations) by Local Operation and Classical Communication (LOCC) (Local Operation and Public Communication, LOPC). More precisely, in the quantum scenario, we show that the a tripartite entangled pure state can be extended by LOCC to a four partite entangled state with the help of a bound entangled state shared among all the parties. The classical analog follows: when bound information is shared by four parties a secret bit of three parties can be distributed among the four using LOPC protocols.

Q3. What is the relation between privacy and non-locality?
A common future to every successful theory concerns the possibility of interconversion between apparently different kind of resources. Two key topics in Quantum Information Science are Quantum Key Distribution (QKD) and Non-Locality. Both rely on the existence of shared entanglement between two or more separated parties. Private states are those entangled states from which a perfectly secure cryptographic key can be extracted. An example of such a state is a maximally entangled state, but there are other private states that are not maximally entangled. Actually, while a maxi-

mally entangled state violates a Bell's inequality, this is not known a priori for the whole set of private states. Understanding their non local properties would thus bring to a better comprehension of the relation between secret-key extraction and violation of Bell's inequalities in the quantum regime. Thus, are all private states non-local? If so, what kind of non-locality do they show?

R3
We show that all states belonging to the class of private states violate the CHSH-Bell inequality. This result is general, as our proof works for any dimension and any number of parties. Private states, then, not only represent the unit of quantum privacy, but also allow two distant parties to establish a different quantum resource, namely non-local correlations. These states contain the strongest form of entanglement as they can give raise to correlations with no classical analogue. More in general, our findings point out an intriguing connection between two of the most intrinsic quantum properties: privacy and non-locality.

Q4. How can we certify genuine randomness?
Non-locality and genuine intrinsic randomness have been the subject of active interest since the early days of quantum physics. Initially, this interest was mainly derived from their foundational and fundamental implications but recently it also has acquired a practical aspect. Recent developments in device independent applications have heightened the need to quantify both the randomness and non-locality inherent in quantum systems. A key point is the guarantee that randomness does not originate from a mere lack of knowledge of the observed system. This allows one to certify that the quantified randomness holds for all observers irrespective of their knowledge of the system. To do it more concrete, classical systems can exhibit at most pseudo randomness since they can always, in principle, be simulated by a mixture of deterministic systems. This result is no longer valid for systems whose correlations violate a Bell inequality. Non-locality is a necessary condition, then, for certifying the presence of true intrinsic randomness. However, which Bell tests are necessary to certify maximal randomness?

R4
We provide a simple recipe to detect Bell tests that allow the certification of maximal randomness. These arguments exploit the symmetries of Bell inequalities and assume the uniqueness of the quantum probability distribution *maximally* violating it. We show how these arguments can be applied to intuit the randomness intrinsic in a probability distribution without resorting to numerical calculations. In particular, we use these arguments to provide Bell tests based on two-outcome measurements that allow the certification of two random bits, the highest randomness attainable in this scenario.

1.2.1 Outline of the Thesis

The thesis in exam is organized as follows. Chapter 2 introduces the basic concepts to understand the results presented in the following chapters. Quantum entanglement, secret correlations, non-local correlations and randomness are briefly explained focusing especially on those features that are relevant to our findings. In chapter 3 we provide an evidence for the activation of the secret-key rate in the bipartite scenario. In chapter 4 the one-to-one correspondence between bound entanglement and bound information is presented. We show that superactivation, unlockability and purification assistance of the Smolin state do have a classical analog. In chapter 5 we show the general proof of the non-locality of private states. In chapter 6 we move to the certification of maximal quantum randomness in Bell tests. Chapter 7 concludes the thesis reviewing briefly our findings and presenting future perspective. Lastly, several appendices are provided to explain technical issues in more detail.

Chapter 2

Background

The aim of this section is to present four strictly related concepts that will be used in the next chapters, namely, quantum entanglement, secret correlations, non-local correlations and random bits. As already stated, the main goal of this thesis is to establish connections among them helping to better understand their role for information purposes.

In this chapter after a brief historical review, we give the necessary background for discussing the technical results shown in this dissertation. We will present the definitions, notations and techniques that will be used in later chapters, as well as several clarifying examples.

2.1 Historical remarks

The first decades of the twentieth century saw an emerging contrast between the experimental results shown by the atomic world and the predictions inferred from the existing framework of classical theory of Science. What many brilliant physicists understood very soon was that a change of paradigm was needed to explain those astonishing facts. What perhaps they did not know was that the required change was so radical.

A counter intuitive concept as that of wave-particle duality was shown to be an intrinsic feature of matter and radiation. As a consequence the su-

perposition principle was straightforwardly extended to what was defined as the *wave function* (or state) of a quantum system. But this was not all. A distinct feature was still missing: in 1927 W. Heisenberg provided an heuristic argument showing a fundamental limit on the precision with which certain pairs of physical properties of a particle (such as position and momentum) could be simultaneously known. The uncertainty relations marked another fundamental difference between classical and quantum mechanics: the one-to-one correspondence between the physical properties of the considered object (and thus the entities of the physical world) and their formal and mathematical representation in the theory came to a sudden end.

The main pillar of the novel view, known as Copenaghen interpretation, was constituted by the fact that a quantum system could not be thought of as possessing individual properties independently of the experimental arrangements. In a nutshell, Bohr and coworkers were destroying the intuitive and consolidate concept of *reality*, deeply rooted in the minds of scientists and layman alike. This was enough to stimulate an immediate reply to the unacceptable conception that the new Physics seemed to require.

In 1935, A. Einstein, B. Podolsky and N. Rosen (EPR) published a seminal paper [EPR35] whose main claim was to show the incompleteness of the quantum theory. In the same year, Schrödinger coined the term "verschränckter Zustand" (entangled state), to refer to the highly singular state used by EPR. He immediately emphasized its non-classical implications:

> *When two systems, of which we know the states by their respective representatives, enters into a temporary physical interaction due to known forces between them, and when after a time of mutual influence the system separate again, then they can no longer be described in the same way as before, viz. by endowing each of them with a representative of its own. I would not call that one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.*

On the other hand the answer of Bohr to EPR did not take much to arrive. It was the beginning of a long and enlightening debate between two of the

greatest scientists of the 20th century.

In the meanwhile, in Computer Science, another revolution was taking place. In the the '40s, Claude Shannon published seminal remarkable papers laying the foundations for the modern theory of information and communication. The key step taken by Shannon was to mathematically define the concept of information. Two main questions were predominant: first, what kind of resources is required to send information over a communication channel? Second, could information be transmitted reliably when sent over a noisy channel?

The answer to the first question was provided in his *noiseless channel coding theorem*, which quantifies the amount of physical resource needed to store the output from an information source. The second answer, the *noisy channel coding theorem*, instead, identifies the maximal noise that an error correcting code can afford in order to protect and then conserve the original sent information. Many devices we use daily strongly rely on the achievements of the classical theory of information.

If the long debate between Bohr and Einstein brought many insightful results, the key question of EPR remained unanswered. The breakthrough came only in 1964, when John Bell, formulating the EPR dilemma in form of assumptions, showed that measurements on an entangled state led manifestly to a contradiction of the assumptions. With Werner's words [WW01b], the Bell's theorem was so crucial that:

> *It is hardly possible to underrate the importance of this discovery, which made it possible to rule out not just a particular scientific theory, but the very way scientific theories had been formulated for centuries.*

Despite its importance, it took almost thirty years for the scientific community to really exploit the importance of Bell's theorem: a practical application was needed to attract a widespread attention.

Almost in the same period moved by a better understanding of how physics constrains our ability to use and manipulate information, Landaurer came to the conclusion that *Information is physical* [Lan61, Lan92].

The main argument discussed, was that information is not a disembodied abstract entity, but it is always tied to a physical representation. In other words, the mathematical terms in which a given theory is expressed are subject to the limitations (and benefits) of our physical world.

Quantum mechanics had a chance.

Unlike classical physics, the act of acquiring information about a quantum system inevitably disturbs the state of the system. The first consequence (the cons) of this fact is that a reliable cloning of quantum information is impossible [WZ82]. The second (the pro) is that the security of a key-distribution protocol could be guaranteed by it. An eavesdropper could be intercepted by the honest parties due to his/her inevitable introduction of errors in the channel [BB84]. Another remarkable consequence of no-cloning was represented by the impossibility of sending information faster than the speed of light (signalling) between remote parties.

Einstein's relativity was safe.

Since the '80s many of the central results of classical information theory were shown to have more powerful quantum analogs [CT91, NC00]. Quantum Information Theory has since then emerged as a vigorous research field combining concepts and tools from Physics, Computer Science, Mathematics and Engineering. New quantum algorithms [Sho94] have been found providing an efficient solution to problems (integer factorization and discrete logarithm) for which there is no known efficient classical algorithm. These algorithms take classical inputs (such as the number to be factored) and yield classical outputs (the factors), but obtain their speedup by using quantum interference among computation paths during the intermediate steps . In quantum communication, entanglement has been shown fundamental for the teleportation of quantum states [BBC$^+$93] and for superdense coding [BW92]. Moreover, entanglement is a key ingredient for the achievement of security in cryptographic scenarios and necessary for the violation of Bell's inequalities.

In fact, the connection between cryptography and non-locality was very smartly addressed by Ekert in 1991 [Eke91]. He showed that the security of the protocol could be guaranteed by the violation of a Bell's inequality.

This result was the missing application which made clear the importance of the Bell's theorem and from which many interesting ideas and applications born under the label Device Independent.

Device-Independent Quantum Information Processing can be considered nowadays as a new paradigm for quantum information processing. The goal is to design protocols for solving relevant information tasks without relying on any assumption on the devices used in the protocol. For instance, device-independent key distribution can certify shared secrecy between two honest users independently of the devices that have been used in the distribution (DIQKD). Another successful application allowed by this approach is the generation of genuine randomness (DIRNG). While it is well known that no real randomness can be generated through deterministic procedures, the correlations exhibited performing certain measurements on entangled states, necessarily certify the randomness of the obtained outcomes. The certificate in this case is again provided by the violation of a Bell's inequality.

2.2 Quantum Entanglement

The deep way that quantum information differs from classical information involve the properties, implications and uses of quantum entanglement. The vast majority of quantum information applications are mainly based on the creation and manipulation of entangled states shared by remote parties. This section presents the main features of entangled states, including the basic tools and problems behind their definition.

2.2.1 Bipartite Scenario

A composite pure system $|\Psi\rangle_{AB}$, belonging to two distant parties A and B (also called Alice and Bob in the sequel) is said to be entangled whenever it cannot be written in a factorized (or product) form, that is

$$|\Psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B, \tag{2.1}$$

where $|\psi\rangle_A$ and $|\psi\rangle_B$ represent states in A and B locations.

Being the pure state description limited by the presence in Nature of decoherence processes, the density matrix formalism is used to fully characterize any quantum (mixed) state. In contrast to a pure state $|\Psi\rangle_{AB}$, which is represented as a vector in a Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, a mixed state is described by a density matrix, i.e. a hermitian, positive-definite linear operator of trace one, acting on the same Hilbert space. In this case a quantum state is said entangled whenever it cannot be written as a convex combination of projectors on product states [Wer89]:

$$\rho_{AB} = \sum_{i=1}^{k} p_i |\psi_i\rangle\langle\psi_i|_A \otimes |\psi_i\rangle\langle\psi_i|_B. \tag{2.2}$$

Beyond this mathematical definition, an entangled state has a clear operational meaning. While two distant observers can prepare a global state (2.2) by performing *Local Operations* (LO) on their subsystems and exchanging *Classical Comunications* (CC) among them, an entangled state requires a joint preparation. In other words, *LOCC protocols cannot create (or increase) entanglement.*

A maximally entangled state (or Bell pair) of two qubits represents the most representative example of a bipartite entangled state and is an essential ingredient in many applications of quantum information theory [Ben95]. Various equivalences are known: one shared Bell pair plus two bits of classical communication can be used to teleport one qubit [BBC$^+$93] and, conversely, one shared Bell pair plus a qubit can be used to send two bits of classical communication via superdense coding [BW92]. It is formally defined (in the computational basis $\{|0\rangle, |1\rangle\}$) as:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right)_{AB} \tag{2.3}$$

and its relevance for communication purposes is due essentially to two main facts: first, for each projective measurement by one of the observers, there exists another measurement by the other observer giving perfectly correlated results. Second, being a pure state, no third party can be correlated with it. State (2.3) represents the basic unit of entanglement and is

also known as *ebit*, for entangled bit. This is because an asymptotically large number of copies of an arbitrary pure entangled state can be converted into another asymptotically large number of ebits in a reversible way [BBPS96, LP99]. For example, suppose that Alice and Bob have a large number N of pairs of particles, each pair in some pure non-maximally entangled state, $|\psi\rangle = \sqrt{p}|00\rangle + \sqrt{1-p}|11\rangle$, where $0 < p < 1/2$. By acting locally and communicating on a classical channel, they can end up with a smaller number of pairs each in the maximally entangled state (2.3). This number correspond to $NE(\psi)$, where $E(\psi)$ is the entropy of entanglement of state ψ:

$$E(\psi) = -\mathrm{tr}\rho_A \log \rho_A = -\mathrm{tr}\rho_B \log \rho_B \tag{2.4}$$

where ρ_A, ρ_B are the reduced density matrix of the state ψ for A and B respectively:

$$\rho_A \ (\rho_B) = \begin{pmatrix} p & 0 \\ 0 & 1-p \end{pmatrix}$$

This process is known in literature as *concentration* of entanglement. The inverse process, of transforming $NE(\psi)$ ebits in N pairs of ψ is also possible and known as *dilution*. Remarkably, the entropy of entanglement provide an exact quantification of the pure state entanglement, and moreover as clear from the previous example, this quantity is conserved in the processes of concentration and dilution. In the mixed state scenario other measures of entanglement have been proposed. To better clarify this point, the following section lists some well known quantifiers and problems of the theory of entanglement.

2.2.2 Quantifying and Distilling Entanglement

As soon as one consider the more realistic scenario of converting pairs of mixed states into pure maximally entangled states, the answer becomes harder.

A generalization of the dilution process can be stated as follows. Let us consider the case in which two (or more) separated parties aim at preparing m copies of a state ρ by LOCC. The answer to the question of how many

ebits they need in order to obtain m copies of the state ρ is provided by the entanglement cost. In particular, the entanglement cost [HHT01], denoted by E_c, quantifies the number of ebits per copy asymptotically needed for the formation of the given quantum state by LOCC. For pure states E_c coincides with the entropy of entanglement previously defined.

The inverse problem is known as *distillability problem* and is a generalization of the concentration process. A composite mixed state $\rho_{AB}$is distillable whenever Alice and Bob can transform k copies of it into a state arbitrarily close to the maximally entangled state (2.3) by LOCC. Thereby, the entanglement of distillation [BDSW96], denoted by E_D, quantifies the amount of ebits per copy (of the given state) that can be obtained from it by LOCC.

For a state ρ_{AB}, $E_c(\rho_{AB}) > 0$ implies that the state is entangled, while $E_D(\rho_{AB}) > 0$ indicates that some pure entanglement can be extracted from it. Clearly, it holds that $E_c \geq E_D$, as one cannot extract from a state more entanglement than needed for its preparation. Note that in the pure state case, $E_c = E = E_D$, due to the reversibility of the concentration and dilution processes.

Interestingly, there are states that display an intriguing form of irreversibility: despite having a positive entanglement cost ($E_c > 0$), they are non-distillable ($E_D = 0$). These states are called *bound entangled* [HHH98]. Consequently, the whole set of entangled states is composed of distillable, or free entangled states, and bound entangled states.

As said, detecting whether a given state is non-distillable is in principle a very hard question, as one has to prove that no LOCC protocol acting on an arbitrary number of copies of the state is able to extract any pure entanglement. However, a very useful result derived in [HHH98] shows that a quantum state that remains Positive under Partial Transposition [Per96] (PPT) is non-distillable. Whether Non-Positivity of the Partial Transposition, or Negative Partial Transposition (NPT), is sufficient for entanglement distillability is probably the main open question at the moment in Entanglement Theory. Evidence [DCLB00, DSS$^+$00] has been given for the existence of NPT states that are bound entangled (see however [Wat04]). Note that the existence of these states would imply that the set of non-distillable states

is not convex and that entanglement of distillation is non-additive [SST01]. A necessary and sufficient condition for the distillability of a quantum state is provided by the following

Theorem 1. *A state ρ acting on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is distillable if and only if there exist a finite integer number $n \geq 1$ and two dimensional projectors $P : \mathcal{H}_A^{\otimes n} \to \mathbb{C}^2$ and $Q : \mathcal{H}_B^{\otimes n} \to \mathbb{C}^2$ such that the state*

$$\rho' = (P \otimes Q)\rho^{\otimes n}(P \otimes Q)^\dagger \tag{2.5}$$

is entangled.

Actually, since the resulting state acts on $\mathbb{C}^2 \otimes \mathbb{C}^2$, this is equivalent to demand that ρ' is NPT, as this condition is necessary and sufficient for entanglement in the two-qubit case [HHH96]. Furthermore, it is worth mentioning here that, if such a projector exists for some number k of copies, the state is said to be $k - distillable$.

2.2.3 Multipartite Scenario

Characterizing the entanglement in a multipartite scenario, in which more parties are provided with some arbitrary quantum state ρ, is quite more complex than in the previous case. This difficulty is connected with the fact that, in the multipartite scenario, one can have many partitions of the remote parties, so the quantum state can be entangled with respect to some of them, while separable in the remaining ones. As before, a straightforward definition of full separability is easily generalized. A quantum state ρ of N particles which can be factorized into local states:

$$\rho = \sum_{i=1} p_i \rho_1^i \otimes \rho_2^i \ldots \otimes \rho_N^i \tag{2.6}$$

is called *completely separable*. As announced, for a complete characterization of multipartite entanglement is necessary to consider all possible groupings of particles of the total system and study the entanglement among such groups. Consider an N-partite quantum state ρ and a possible partition

P=$\{p_1, p_2, \ldots, p_k\}$ of the same, where $k \leq N$. The state ρ is said *k-separable* in the P partition if it can be written as:

$$\rho = \sum_{i=1} p_i \widetilde{\rho}_1^{\,i} \otimes \widetilde{\rho}_2^{\,i} \ldots \otimes \widetilde{\rho}_k^{\,i} \tag{2.7}$$

where $\widetilde{\rho}_j^{\,i}$ represent the quantum state of the jth group of particles in the P partition. If the N-partite quantum state does not admit any sort of decomposition (2.7), this means that all particles are entangled with each other, so the state is said *genuine multipartite entangled*.

Another difficulty in the multipartite scenario comes from the fact that it is not known whether it is possible to define a unit of multipartite entanglement [LPSW05]. The question of which is the minimal set of states that N parties should share in order to generate any N-partite pure state by using LOCC in the asymptotic scenario in a reversible manner is still open. This set it has been termed MREGS from minimal reversible entanglement generating set. In the (asymptotic) tripartite scenario, for example, the set

$$G3 = \{|GHZ\rangle_{ABC}, |EPR\rangle_{AB}, |EPR\rangle_{AC}, |EPR\rangle_{BC}\}$$

where $|EPR\rangle_{ij}$ is the ebit (2.3) between party i and j and $|GHZ\rangle$ is the state:

$$|GHZ\rangle = \frac{1}{\sqrt{2}} \left(|000\rangle + |111\rangle\right) \tag{2.8}$$

shared by ABC in the computational basis, was conjectured to be a good candidate for generating all tripartite pure states. Unfortunately, in Ref. [AVC03] a counterexample was provided falsifying this conjecture. Actually, it is even known whether an MREGS consisting of a finite number of states exists.

2.3 Secret Correlations

The main scope of this section is to introduce the secret-key agreement scenario together with the natural concept of secret correlations. This scenario

consists of two honest parties, again Alice and Bob, who have access to correlated information, described by two random variables X and Y. These variables are also correlated to a third random variable Z that belongs to an adversarial party, the eavesdropper Eve, denoted by E. All the correlations among the three parties are described by the probability distribution $P(XYZ)$. The aim of the honest parties is to map their initial correlations into a secret key by *Local Operations and Public Communications*(LOPC), which is the natural set of operations at their disposal.

They will share a perfect secret bit whenever $P(XYZ)$ is such that the eavesdropper is factored out, $P(XY) \times P(Z)$, and their variables $(X, Y = 0, 1)$, are perfectly correlated and random, $P(X = Y = 0) = P(X = Y = 1) = 1/2$. This scenario is defined as the classical analogue of the entanglement scenario. Here, a secret bit represents the equivalent of a maximally entangled state. This analogy is mainly based on the fact that secret correlations cannot be created by LOPC protocols, in the same fashion as entanglement cannot be created by LOCC protocols.

Additionally, other reasonable analogies have been shown in [CP02]. As in the quantum scenario, if the parties share N copies of a classical resource distributed according to:

$$P(X = i, Y = j, Z = k) = \delta_{ij} p_i \tilde{P}(Z = k) \tag{2.9}$$

they can transform it reversibly in a new distribution $Q(X = i, Y = j, Z = k) = \delta_{ij} q_i \tilde{Q}(Z = k)$. This is the classical equivalent of the concentration or dilution process. This follows from the fact that (2.9) can be obtained by measuring a pure quantum bipartite in its Schmidt basis. Since the entanglement concentration process is performed in the Schmidt bases, the quantum protocol directly translates into a classical protocol for distributions (2.9). As for the quantum case, the entropy of secrecy, quantifies the amount of sbit, $q_i = 1/2$, that can be produced per copy of the original distribution p_i as follows:

$$\frac{K}{N} = -\sum_i p_i \log_2 p_i$$

The picture becomes harder when considering correlations $P(X = i, Y = j, Z = k)$ in which the eavesdropper is not factored out. This case is analogous to the mixedness of a pure state under the decoherence effects of the environment (see eq. (2.1)). Similarly as above, the goal in this case is to quantify its secrecy content.

The classical analogue of E_c is the information of formation, denoted by I_f [RW03]. It is said that the probability distribution $P(XYZ)$ contains secret correlations (or secret bits) whenever $I_f(P(XYZ)) > 0$. For distillation, the natural classical analog is the secret-key rate [MW99], denoted by $S(X : Y \| Z)$, which quantifies the number of secret bits that can be distilled from given correlations by LOPC. Thus, given the three random variables (X, Y, Z), if Bob's random variable Y provides more information about Alice's X than Eve's Z does (or vice versa), then this advantage can be exploited for generating a secret key. This can be expressed as:

$$S(X : Y||Z) \geq \max\{I(X : Y) - I(X : Z), I(Y : X) - I(Y : Z)\} \quad (2.10)$$

where $I(P : Q)$ is the mutual information among two random variables P and Q:

$$I(P : Q) = H(P) + H(Q) - H(PQ) \quad (2.11)$$

and $H(S)$ is the Shannon Entropy of the random variable S. Although in Ref. [CK78], the positivity of the relation (2.10) was shown to be a sufficient condition for one-way communication secret-key agreement, new protocols were later devised able to give a positive secret key rate even for those cases in which the left hand side of (2.10) is negative.

In [Mau93], Maurer introduced the *advantage distillation* (AD) protocol, which allows two honest parties to extract a secret key even in cases in which Bob has less information than Eve about Alice's symbols. Crucial to achieve this task is feedback, that is, *two way communication* between the honest parties. The general structure of an AD protocol is as follows [AGS03] (without loss of generality we assume that Alice's and Bob's variables have the same size d): Alice first generates randomly a value ζ. She chooses a vector of N symbols from her string of data, $\mathbf{a} = (a_1, \ldots, a_N)$, and publicly announces their positions to Bob. Later she sends him the

N-dimensional vector $\bar{\mathbf{a}}$ whose components $\bar{a}_k$ are such that $a_k \oplus \bar{a}_k = \zeta$ holds $\forall k$. Here, $\oplus$ is the sum modulo d. Bob sums $\bar{\mathbf{a}}$ to his corresponding symbols. If he obtains always the same value χ, then he accepts (this means that with very high probability $\chi = \zeta$) otherwise both discard the N symbols.

Although its yield is very low with increasing N, AD protocols allow the honest parties to distill a key even in a priori disadvantageous situations in which Eve has more information than Bob on Alice's symbols. Such protocols are used in what follows to estimate the distillability properties of the given correlations. Obviously, the fact that one is unable to map some correlations into a secret key by AD protocols does not mean that these correlations are non-distillable. At best, it can be interpreted as some evidence of non-distillability.

The protocols introduced so far give us a lover bound on the secret-key rate in the one and two-way communication scenario, respectively. We now move to describe known upper bounds on the secret-key rate. Intuitively, the fact that no secret key can be derived by the honest parties whenever Bob's information is independent from Alice's random variable, given Eve's information is captured by the inequality:

$$S(X:Y||Z) \leq I(X:Y|Z).$$

If Alice's and Bob's symbols are uncorrelated $I(X:Y|Z) = 0$, hence $S(X:Y||Z) = 0$. However, it was realized that this bound is not tight. The possibility for an adversary to process her variable Z, i.e., to send Z over some channel characterized by $P_{(\bar{Z}|Z)}$, can lead to situations in which $I(X:Y|\bar{Z}) < I(X:Y|Z)$. To take this in account, the intrinsic information [MW99] must be used. It is defined as the minimal mutual information between X and Y conditioned on $\bar{Z}$, where $\bar{Z}$ is the best (from the eavesdropper's point of view) mapping of the random variable Z that the eavesdropper can perform, i.e. $Z \to \bar{Z}$:

$$I(X;Y \downarrow Z) := \min_{P_{\overline{Z}|Z}} \left[I(X;Y|\overline{Z}) : P_{XY\overline{Z}} = \sum_z P_{XYZ} \cdot P_{\overline{Z}|Z} \right] \qquad (2.12)$$

In Ref [CRW03] it was shown that there is no loss of generality in considering the output alphabet $\bar{Z}$ of the same size of the input alphabet Z. This measure plays a relevant role in key-agreement scenarios since it allows to bound the two main quantifiers previously defined:

$$S(X;Y\|Z) \leq I(X;Y \downarrow Z) \leq I_f(X;Y|Z) \tag{2.13}$$

Along the connection with entanglement theory, a main open question was risen in Ref. [GW00]: is it possible to characterize classical correlations which cannot be distilled but which are shown to contain strictly positive information of formation, or simply $I(X;Y \downarrow Z) > 0$? A distribution $P(XYZ)$ is said to contain *bound information* if the following relations hold:

$$S(X:Y||Z) = 0 \quad I(X;Y \downarrow Z) > 0. \tag{2.14}$$

In a nutshell, although these correlations cannot be distributed by LOPC they would not allow the honest parties to distill secrecy by LOPC, even when sharing an infinite number of instances of $P(XYZ)$.

If shown, these correlations would constitute a classical cryptographic analog of bound entanglement [GW00]. Compared to the entanglement scenario, identifying a single example of non-distillable correlations is much harder, due to the lack of a simple mathematical criterion, as the Partial Transposition [Per96], to detect it. In a multipartite scenario, say of three honest parties plus an eavesdropper, the possibility of splitting the honest parties into different bipartitions hugely simplifies the problem and, indeed, there are examples of correlations that require secret bits for the preparation and from which no secret bits can be extracted [ACM04]. The problem remains open for two honest parties, although evidence has been provided for the existence of bound information [GW00].

Finally, another concept that we will use in the sequel is that of *binaryzation*, which can be understood as the classical analog of the quantum projection onto 2-qubit subspaces used in Theorem 1. As in the quantum case, Alice and Bob agree on two possible values, not necessarily the same,

and discard all instances in which their random variables take different values. Then, they project their initial distribution onto a smaller (and usually simpler) two-bit distribution.

2.3.1 Link between entanglement and secret key-agreement

It is clear from the previous discussion that the entanglement and secret-key agreement scenarios have a similar formulation. One can go further and establish connections between the entanglement of bipartite quantum states and the tripartite probability distributions that can be derived from them [GW00]. Not surprisingly, the transition from quantum states to classical probabilities is through measurements (on the quantum states). Note also that, while in the quantum case the state between Alice and Bob also specifies the correlations with the environment, possibly under control of the eavesdropper, in the classical cryptographic scenario it is essential to define the correlations with the eavesdropper for the problem to be meaningful.

As mentioned, if Alice and Bob share a state ρ_{AB}, the natural way of including Eve is to assume that she owns a purification of it. In this way the global state of the three parties is a pure tripartite $|\psi_{ABE}\rangle$ such that $\rho_{AB} = \mathrm{tr}_E\left(|\psi_{ABE}\rangle\langle\psi_{ABE}|\right)$. After this purification, measurements by the three parties, M_X, M_Y and M_Z, respectively, map the state into a tripartite probability distribution:

$$P(X,Y,Z) = \mathrm{tr}\left(M_X \otimes M_Y \otimes M_Z \; |\psi_{ABE}\rangle\langle\psi_{ABE}|\right) \tag{2.15}$$

It has been shown that: *i)* if the initial quantum state is separable, there exists a measurement by the eavesdropper such that the probability distribution (2.15) has zero intrinsic information for all measurements by Alice and Bob [GW00, CLL04] and also zero information of formation [AG05] and *ii)* if the initial state is entangled, there exist measurements by Alice and Bob such that the probability distributions (2.15) has strictly positive intrinsic information for all measurements by Eve [AG05].

2.4 Non-Local Correlations

While the question of EPR [EPR35] led immediately Shrödinger [Sch35] to recognize the intrinsic novelty of the entanglement, it took almost thirty years to rule out, at least theoretically, the basic hypothesis of a theory à la EPR.

In 1964 J. S. Bell [Bel64] provided a mathematical argument demonstrating that the probabilities of the outcomes obtained when applying suitable measurements on some entangled states could not be explained by a local realistic model as the one suggested by EPR.

2.4.1 Bipartite scenario

To illustrate the elegant theorem provided by Bell, it is sufficient to consider two distant observers (A and B) able to perform m possible local measurements ($x, y = 1 \dots m$) of r possible results, ($a, b = 1 \dots r$), on the part of a shared physical system ρ which they can access to. As in a black box approach, it is enough to say that for each run of the experiment, Alice and Bob can freely choose between a finite number m of settings x and y, obtaining always one outcome each, a and b, among d possible results.

After a sufficient large number of runs, they can thus estimate their conditional probability distribution $P(ab|xy)_\rho$. Moreover, two additional requirements are needed: (i) each local measurement defines space-like separated events, and (ii) the choice of the measurement setting at each side is made at the moment of measuring. The observed correlations $P(ab|xy)_\rho$ are compatible with a local realistic theory [Bel64] when they can be derived by averaging over some hidden (classical) variable λ the product of the two local distributions $P^A(a|x,\lambda)$, $P^B(b|y,\lambda)$:

$$P_L(ab|xy)_\rho = \int P^A(a|x,\lambda)P^B(b|y,\lambda)\sigma(\lambda)d\lambda, \tag{2.16}$$

where $\sigma(\lambda)$ refers to the probability measure according to which λ is distributed. The locality condition imposes that the local distributions $P^A(a|x,\lambda)$, $P^B(b|y,\lambda)$ can only depend on the chosen setting and on the hidden-variable λ, on which no restrictions are generally imposed. Model (2.16) was

shown to be equivalent to the existence of a joint probability distribution $P(a^{(1)}, \ldots, a^{(m)}, b^{(1)}, \ldots, b^{(m)})$ involving all local measurements (from 1 to m), such that the marginal probabilities reproduce the observed measured outcomes of the given experiment [Fin82].

The distribution $P(ab|xy)_\rho$ (obtained by measurements on some physical system ρ) is said *non-local*, if it does not admit a local description (2.16). If ρ is a quantum state shared by two distant observers, the distribution $P(ab|xy)_\rho$ reads:

$$P_Q(ab|xy)_\rho = tr(\rho M_{a|x} \otimes M_{b|y}), \tag{2.17}$$

where the positive operators $M_{a|x}$ and $M_{b|y}$ satisfy the completeness relation, $\sum_k M_{k|x} = \mathbb{I}$, for $k = a, b$.

Bell showed that the correlations arising when certain measurements are made on a composite system of two spins-1/2 particles in a singlet state[1]:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle\right)_{AB} \tag{2.18}$$

with $|0\rangle$ and $|1\rangle$ representing the state *up* and *down* of the spin of a particle, could not be expressed as (2.16). This was the evidence, at least theoretically, that quantum mechanics cannot be a local realistic theory.

But another step was still missing. Bell's theorem in his original formulation was not directly testable in a lab, so in 1969, Clauser, Horne, Shimony and Holt addressed this problem, deriving an inequality, nowadays known as the CHSH [CHSH69] inequality, that could confirm experimentally the theoretical result of Bell. Consider an experiment where two separated parties measure one of two possible observables, $\{A_1, A_2\}$ and $\{B_1, B_2\}$ with outcomes ± 1. For any local theory (2.16), the following inequality:

$$|\langle A_1 B_1\rangle + \langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle| \leq 2 \tag{2.19}$$

is bounded by 2. A violation of the CHSH inequality thus is sufficient for certifying the presence of nonlocal correlations.

[1]Note that this state is unitarily equivalent to the state (2.3). Together with the two states $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ they form an orthonormal basis on $\mathbb{C}^2 \otimes \mathbb{C}^2$ known as Bell basis (or Bell states).

The state (2.18), with opportune measurements can violate the CHSH inequality, up to $2\sqrt{2}$, showing then the non local character of quantum mechanics. In particular, in the '80s, it was shown by Tsirelson [Tsi80] that this is the maximal bound achievable by quantum mechanics. It is somhow surprising that considering states on Hilbert spaces of higher dimension does not lead to any improvement on this bound.

2.4.2 Multipartite scenario

The extension of a local model as (2.16) to the multipartite case, is rather straightforward:

$$P_L(a_1 \dots a_N|x_1 \dots x_N) = \int P^{A_1}(a_1|x_1,\lambda) \dots P^{A_N}(a_N|x_N,\lambda)\sigma(\lambda)d\lambda \tag{2.20}$$

But, as already observed for multipartite entanglement, the presence of more parties implies a richer structure for the arising correlations. As a consequence of that, it is not enough to talk only of local or non-local correlations, but the class of partially (non-)local correlations has to be taken in account. Partially local correlations are those that can be obtained from an N-partite system in which subsets of the N parties form extended systems, which however behave local with respect to each other. Assuming that parties $1, \dots, k$ form such a subset and the remaining parties $k+1, \dots, N$ form the other, the partially local correlations can be written as:

$$P_{pL}(a_1 \dots a_N|x_1 \dots x_N) = \int P(a_1 \dots a_k|x_1 \dots x_k,\lambda)P(a_{k+1} \dots a_N|x_{k+1} \dots x_N,\lambda)\sigma(\lambda)d\lambda \tag{2.21}$$

A model is said to have partially local correlations when the correlations are of the form (2.21) or when they can be written as a convex combination of the r.h.s. of (2.21) for different possible partitions of the N parties into two subsets. To make this more clear, we report in the following the early model considered by Svetlichny [Sve87]. For $N = 3$, only three different

partitions are possible. Model (2.21) is thus extended to the form:

$$P_{pL}(a_1a_2a_3|x_1x_2x_3) = \int d\lambda (P(a_1|x_1,\lambda)P(a_2,a_3|x_2,x_3,\lambda)p_1\sigma_1(\lambda) + P(a_2|x_2,\lambda)P(a_1,a_3|x_1,x_3,\lambda)p_2\sigma_2(\lambda) + P(a_3|x_3,\lambda)P(a_1,a_2|x_1,x_2,\lambda)p_3\sigma_3(\lambda)) \quad (2.22)$$

where $P(a_1,a_2|x_1,x_2,\lambda)$ and the other two joint probability terms can be any probability distributions [2]. Models whose correlations cannot be written in this form are said to contain *genuine tripartite non-locality*. The generalization to more than three parties is straightforward.

2.4.3 Link between entanglement and non-locality

Given a separable state (2.6) it is always possible to construct a model which reproduces correlations compatible with eq. (2.20). Let us show this for the bipartite case. The N-partite generalization follows straighforwardly from the bipartite proof. Consider the separable state (see eq. (2.2)):

$$\rho_{AB} = \sum_{i=1}^{k} p_i \rho_A^i \otimes \rho_B^i, \quad (2.23)$$

on which two parties, A and B, can perform local measurements $M_{a|x}$, $M_{b|y}$. As already said the conditional probability distribution that A gets outcome a when measuring x and B gets outcome b when measuring y reads:

$$p_Q(ab|xy)_\rho = tr(\rho_{AB} M_{a|x} \otimes M_{b|y}). \quad (2.24)$$

[2] Recently it has been shown that even though these terms can be signalling, they need to respect a time order sequence [GWAN11].

By substituting eq.(2.23) into eq.(2.24) the following expression is given:

$$p_Q(ab|xy)_\rho = \sum_{i=1}^{k} p_i \mathrm{tr}(\rho_A^i M_{a|x}) \mathrm{tr}(\rho_B^i M_{b|y}) \\ = \sum_{i=1}^{k} p_i P^A(a|x,i) P^B(b|y,i) \quad (2.25)$$

where $P^A(a|x,i)$ is the probability to find outcome a when measuring x on the state ρ_A^i and analogous for $P^B(b|y,i)$. It is thus evident that expression (2.25) is just a particular case of model (2.16). Here, the hidden variable (shared randomness) is represented by the index i and distributed according to p_i.

The generality of this argument thus implies that entanglement is necessary to violate any local-realistic model. In the '90s Gisin [Gis91] showed that in the bipartite case any pure entangled state does violate the CHSH inequality. In later years, Popescu and Rorlich [PR92] extended his proof to the multipartite scenario (we derive a simple argument inspired by their proof in Appendix C).

It was then believed that if any entangled state violates a Bell inequality. However, Werner [Wer89] showed that bipartite entangled states exist whose correlations admit a local description for an arbitrary number of (projective) measurements. Later, Barrett [Bar02] generalized the model to general measurements (POVM). Another local model was even provided for the tripartite case [TA06] for a genuine tripartite entangled state. So, as for any entanglement problem the picture was subtler than initially expected.

2.5 Randomness

Although the concept of randomness was already known to ancient societies, it was only with the advent of computers that programmers understood the need of introducing randomness into computer programs. Nowadays many

applications strongly rely on the generation of numbers *chosen at random*, such as generating data encryption keys, simulating and modelling complex phenomena and for selecting random samples from larger data sets. As known, they are also very used for games and gambling. Generally, there are two main approaches for generating random numbers using a computer: Pseudo-Random Number Generators (PRNGs) and True Random Number Generators (TRNGs). Essentially, PRNGs are algorithms that use mathematical formulae or simply pre-calculated tables to produce sequences of numbers that appear random. A good example of a PRNG is the linear congruential method. The second ones, TRNGs extract randomness from physical phenomena as atmospheric noise, resistance noise generators, noise-diode circuits combined with scrambled rap music, etc...

Very recently the intrinsic randomness inherent in quantum mechanical systems has inspired numerous experimental realizations of quantum random generators. These implementations are sometimes based on the time at which radioactive nuclei decay or on the path a photon chooses when impacts with a 50:50 beamsplitter. Devices of this kind are already available in the market. Still, some pitfalls can be identified in these kind of approaches: if from one side, processing analog signals it is known to be a difficult task, from the other, a possible malfunctioning is hardly detectable.

To overcome this difficulties a new approach based on entanglement and non-locality has been recently suggested [Col09, PAM$^+$10]. The idea behind it is that the correlations shown when measuring certain entangled states can violate a Bell's inequality, and this fact is used to certify the presence of randomness in the obtained outcomes (we will explain this in detail in chapter 6).

When discussing single numbers, a random number is a ill-defined concept. In order for it to be meaningful, one has to analyze very long sequences of numbers and carefully check that each value in the sequence is equally probable, i.e. uniformly distributed. In a nutshell a sequence of random numbers is a sequence in which each number is statistically independent from the others. This argument lead naturally to interpret randomness as lack of predictability: numbers that are statistically independent are completely unpredictable. In order to quantify the randomness inherent in a

given process the concept of predictability hence turns out to be useful.

2.5.1 Definitions

Let us consider a tester who is paid to establish if a given box can be used as a random number generator. The box he/she receives consists of two buttons (1 and 2) and two lights (Green and Red). Every time he/she presses one button, one of the two lights immediately flashes. After many days pressing buttons and writing down which lights flashes, given the chosen input, the tester introduces the obtained string of outputs in a program to test if the box under examination gives random outputs. Let us suppose that he/she can estimate that:

$$\begin{aligned} P(G|1) = P(R|1) = \frac{1}{2} \\ P(G|2) = P(R|2) = \frac{1}{2} \end{aligned} \tag{2.26}$$

and that moreover the string of obtained outcomes passes the test checked by the program. Does this means that the outcomes are really random? If so, can the box be used as a random generator for a virtual casino?

First, if the answer to first question was yes, nobody (apart from the provider) could know if the string was already stored in the box (thus perfectly known by the provider) and just revealed by the tester in every trial.

Second, even without any internal memory the provider could prepare a box which is remotely controlled. What the provider does is just to prepare with probability 1/2 two possible behaviours for the box:

$$(GG|12) \text{ or } (RR|12) \tag{2.27}$$

where the list $(L_1, L_2|x_1, x_2)$ means that the tester who receives this (behaviour) box will get outcome L_1 pressing button x_1 and outcome L_2 pressing button x_2. Thus, from the previous arguments it sounds reasonable that just one tester is not sufficient to answer to the previous questions about the certification of true randomness.

The simplest extension of this scenario is then given by the CHSH test that we explained in the previous section. Two parties A and B that can freely choose to perform one of two dichotomic measurements $M_{a|x}$, $M_{b|y}$ (with $x = 1, 2$ and $a = \pm 1$ and analogously for B) on their part of the system ρ_{AB}, can (after many trials) estimate the probability distribution:

$$p(ab|xy)_\rho \tag{2.28}$$

Note that conciseness we are using a different notation now. Inputs x, y refer to which button is chosen by the parties and $a, b = \pm 1$ refer to the lights which flash, Red or Green. Conceptually, apart from having introduced a second user, there is no difference with the previous single party scenario. If we restrict ρ to be a quantum system, then:

$$p(ab|xy)_\rho = tr(\rho_{AB} M_{a|x} \otimes M_{b|y}), \tag{2.29}$$

Additionally, in the case of two-outcomes measurements we are considering the following identity holds:

$$p(ab|xy)_\rho = \frac{1}{4}\left(1 + a\langle M_x\rangle + b\langle M_y\rangle + ab\langle M_x M_y\rangle\right). \tag{2.30}$$

where $M_x = M_{+1|x} - M_{-1|x}$, and $M_y = M_{+1|y} - M_{-1|y}$.

In the described a scenario, a possible way to quantify the randomness of the pair (a, b) resulting from the measurement of observables x, y when ρ is a pure state, $\rho = |\psi\rangle\langle\psi|$ is through the *guessing probability*[AMP12]:

$$G(\psi, x, y) = \max_{ab} p(ab|xy)_\psi. \tag{2.31}$$

This quantity corresponds to the probability of the best guess for outcome (a, b) (since this is the one that occurs with higher probability). A more intuitive way to express (2.31) is through the amount of obtainable bits calculated by the *min-entropy*, $H_\infty(\psi, x, y) = -\log_2 G(\psi, x, y)$. If a given pair of outcomes (a, b) is certain to occur, then the guessing probability takes its maximal value 1 which corresponds to 0 bits of min-entropy. If all four possible pairs of outcomes are equally probable, it takes its minimal value 1/4 corresponding to 2 bits of min-entropy.

If system ρ_{AB} is in a mixed state, the maximization runs over all the pure-state decompositions as follows:

$$G(\rho, x, y) = \max_{q_m, \psi_m} \sum q_m G(\psi_m, x, y) \tag{2.32}$$

where $\rho = \sum_m q_m |\psi_m\rangle\langle\psi_m|$.

The definitions given so far are both state dependent and as we will see can lead to an unwanted incongruence. To overcome that a more general definition can be given which is independent from its quantum realization:

$$G(P, x, y) = \max_{\{\rho, M\} \mapsto P} G(\rho, x, y) \tag{2.33}$$

where $\{\rho, M\}$ is any quantum realization that is *P-compatible*, namely $P = tr(\rho M)$ and $M = M_{a|x} \otimes M_{b|y}$. Similarly, a realization-independent guessing probability can be defined for the single party $G(P, x)$ whose min-entropy can vary between 0 and 1. Note that in the previous definitions no assumption is made about the dimension of the Hilbert space on which ρ and M are defined. This approach is the key idea behind the device independent scenario paradigm.

2.5.2 Link between Randomness and Non-locality

A probability distribution is said local deterministic if every outcome obtained locally by the parties is generated deterministically by the value of the chosen input. If a measurement v (w) is made by party A (B) then $a = f(v)$ ($b = g(y)$), where $f(g)$ is a deterministic function of the input v (w). Note that due to the no-signalling condition the output of the parties can just depend on the local choice of their input. It is thus clear that the guessing probability is equal to 1 in this case. Interestingly this is true for any local distribution.

As proven by Fine [Fin82], every local distribution can be written as a convex combination of local deterministic distributions (see Appendix D). It is a trivial exercise to find a pure-state (and measurement) representation that give deterministic outcomes. Thus, each term $G(\psi_m, x, y)$ appearing

in eq. (2.32) is equal to 1 and together with $\sum_m q_m = 1$ this implies that the guessing probability $G(P, x, y)$ is equal to 1 for any local distribution. Analogously in order for the min-entropy $H_\infty(P, x, y)$ to be different from 0 the probability distribution in exam has to violate a Bell's inequality (see Appendix D). Thus, a violation of a Bell's inequality is a necessary condition for $H_\infty(P, x, y) > 0$.

In the following we provide some example to clarify the definitions given above. Consider the following probability distribution:

$$p(ab|\bar{x}\bar{y}) = \frac{1}{4} \quad \forall a, b. \tag{2.34}$$

In what follows, we study different quantum realizations of it. A first way to fulfil (2.34) is by measuring the maximally entangled state, $\psi = (|00\rangle + |11\rangle)/\sqrt{2}$ choosing $A_{\bar{x}} = \sigma_x$ and $B_{\bar{y}} = \sigma_z$. Since ψ is a pure state definition (2.31) can be used, which gives $H_\infty(\psi, \bar{x}\bar{y}) = 2$ bits. An alternative way to fulfil (2.34) is by measuring the state $\rho = (|00\rangle\langle 00| + |11\rangle\langle 11|)/2)$ with the same observables $A_{\bar{x}}$, $B_{\bar{y}}$ defined above. Since the state is mixed, definition (2.32) must be used. A straightforward calculation shows that under the previous decomposition of ρ the value $H_\infty(\rho, \bar{x}\bar{y}) = 1$ bit is obtained. Note that one could in principle look for better decompositions of ρ which could give $H_\infty(\rho, \bar{x}\bar{y}) < 1$.

Let us consider a new example. Let $p(ab|xy)$ be the distribution arising by measuring the maximally entangled state, $\psi = (|00\rangle + |11\rangle)/\sqrt{2}$ with $A_1 = B_1 = \sigma_z$ and $A_2 = B_2 = \sigma_x$. The choice of settings $(1, 2)$ could in principle contain some randomness since the distribution $p(ab|12)$ is equal to $1/4$ for each a, b. But, it is immediately observed that the whole probability distribution derived in this way does not violate the CHSH inequality (2.19). In fact, there must exist a separable state and some measurements reproducing the whole distribution. The guessing probability for this quantum realization is equal to 1 even for the input's choice $(1, 2)$ ($H_\infty(P, 12) = 0$). In fact, the separable state and measurements which accomplish that are the following:

$$\rho_{AB} = \frac{1}{4} \sum_{ij=0}^{1} (|ij\rangle\langle ij|_A \otimes |ij\rangle\langle ij|_B) \tag{2.35}$$

$$A_1 = B_1 = \sigma_z \otimes \mathbb{I}, \quad A_2 = B_2 = \mathbb{I} \otimes \sigma_x. \tag{2.36}$$

All these examples show how, given a probability distribution $p(ab|xy)$, different quantum realizations lead to different values of the guessing probability. The realization-independent definition (2.33) avoids all these inconsistencies.

Chapter 3

Can bipartite classical information resources be activated?

Non-additivity is one of the distinctive traits of Quantum Information Theory: the combined use of quantum objects may be more advantageous than the sum of their individual uses. Non-additivity effects have been proven, for example, for quantum channel capacities, entanglement distillation or state estimation. In this chapter we consider whether non-additivity effects can also be found in Classical Information Theory. We work in the secret-key agreement scenario in which two honest parties, having access to correlated classical data that are also correlated to an eavesdropper, aim at distilling a secret key. Exploiting the analogies between the entanglement and the secret-key agreement scenario, we show that correlations with (conjectured) bound information become secret-key distillable when combined.

Introduction

Classical communication systems are governed by classical information theory, a vast discipline whose birth coincides with a seminal paper of Claude Shannon [Sha48]. Among his contributions, Shannon introduced the concept of channel capacity, which quantifies the maximum communication rate that can be achieved over a classical channel. One key feature of the channel capacity is its additivity: the total capacity of several channels used in parallel is simply given by the sum of their individual capacities. This fact implies thus that the channel capacity completely specifies channel's ability to convey classical information.

Moving to the quantum domain, the quantum channel capacity captures the ability of a quantum channel to transmit quantum information. Smith and Yard [SY08] proved recently that the quantum capacity is not additive. In particular, they provide examples of two channels with zero quantum capacity that define a channel with strictly positive quantum capacity when combined. This intriguing quantum effect is known as activation and can generally be understood as follows: the combined use of quantum objects can be more advantageous than the sum of their individual uses. In the last years, an intense effort has been devoted to the study of non-additivity effects in Quantum Information Theory. Classical and private communication capacity of quantum channels were later shown not to be additive in Refs [Has09, LWZG09]. Nowadays, non-additivity is considered to be one of the distinctive traits of Quantum Information Theory.

Before the results by Smith and Yard, however, non-additivity effects had also been observed in Entanglement Theory in the context of entanglement distillation. There, one is interested in the problem of whether pure-state entanglement –pure entanglement in what follows– can be extracted from a given state shared by several observers using local operations and classical communication (LOCC). In Ref. [SST03], the authors provide examples of multipartite states that (i) are non-distillable (bound) when considered separately but (ii) define a distillable state when taken together. Moving to the case of two parties, and leaving aside activation-like results as those of [HHH99], it remains unproven whether entangled states can

be activated. There is however some evidence of the existence of pairs of bound (non-distillable) entangled states that give a distillable state when combined [SST01, VW02].

In this chapter we are interested in the question of whether non-additivity effects can be observed in Classical Information Theory. As mentioned, classical channel capacities are known to be additive. Therefore, we move our considerations to distillation scenarios. In particular, we focus on the classical secret-key agreement scenario in which two honest parties, having access to correlated random variables, also correlated with an adversary, aim at establishing a secret key by local operations and public communication (LOPC). While the activation of classical resources has been shown in a multipartite key-agreement scenario in [ACM04, PB11], here we consider the more natural case of two honest parties. In our study, we exploit the analogies between the secret-key agreement and entanglement scenario noted in [GRW02]. Based on the results of [VW02], we provide evidence that activation effects may be possible in the completely classical bipartite key-agrement scenario. Our findings, therefore, suggest that the classical secret-key rate is non-additive.

This chapter is structured as follows. Section 3.1 introduces the quantum scenario, namely the quantum states and the protocol of activation. In section 3.2 we derive their classical analog. Section 3.3 concludes with a discussion on how our findings are related to other results and conjectures in the field.

3.1 Quantum Activation

As mentioned, we start by presenting the example of activation of distillable entanglement given in Ref. [VW02]. After introducing the states involved in this example, we review their distillability properties and the quantum protocol that attains the activation.

3.1.1 Quantum States

States that are invariant under a group of symmetries play a relevant role in the study of entanglement. The two classes of symmetric states considered here are *Werner* states [Wer89] and the *symmetric* states of Ref. [VW01, VW02], named in what follows symmetric states for the sake of brevity.

Werner States

Acting on an Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ with dimensions $dim(\mathcal{H}_A) = dim(\mathcal{H}_B) = d$, and commuting with all unitaries $U \otimes U$, Werner states can be expressed as:

$$\rho_W(p) = p\frac{\mathcal{A}_d}{tr(\mathcal{A}_d)} + (1-p)\frac{\mathcal{S}_d}{tr(\mathcal{S}_d)} \tag{3.1}$$

where $\mathcal{A}_d = (\mathbb{1} - \Pi_d)/2$, $\mathcal{S}_d = (\mathbb{1} + \Pi_d)/2$ are the projector operators onto the antisymmetric and symmetric subspaces, Π_d is the flip operator and $tr(\mathcal{A}_d) = d(d-1)/2$, $tr(\mathcal{S}_d) = d(d+1)/2$. It is known that states (3.1) are entangled and NPT iff $p > p_s = 1/2$. Moreover they are distillable, actually $1-distillable$, if $p > p_{1d} = 3\tau/(1+3\tau)$, where $\tau = tr(\mathcal{A}_d)/tr(\mathcal{S}_d)$. The states are conjectured to be bound entangled for $p_s < p \leq p_{1d}$.

Symmetric States

Acting on an Hilbert space $\mathcal{H} = \mathcal{H}_{A1} \otimes \mathcal{H}_{A2} \otimes \mathcal{H}_{B1} \otimes \mathcal{H}_{B2}$, the symmetric states under consideration commute with all unitaries of the form $W = (U \otimes V)_A \otimes (U \otimes V^*)_B$ (where V^* is the complex conjugate of V). These states can be represented in a compact form as [VW01]:

$$\sigma = \sum_{i=1}^{4} \lambda_i P_i / tr[P_i]$$

where $P_1 = \mathcal{A}_d^{(1)} \otimes \mathbb{P}_d^{(2)}$, $P_2 = \mathcal{S}_d^{(1)} \otimes \mathbb{P}_d^{(2)}$, $P_3 = \mathcal{A}_d^{(1)} \otimes (\mathbb{1} - \mathbb{P}_d)^{(2)}$, $P_4 = \mathcal{S}_d^{(1)} \otimes (\mathbb{1} - \mathbb{P}_d)^{(2)}$. $\mathbb{P}_d$ and $\mathbb{1} - \mathbb{P}_d$ represent the projector onto the maximally

entangled state $|\psi_d^+\rangle = 1/\sqrt{d}\sum_{i=1}^{d}|ii\rangle$, and its orthogonal complement, respectively. In Ref. [VW02] the authors identify a region in the space of parameters λ_i so that the state σ (i) is bound entangled but (ii) gives a distillable state when combined with a Werner state in the conjectured region of bound entanglement. Among all the states with these properties, we focus here on:

$$\sigma(q) = q\frac{\mathcal{A}_d}{tr(\mathcal{A}_d)} \otimes \mathbb{P}_d + (1-q)\frac{\mathcal{S}_d}{tr(\mathcal{S}_d)} \otimes \frac{(\mathbb{1} - \mathbb{P}_d)}{tr(\mathbb{1} - \mathbb{P}_d)} \tag{3.2}$$

where $q = 1/(d+2)$. This state is a *universal activator*, in the sense that it defines a distillable state when combined with any entangled Werner state. It is also relevant for what follows to study the distillability properties of states (3.2) for any value of q and $d = 3$. These states are NPT and 1-distillable for $q > 1/5$. The latter follows from the fact that in this region, there exist local projections on two-qubit subspaces mapping states (3.2) onto an entangled two-qubit state. The qubit subspaces are spanned by $|00\rangle, |01\rangle$ on Alice's side and $|10\rangle, |11\rangle$ on Bob's. Figure 3.1 summarizes the main entanglement properties of these states.

3.1.2 Protocol for Quantum Activation

As already announced, any entangled Werner state, and in particular any conjectured bound entangled Werner state, gives a distillable state when combined with the universal activator $\sigma(q)$ with $q = 1/(d+2)$, simply denoted as σ. If initially the two parties are sharing a Werner state ρ acting on $\mathcal{H}_0 = \mathcal{H}_{A_0} \otimes \mathcal{H}_{B_0}$ and a symmetric state σ acting on $\mathcal{H}_{1,2} = \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} \otimes \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$, each party applies a projection onto a maximally entangled states on $\mathcal{H}_{A_0} \otimes \mathcal{H}_{A_1}$ and $\mathcal{H}_{B_0} \otimes \mathcal{H}_{B_1}$ respectively. The resulting state is an isotropic state ρ_{iso} acting on $\mathcal{H}_{A_2} \otimes \mathcal{H}_{B_2}$. Recall that isotropic state are $U \otimes U^*$ invariant and defined by the convex combination of a maximally entangled state and white noise, $\mathbb{I}/d^2$. One can see that the resulting isotropic state has an overlap with a maximally entangled state, $\mathrm{tr}(\rho_{iso}\mathbb{P}_d)$, larger than $1/d$ for any entangled Werner state. As shown in [HH99], this condition is sufficient for distillability.

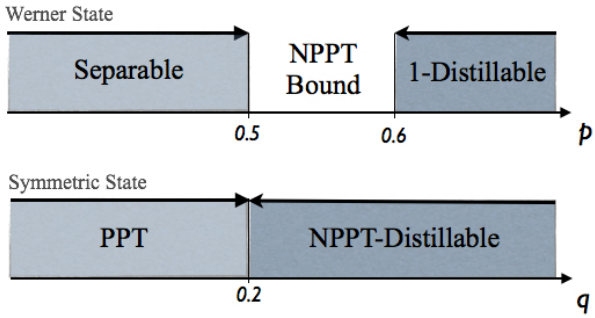

Figure 3.1: Entanglement properties of Werner, ρ_W, and symmetric state, $\sigma(q)$, for the qutrit case ($d = 3$). In the region between separability and 1-distillability, ρ_W is NPPT and conjectured bound. The point $q = 0.2$ represents the extremal value for which states $\sigma(q)$ are PPT, thus not distillable. For larger values of q the states are distillable (in particular, 1-distillable).

3.2 Classical Activation

This section presents our main results. Exploiting the analogies between the entanglement and secret-key agreement scenarios, we study whether it is possible to derive a cryptographic classical analog of the activation of distillable entanglement between bipartite quantum states given above Ref. [VW02]. We map the involved quantum states onto probability distributions and study their secrecy properties. After applying classical distillation protocols, we show how the honest parties are able to distill a secret key from each of the distributions for the same range of parameters as in the quantum regime ($E_D > 0$). Finally, we introduce a distillation protocol analogue to the one used for the quantum activation. We prove that this protocol activates probability distributions containing conjectured bound information, although we cannot completely recover the quantum region.

We first associate probability distributions to all the previous quantum states. In order to do so, we purify the initial bipartite noisy quantum states ρ_{AB} by including an environment, and then map the tripar-

tite quantum states $|\psi_{ABE}\rangle$ onto probability distributions by performing some local measurements, see (2.15). The procedure to choose these measurements is always the same: computational bases for the honest parties, and general measurements for Eve. More precisely, denoting by X and Y the result obtained by Alice and Bob, this effectively projects Eve's system onto the pure state $|e_{XY}\rangle = \langle XY|\psi_{ABE}\rangle$ with probability $P(XY) = \langle XY|\rho_{AB}|XY\rangle$. Given that, the measurement that Eve applies is the one that minimizes her error probability when distinguishing the states in the ensemble $\{|e_{XY}\rangle, P(XY)\}$. Note that this choice of measurement may not necessarily be optimal from Eve's point of view in terms of the secret correlations between Alice and Bob, but it seems a natural choice. This procedure is applied to the two family of states, namely Werner and symmetric. Because of the symmetries of these states, the measurements minimizing Eve's error probability can be analytically determined using the results of Refs [Hel76, EF01].

In order to characterize the secrecy properties of the obtained probability distributions, we compute the intrinsic information when numerically possible and use AD protocols for distillability. We stress that the considered protocols distill a secret key in the same region of parameters in which entanglement distillation was possible for the initial quantum states. Finally, we introduce a quantum-like activation protocol that maps the two probability distributions into a new distribution in which Alice and Bob each have a bit. We then prove that an AD protocol allows distilling a secret key for some value of the parameters in which the initial quantum states were non-distillable. However, we are unable to close all the gap between entanglement and 1-distillability for the Werner state.

3.2.1 Probability Distributions

We map now quantum states to probability distributions through measurements on them (as discussed in section 2.3).

Werner states distribution

We start by mapping the Werner states of two qutrits onto a probability distribution P_{XYZ} following the recipe explained in the previous section. In this way, we get a one-parameter family of probability distributions P_{XYZ}, (see Table 3.1 for details), which depends just on the same parameter p defining the initial Werner state (3.1). The resulting distributions are given in Table 3.1. The indices for Eve's symbols specify her guess on Alice's and Bob's symbols or, in other words, if Eve outcome is $Z = z_{ij}$, the most probable outcomes for Alice and Bob are $X = i$ and $Y = j$.

	0	1	2
0	$\lambda_1 \quad (z_{00})$	$\frac{\lambda_1+\lambda_2}{2}$ $\begin{cases}\delta_Z & (z_{10})\\ 1-\delta_Z & (z_{01})\end{cases}$	$\frac{\lambda_1+\lambda_2}{2}$ $\begin{cases}\delta_Z & (z_{20})\\ 1-\delta_Z & (z_{02})\end{cases}$
1	$\frac{\lambda_1+\lambda_2}{2}$ $\begin{cases}\delta_Z & (z_{01})\\ 1-\delta_Z & (z_{10})\end{cases}$	$\lambda_1 \quad (z_{11})$	$\frac{\lambda_1+\lambda_2}{2}$ $\begin{cases}\delta_Z & (z_{21})\\ 1-\delta_Z & (z_{12})\end{cases}$
2	$\frac{\lambda_1+\lambda_2}{2}$ $\begin{cases}\delta_Z & (z_{02})\\ 1-\delta_Z & (z_{20})\end{cases}$	$\frac{\lambda_1+\lambda_2}{2}$ $\begin{cases}\delta_Z & (z_{12})\\ 1-\delta_Z & (z_{21})\end{cases}$	$\lambda_1 \quad (z_{22})$

Table 3.1: Tripartite probability distributions derived from Werner states (3.1). The parameters in the table are as follows: $\lambda_1 = (1-p)/6$, $\lambda_2 = p/3$ and $\delta_Z = (\sqrt{\lambda_1} - \sqrt{\lambda_2})^2/(2(\lambda_1+\lambda_2))$. Rows (columns) represent Alice's (Bob's) symbols. Eve's symbols are shown in parenthesis. For example, the cell $(X = 0, Y = 1)$ shows that whenever Alice and Bob get (0,1) (which happen with probability $(\lambda_1+\lambda_2)/2$), Eve correctly guesses the symbol z_{01} with probability $1-\delta_Z$, and makes an error (symbol z_{10}) with probability δ_Z.

As done for entanglement, we now characterize these distributions in terms of their secret correlations. Recall that for the quantum case and qutrits, the state was entangled for $p > p_s = 1/2$ and conjectured non-distillable for $p \leq p_{1d} = 3/5$. As we show next, the same values appear for the analogous classical distributions. Concerning the point p_s, we compute

the intrinsic information of the distributions in Table 3.1 by numerical optimization over all possible channels by Eve. Of course, one can never exclude the existence of local minima and, therefore, that the intrinsic information is strictly smaller than what numerically obtained. One may wonder why this computation is necessary. For instance, at the point $p = p_s$ the quantum state is separable and, then, it is known that there exists a measurement by Eve such that the intrinsic information between Alice and Bob is zero for all measurements. Note however that in terms of intrinsic information, the optimal measurement by Eve is the one that prepares on Alice and Bob the ensemble of product states compatible with the separable state Alice and Bob share. This measurement is not necessarily the same as the one minimizing Eve's error probability when Alice and Bob measure in the computational bases. The same applies to the entanglement region. While there are measurements such that Alice and Bob share secret correlations no matter which measurement Eve performs, these measurements are not on the computational bases.

Using the numerical insight, we find a conjectured optimal channel that reproduces the numerical results. The optimal channel gives zero intrinsic information exactly at the point $p = p_s$. It maps Eve's symbols z_{ii} onto z_{ij} with $i \neq j$ with equal probability ($i, j = 0, 1, 2$). Its easy form leads to the following analytical expression for $I(X;Y \downarrow Z)$:

$$I(X;Y \downarrow Z) = -\log(1-x^2) - x \log\left(\frac{1+x}{1-x}\sqrt{\frac{\tau-2x}{\tau+2x}}\right) + \frac{\tau}{4}\log\left(\tau^2-4x^2\right) + \left(1-\frac{\tau}{2}\right)\log(2-\tau)$$

where $\tau = 1+p$, $x = \sqrt{2p(1-p)}$. Figure 3.2 shows the behavior of this quantity in the region of interest.

Moving to the distillability properties, we study AD protocols and identify a value of p for which positive secret-key rate can be obtained by the two honest parties through these protocols. The considered protocol is the

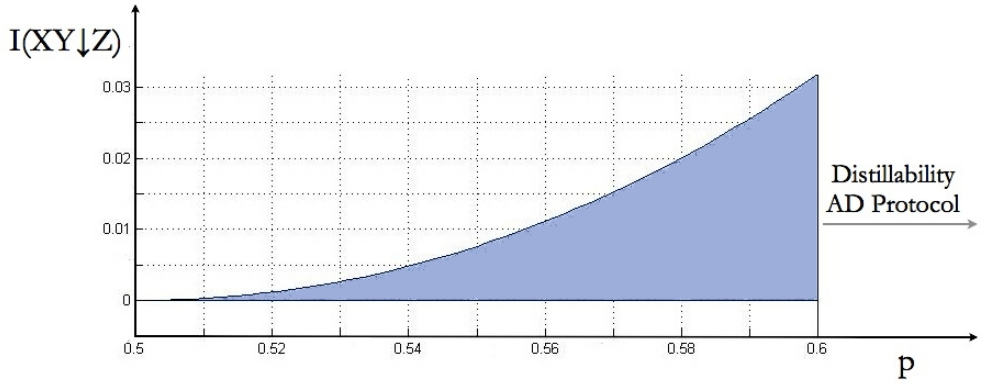

Figure 3.2: Behaviour of the intrinsic information for the P_{XYZ} relative to the Werner state. Note that: i) $I(X;Y \downarrow Z)$ is equal to 0 at point $p = 0.5$ which corresponds to the last point of separability for the Werner state; ii) $I(X;Y \downarrow Z)$ is strictly positive at point $p = 0.6$ which corresponds to the extreme value of p for which it is 1-copy distillable.

quantum analogue of the quantum one and uses a binaryzation. Alice and Bob first discard one (but the same) of their symbols. Then, one of the parties, say Bob, applies a local permutation to his symbols. For example, if they agreed on discarding symbol 2, then Bob applies $0 \leftrightarrow 1$. Alice and Bob now apply AD to the resulting two-bit distribution. This distribution is shown in Table 3.2.

From the obtained table, it is possible to estimate the dependence of Bob's and Eve's errors on the size of the blocks used for AD, denoted by N. Recall that in the case of bits the protocols works as follows: Alice generates a random bit ζ and chooses N symbols $\mathbf{a}$ from her list of data. She then sends to Bob the information about these symbols and the vector $\bar{\mathbf{a}}$ such that $a_i \oplus \bar{a}_i = \zeta, \forall i$. Bob takes the symbols in his list corresponding to those chosen by Alice, $\mathbf{b}$, and accepts only when $\chi = b_i \oplus \bar{a}_i, \forall i$. Bob's error probability β_N is now easy to compute. Denote by β the error probability in the initial two-bit probability distribution, $\beta = P(X \neq Y) = 2\lambda_1/(3\lambda_1 + \lambda_2)$. Bob accepts a bit whenever either all his N symbols are identical to

those of Alice, which happens with probability $(1-\beta)^N$, or all his symbols are different, whose probability is β^N. Thus, the probability of accepting a wrong bit conditioned on acceptance is given by:

$$\beta_N = \frac{\beta^N}{\beta^N + (1-\beta)^N} \leqslant \left(\frac{\beta}{1-\beta}\right)^N. \tag{3.3}$$

The upper bound becomes tight in the limit $N \to \infty$.

	0	1
0	$\frac{\lambda_1+\lambda_2}{2}\begin{cases}\delta_Z & (z_{11})\\ 1-\delta_Z & (z_{00})\end{cases}$	$\lambda_1 \quad (z_{01})$
1	$\lambda_1 \quad (z_{10})$	$\frac{\lambda_1+\lambda_2}{2}\begin{cases}\delta_Z & (z_{00})\\ 1-\delta_Z & (z_{11})\end{cases}$

Table 3.2: Two-bit distribution resulting from projecting the initial distribution of Table 3.1 on the space $X, Y = 0, 1$ and after Bob permutes his symbol. For the sake of clarity, we apply a permutation also on the second index of Eve's symbols, that is $z_{ij} \to z_{i1-j}$. All the terms in the table should be normalized by a factor $3\lambda_1 + \lambda_2$.

We now move to the estimation of Eve's error ϵ_N. As her information is probabilistic, there is always a non-zero probability that she makes a mistake. For the estimation we compute a lower bound on the error given by all the cases in which the N symbols observed by Eve do not provide her any information about the value of the bit generated by Alice. In the computation, it is simpler to use Eve's probabilities conditioned on the fact that Alice and Bob have made no mistake after AD (which means that no mistake has occurred for any of the N symbols). Or in other words, we only consider the terms in the diagonal of Table 3.2. This does not make any difference for what follows as in the limit $N \to \infty$ the probability of Bob accepting a wrong symbol goes to zero. After Bob's acceptance, Eve knows

that the actual string $\mathbf{a}$ used by Alice is either equal to $\bar{\mathbf{a}}$ (the one sent on the public channel) when $\zeta = 0$, or $\bar{\mathbf{a}}'$ (the permuted one, that is, $\bar{a}'_i = 1 - \bar{a}_i$) when $\zeta = 1$. Clearly, all the events in which the N symbols observed by Eve, $Z^{(i)}$, are such that $P(Z^{(1)}.. Z^{(N)}|\mathbf{a} = \bar{\mathbf{a}}) = P(Z^{(1)}.. Z^{(N)}|\mathbf{a} = \bar{\mathbf{a}}')$ do not give her any information about ζ. In these cases, Eve has to randomly guess Alice's symbol and makes an error with probability 1/2. Due to the symmetry in the diagonal of Table 3.2, that is, $P(Z = z_{00}|X = 0) = P(Z = z_{11} = 1|X = 1)$ and $P(Z = z_{11}|X = 0) = P(Z = z_{00}|X = 1)$, all the events where Eve has exactly $N/2$ of her symbols equal to z_{00} and $N/2$ equal to z_{11} satisfy the previous condition and, thus, contribute to her error. Counting all the possible ways of distributing these cases leads to the following lower bound on Eve's error probability [GW99]:

$$\epsilon_N \geqslant \frac{1}{2} \left(\begin{array}{c} N \\ N/2 \end{array} \right) \delta_Z^{N/2} (1 - \delta_Z)^{N/2} \tag{3.4}$$

where δ_Z is the probability for Eve to guess wrongly conditioned on those cases in which Alice and Bob's symbols coincide (this value is made explicit in the caption of Figure 3.1). The asymptotic behavior of (3.4), after applying the Stirling's approximation $(n!)^2 \simeq (2n)!/2^{2n}$ and expanding the binomial coefficient can be expressed as:

$$\epsilon_N \geqslant c(2\sqrt{\delta_Z(1 - \delta_Z)})^N, \tag{3.5}$$

with c being a positive constant.

By comparing Eqs. (3.3) and (3.5) one concludes that whenever

$$\frac{\beta}{1 - \beta} < 2\sqrt{\delta_Z(1 - \delta_Z)} \tag{3.6}$$

key distillation is possible. This follows from the fact that, if this condition holds, Bob's error is exponentially smaller than Eve's with N. This in turn implies that it is possible to choose a value of N such that Alice-Bob mutual information is larger than Alice-Eve and one-way distillation techniques can distill a secret key (we show this in appendix A). From (3.5) one gets that AD works whenever $p > 3/5$, as for 1-distillability in the quantum case.

Before concluding this part, we would like to mention that the same range of parameters for distillation is obtained if one applies the generalized AD protocol of Ref. [AGS03].

Symmetric states distribution

We apply the same machinery to the symmetric states $\sigma(q)$. Again, the symmetries of the states allow the explicit computation of the measurement by Eve minimizing her error probability for any value of q. The obtained distributions, denoted by $Q_{X1,Y1,X2,Y2,\tilde{Z}}$, is significantly more complex and shown in Appendix A. It consists of two trits for Alice, (X_1, X_2) and two trits for Bob, (X_2, Y_2), while Eve's variable can take 63 possible values. It is now much harder to estimate the secrecy properties of the distribution. For instance, we did not make any attempt to compute the intrinsic information. However, we are able to show that Alice and Bob can distill a secret key whenever $q > 1/5$ as in the quantum regime.

To simplify our task, we exploit again the concept of *binaryzation*. Inspired by the quantum projections used for the distillation of $\sigma(q)$, Alice and Bob select two outcomes on each side, namely $00, 01$ for Alice and $10, 11$ for Bob. The obtained two-bit distribution is shown in Table 3.3.

They apply the standard bit AD protocol to this distribution. As before, Bob's error can be easily computed, getting the same as in Eq. (3.3), but now with β equal to $3(1-q)/(5+11q)$. The estimation of Eve's error is much more cumbersome. As above, the main idea is to derive a lower bound on it based on those instances in which Eve's symbols do not provide her any information about the symbol ζ Alice used for AD. Again, one can restrict the analysis to the terms in the diagonal of Table 3.3. The main difference in comparison with the simple case discussed above is the larger number of symbols for Eve. However, given the symmetry of the distribution 3.3 it is

	0 [10]	1 [11]
0 [00]	$\frac{1+7q}{5+11q}$ $\begin{cases} P_G & (\tilde{z}_{0100}) \\ P_L & (\tilde{z}_{0111}) \\ P_L & (\tilde{z}_{0122}) \\ P_B & (\tilde{z}_{1000}) \\ P_H & (\tilde{z}_{1011}) \\ P_H & (\tilde{z}_{1022}) \end{cases}$	$\frac{3(1-q)}{2(5+11q)}$ $\begin{cases} 1/2 & (\tilde{z}_{0101}) \\ 1/2 & (\tilde{z}_{1001}) \end{cases}$
1 [01]	$\frac{3(1-q)}{2(5+11q)}$ $\begin{cases} 1/2 & (\tilde{z}_{0110}) \\ 1/2 & (\tilde{z}_{1010}) \end{cases}$	$\frac{1+7q}{5+11q}$ $\begin{cases} P_L & (\tilde{z}_{0100}) \\ P_G & (\tilde{z}_{0111}) \\ P_L & (\tilde{z}_{0122}) \\ P_H & (\tilde{z}_{1000}) \\ P_B & (\tilde{z}_{1011}) \\ P_H & (\tilde{z}_{1022}) \end{cases}$

Table 3.3: Two-bit distribution obtained as a result of the binaryzation applied to $Q_{X1,Y1,X2,Y2,\tilde{Z}}$. Note that we have relabeled the old symbols (shown in square brakets) by 0 and 1, in the following we use $\tilde{X}, \tilde{Y}$ to refer to them. The parameters in the table are as follows: $\alpha = \sqrt{8q/(1+7q)}$ and $\gamma = \sqrt{(1-q)/(2(1+7q))}$, $P_G = (\alpha + 2\gamma)^2/6$, $P_B = (-\alpha + 2\gamma)^2/6$, $P_L = (\alpha - \gamma)^2/6$, $P_H = (\alpha + \gamma)^2/6$.

enough to consider Eve's symbols pair-wise:

$$\begin{aligned}
P(\tilde{Z}=\tilde{z}_{0100}|\tilde{X}\tilde{Y}=00) &= P(\tilde{Z}=\tilde{z}_{0111}|\tilde{X}\tilde{Y}=11) = \bar{\delta}_1 \\
P(\tilde{Z}=\tilde{z}_{0100}|\tilde{X}\tilde{Y}=11) &= P(\tilde{Z}=\tilde{z}_{0111}|\tilde{X}\tilde{Y}=00) = \bar{\eta}_1 \\
P(\tilde{Z}=\tilde{z}_{1000}|\tilde{X}\tilde{Y}=00) &= P(\tilde{Z}=\tilde{z}_{1011}|\tilde{X}\tilde{Y}=11) = \bar{\delta}_2 \\
P(\tilde{Z}=\tilde{z}_{1000}|\tilde{X}\tilde{Y}=11) &= P(\tilde{Z}=\tilde{z}_{1011}|\tilde{X}\tilde{Y}=00) = \bar{\eta}_2
\end{aligned}$$

where we have used $\tilde{X},\tilde{Y}$ to denote the re-labeling of Alice and Bob's symbols. Note that the last two subindexes of Eve's symbols are those that give her information about Alice's (and Bob's) symbol. Symbols $\tilde{z}_{**22}$ give her no information about Alice's symbols, so we sum them, their total probability being δ_3. Given the public string $\bar{\mathbf{a}}_N$, one can see that all those cases for which Eve has the same number n_1 of $\tilde{z}_{0100}$ and $\tilde{z}_{0111}$ and the same number n_2 of $\tilde{z}_{1000}$ and $\tilde{z}_{1011}$, with $N=2n_1+2n_2+2n_3$ and where $2n_3$ is the total number of symbols $\tilde{z}_{**22}$, contribute to her error. Thus, counting all these cases leads to the following lower bound on Eve's error:

$$\epsilon_N \geqslant \frac{1}{2}\sum_{n_1,n_2,n_3}\frac{N!}{(2n_1)!(2n_2)!(2n_3)!}\left(2\sqrt{\delta_1\eta_1}\right)^{2n_1}\left(2\sqrt{\delta_2\eta_2}\right)^{2n_2}(\delta_3)^{2n_3} \tag{3.7}$$

where δ_i and η_i are the probabilities shown above but normalized (since as already stated we are considering the asymptotic case). After Stirling's approximation and summing eq. (3.7) the following compact form is obtained:

$$\epsilon_N \geqslant c\left(2\sqrt{\delta_1\eta_1}+2\sqrt{\delta_2\eta_2}+\delta_3\right)^N$$

with c being a positive constant. Comparing the scaling of the errors, one has that AD works whenever

$$\frac{\beta}{1-\beta} < 2\sqrt{\delta_1\eta_1}+2\sqrt{\delta_2\eta_2}+\delta_3 \tag{3.8}$$

where the right hand side is equal to $(\alpha+\gamma)^2/3$ (the values of α and γ are reported in the caption of Table 3.3). Simple algebra shows that eq. (3.8) is satisfied whenever $q > \tilde{q} = 0.2$, as announced.

3.2.2 Protocol for Classsical Activation

Inspired by the quantum activation example of Ref. [VW02], we consider the following classical protocol. Alice and Bob have access to the trits X and Y, whose correlations are described by P_{XYZ}, and the two trits (X_1, X_2) and (Y_1, Y_2) correlated according to $Q_{X1,Y1,X2,Y2,\tilde{Z}}$. Alice (Bob) keeps X_2 (Y_2), and only X_2 (Y_2), whenever $X = X_1$ ($Y = Y_1$); otherwise they discard all the symbols. This filtering projects the initial probability into a slightly simpler two-trit distribution. The new probability distribution $Q^*(X_2, Y_2, E)$ reads:

$$Q^*(X_2, Y_2, E) = \sum_{x,y=0}^{2} P(X = x, Y = y, Z) Q(X_1 = x, Y_1 = y, X_2, Y_2, \tilde{Z}) \tag{3.9}$$

where $E = [Z, \tilde{Z}]$ is the collection of Eve's ymbols. Finally Alice and Bob binaryze their symbols by discarding one of the three values (the same for both), say 2. The resulting distribution is shown in Table 3.4.

As above, we use AD protocols to estimate the value of p for which Alice and Bob can extract a positive secret key rate if they are sharing pairs of bits distributed according to Table 3.4. We are able to prove that whenever $p > p_c \simeq 0.513$ an AD protocol allows distilling a secret key from the distribution in Table 3.4 and, thus, a form of activation is possible. Unfortunately, we are unable to reach the point $p = 0.5$, as in the quantum scenario. However, our analysis suggests that the secret key rate is non-additive for some values of p. In the following we summarize the key steps leading to this result.

As mentioned, the values of interest for P_{XYZ} and $Q_{X1,Y1,X2,Y2,\tilde{Z}}$ are, $0.5 < p \leqslant 0.6$ and $q = 0.2$, respectively. The distribution $Q^*(X_2, Y_2, E)$ resulting from the local filtering by the honest parties depends on the parameter p. In order to estimate Eve's error we follow a similar argument

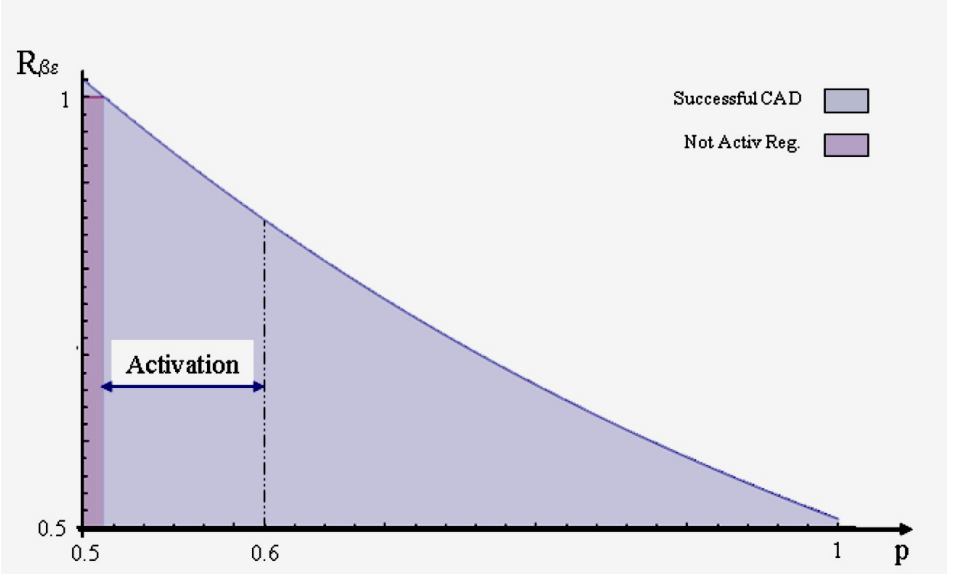

Figure 3.3: The CAD protocol certifies that if the Werner state distribution (Table 3.1) is taken with $p > 0.513$ positive secrecy can be extracted by the honest parties. Unfortunately, we cannot completely close the gap up to $p = 0.5$. This would have shown a direct correspondence between the quantum and the classical scenario.

	0	1
0	$\frac{\lambda_1(1-q)}{72c_N}\begin{cases}2/3 & (z_{ii},\tilde{z}_{ii00})\\ 1/6 & (z_{ii},\tilde{z}_{ii11})\\ 1/6 & (z_{ii},\tilde{z}_{ii22})\end{cases}$ $\Lambda s_N\begin{cases}\delta_Z P_G+(1-\delta_Z)P_B & (z_{ts},\tilde{z}_{st00})\\ \delta_Z P_L+(1-\delta_Z)P_H & (z_{ts},\tilde{z}_{st11})\\ \delta_Z P_L+(1-\delta_Z)P_H & (z_{ts},\tilde{z}_{st22})\\ \delta_Z P_B+(1-\delta_Z)P_G & (z_{ts},\tilde{z}_{ts00})\\ \delta_Z P_H+(1-\delta_Z)P_L & (z_{ts},\tilde{z}_{ts11})\\ \delta_Z P_H+(1-\delta_Z)P_L & (z_{ts},\tilde{z}_{ts22})\\ \delta_Z P_B+(1-\delta_Z)P_G & (z_{st},\tilde{z}_{st00})\\ \delta_Z P_H+(1-\delta_Z)P_L & (z_{st},\tilde{z}_{st11})\\ \delta_Z P_H+(1-\delta_Z)P_L & (z_{st},\tilde{z}_{st22})\\ \delta_Z P_G+(1-\delta_Z)P_B & (z_{st},\tilde{z}_{ts00})\\ \delta_Z P_L+(1-\delta_Z)P_H & (z_{st},\tilde{z}_{ts11})\\ \delta_Z P_L+(1-\delta_Z)P_H & (z_{st},\tilde{z}_{ts22})\end{cases}$	$\frac{\lambda_1(1-q)}{48c_N}\begin{cases}1 & (z_{00},\tilde{z}_{0001})\\ 1 & (z_{11},\tilde{z}_{1101})\\ 1 & (z_{22},\tilde{z}_{2201})\end{cases}$ $\frac{\Lambda(1-q)}{96c_N}\begin{cases}1/2 & (z_{01},\tilde{z}_{0101})\\ 1/2 & (z_{01},\tilde{z}_{1001})\\ 1/2 & (z_{10},\tilde{z}_{0101})\\ 1/2 & (z_{10},\tilde{z}_{1001})\\ 1/2 & (z_{02},\tilde{z}_{0201})\\ 1/2 & (z_{02},\tilde{z}_{2001})\\ 1/2 & (z_{20},\tilde{z}_{0201})\\ 1/2 & (z_{20},\tilde{z}_{2001})\\ 1/2 & (z_{12},\tilde{z}_{1201})\\ 1/2 & (z_{12},\tilde{z}_{2101})\\ 1/2 & (z_{21},\tilde{z}_{1201})\\ 1/2 & (z_{21},\tilde{z}_{2101})\end{cases}$
1	$\frac{\lambda_1(1-q)}{48c_N}\begin{cases}1 & (z_{00},\tilde{z}_{0010})\\ 1 & (z_{11},\tilde{z}_{1110})\\ 1 & (z_{22},\tilde{z}_{2210})\end{cases}$ $\frac{\Lambda(1-q)}{96c_N}\begin{cases}1/2 & (z_{01},\tilde{z}_{0110})\\ 1/2 & (z_{01},\tilde{z}_{1010})\\ 1/2 & (z_{10},\tilde{z}_{0110})\\ 1/2 & (z_{10},\tilde{z}_{1010})\\ 1/2 & (z_{02},\tilde{z}_{0210})\\ 1/2 & (z_{02},\tilde{z}_{2010})\\ 1/2 & (z_{20},\tilde{z}_{0210})\\ 1/2 & (z_{20},\tilde{z}_{2010})\\ 1/2 & (z_{12},\tilde{z}_{1210})\\ 1/2 & (z_{12},\tilde{z}_{2110})\\ 1/2 & (z_{21},\tilde{z}_{1210})\\ 1/2 & (z_{21},\tilde{z}_{2110})\end{cases}$	$\frac{\lambda_1(1-q)}{72c_N}\begin{cases}1/6 & (z_{ii},\tilde{z}_{ii00})\\ 2/3 & (z_{ii},\tilde{z}_{ii11})\\ 1/6 & (z_{ii},\tilde{z}_{ii22})\end{cases}$ $\Lambda s_N\begin{cases}\delta_Z P_L+(1-\delta_Z)P_H & (z_{ts},\tilde{z}_{st00})\\ \delta_Z P_G+(1-\delta_Z)P_B & (z_{ts},\tilde{z}_{st11})\\ \delta_Z P_L+(1-\delta_Z)P_H & (z_{ts},\tilde{z}_{st22})\\ \delta_Z P_H+(1-\delta_Z)P_L & (z_{ts},\tilde{z}_{ts00})\\ \delta_Z P_B+(1-\delta_Z)P_G & (z_{ts},\tilde{z}_{ts11})\\ \delta_Z P_H+(1-\delta_Z)P_L & (z_{ts},\tilde{z}_{ts22})\\ \delta_Z P_H+(1-\delta_Z)P_L & (z_{st},\tilde{z}_{st00})\\ \delta_Z P_B+(1-\delta_Z)P_G & (z_{st},\tilde{z}_{st11})\\ \delta_Z P_H+(1-\delta_Z)P_L & (z_{st},\tilde{z}_{st22})\\ \delta_Z P_L+(1-\delta_Z)P_H & (z_{st},\tilde{z}_{ts00})\\ \delta_Z P_G+(1-\delta_Z)P_B & (z_{st},\tilde{z}_{ts11})\\ \delta_Z P_L+(1-\delta_Z)P_H & (z_{st},\tilde{z}_{ts22})\end{cases}$

Table 3.4: The initial probability distributions P_{XYZ} and $Q_{X1,Y1,X2,Y2,\tilde{Z}}$ are mapped through the classical protocol to the new probability distribution $Q^*(X_2,Y_2,E)$ shown above. From it we derive the minimum value of p for which positive secret key can be extracted by A and B. The parameters appearing above are expressed as a function of p and q: $\Lambda=(\lambda_1+\lambda_2)/2$, $c_N=(\lambda_1+\lambda_2)(5+11q)/48+5\lambda_1(1-q)/24$, $s_N=(1+7q)/(144c_N)$, $i,s,t=0,1,2$ with $s\neq t$ and $s<t$. The optimal q corresponds to 1/5.

as for $Q_{X1,Y1,X2,Y2,\tilde{Z}}$, now adapted to this slightly more complex case. Despite the big amount of symbols on Eve's side (see Table 3.4), the symmetry in the distribution leads to six main classes that are relevant for the AD analysis (appendix A further clarifies this point). These arguments lead to the following bound on Eve's error:

$$\epsilon_N \geqslant \frac{1}{2} \sum_{n_1,n_2\ldots n_6} \frac{N!}{(2n_1)!\ldots(2n_6)!} \left(6\sqrt{\delta_1\ \eta_1}\ \right)^{2n_1} \ldots \left(6\sqrt{\delta_5\ \eta_5}\right)^{2n_5} \delta_6^{2n_6} \tag{3.10}$$

where $\sum_{i=1}^{6} 2n_i = N$. Note that as before the terms $\delta_i\eta_i$ with $i = 1\ldots5$ take into account those cases in which Eve has n_i symbols that coincide with the public string sent by Alice and n_i symbols that are opposite to those appearing in the public string. The last term, δ_6, as before, refers to the sum of probabilities for which Eve has no information at all (see details in appendix A). In the asymptotic case we are treating here, Eq. (3.10) converges to a multinomial distribution, namely:

$$\epsilon_N \geqslant c\left(6\left(\sqrt{\delta_1\ \eta_1}\ + \ldots \sqrt{\delta_5\ \eta_5}\right) + \delta_6\right)^N \tag{3.11}$$

with c being a positive constant. Bob's error is much easier to compute, getting $\beta = (3\lambda_1 + \lambda_2)(1-q)/(16c_N)$. Putting these two terms together, we have that the AD protocols works whenever:

$$\frac{\beta}{1-\beta} < 6\left(\sqrt{\delta_1\ \eta_1}\ + \ldots \sqrt{\delta_5\ \eta_5}\right) + \delta_6 \tag{3.12}$$

Figure 3.3 shows the ratio between the left hand side and the right hand side, $R_{\beta\epsilon}$, as a function of the parameter p. As above, whenever $R_{\beta\epsilon} < 1$, the AD protocol succeeds. The point at which $R_{\beta\epsilon} = 1$ corresponds to $p = 0.513$, as already announced.

3.3 Conclusions

Non-additivity is an ubiquitous phenomenon in Quantum Information Theory due to the presence of entanglement. In this work, we provide some

evidence for the existence of similar effects for secret classical correlations. Exploiting the analogies between the entanglement and secret-key agreement scenario, we have shown that two classical distributions from which no secrecy can be extracted by AD protocols can lead to a positive secret key rate when combined.

The evidence we provide is somehow similar to the conjectured example of activation for bipartite entangled states. Note however that, in the quantum case, one of the two states is provably bound. As mentioned several times, it could well happen that one, or even the two probability distributions considered here are key-distillable. Indeed, there exist examples of bound entangled states from which one can obtain probability distributions with positive secret-key rate [HHHO05]. Note however that all the known examples of bound entangled states with non-zero privacy are based on the existence of ancillary systems on the honest parties, known as shields, that prevent Eve from having the purification of the systems Alice and Bob measure to construct the key. If any of the probability distributions constructed here were key distillable, they would constitute a novel example of secret correlations from a bound entangled state that does not fit in the construction of [HHHO05].

Chapter 4

Superactivation, unlockability, and secrecy distribution of bound information

Bound information, a cryptographic classical analogue of bound entanglement, is defined as secret classical correlations that despite containing secrecy, do not allow separate parties to extract it. The existence of this kind of correlations was conjectured in the bipartite case and later shown in the multipartite case. In this chapter, we provide a new example of bound information in the four-partite scenario. Later, we prove that this bound information shares the same properties as the original quantum state from which it is derived, namely, superactivation in a finite-copy scenario and unlockability. We also show that the bound entangled state in exam, and also the derived bound information, can be used to distribute multipartite pure-state entanglement and secret correlations, respectively.

4.1 Introduction

Following the analogy between entanglement and secret-key agreement, Gisin and Wolf conjectured and gave evidence for the existence, in the bipartite scenario, of a classical analog of bound entanglement, the so-called bound information. Despite firstly defined as a bipartite concept, the bound information can unambiguously generalised to more honest parties plus an eavesdropper. In the four partite case, for example, $P(A, B, C, D, \mathcal{E})$ it is said to contain bound information if *i)* no pair of honest parties, even with the help of the other ones, can generate a secret key from any instances of $P(A, B, C, D, \mathcal{E})$, *ii)* $P(ABCD\mathcal{E})$ cannot be distributed by LOPC operations.

Remarkably, while only conjectured in the bipartite case, a proof of bound information was provided in the three-partite case. This result was possible due to the possibility to consider different bipartitions for which the intrinsic information is zero (see below). The probability distribution was derived directly by measuring a bound entangled state in the computational basis of the separated parties and then shown to be bound by means of classical tools. Additionally it was proved that such a bound information could be activated in the asymptotic case of many copies, analogously to the entanglement scenario.

In this chapter we provide a novel example of multipartite bound information, which in contrast with the previous example, can be activated in the finite copy scenario. As a consequence of that, no advantage distillation protocols are needed to show the positivity of the key rate of the combined distributiions. Additionally, we show that as for the quantum case, the obtained bound information is shown to be unlockable. All these findings are based on the interesting properties of the Smolin state introduced in Ref. [Smo01] that we could translate to the classical scenario.

Finally, we provide another useful feature of the correlations in exam to distribute pure-state entanglement and multipartite sbits. In the quantum scenario, we show that the tripartite GHZ state can be extended to the four-partite GHZ state using LOCC, given that a four-partite bound entangled state is shared among parties. As expected, we show this to be true for the

classical analogue too: when bound information is shared by four parties, an sbit of three parties can be distributed over the four parties using LOPC.

This chapter is organized as follows. Sec. 4.2, briefly defines and reviews the properties of the Smolin states. In Sec. 4.3, the existence of bound information is shown and the properties of unlockability and superactivation are translated from the quantum to the classical case. In Sec. 4.4, it is shown that bound entangled state (bound information) together with LOCC (LOPC) can be used to extend GHZ states (sbits) from three to four parties.

4.2 The Smolin State

Let us first briefly review the properties of the Smolin state presented in Ref. [Smo01]. The Smolin state is a four-partite bound entangled state, shared by, say Alice, Bob, Clare and David:

$$\rho_{ABCD} = \frac{1}{4}\sum_i |\psi_i\rangle_{AB}\langle\psi_i| \otimes |\psi_i\rangle_{CD}\langle\psi_i|, \tag{4.1}$$

where $|\psi_1\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, $|\psi_2\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$, $|\psi_3\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$, and $|\psi_4\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$. This state has been exploited to derive intriguing effects of bound entanglement such as the unlockability and the superactivation in a finite-copy scenario [Smo01]. Let us summarize the properties in the following.

i) Invariance under permutations. The state is symmetric under any exchange of parties, i.e. $\rho_{ABCD} = \rho_{ABDC} = \rho_{ADBC}$.

ii) Undistillability. Looking at the bipartite splitting $AB : CD$ in the state in Eq. (4.1), it is clear that the state is separable across the cut. Then, from the property i), it follows that the state is separable in all bipartitions across two parties versus the others, such as $AC : BD$ and $AD : BC$. This already shows that no pair of parties can distill entanglement, and therefore the state is undistillable.

iii) Unlockability. An important property of the state is the unlockability of entanglement. This can be seen when two parties among the four join together and apply collective operations to discriminate among the four Bell states. Announcing the measurement outcome, the two joined parties can allow the other two parties to know which Bell state they share. Consequently, applying local unitaries depending on the announced outcome, they can finally distill the Bell state $|\psi_1\rangle$. This shows that the Smolin state is entangled, and also bound entangled together with the property ii).

4.2.1 Quantum superactivation with finite copies

As said, one of the intriguing effects shown in entanglement theory is that of activation of bound entangled states. It is based on the fact that the combination of two (or more) bound entangled states, thus *per se* non-distillable, can be brought to a state which is indeed distillable. The Smolin state was in particular exploited to show a stronger version of such an effect. Termed superactivation, it refers to the superadditivity of the distillable entanglement: given two mixed states ρ_1, ρ_2, $E_D(\rho_1 \otimes \rho_2) > 0$ despite the fact that $E_D(\rho_1) = E_D(\rho_2) = 0$. This was shown in Ref. [SST03] without the restrictions of the earlier types of activation of bound entanglement [DC00]. The quantum activation protocol works as follows. Suppose that, now including a fifth party, Elena, two copies of the Smolin state are shared by the five parties in the following way,

$$\rho_{A_1C_1B_1D} \otimes \rho_{A_2B_2C_2E}, \tag{4.2}$$

where the first and the second copies are labeled. Then, David and Elena distill an ebit, applying the following protocol, see also Fig. 4.1. First, Alice teleports her qubit state of A_2 to Clare sacrificing the unknown Bell state shared between A_1 and C_1. Clare is then with two qubits $C_1^{'}$ and C_2 where $C_1^{'}$ is in the teleported state from A_2. Next, Bob teleports his qubit state of B_2 to D using the unknown Bell state shared between B_1 and D. Then, David is now with $D^{'}$ in the teleported state from B_2. Finally, due to the

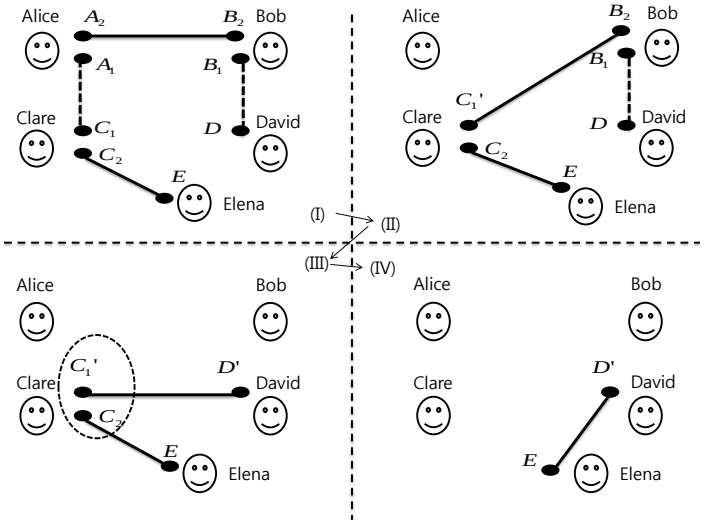

Figure 4.1: The activation protocol for both the quantum and classical scenarios is shown. For the quantum scenario, two Smolin states $\rho_{A_1C_1B_1D}$ and $\rho_{A_2B_2C_2E}$ are drawn with the dashed and solid lines, respectively. For the classical scenario, the Smolin states are simply replaced with the bound information in (4.5). In both cases, the first step in the protocol (shown in I→II) is that Alice teleports her state in the system A_2 to C_1 using the correlation between A_1C_1. In the second step (shown in II→III), Bob teleports the state of his system B_2 to D sacrificing the correlation existing in B_1D. Then, the resulting distribution over the remaining three parties, Clare holding two systems, David, and Elena is in fact the Smolin state if the scenario is with quantum systems, or the bound information in (4.5) if it is with classical systems. Finally (shown in III→IV), Clare measures her systems and announces the outcomes, so that David and Elena distill an ebit or an sbit.

structure of the Smolin state, the state $C_1^{'}C_2D^{'}E$ shared by Clare, David, and Elena results in the Smolin state. Since Clare holds two qubits $C_1^{'}$ and C_2, she can discriminate among Bell states and announces the result, by which David and Elena can distill an ebit.

A possible extension of the previous ideas is obtained by symmetrizing the state in Eq. (4.2) with more copies as follows,

$$\rho_{ABCD} \otimes \rho_{ABCE} \otimes \rho_{ABDE} \otimes \rho_{ACDE} \otimes \rho_{BCDE}. \tag{4.3}$$

Any two parties among the five can in this fashion distill ebits among each other. When ebits are shared by every two parties, it follows that multipartite pure entangled states can be distilled. This finally shows that multipartite bound entangled states can be superactivated. It is worth noting that in this activation scenario, the distillable entanglement defined in the asymptotic limit becomes immediately positive with a finite number of copies.

4.3 Bound information

Even though originally defined for the bipartite case, the concept of bound information can be unambiguously defined also for the multipartite case. Given a probability distribution $P(A, B, C, D, \mathcal{E})$, in which we have now included an eavesdropper which holds the random variable $\mathcal{E}$ (see chapter 2), $P(A, B, C, D, \mathcal{E})$ it is said to contain bound information if *i)* no pair of honest parties, even with the help of the other ones[1], can generate a secret key from any instances of $P(A, B, C, D, \mathcal{E})$[2] *ii)* $P(ABCD\mathcal{E})$ cannot be distributed by LOPC operations. More precisely, a large number of realizations of the random variable A, B, C and D distributed according to $P(A, B, C, D)$, the reduced probability distribution, cannot be distributed

[1]It is worth specifying, the meaning of this statement. The others parties can provide help to say pair A, B communicating publicly the outcome they obtained, etc... but it is important that this help is provided through the public channel.

[2]Note that when we refer to number of copies (or instances) of a given $P(A, B, ...)$ we mean the number of samples which are distributed according to $P(A, B, ...)$.

among the honest parties if the broadcasted messages can contain at most the information of the $\mathcal{E}$ variable.

As mentioned in chapter 2, a useful tool to show that the secret-key rate is zero (for example in the bipartition $AB : CD$), is given by the intrinsic information:

$$S(AB;CD\|\bar{\mathcal{E}}) \leq I(AB;CD \downarrow \bar{\mathcal{E}}) = 0 \tag{4.4}$$

In the following sections, using these arguments, we show that measurements on the Smolin states in the computational basis in fact give bound information. We then show that bound information can be superactivated in a finite-copy scenario, analogously to the quantum case.

4.3.1 Bound information and the unlockability

The existing link between entanglement and secret-key agreement scenario has been already discussed in section 2.3. Accordingly, the entanglement properties can be related to the cryptographic properties of the probability distributions that are obtained by measuring given quantum states. Without loss of generality, one assume that Eve has access to the rest of legitimate parties, and this is expressed by the fact that Eve holds the purification. When the Smolin state ρ_{ABCD} is shared, one can find a state $|\psi\rangle_{ABCD\mathcal{E}}$ such that $\rho_{ABCD} = \mathrm{tr}_{\mathcal{E}}|\psi\rangle\langle\psi|_{ABCD\mathcal{E}}$. In this way, Eve is naturally included and her correlations with the legitimate parties are readily shown. Denoted by positive operator M_α of party α, the probability distribution $P_{ABCD\mathcal{E}}$ of the five parties reads,

$$P(ABCD\mathcal{E}) = \mathrm{tr}[M_A \otimes M_B \otimes M_C \otimes M_D \otimes M_{\mathcal{E}}|\psi\rangle\langle\psi|_{ABCD\mathcal{E}}].$$

In the hypothesis in which the measurements applied by the honest parties are in the computational basis. The probability distribution is explicitly

given by,

A	C	B	D	$\mathcal{E}$	$P_{ACBD\mathcal{E}}$
0	0	0	0	ϵ_1	1/8
0	0	1	1	ϵ_2	1/8
1	1	0	0	ϵ_2	1/8
1	1	1	1	ϵ_1	1/8
0	1	0	1	ϵ_3	1/8
0	1	1	0	ϵ_4	1/8
1	0	0	1	ϵ_4	1/8
1	0	1	0	ϵ_3	1/8

. (4.5)

In what follows, we show that the distribution (4.5) contains bound information which is also unlockable. These features are thereby shown to be in a one-to-one correspondence with those shown by the quantum state 4.1.

i') *Invariance under permutations.* The distribution (4.5) is invariant under permutations of parties, i.e. $P_{ACBD\mathcal{E}} = P_{ABCD\mathcal{E}} = P_{ADBC\mathcal{E}}$.

ii') *Undistillability.* The distribution $P(A, C, B, D, \mathcal{E})$ is undistillable in every bipartition across two parties versus the others. That is, for instance in the bipartition between AC and BD, it holds that

$$I(AC : BD \downarrow \mathcal{E}) = 0, \tag{4.6}$$

where Eve's local mapping is given by, $\epsilon_2 \to \epsilon_1$ and $\epsilon_3 \to \epsilon_4$. From the relation in 4.4, it follows that $S(AC : BD\|\mathcal{E}) = 0$. Then, the permutational invariance in (i') implies $S(AB : CD\|\mathcal{E}) = S(AD : BC\|\mathcal{E}) = 0$, and therefore none of two parties can distill an sbit.

iii') *Unlockability.* The secret correlations existing in (4.5) are unlockable. Suppose two parties, for instance B and D, join together and post-select either case in which they got the same outcome or those in which they got the opposite one. Let us now restrict to the case that B and D accept when they share the same bit values. Then, the

distribution is given by

A	C	B	D	$\mathcal{E}$	$P_{ACBD\mathcal{E}}$
0	0	0	0	ϵ_1	1/4
0	0	1	1	ϵ_2	1/4
1	1	0	0	ϵ_2	1/4
1	1	1	1	ϵ_1	1/4

. (4.7)

This means that an sbit is distilled between A and C, since it is clear in the distribution (4.7) that i) $P_{AC}(0,0) = P_{AC}(1,1) = 1/2$ and ii) $P_{AC\mathcal{E}}(a,c,e) = P_{AC}(a,c)P_{\mathcal{E}}(e)$. For the other case that B and D accept whenever they share different bit values, applying the bit-flip operation either A and C, Alice and Clare can distill an sbit. From the symmetry property in (i'), it immediately follows that any two parties who join and collaborate to identify the shared state can allow the other two parties to distill an sbit. As an sbit is distilled, this also means that the probability distribution in (4.5) consists of secret correlations. Together with the undistillability in (ii'), it is shown that the distribution in (4.5) indeed contains bound information.

4.3.2 Classical superactivation with finite copies

In this subsection, we show that bound information can be superactivated in a finite-copy scenario. We first show that an sbit can be distilled by two parties when two instances of bound information (4.5) are shared between five parties as done in the quantum protocol.

Let us consider the following probability distribution:

$$P_{ABCDE} = P_{A_1C_1B_1D}\ P_{A_2B_2C_2E}, \tag{4.8}$$

where each four-partite distribution is shown in Eq. (4.5) and the first and the second copies are labeled. Note that the distribution in Eq. (4.8) can also be obtained by directly measuring the tensored state in (4.2) in the computational basis. Expressing Eq. (4.5) in the simpler form, shown in the appendix B.1, the distribution in Eq. (4.8) is reported in table 4.3.2.

The classical analogue of the quantum teleportation, which is to be used in our activation protocol, is the one-time pad. This procedure allows to transmit safely a classical bit on a public channel by means of an sbit. It works as follows. Assume that an sbit s, is shared by two honest parties. The sender encodes a message x and publicly announces the addition $(x+s)$, so that the receiver can decode the message by adding the shared sbit, $(x+s)+s$. Since the value of the sbit s is not known to anyone else, one can only guess a random bit from the public communication. For convenience in the sequel we refer to it as *teleportation* of classical bits.

A_1	A_2	B_1	B_2	C_1	C_2	D	E	$\mathcal{E}_1$	$\mathcal{E}_2$
i	j	i	j	i	j	i	j	ϵ_1	f_1
i	j	i	j	i	$j+1$	i	$j+1$	ϵ_1	f_2
i	j	i	$j+1$	i	j	i	$j+1$	ϵ_1	f_3
i	j	i	$j+1$	i	$j+1$	i	j	ϵ_1	f_4
i	j	$i+1$	j	i	j	$i+1$	j	ϵ_2	f_1
i	j	$i+1$	j	i	$j+1$	$i+1$	$j+1$	ϵ_2	f_2
i	j	$i+1$	$j+1$	i	j	$i+1$	$j+1$	ϵ_2	f_3
i	j	$i+1$	$j+1$	i	$j+1$	$i+1$	j	ϵ_2	f_4
i	j	i	j	$i+1$	j	$i+1$	j	ϵ_3	f_1
i	j	i	j	$i+1$	$j+1$	$i+1$	$j+1$	ϵ_3	f_2
i	j	i	$j+1$	$i+1$	j	$i+1$	$j+1$	ϵ_3	f_3
i	j	i	$j+1$	$i+1$	$j+1$	$i+1$	j	ϵ_3	f_4
i	j	$i+1$	j	$i+1$	j	i	j	ϵ_4	f_1
i	j	$i+1$	j	$i+1$	$j+1$	i	$j+1$	ϵ_4	f_2
i	j	$i+1$	$j+1$	$i+1$	j	i	$j+1$	ϵ_4	f_3
i	j	$i+1$	$j+1$	$i+1$	$j+1$	i	j	ϵ_4	f_4

Table 4.1: The probability distribution $P_{ABCDE\mathcal{E}}$ of five honest parties plus the eavesdropper is shown. Symbols i, j can take values $0, 1$ and represent the classical bits hold by the parties. Note moreover that the eavesdropper hold two symbols, one for each original probability distribution.

The activation protocol is obtained by translating the quantum one, and works as follows, see also Fig. 4.1. First, Alice teleports her bit in A_2 to Clare, using the sbit A_1C_1. The new value in the register of Clare is thus updated to $C_1^{'} = C_1 + A_1 + A_2$, and the probability distribution is mapped to:

B_1	B_2	$C_1^{'}$	C_2	D	E	$\mathcal{E}_1$	$\mathcal{E}_2$
i	j	j	j	i	j	ϵ_1	f_1
i	j	j	$j+1$	i	$j+1$	ϵ_1	f_2
i	$j+1$	j	j	i	$j+1$	ϵ_1	f_3
i	$j+1$	j	$j+1$	i	j	ϵ_1	f_4
$i+1$	j	j	j	$i+1$	j	ϵ_2	f_1
$i+1$	j	j	$j+1$	$i+1$	$j+1$	ϵ_2	f_2
$i+1$	$j+1$	j	j	$i+1$	$j+1$	ϵ_2	f_3
$i+1$	$j+1$	j	$j+1$	$i+1$	j	ϵ_2	f_4
i	j	$j+1$	j	$i+1$	j	ϵ_3	f_1
i	j	$j+1$	$j+1$	$i+1$	$j+1$	ϵ_3	f_2
i	$j+1$	$j+1$	j	$i+1$	$j+1$	ϵ_3	f_3
i	$j+1$	$j+1$	$j+1$	$i+1$	j	ϵ_3	f_4
$i+1$	j	$j+1$	j	i	j	ϵ_4	f_1
$i+1$	j	$j+1$	$j+1$	i	$j+1$	ϵ_4	f_2
$i+1$	$j+1$	$j+1$	j	i	$j+1$	ϵ_4	f_3
$i+1$	$j+1$	$j+1$	$j+1$	i	j	ϵ_4	f_4

. (4.9)

Next, Bob teleports his value in B_2 to David sacrificing the sbit B_1D. David holds a new value $D' = D + B_1 + B_2$, for which the probability distribution of the four parties is now given by

$C_1^{'}$	C_2	$D^{'}$	E	$\mathcal{E}_1$	$\mathcal{E}_2$
j	j	j	j	ϵ_m	f_1
j	$j+1$	j	$j+1$	ϵ_m	f_2
j	j	$j+1$	$j+1$	ϵ_m	f_3
j	$j+1$	$j+1$	j	ϵ_m	f_4

(4.10)

where $m = 1, 2, 3, 4$. The explicit form of the distribution of Eq. (4.10) is shown in the appendix B.2. Now, the distribution in Eq. (4.10) is identical

to the bound information in Eq. (4.5). Remind that the secret correlations in (4.5) are unlockable, as shown in section 4.3.1. The nice things now is that the bits $C_1^{'}$ and C_2 are known to the same party, Clare. She thus can announces if her two values are the same or not. Conditioned on that, by applying local operations David and Elena can share a secret bit. If it is announced that $C_1^{'}$ and C_2 are equal they have it already. In the case in which $C_1^{'} \neq C_2$, either David or Elena applies the bit-flip operation. This shows that an sbit can be distilled between D and E.

Analogously to what discussed for the quantum case, by symmetrizing the distribution in Eq. (4.8) as follows:

$$P_{ABCD\mathcal{E}_1} P_{ABCE\mathcal{E}_2} P_{ABDE\mathcal{E}_3} P_{ACDE\mathcal{E}_4} P_{BCDE\mathcal{E}_5}, \tag{4.11}$$

any two parties among the five can distill sbits against an eavesdropper who holds the five random variables $\mathcal{E}_1\mathcal{E}_2\mathcal{E}_3\mathcal{E}_4\mathcal{E}_5$. This fact is enough to allow them to share multipartite secrecy.

4.4 Distribution of entanglement and secrecy

In this section, we show a usefulness of undistillable correlations for distributing multipartite distillable correlations in the quantum and classical scenario,respectively. In the quantum scenario, we consider distribution of multi-partite GHZ state,

$$|\phi_N\rangle = (|0\rangle^{\otimes N} + |1\rangle^{\otimes N})/\sqrt{2}.$$

We show that tripartite GHZ state can be deterministically extended into four parties using LOCC when the Smolin state is shared by the four parties.

We also derive a classical analogue of the quantum state distribution. Multipartite sbits of N parties, say $A_1, \cdots, A_N$, is a classical analogue of the N-partite GHZ state, being defined as the following probability distribution

$$\begin{aligned} P_{A_1,\cdots,A_N}(a_1,\cdots,a_N) &= \delta_{a_1,a_2}\delta_{a_2,a_3}\cdots\delta_{a_{N-1},a_N}/2, \\ P_{A_1,\cdots,A_N,\mathcal{E}}(a_1,\cdots,e) &= P_{A_1,\cdots,A_N}(a_1,\cdots,a_N)P_{\mathcal{E}}(e). \end{aligned}$$

We then show that the tripartite sbit can be extended into four parties using LOPC when the bound information in Eq. (4.5) is shared by the four parties. Note that in both quantum and classical scenarios the distribution scheme works deterministically.

4.4.1 Quantum scenario

Suppose that Alice, Bob, Clare, and David share the Smolin state, and that only three of them, say Alice, Bob, and Clare, additionally share a tripartite GHZ state as follows

$$\mu_{ABCD} = |\eta\rangle\langle\eta|_{ABCD} \otimes \rho_{ABCD} \tag{4.12}$$

where $|\eta\rangle_{ABCD} = |\phi_3\rangle_{ABC} \otimes |+\rangle_D$ and $|+\rangle_D = (|0\rangle + |1\rangle)/\sqrt{2}$. Let Λ_α for $\alpha = A, B, C, D$ denote the local operation performed by the party α. The goal is now to show that the state μ_{ABCD} can be transformed to $|\phi_4\rangle$ using some local operations Λ_α. To this end, the local operation, $\Lambda_\alpha : \mathbb{C}^2 \otimes \mathbb{C}^2 \to \mathbb{C}^2$, mapping from two-qubit to a single qubit states, can be explicitly constructed in terms of the Kraus operators, $K_0^\alpha = |0\rangle\langle 00| + |1\rangle\langle 11|$ and $K_1^\alpha = |0\rangle\langle 01| + |1\rangle\langle 10|$ as follows

$$\Lambda_\alpha(\cdot) = \sum_{i=0,1} K_i^\alpha(\cdot)K_i^{\alpha\dagger}. \tag{4.13}$$

Now, if the four parties apply the local operation (4.13) to the state in (4.12) the probability of getting measurement outcomes (i_A, j_B, k_B, l_D) is given by:

$$\mathrm{tr}[\mu_{ABCD} K_{i_A}^{A\dagger} K_{i_A}^A \otimes K_{j_B}^{B\dagger} K_{j_B}^B \otimes K_{k_C}^{C\dagger} K_{k_C}^C \otimes K_{l_D}^{D\dagger} K_{l_D}^D],$$

In this case the state post-projection is

$$|\phi^v\rangle = \mathbb{1}_A \otimes \mathbb{1}_B \otimes \mathbb{1}_C \otimes (\sigma_D^x)^v |\phi_4\rangle, \tag{4.14}$$

where $v = i_A + j_B + k_B + l_D$ and σ_D^x denotes the Pauli matrix σ_x in the David's side. By means of classical communication the four parties can compute $v = i_A + j_B + k_C + l_D$. If v is an even number, this means that the four-partite GHZ state is already shared. Otherwise, David applies the σ_x operation to his qubit, and the four-partite GHZ state is obtained.

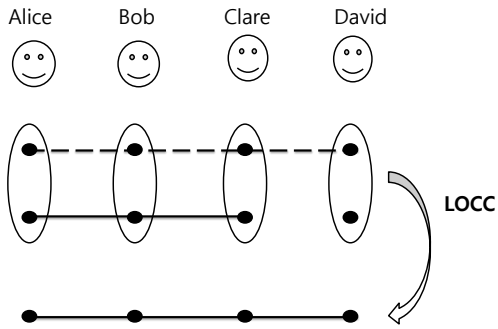

Figure 4.2: Distribution of multipartite pure entanglement and secret key: Four parties share the Smolin states (dashed line) and are allowed to apply LOCC. Then, the tripartite GHZ state (solid line) can be distributed over the four parties using LOCC. The classical analogue also follows: the tripartite sbit can be distributed over the four using LOPC when the four-partite bound information in Eq. (4.5) is shared.

4.4.2 Classical scenario

On the classical side, suppose now that the four parties share the bound information distributed according to (4.5) and that only three of them, say Alice, Bob, and Clare, share an sbit in the unknown value s, $s \in \{0,1\}$. Let i_k denote the bit value of the k-th party, $k = A, B, C, D$. The goal here is to extend the sbit from three to four parties by only using LOPC. As a result of that, David will be sharing a secret bit with the rest of the honest parties, A, B, C.

The distribution protocol works as follows, see also Fig. 4.2. Each of the three parties sharing the sbit s, individually and locally computes the parity of the two bits in their posses, the sbit s and the other from the bound information i_k for $k = A, B, C$. The distribution (4.5), written in the compact form (B.1), is hence modified as follows

A	C	B	D	$\mathcal{E}$	$P_{ABCD\mathcal{E}}$
$s+i$	$s+i$	$s+i$	i	ϵ_1	$1/8$
$s+i$	$s+i$	$s+i+1$	$i+1$	ϵ_2	$1/8$
$s+i$	$s+i+1$	$s+i$	$i+1$	ϵ_3	$1/8$
$s+i$	$s+i+1$	$s+i+1$	i	ϵ_4	$1/8$

. (4.15)

Afterwards, each of them publicly announces the parity bit $s + i_k$, so that David can compute the sum $v_D = \sum_{k=A,B,C}(s + i_k)$. He thus can add v_D to his bit i_D,

A	C	B	D	$\mathcal{E}$	$P_{ABCD\mathcal{E}}$
$s+i$	$s+i$	$s+i$	$i+v_D$	ϵ_1	$1/8$
$s+i$	$s+i$	$s+i+1$	$i+1+v_D$	ϵ_2	$1/8$
$s+i$	$s+i+1$	$s+i$	$i+1+v_D$	ϵ_3	$1/8$
$s+i$	$s+i+1$	$s+i+1$	$i+v_D$	ϵ_4	$1/8$

. (4.16)

From the relation holding for the distribution (4.5), $\sum_{k=A,B,C,D} i_k = 0$, it is immediate to check that

$$i_D + \sum_{k=A,B,C} s + i_k = s. \tag{4.17}$$

for each i_D. This shows that a multipartite sbit can be distributed securely via bound information together with LOPC.

4.5 Conclusions

We have shown a case of four-partite bound information and its properties, unlockability and superactivation. All these are obtained by deriving classical analogues of the Smolin state and its quantum effects, super-activation and unlockability in bound entangled states. It would be interesting to investigate which properties of quantum correlations can or cannot have their classical counterparts. For instance, existence of bipartite bound information remains open and is a challenging issue. Finally, we have shown a usefulness of undistillable correlations: bound entanglement and bound information can be used to distribute a multipartite GHZ state and multipartite sbits in quantum and classical scenarios, respectively.

Chapter 5

All private state are non-local

Private states are those quantum states from which a perfectly secure cryptographic key can be extracted. They represent the basic unit of quantum privacy. In this chapter we show that all states belonging to this class violate a Bell inequality. This result establishes a connection between perfect privacy and nonlocality in the quantum domain.

Introduction

A key step when comparing and quantifying resources consists of the identification of the basic unit for each of them. It is well established that a Bell state, that is, a two-qubit maximally entangled state, represents the basic unit of entanglement, known as *e*-bit (see section 2.2 [BBPS96]) . Moving to secret correlations, Horodecki *et al.* showed that private states are the basic unit of privacy in the quantum domain [HHHO05, HHHO09]. Clearly, all these states are entangled, as entanglement is a necessary condition for secure key distribution [CLL04, AG05]. However, a Bell state is just the simplest state belonging to the larger class of private states. This implies that the distillation of privacy from quantum states is not equivalent to

entanglement distillation, as it was commonly believed. Indeed, key (entanglement) distillation from a quantum state ρ can be understood as the process of extracting copies of private (Bell) states out of many copies of ρ. This nonequivalence is behind the existence of bound entangled states that, though not allowing for distillation of the Bell states [HHH98], are a resource for secure key distillation [HHHO05, HHHO09].

Beyond these results, however, the principles allowing for secure key distillation from quantum resources, a crucial question in QIT, are hardly understood. In order to achieve this, it is essential to identify the quantum properties common to all private states. It is well known that Bell states are nonlocal since they violate the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality [CHSH69]. Moved by this fact, one could ask whether all private states violate a Bell inequality. This is *a priori* unclear, as private states may exhibit radically different entanglement properties [HHHO09].

In this chapter we address the above question and show that all private states are indeed nonlocal. This result is general, as our proof works for any dimension and any number of parties. Private states, then, not only represent the unit of quantum privacy, but also allow two distant parties to establish a different quantum resource, namely, nonlocal correlations. These states contain the strongest form of entanglement as they can give rise to correlations with no classical analogue. More generally, our findings point out an intriguing connection between two of the most intrinsic quantum properties: privacy and nonlocality.

5.1 Private states

Before proceeding with the proof of our results, we recall in what follows the notions of private states [HHHO05, HHHO09, HA06, AH09a].

In general, these are N–partite states that can be written as

$$\Gamma^{(d)}_{\mathsf{AA'}} = \frac{1}{d} \sum_{i,j=0}^{d-1} (|i\rangle\langle j|)^{\otimes N}_{\mathsf{A}} \otimes U_i \rho_{\mathsf{A'}} U_j^{\dagger}, \tag{5.1}$$

where $\rho_{\mathsf{A'}}$ is some density matrix, $\{U_i\}$ a set of unitary operations, and $\mathsf{A} =$

$A_1 \dots A_N$ and $\mathsf{A}' = A'_1 \dots A'_N$ are multi–indices referring to subsystems. The subsystem marked with the subscript A consists of N qudits and is called the key part. The remaining subsystem is the shield part and is defined on some arbitrary finite-dimensional product Hilbert space $\mathcal{H}' = \mathcal{H}'_1 \otimes \dots \otimes \mathcal{H}'_N$. Party i holds one particle from the key part A_i and one from the shield part A'_i. The key point behind the private states is that $\log_2 d$ bits of perfectly secure bits of cryptographic key can be extracted from $\Gamma^{(d)}_{\mathsf{AA}'}$ [HHHO05, HPHH08].

5.1.1 Cryptographically secure states

In order to clarify the relevance which private states have in the cryptographic scenario it is worth recalling here some useful definitions.

Definition: A state $\rho_{ABA'B'}$ on a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'}$ is called *secure* with respect to a basis $\mathcal{B} = \{|e_i\rangle_A |f_j\rangle_B\}_{i,j=1}^d$ if the state obtained via measurement on AB subsystem of its purification in the $\mathcal{B}$ basis followed by tracing out $A'B'$ subsystem is product with Eve's subsystem:

$$\left(\sum_{i,j=0}^{d-1} p_{ij} |e_i f_j\rangle\langle e_i f_j|_{AB} \right) \otimes \rho_E \tag{5.2}$$

Moreover if the distribution is such that $p_{ij} = 1/d\ \delta_{ij}$ the state $\rho_{ABA'B'}$ is said to have a $\mathcal{B}$-key:

$$\left(\sum_{i=0}^{d-1} \frac{1}{d} |e_i f_i\rangle\langle e_i f_i|_{AB} \right) \otimes \rho_E \tag{5.3}$$

The states previously introduced are often referred as *ccq* state to indicate the fact that parties A and B did a measurement so obtaining a classical outcome while on the eavesdropper's side the state is still at a quantum level, namely no measurement has been still performed. Additionally, it is possible to express the state (5.1) in the easier form (where we consider just

two parties for sake of clarity):

$$\rho_{ABA'B'} = UP^{+}_{AB} \otimes \sigma_{A'B'}U^{\dagger} \tag{5.4}$$

where P^{+}_{AB} is the projector on a d-dimensional maximally entangled state, $\sum_i 1/\sqrt{d}|e_i f_i\rangle$ and U is the *twisting* unitary defined in [HHHO09]:

$$U = \sum_{k,l=0}^{d-1} |e_k f_l\rangle\langle e_k f_l|_{AB} \otimes U^{kl}_{A'B'} \tag{5.5}$$

Now, from Theorem 1 in [HHHO09] it is known that two states which are related by a twisting operation U, i.e. $\rho_{ABA'B'} = U\xi_{ABA'B'}U^{\dagger}$, have the same ccq state, namely $\tilde{\rho}_{ABE} = \tilde{\sigma}_{ABE}$. Thereby, taking $\xi_{ABA'B'} = P^{+}_{AB} \otimes \sigma_{A'B'}$ it is clear, that the obtained ccq state is a $\mathcal{B}$-key as shown in (5.3), so it is $\rho_{ABA'B'}$. From this, it directly follows that $\log_2 d$ bits of perfectly secure bits of cryptographic key can be extracted.

Regard the non-locality feature shown by some given correlations we remind to section 2.4 for a brief overview.

5.2 All private states are nonlocal

We are in position to prove our main result. We divide the proof into two parts. First, following the ideas of Ref. [HA06], we show that using local quantum operations (represented by appropriately chosen quantum channels) *without* any use of classical communication, the key part of any private state (subsystem A), can be brought to the form

$$\varrho^{(d)}_{N} = \sum_{k,l=0}^{d-1} \alpha_{kl}(|k\rangle\langle l|)^{\otimes N} \tag{5.6}$$

with $\alpha_{kk} = 1/d$ and at least one off-diagonal element nonzero; i.e., there exists a pair of indices $k < l$ such that $\alpha_{kl} \neq 0$. Note that the shield part is discarded during this process. Second, we show that any state of the

form (5.6) with $\alpha_{kl} \neq 0$ is nonlocal. Finally, the fact that local operations without classical communication cannot produce a nonlocal state from a local one implies that all private states are nonlocal.

Let us now proceed with the first part of the proof. For this aim we assume that the ith party performs, on its subsystems A_i and A'_i, the quantum operation represented by the following quantum channel

$$\Lambda^{(i)}(\cdot) = V^{(i)}(\cdot)V^{(i)\dagger} + W^{(i)}(\cdot)W^{(i)\dagger}, \tag{5.7}$$

where the Kraus operators $V^{(i)}$ and $W^{(i)}$ are given by

$$V^{(i)} = \sum_k |k\rangle\langle k|_{A_i} \otimes \widetilde{V}_k^{(i)}, \qquad W^{(i)} = \sum_k |k\rangle\langle k|_{A_i} \otimes \widetilde{W}_k^{(i)},$$

The operators $\widetilde{V}_k^{(i)}$ and $\widetilde{W}_k^{(i)}$ act on the shield part belonging to the ith party (the A'_i subsystem) and are chosen so that they define a proper quantum measurement. Precisely, given $\widetilde{V}_k^{(i)}$ we define the second Kraus operator to be $\widetilde{W}_k^{(i)} = (\mathbb{I} - \widetilde{V}_k^{(i)\dagger}\widetilde{V}_k^{(i)})^{1/2}$, with $\mathbb{I}$ being the identity matrix acting on the A'_i subsystem. Application of all the channels $\Lambda^{(i)}$ to $\Gamma^{(d)}_{\mathsf{AA'}}$ results in the following state

$$\bigotimes_{i=1}^{N} \Lambda^{(i)}(\Gamma^{(d)}_{\mathsf{AA'}}) = \frac{1}{d}\sum_{k,l=0}^{d-1} |k\rangle\langle l|^{\otimes N} \otimes \sum_{n=1}^{2^N} X_k^{(n)} U_k \varrho_{\mathsf{A'}} U_l^\dagger X_l^{(n)\dagger},$$

where matrices $X_k^{(n)}$ are defined as members of the 2^N–element set $\{\widetilde{V}_k^{(i)}, \widetilde{W}_k^{(i)}\}^{\otimes N}$. Explicitly, one has $X_k^{(1)} = \widetilde{V}_k^{(1)} \otimes \ldots \otimes \widetilde{V}_k^{(N)}, X_k^{(2)} = \widetilde{V}_k^{(1)} \otimes \ldots \otimes \widetilde{V}_k^{(N-1)} \otimes \widetilde{W}_k^{(N)}$, and so on. Tracing now the shield part we get the promised state (5.6) with α_{kl} given by

$$\alpha_{kl} = \mathrm{tr}\left[\bigotimes_{i=1}^{N} \left(\widetilde{V}_l^{(i)\dagger}\widetilde{V}_k^{(i)} + \widetilde{W}_l^{(i)\dagger}\widetilde{W}_k^{(i)}\right) U_k \varrho U_l^\dagger\right]. \tag{5.8}$$

One also finds that, since by construction $\widetilde{V}_k^{(i)\dagger}\widetilde{V}_k^{(i)} + \widetilde{W}_k^{(i)\dagger}\widetilde{W}_k^{(i)} = \mathbb{I}$ for any i, the diagonal elements α_{kk} of this state are equal to $1/d$.

Now we need to show that at least one of the above coefficients is nonzero. In other words, for some fixed pair of k and l ($k < l$) we need to choose the operators $\widetilde{V}_k^{(i)}$ and $\widetilde{V}_l^{(i)}$ in such a way that α_{kl} is nonzero. To this aim we simplify a little our considerations by assuming that the operators $\widetilde{V}_k^{(i)}$ and $\widetilde{V}_l^{(i)}$ corresponding to ith party are positive and diagonal in the same basis. Thus, we can write these particular operators in the form

$$\widetilde{V}_k^{(i)} = \sum_m v_m^{(i)} |e_m^{(i)}\rangle\langle e_m^{(i)}|, \qquad \widetilde{V}_l^{(i)} = \sum_m \overline{v}_m^{(i)} |e_m^{(i)}\rangle\langle e_m^{(i)}|,$$

where we assume that the eigenvalues satisfy $v_m^{(i)}, \overline{v}_m^{(i)} \in [0,1]$ and the eigenvectors $|e_m^{(i)}\rangle$ are orthonormal, i.e., $\langle e_m^{(i)}|e_n^{(i)}\rangle = \delta_{mn}$ (note that the fixed indices k, l we are interested in are omitted in the right–hand side of the previous expression). This, in turn means that the operators $\widetilde{W}_k^{(i)}$ and $\widetilde{W}_l^{(i)}$ are also diagonal in the basis $\{|e_m^{(i)}\rangle\}$, and have eigenvalues $(1 - v_m^{(i)2})^{1/2}$ and $(1 - \overline{v}_m^{(i)2})^{1/2}$, respectively. As a consequence the operator appearing in parenthesis in Eq. (5.8) simplifies to

$$\widetilde{V}_l^{(i)\dagger}\widetilde{V}_k^{(i)} + \widetilde{W}_l^{(i)\dagger}\widetilde{W}_k^{(i)} = \sum_m \beta_m^{(i)} |e_m^{(i)}\rangle\langle e_m^{(i)}|, \tag{5.9}$$

where its eigenvalues are given by $\beta_m^{(i)} = v_m^{(i)}\overline{v}_m^{(i)} + (1 - v_m^{(i)2})^{1/2}(1 - \overline{v}_m^{(i)2})^{1/2}$ and obviously satisfy $0 \leq \beta_m^{(i)} \leq 1$. Now, putting Eq. (5.9) to Eq. (5.8), we get

$$\begin{aligned} \alpha_{kl} \;=\; & \sum_{m_1,\ldots,m_N} \beta_{m_1}^{(1)} \ldots \beta_{m_N}^{(N)} \\ & \times \langle e_{m_1}^{(1)}| \ldots \langle e_{m_N}^{(N)}| U_k \rho U_l^\dagger |e_{m_1}^{(1)}\rangle \ldots |e_{m_N}^{(N)}\rangle. \end{aligned} \tag{5.10}$$

Finally, to prove that $\alpha_{kl} \neq 0$ it suffices to notice that for any nonzero matrix X (and in particular $U_k \rho U_l^\dagger$) there always exists at least one N partite product vector $|\psi\rangle = |\psi_1\rangle \ldots |\psi_N\rangle$ such that $\langle\psi|X|\psi\rangle$ is nonzero. Otherwise, if for all such vectors $\langle\psi|X|\psi\rangle = 0$, the matrix X has to be the zero matrix (see Lemma 2 of Ref. [idZHSL98]).

As just discussed, there exists a product vector $|\psi\rangle$ such that $\langle\psi|U_k\rho U_l^\dagger|\psi\rangle \neq 0$ for a pair of indices $k < l$. Therefore we can always chose $\widetilde{V}_k^{(i)}$ and $\widetilde{V}_l^{(i)}$ for each party in such way that $|\psi\rangle$ is one of the product vectors appearing in Eq. (5.10) (more precisely, $|\psi_i\rangle$ can be set as one of eigenvectors of $\widetilde{V}_k^{(i)}$ and $\widetilde{V}_l^{(i)}$). Now, we can use the freedom in the numbers $\beta_m^{(i)}$ in such a way that $\alpha_{kl} \neq 0$, which is exactly what we wanted to prove. Actually, we can always choose $\widetilde{V}_{k(l)}^{(i)}$ so that at least one of the coefficients α's in each row and column of $\varrho_N^{(d)}$ is nonzero.

Let us move to the second part of the proof. In what follows we show that any state of the form (5.6) is nonlocal. First we will consider the bipartite case and then we will move to the multipartite scenario.

5.2.1 Bipartite case ($d = 2$)

A generic form of the simplest example of bipartite private states (two–qubit key part) reads (zeros denote null matrices of adequate dimension)

$$\Gamma_{\mathsf{AA}'}^{(2)} = \frac{1}{2}\begin{pmatrix} U_0\rho_{\mathsf{A}'}U_0^\dagger & 0 & 0 & U_0\rho_{\mathsf{A}'}U_1^\dagger \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ U_1\rho_{\mathsf{A}'}U_0^\dagger & 0 & 0 & U_1\rho_{\mathsf{A}'}U_1^\dagger \end{pmatrix}. \tag{5.11}$$

After applying the previous local quantum operations to this state the parties are left with a two-qubit state:

$$\varrho_2^{(2)} = \begin{pmatrix} 1/2 & 0 & 0 & \alpha_{01} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \alpha_{01}^* & 0 & 0 & 1/2 \end{pmatrix}. \tag{5.12}$$

Since we already know that $\alpha_{01} \neq 0$, it follows from the criterion proposed in Ref. [HHH95] that the above state violates the CHSH-Bell inequality [CHSH69] (here written in the equivalent Clauser-Horne form [CH74])

$$\begin{aligned} P(A_1B_1) + P(A_2B_1) \quad &+ \quad P(A_1B_2) - P(A_2B_2) \\ &- \quad P(A_1) - P(B_1) \leq 0. \end{aligned} \tag{5.13}$$

Here $P(A_iB_j)$ denotes the probability that Alice and Bob obtain the first result upon the measurement of observables A_i and B_j $(i,j=1,2)$. Recall that the CHSH test involves the measurement of two dichotomic observables per site.

5.2.2 Bipartite case ($d>2$)

For higher dimensional bipartite private states we use the fact that the inequality (5.13) only involves one measurement outcome for each of the observables. For this purpose, let us first assume that some α_{kl} is nonzero and rewrite $\varrho_2^{(d)}$ (cf. Eq. (5.6)) as

$$\varrho_2^{(d)} = \begin{pmatrix} \ddots & \vdots & & \vdots & \\ \cdots & 1/d & \cdots & \alpha_{kl} & \cdots \\ & \vdots & \ddots & \vdots & \\ \cdots & \alpha_{kl}^* & \cdots & 1/d & \cdots \\ & \vdots & & \vdots & \ddots \end{pmatrix}. \tag{5.14}$$

The marked 2×2 submatrix can be seen, up to a normalization factor $2/d$, as a two-qubit state like the one given in Eq. (5.12). As we have just shown, any such two-qubit state with nonzero off-diagonal element is nonlocal. Therefore, to prove nonlocality of $\varrho_2^{(d)}$ we can design the observables A_i and B_i $(i=1,2)$ so that their first outcomes correspond to one-qubit projectors (embedded in $\mathbb{C}^d$) leading to the violation of (5.13) by the corresponding two-qubit state. Precisely, we take the projectors $\mathcal{P}_A^{(i)} = |\psi_i\rangle\langle\psi_i|$ and $\mathcal{P}_B^{(i)} = |\widetilde{\psi}_i\rangle\langle\widetilde{\psi}_i|$ $(i=1,2)$, where the pure states $|\psi_i\rangle$ and $|\widetilde{\psi}_i\rangle$ are of the general one-qubit form $a|k\rangle + b|l\rangle$. The remaining outcomes (which are irrelevant from the point of view of the inequality (5.13)) of the involved observables $A_i(B_i)$ can just correspond to projectors $\mathbb{I} - \mathcal{P}_{A(B)}^{(i)}$ $(i=1,2)$.

Now, by using these settings in the CHSH test (5.13), one sees that the state (5.14) leads to almost the same violation as for the two-qubit state in Eq. (5.12) with the only difference being the normalization factor $2/d$. Clearly, this does not cause any problem since the same factor appears in

all the terms of the inequality. Therefore it *does not* change the sign of the CHSH parameter (5.13). As a conclusion the CHSH-Bell inequality for any bipartite state $\varrho_2^{(d)}$ is also violated.

5.2.3 Multipartite case

We now move to the multipartite case. In order to prove the nonlocality of the states (5.6) for an arbitrary number of parties we exploit the fact that, given a generic N-partite state, ρ_N, if local projections of $N-m$ particles onto a product state leave the remaining m particles in a nonlocal state, ρ_m, necessarily the initial state ρ_N has to be nonlocal. This follows from the fact that one cannot produce a nonlocal state from a local one in this way. This reasoning was firstly used in Ref. [PR92] in the context of proving the nonlocality of general multipartite pure entangled states (in the appendix C we give a simple argument that allows to prove the non locality of a multipartite state).

Indeed, denote by A_i $(i = m+1, \ldots, N)$ the local measurements (with outcomes a_i) by the previous $N-m$ parties such that for one of the outcomes, say 0, the state ρ_m shared by the remaining m parties is nonlocal. For the sake of simplicity we assume that the nonlocality of this m-partite state can be proven with only two measurements per site, A_i and A_i' with outcomes a_i and a_i' $(i = 1, \ldots, m)$ (our reasoning can be trivially adapted to Bell tests involving more measurements). According to Fine's result (see section 2.4), there cannot exist a joint probability distribution $P(a_1, a_1', \ldots, a_m, a_m' | a_{m+1} = 0, \ldots, a_N = 0)$ reproducing the observed outcomes for the m parties conditioned on the fact that the measurement result for the remaining $N-m$ parties was equal to 0. Now, consider a Bell test for the initial N-partite state ρ_N where the parties apply all the previously introduced measurements. Assume that the obtained statistics can be described by a local model. Then, there exists a joint probability distribution $P(a_1, a_1', \ldots, a_m, a_m', a_{m+1}, \ldots, a_N')$. But this would immediately imply the existence of the joint probability distribution $P(a_1, a_1', \ldots, a_m, a_m' | a_{m+1} = 0, \ldots, a_N = 0)$, which is in contradiction with the fact that ϱ_m is nonlocal. Thus, the initial state ρ_N has to be nonlocal.

Using this argument, in order to prove the nonlocality of multipartite states $\varrho_N^{(d)}$ it is enough to build local projections mapping these states into a nonlocal state of a fewer number of particles. Consider the local projections P_ϕ onto $|\phi\rangle = (1/\sqrt{d})(|0\rangle + \ldots + |d-1\rangle)$. Projecting an arbitrary subset of $N-m$ particles of $\varrho_N^{(d)}$ onto P_ϕ the remaining m parties are left with following m–partite state

$$\varrho_m^{(d)} = \sum_{k,l=0}^{d-1} \alpha_{kl} (|k\rangle\langle l|)^{\otimes m}. \tag{5.15}$$

Thus, if $N-2$ parties apply the projector P_ϕ to the state (5.6), the remaining two parties are left with a bipartite private state $\varrho_2^{(d)}$. However, we have just shown that this state is nonlocal. Thus, $\varrho_N^{(d)}$ must also be nonlocal.

5.3 Conclusion

Private states play a relevant role in QIT because they represent perfectly secure bits of cryptographic key [HHHO05, HHHO09, AH09a]. Knowing their entanglement properties is crucial to understand the mechanism allowing for secure key distribution from quantum states. In general, private states are thought to have a weaker form of entanglement than Bell states. However, we have shown here that all private states are nonlocal. They have, then, the strongest form of quantum correlations, since the results of local measurements on these states cannot be reproduced by classical means.

Finally, it would be interesting to study how our findings can be related to the Peres conjecture [Per99], a long-standing open question in quantum information theory. This conjecture states that bound entangled states do not violate any Bell inequality. The intuition is that these states have a very weak form of quantum correlations. Then, all the correlations obtained from these states should have a classical description. Note, however, that there exist bound entangled states with positive partial transposition which are arbitrarily close (in the trace norm) to private

states [HHHO05, HHHO09, HPHH08, AH09a, AH09b]. This is indeed the reason why these examples of bound entangled states have nonzero distillable cryptographic key. But, as shown here, all private states are nonlocal. One would then be tempted to conclude that these bound entangled states are also nonlocal. Interestingly, the situation is subtler than initially thought. In fact, recall that the nonlocality of private states has been proven here by showing the violation of the CHSH-Bell inequality. Unfortunately, this inequality cannot be violated by bound entangled states with positive partial transposition [WW00]. This implies that the violation of this inequality by private states arbitrarily close to bound entangled states has to be very small. In view of all these findings it appears interesting to analyze the nonlocal properties of bound entangled states with positive distillable secret key.

Chapter 6

Maximal randomness from Bell tests

Among the remarkable features of quantum mechanics, its non-local character and its intrinsic randomness play a crucial role. The non-local correlations exhibited when measuring entangled particles can be used to certify the presence of genuine randomness in Bell's test experiments. However, it has recently been shown that, while non-locality is necessary for randomness certification, it is unclear when and why non-locality certifies maximal randomness. We provide here a simple argument to certify the presence of maximal genuine randomness based on symmetries of a Bell's inequality and the existence of a unique quantum probability distribution that maximally violates it. Using our findings, we show that maximal randomness can be certified through Mermin type inequalities and from certain bipartite Bell tests.

6.1 Introduction

Non-locality and intrinsic randomness inherent in quantum correlations go to the very heart of quantum weirdness. They have been the subject of keen interest since the early days of quantum physics. This interest, which

was initially derived from its foundational implications has recently also acquired a practical aspect due to the rapid developments of the device independent paradigm. In the past few years, developments in device independent quantum key distribution and randomness generation have heightened the need to quantify both non-locality and randomness inherent in quantum systems.

The existence of genuine randomness is intimately related to the notion of non-locality, the exact relationship between the two quantities has not yet been characterized. Recently, it was shown how the CHSH inequality could be used to bound the randomness shown by probability distributions arising from measurements on quantum entangled states [PAM$^+$10].

These results were moreover extended to non-tight Bell inequalities in [AMP12]. There, the authors proved that the probability distribution maximally violating the CHSH inequality (see section 2.4) contains locally the maximum possible one bit of randomness irrespective for every party and every measurement setting. However, there is strictly less than 2 random bits globally ($1,23$ bits). Furthermore, they proved that the quantum distribution saturating the non-tight inequality $I_\alpha = \alpha\langle A_1B_1\rangle + \alpha\langle A_1B_2\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle$ also contain a maximum local randomness of 1 bit for party A, but remarkably, it is possible to obtain asymptotically close to 2 random bits, by measuring state arbitrarily close to product states. This is reminiscent of the behaviour of other quantities of interest such as the detection efficiency [Ebe93]. Still, it is difficult to develop an intuitive grasp of the probability distributions from which one may expect the highest randomness. A priori it is thus unclear when and why maximal randomness is certified by a given Bell inequality. Our present work is an attempt to further understanding this subtle relation.

We approach this question from an operational point of view so our results can be relevant under a cryptographic perspective. As such, not only is quantification important, but also the certification. We require that the randomness is guaranteed not to originate from a mere lack of knowledge about the system. We make this more concrete with the observation that, strictly speaking, classical systems can exhibit at most pseudo randomness since they can always, in principle, be simulated by a mixture of determin-

istic systems. Those systems whose correlations cannot be so simulated, do violate a Bell inequality [Bel64] hence are guaranteed to contain genuine intrinsic randomness. As well known, the correlations shown by certain measurements on entangled quantum states violate a Bell inequality, hence ensuring the randomness of the produced outcomes.

Despite some works [PAM+10, Col09, AMP12] investigated the existing relation between non-locality and randomness, it is still unclear when non-locality certifies *maximal* randomness. In this chapter we demonstrate that in several important cases, simple arguments combining the symmetry of a Bell inequality and the uniqueness of the quantum probability distribution that *maximally* violates it can give interesting insights in that direction.

These arguments are extremely useful to intuit the intrinsic randomness that can be obtained in a given scenario. Once the probability distribution is known, no numerical calculations are generally required. This makes them powerful tools to study randomness, always under the assumption of uniqueness mentioned above.

After presenting the basic background and a simple explanation of our method for the CHSH case, we tackle more complex scenarios, showing the validity of our approach. In the last section we discuss the assumption of uniqueness and the possible limitations for no-signalling post-quantum theories.

6.2 Preliminaries

This section briefly introduces the main definitions and techniques used in the rest of the chapter. For a more exhaustive explanation see section 2.5.

6.2.1 Bell tests and quantum distributions

A general Bell test (N, M, d) consists of N separated parties owing part of a system on which they can freely make one of M possible measurements. Each measurement has d possible outcomes. Along this *device independent approach*, the relevant quantities are thus the conditional probabilities of

outcomes given a chosen measurement string (without reference to the underlying states and dimension): $P(a_1, \ldots, a_N|x_1, \ldots, x_N)$ where a_i is the outcome of a measurement x_i by party $1 \leq i \leq N$. We consider only quantum distributions unless specified otherwise. In other words, P has at least one quantum representation comprising a quantum state ρ in an arbitrary dimensional Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_N$ and a set of measurement operators $M(a_i|x_i)$ summing to unity on $\mathcal{H}_i$ for $i \in \{1, N\}$ such that,

$$P(a_1, \ldots, a_N|x_1, \ldots, x_N) = tr[\rho M_{a_1|x_1} \ldots M_{a_N|x_N}] \tag{6.1}$$

6.2.2 Randomness

We aim at certifying randomness in a joint probability distribution independent of its quantum realization (see Sec. 2.5 for more details). To this end, we adopt an operational approach where randomness is related to guessing correctly the outcome of some joint measurement, $\vec{x} = (x_1, x_2, \ldots, x_N)$. Since the best one can do is to simply output the most probable outcome string, we quantify randomness with the *guessing probability*,

$$G(P; \vec{x}) = \max_{\vec{a}} P(\vec{a}|\vec{x}) \tag{6.2}$$

where $\vec{a} = (a_1, a_2, \ldots, a_N)$. The guessing probability can be expressed in bits with the *min-entropy* defined as

$$H_\infty(P; \vec{x}) = -\log_2 G(P; \vec{x}) \tag{6.3}$$

The min-entropy can be analogously defined for any subset of parties.

If $d = 2$, i.e. dichotomic measurements, then each party locally can have at most 1 bit of randomness and globally there can be at most N bits of randomness. The larger the value $G(P; \vec{x})$, the lower the randomness since a higher probability of guessing the outcomes intuitively corresponds to lower randomness. In Ref. [AMP12] it was made clear that randomness and non-locality are intimately related although inequivalent physical quantities. As pointed out in the same reference, the violation of *some* Bell inequality is a necessary and sufficient condition for $G(P, \vec{x}) < 1$ or equivalently $H_\infty(P, \vec{x}) > 0$ (see Sec. 2.5).

For $(N, M, d) = (2, 2, 2)$, the largest possible amount of randomness corresponds to 2 bits, which is obtained when $G(P; x_0, y_0) = 1/4$ for an input pair (x_0, y_0). From the existing relation:

$$P(a, b|x, y) = \frac{1}{4}(1 + a\langle A_x\rangle + b\langle B_y\rangle + ab\langle A_x B_y\rangle)$$

this implies that for the input pair (x_0, y_0), $\langle A_{x_0}\rangle = \langle B_{y_0}\rangle = \langle A_{x_0} B_{y_0}\rangle = 0$.

6.3 Symmetries, uniqueness and randomness

In this section we demonstrate explicitly that, for $(2, 2, 2)$ the symmetry of the CHSH inequality:

$$I \equiv \langle A_1 B_1\rangle + \langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle \leq 2$$

and the uniqueness of the quantum distribution maximally violating it, certify genuine randomness. We achieve this in two steps.

First, let $\mathcal{P}^*$ be a distribution that saturates the maximum quantum violation of the CHSH, $I(\mathcal{P}^*) = 2\sqrt{2}$. Applying the symmetry transformation $\mathcal{T}_s$, $a_{1,2} \mapsto -a_{1,2}$ and $b_{1,2} \mapsto -b_{1,2}$ (where $a_i, b_j \in [-1, 1]$), a new distribution $\mathcal{P}^{**} = \mathcal{T}_s(\mathcal{P}^*)$ is obtained which also maximally violates the *same* CHSH and differs from $\mathcal{P}^*$ only in the marginals, namely $\langle A_i\rangle^{**} = -\langle A_i\rangle^*$, $\langle B_j\rangle^{**} = -\langle B_j\rangle^*$. Note that under the transformation $\mathcal{T}_s$ the coefficients appearing in the CHSH inequality are left unchanged.

Second, we invoke the uniqueness of the distribution saturating CHSH [AMP12], implying that $\mathcal{P}^* = \mathcal{P}^{**}$. Consequently all marginals are zero implying $G(P; x) = G(P; y) = 1/2$ which, from (6.3), certifies that every party obtains *1 bit of local randomness.*

In what follows, we systematically apply this procedure. Firstly, we look for transformations that do not change the given Bell's inequality. Later, we apply this transformations to the distribution that maximally violates the inequality. By imposing the uniqueness of this distribution, we infer the existence of maximal randomness.

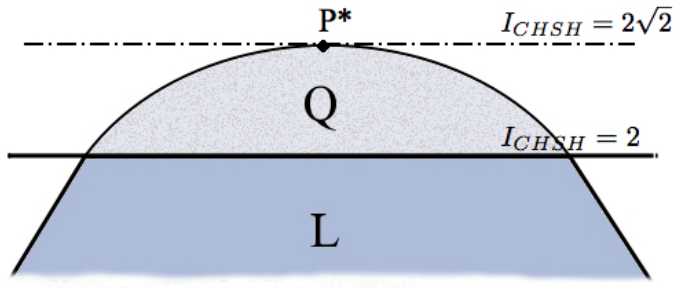

Figure 6.1: A slice of the local and quantum set, L and Q, are shown for the (2,2,2) Bell scenario. The point P^* represents the maximal quantum violation of the CHSH inequality, known as the Tsirelson bound. There is a unique quantum realization for these correlations (see Sec. 2.4 and the Appendix D for more details.)

6.3.1 Chained inequalities

In the following, we demonstrate that this simple idea can be extended to more complex scenarios. The chained Bell inequalities, which is an extension of the CHSH inequality to more settings per party [BC56], can be compactly represented as:

$$C_d^M = \sum_{i=1}^{M} \langle [A_i - B_i]_d \rangle + \langle [B_i - A_{i+1}]_d \rangle \geqslant d - 1 \tag{6.4}$$

where A_i and B_i are measurement choices for Alice and Bob and by definition $A_{M+1} = A_1 + 1$. The square brakets denote sum modulo d. Next, we show that all measurement outcomes are maximally random at the point of maximal quantum violation.

As first step, we consider the transformation: $a_i \mapsto a_i + 1$ and $b_i \mapsto b_i + 1$ for every i.

Second, for a distribution P maximally violating C_d^M, such a transformation will map say $P(0|A) \to P(1|A)$,$P(1|A) \to P(2|A) \ldots$ $P(d-1|A) \to P(0|A)$ and the same on Bob's side.

Third, assuming that the two distributions must coincide since P is unique, lead to $P(0|A) = P(1|A) = \cdots = P(d-1|A) = 1/d$. In other words, Alice and Bob locally have a uniform outcome distribution corresponding to the 1-*dit of local randomness*.

6.3.2 Two bits of randomness for $(2, M, 2)$ for odd M

From now on, even though we are going to consider more complex scenarios, the number of outcomes for each setting will be restricted to $d = 2$. As already anticipated, in this case the probability distributions can be fully parametrized in terms of correlators:

$$P(\vec{a}|\vec{x}) = \frac{1}{2^N}(1 + \sum_{i=1}^{N} a_i\langle A_i\rangle + \sum_{i<j} a_i a_j\langle A_i A_j\rangle + \sum_{i<j<k} a_i a_j a_k\langle A_i A_j A_k\rangle + \\ + \cdots + a_1 a_2 \ldots a_N\langle A_1 A_2 \ldots A_N\rangle) \quad (6.5)$$

where all the correlators have values in the interval $[-1, 1]$.

In order to certify maximal randomness for a given input $\vec{x} = \vec{x_0}$, one needs to show that the distribution $P(\vec{a}|\vec{x_0})$ is uniform. It is straightforward to see that this condition is satisfied when all the correlators in (6.5) are identically equal to zero. Using that, we will show that for certain input pairs (specified below), the maximum of 2 bits can be certified by the maximal violation of the chained inequality. Expression (6.4), for M dichotomic measurements (with $a_i, b_j \in [-1, 1]$) can be rewritten as follows:

$$C_2^M = \left| \sum_{i=1}^{M} \langle A_i B_i\rangle + \sum_{i=1}^{M-1} \langle A_{i+1} B_i\rangle - \langle A_1 B_M\rangle \right| \quad (6.6)$$

Our arguments apply to the case of odd number of measurements M ($M = 2k + 1$ with $k \in \mathbb{N}$). In this case, symmetry arguments and the assumption of a unique distribution maximizing (6.6) lead to 2 bits of certified randomness.

Consider the distribution P that maximally violates (6.6). Once again, we would like to identify a transformation that leaves the coefficients of C_2^M invariant and such that allows us to put at least one full correlator say $\langle A_k B_l \rangle$ equal to zero (together with $\langle A_k \rangle$, $\langle B_l \rangle$). Here, we give the proof for $\langle A_1 B_\eta \rangle$ with $\eta = k + 1$. Generally, for a odd number M of measurements, this can be shown for all the correlators of the form $\langle A_i B_{i+k} \rangle$ for all i, $i < M$.

The following transformation satisfy the conditions specified above:

1. $a_1 \mapsto -a_1$ and no change in b_η.
2. $B_1 \leftrightarrow B_M$
3. $A_M \leftrightarrow A_2$
4. $B_2 \leftrightarrow B_{M-1}$

and so on up to $A_{k+1} \leftrightarrow A_{k+2}$. Here the symbol $\leftrightarrow$ is used to indicate a change of labelling for the input of the new distribution. The assumption that the distribution that maximally violates (6.6) is unique leads to $\langle A_1 B_\eta \rangle = -\langle A_1 B_\eta \rangle$, ergo $\langle A_1 B_\eta \rangle = 0$. This, combined with the results obtained in the previous section, $\langle A_1 \rangle = 0 = \langle B_\eta \rangle$, implies that, $P(a, b|x = 1, y = \eta) = \frac{1}{4}(1 + a\langle A_1 \rangle + b\langle B_\eta \rangle + ab\langle A_a B_\eta \rangle) = 1/4$ and from (6.3), $H_\infty(P(a, b|x = 1, y = \eta)) = 2$. So that 2 bits of randomness are certified.

6.3.3 Mermin inequalities

Mermin inequalities [Mer90] of N parties are defined recursively as,

$$M_N = \frac{1}{2} M_{N-1}(A_N + A'_N) + \frac{1}{2} M'_{N-1}(A_N - A'_N) \tag{6.7}$$

where M_2 is the CHSH inequality and M'_{N-1} is obtained from M_{N-1} by exchanging all A_j and A'_j. These inequalities have been studied extensively and are very relevant candidate inequalities to study certified randomness.

We are able to show up to the maximum possible randomness of N bits for these inequalities. However, before providing the general proof it will be useful to restrict it to the tripartite case. Expression (6.7) in this case reads:

$$M_3 = \langle A_1' A_2 A_3 \rangle + \langle A_1 A_2' A_3 \rangle + \langle A_1 A_2 A_3' \rangle - \langle A_1' A_2' A_3' \rangle \leqslant 2 \tag{6.8}$$

Analoguous to the chained inequalities, one can show full global randomness for those measurement combinations not appearing in M_3. For instance, let us consider $\langle A_1 A_2 A_3 \rangle$ (as well as all marginals) in the probability distribution $\mathbb{P}$ that maximally violates M_3. Under the transformation: $a_1 \mapsto -a_1$, $a_2' \mapsto -a_2'$, $a_3' \mapsto -a_3'$, M_3 remains unchanged while $\langle A_1 \rangle_{\mathbb{P}} \mapsto -\langle A_1 \rangle_{\mathbb{P}}$, $\langle A_1 A_2 \rangle_{\mathbb{P}} \mapsto -\langle A_1 A_2 \rangle_{\mathbb{P}}$, $\langle A_1 A_3 \rangle_{\mathbb{P}} \mapsto -\langle A_1 A_3 \rangle_{\mathbb{P}}$ and $\langle A_1 A_2 A_3 \rangle_{\mathbb{P}} \mapsto -\langle A_1 A_2 A_3 \rangle_{\mathbb{P}}$. Hence, the existence of uniqueness implies all these correlators in $\mathbb{P}$ to be equal to zero. A similar reasoning ($a_2 \mapsto -a_2$, $a_1' \mapsto -a_1'$ and $a_3' \mapsto -a_3'$ and then $a_3 \mapsto -a_3$, $a_1' \mapsto -a_1'$ and $a_2' \mapsto -a_2'$) can be used to show that $\langle A_2 \rangle_{\mathbb{P}} = \langle A_3 \rangle_{\mathbb{P}} = \langle A_2 A_3 \rangle_{\mathbb{P}} = 0$ as required for $G(\mathbb{P}; A_1, A_2, A_3) = 1/8$ or $H_\infty = 3$. This shows that violating maximally the Mermin inequality M_3, 3 bits of full global randomness can be certified. In the following we generalize this proof to the case of arbitrary odd N.

6.3.4 Full randomness of N-bits from Mermin inequalities of odd N

Let M_N denote a Mermin inequality of $N = 2J + 1$ sites. There is a choice between two dichotomic measurements A_i and A_i' at site i. We fix the convention that A_i corresponds to the setting of even parity and A_i' to odd parity [1]. Let $\mathbb{P}$ be the quantum distribution saturating the inequality, i.e. $M_N(\mathbb{P}) = 2^{N-1}$. The property of interest to us is that a Mermin inequality of odd sites contains only correlators having the same parity. In particular if M_N is of odd parity then every correlator appearing in it consists of an odd number of primed observables (see Eq. (6.8) for instance).

[1] Note that in this notation, the unprimed term corresponds to 0 (mod 2) and primed term to 1 (mod 2)

As before, one can see that every correlator of $\mathbb{P}$ not appearing in the M_N (those of even parity) is identically zero.

To see this, let us assume that M_N contains all the odd parity full correlator terms and consider an even parity full-correlator, $\langle X_1 X_2 \dots X_N \rangle_{\mathbb{P}}$ where $X_i = A_i$ or A_i'. We would like to show that every correlator and marginal consisting of a subset of $K = \{X_1, X_2, \dots, X_N\}$ is zero. To do this, we need to consider a transformation that flips their sign while keeping M_N fixed. Let us denote the outcome of X_i by x_i and denote by $Corr(X_{i_0})_{\mathbb{P}}$ the set of every marginal and full-correlator containing $X_{i_0} \in K$. Notice that $\mathcal{S}_1 : \{x_{i_0} \mapsto -x_{i_0}; x_j \text{unchanged} \, \forall 1 \leq j \neq i_0 \leq N\}$ is a transformation under which $Corr(X_{i_0})_{\mathbb{P}} \mapsto -Corr(X_{i_0})_{\mathbb{P}}$. We show below that M_N remains unchanged if we complement $\mathcal{S}_1$ with $\mathcal{S}_2 : \{x_j' \mapsto -x_j' \forall 1 \leq j \neq i_0 \leq N\}$ with the definition $(a')' = a$. Since $X_j' \notin Corr(X_{i_0})$, this set is unmodified under $\mathcal{S}_2$. Moreover, every term of M_N is unchanged under $\mathcal{S}_2 \circ \mathcal{S}_1$.

For the original even parity term we started with, $\mathcal{S}_2 \circ \mathcal{S}_1(\langle X_1 X_2 \dots X_N \rangle) = -\langle X_1 X_2 \dots X_N \rangle$. Every odd parity full-correlator can be obtained from $\langle X_1 X_2 \dots X_N \rangle$ by swapping inputs at an odd number of places. However, the transformation $\mathcal{S}_2 \circ \mathcal{S}_1$ is such at every site, either the outcome of A_i or A_i' flips sign but not both. Hence, every local swap at any location introduces an additional factor of -1. All the desired correlators can be shown to be zero by running the argument for $1 \leq i_0 \leq N$.

6.3.5 $N-1$ bits of randomness from a Mermin inequality of even N

By the recursion relation defined in Eq.(6.7), a Mermin inequality of even parties N, can be expressed in terms of Mermin inequalities of odd $N-1$ parties. Assuming M_{N-1} contains only the odd parity terms and M_{N-1}' the even parity terms, let $\mathbb{P}_{N-1}$ be the unique distribution satisfying $M_{N-1}(\mathbb{P}_{N-1}) = Q_{max}$. From the previous section, every full even parity correlator in $\mathbb{P}_{N-1}$ vanishes. Let one of them be $\langle X_1 X_2 \dots X_{N-1} \rangle \in \mathbb{P}_{N-1}$. If we take $\mathbb{P}_N$ to denote the unique distribution satisfying $M_N(\mathbb{P}_N) = Q_{max}$ and consider the same correlator $\langle X_1 X_2 \dots X_{N-1} \rangle \in \mathbb{P}_N$, we can use symmetry arguments

to show that this must be identically zero as well.

$\langle X_1 X_2 \dots X_{N-1} \rangle \in M'_{N-1}$. From the previous section, any symmetry transformation $\mathcal{S}$ leading to $x_1 x_2 \dots x_{N-1} \mapsto -x_1 x_2 \dots x_{N-1}$ can be complemented by another symmetry transformation $\mathcal{S}_1$ involving only the first $N-1$ parties under which $M'_{N-1} \mapsto -M'_{N-1}$ and $M_{N-1} \mapsto M_{N-1}$. Using the recursion relation (6.7) and making the transformation $\mathcal{S}_1 \circ \mathcal{S}$, we obtain

$$B_N \mapsto B_{N-1}(A_N + A'_N) - B'_{N-1}(A_N - A'_N) \tag{6.9}$$

The further transformation $A_N \leftrightarrow A'_N$ gives the rest.

Bell's Inequalities	Quantum		Uniqueness
	Local	Global	
CHSH (2,2,2)	1-bit	–	anl
CGLMP (2,M,d)	1-dit	–	num
Chain (2,M,2)	1-bit	2-bits	num
Mermin (N_{odd},2,2)	1-bit	N-bits	anl
Mermin (N_{even},2,2)	1-bit	$(N-1)$bits	anl

6.3.6 Maximum global randomness cannot be certified for non-signalling distributions

We briefly touch on non-signalling (NS) correlations in this section. As discussed in the Appendix D, the NS set of correlations comprise a larger set than the quantum one. We show by construction that certification of full global randomness for NS distributions is impossible, as a principle, in certain cases. For any general full correlator inequality, let us construct a probability distribution with marginal correlators zero. In this case, positivity is always respected no matter what value is assigned to the full correlators including, in particular, those points that maximally violate the chosen Bell inequality. Since certification requires the full correlators to vanish, this simple observation precludes certifying full ramdomness in these cases.

In order to do this more concrete let us consider the simplest case once again, the $(2, 2, 2)$. In general, the requirement of positivity of the probabilities constrains the feasible non-signalling points to a strict subset of the 8-dimensional hypercube parametrized by 4 correlators and 4 marginals each with values lying in $[-1, +1]$ where

$$\begin{aligned} P(a, b|x, y) = \frac{1}{4}(1 + a\langle A_x\rangle + b\langle B_y\rangle + ab\langle A_x B_y\rangle) \geq 0 \\ P(a|x) = \frac{1}{2}(1 + a\langle A_x\rangle) \geq 0 \\ P(b|y) = \frac{1}{2}(1 + b\langle B_y\rangle) \geq 0 \end{aligned} \tag{6.10}$$

Now with reference to the CHSH inequality, we can easily construct a distribution with all marginals zero which maximally violates it. In this case, Eq (6.10) is trivially satisfied for any value of the correlator $\langle A_x B_y\rangle$, including the extremal ones of ± 1. Since global randomness requires certifying that $\langle A_x B_y\rangle = 0$ for some $x = x_0, y = y_0$, no such certificate is possible *either by symmetry arguments or otherwise.*

Indeed, the extremal points of the NS set for $(2, M, 2)$ and $(2, 2, d)$ and $(3, 2, 2)$ are characterized [JM05, BLM$^+$05, PBS11] and one sees explicitly that in no case full global randomness can be certified.

6.4 Uniqueness

In the previous sections we assumed the uniqueness of the probability distribution maximally violating a Bell inequality. In this, we will show that this is true in several cases and that such an assumption can be justified in others.

$(2, 2, 2)$: It is known that all extremal correlations of $(2, 2, 2)$ have a unique quantum representation [Tsi87, FFW11]. Moreover, for any Bell experiment of at most 2 dichotomic measurements per party, it has been shown that every probability distribution in the quantum set Q allows a representation in terms of qubits and projective measurements [Mas06,

AMP12]. In particular the Bell states under given measurements are known to maximally violate the CHSH inequality.

$(N, 2, 2)$: It has been shown that the $\mathbb{P}$ maximally violating a B-K (in particular, Mermin) inequality is extremal and has a unique quantum representation [FFW11, WW01a]. The GHZ state of N qubits is known to be the unique state which maximally violate it [Che04, GBP98, SG01].

$(2, M, 2)$: For $M = 3$, all extremal correlations are guaranteed to have a unique quantum representation [Tsi87, FFW11]. We also have numerical evidence that the distribution saturating the Chained inequality is unique. Unfortunately, for $M > 3$, we do not have any direct evidence of uniqueness.

6.5 Conclusions

We have demonstrated that simple arguments of symmetry can be used to reach significant conclusions regarding the randomness encoded in quantum probability distributions in a device independent manner. In particular, we can show full global randomness in the experimentally feasible scenario of the Mermin inequalities. The only ingredients used are the symmetry, the chosen Bell inequality and the uniqueness of the distribution saturating it. In several important cases, we point out that uniqueness is already known to exist or state the case for it.

However, in some cases uniqueness does not exist. One example are the so-called lifted Bell inequalities. A tight Bell inequality of a smaller space can be *lifted* in a sense made precise in [Pir05] to a tight Bell inequality in a higher space, either with more parties, measurements or outcomes. For example, $(CHSH-2)_{AB} \otimes C_1 \leq 0$ is a tight Bell inequality of $(3, 2, 2)$ in which on one setting of party C appears. In this case, a family of distributions $\mathbb{P}(C_2)$ saturate this inequality for any value of C_2.

Chapter 7

Overview and future perspective

The results reported in this dissertation contribute to a better identification and characterisation of several resources appearing in the quantum framework. In particular, we tried to go a step forward in the clarification of the existing connections among secrecy, entanglement, non-locality and randomness.

We first asked if non-additivity effects, typical from the quantum scenario, could exist even in the classical framework. We provided some evidence for the existence of similar effects for secret classical correlations. Exploiting the analogies between the entanglement and secret-key agreement scenario, we have shown that two classical distributions from which no secrecy can be extracted by AD protocols can lead to a positive secret key rate when combined. The evidence we gave is somehow similar to the conjectured example of activation for bipartite entangled states. The difference being here that we cannot ensure that any of the two distributions is really bound. Of course, it still remains open a proof of the existence of bipartite bound information, which is connected to the search for criteria able to detect the non-distillability of classical tripartite correlations.

Additionally, we have shown a case of four-partite bound information

and its properties, unlockability and superactivation. In this more general case, a proof of the existence of bound information was possible due to the freedom one has to consider different set of bipartitions. All the properties are obtained by deriving classical analogues of the Smolin state and its quantum effects as super-activation and unlockability. We have also shown a usefulness of undistillable correlations: bound entanglement and bound information can be used to distribute pure multipartite state (GHZ) and multipartite sbits in quantum and classical scenarios, respectively. As an open question, it would be interesting to investigate which properties of quantum correlations can or cannot have their classical counterparts.

Later, we asked about the non-local features of those states (private states) which represent perfectly secure bits of cryptographic key. We have shown that all private states are nonlocal. In particular, that they violate the CHSH-Bell inequality. It would be interesting to further study this question in the multipartite scenario and understand whether all multipartite private states contain genuine multipartite non-locality.

Finally, we have demonstrated that simple arguments of symmetry can be used to reach significant conclusions regarding the randomness encoded in quantum probability distributions in a device independent manner. In particular, we have shown that full global randomness can be certified in the experimentally feasible scenario of the Mermin inequalities. The only ingredients used are the symmetry of a given Bell inequality and the assumption on the uniqueness of the quantum distribution maximally violating it. It would be interesting to study how these findings generalize to general non-signalling correlations and whether maximal randomness certification is also possible in this scenario.

Appendix A

Bipartite Bound Information

After the advantage distillation (AD) has been performed by the honest parties, they are left with one bit for which the probability of error can be written as:

$$\epsilon_B \lesssim \lambda_B \mu_B^N \tag{A.1}$$

where λ_B is a positive constant and μ_B is the initial error which scales with N, with N the length of the block used in the AD protocol.

On Eve's side, her error can be also expressed compactly as:

$$\epsilon_E \gtrsim \lambda_E \mu_E^N \tag{A.2}$$

where we recall that it has been estimated (in particular, lower bounded) counting those cases in which she has to guess with probability one half the symbol which Alice and Bob are sharing.

With this in mind, we want to show that if $\mu_B < \mu_E$ then exists an N for which the bound

$$I(A:B) - I(A:E) \tag{A.3}$$

becomes positive. This condition is sufficient to let the honest parties exchanging a secret key by one-way protocol. As expressed in the main text, this bound represent the mutual information between Alice-Bob and Alice-Eve, respectively. The first element is easily calculated and corresponds

to:

$$I(A:B) = 1 - h(\epsilon_B) \tag{A.4}$$

where $h(\epsilon_B)$ is the binary entropy, $h(\epsilon_B) = -\epsilon_B \log \epsilon_B - (1-\epsilon_B)\log(1-\epsilon_B)$. The second element is given by:

$$I(A:E) = H(A) - H(A|E) = 1 - \sum_e P(E=e)H(A|E=e) \tag{A.5}$$

where $H(A)$ is the Shannon entropy of the random variable A and the sum runs over all possible symbols ($e = i_1 \dots i_N$) Eve can obtain, conditioned to those composing the block of N. Additionally, the term $H(A|E)$ can be decomposed as follows:

$$H(A|E) = \sum_{e_b} P(E=e_b)H(A|E=e_b) + \sum_{e_r} P(E=e_r)H(A|E=e_r) \tag{A.6}$$

where e_b, refers to all those sequences for which Eve has no information ($P_{guess}^{Eve} = 1/2$) and e_r refers to the remaining sequences. If we conservatively assume that in the remaining ones she has full information, the previous expression reduces to:

$$H(A|E) = \sum_{e_b} P(E=e_b) \tag{A.7}$$

since the elements $H(A|E=e_b) = 1$ and $H(A|E=e_r) = 0$ (because $P(A=0|E=e_b) = P(A=1|E=e_b) = 1/2$ and $P(A=0|E=e_r) = P(A=1|E=e_r) = 1$). Generally, the previous expression represents a lover bound on $H(A|E)$, so that:

$$H(A|E) \geq \sum_{e_b} P(E=e_b) \tag{A.8}$$

furthermore, from what already said:

$$\frac{1}{2}\sum_{e_b} P(E=e_b) \geq \lambda_E \mu_E^N \tag{A.9}$$

since in our estimation of the lover bound of Eve's error we tried to take in account those cases for which $P_{guess}^{Eve} = 1/2$.

By using the previous relations, eq.(A.3) hence reads:

$$I(A:B) - I(A:E) \geq -\epsilon_B |\log \epsilon_B| + (1-\epsilon_B)\log(1-\epsilon_B) + 2\lambda_E \mu_E^N \quad \text{(A.10)}$$

What we are interested in now is to show that exists some N big enough such that the l.h.s. of eq. (A.10) becomes positive. Firstly, for N large since ϵ_B goes to zero, $(1-\epsilon_B)\log(1-\epsilon_B)$ goes also to zero. Given that, by eq. A.1) we can write the l.h.s. of (A.10) as:

$$2\lambda_E \mu_E^N \left(1 - \frac{\lambda_B \mu_B^N (N|\log \mu_B| + |\log \lambda_B|)}{2\lambda_E \mu_E^N}\right) \quad \text{(A.11)}$$

It is thus evident that, from the fact that $\mu_B < \mu_E$ and for large N the last expression tends to $2\lambda_E \mu_E^N$ which is indeed a positive number. This ends the proof.

A.1 Schematic representation of the probability distribution Q

This appendix shows the probability distribution obtained by Alice, Bob and Eve after measuring the symmetric state (3.2). Being the table very big we try to give here a schematic representation of it which can be equivalently useful to the reader to follow our arguments. It reads:

	00	01	02	10	11	12	20	21	22
00	(1_u)	$+$	$+$	(2_u)	$*$	$*$	(2_w)	$*$	$*$
01	$+$	(1_u)	$+$	$*$	(2_u)	$*$	$*$	(2_w)	$*$
02	$+$	$+$	(1_u)	$*$	$*$	(2_u)	$*$	$*$	(2_w)
10	(2_u)	$*$	$*$	(1_v)	$+$	$+$	(2_v)	$*$	$*$
11	$*$	(2_u)	$*$	$+$	(1_v)	$+$	$*$	(2_v)	$*$
12	$*$	$*$	(2_u)	$+$	$+$	(1_v)	$*$	$*$	(2_v)
20	(2_w)	$*$	$*$	(2_v)	$*$	$*$	(1_w)	$+$	$+$
21	$*$	(2_w)	$*$	$*$	(2_v)	$*$	$+$	(1_w)	$+$
22	$*$	$*$	(2_w)	$*$	$*$	(2_v)	$+$	$+$	(1_w)

Table A.1: Schematic view of the distribution $Q_{X1,Y1,X2,Y2,\tilde{Z}}$. Due to the lack of space, cells have been grouped in terms of probability distributions and number of elements (symbols) as explained below.

The joint probabilities $P(X_1 = i, Y_1 = k, X_2 = j, Y_2 = l)$ between the honest parties are distributed as follows:

- cells of type (1_i), with $i = u, v, w$ are equal to $\frac{1-q}{72}$
- cells of type (2_i), with $i = u, v, w$, are equal to $\frac{1+7q}{144}$;
- cells of type $*$, are equal to $\frac{1-q}{48}$;

- cells of type + , are equal to $\frac{1-q}{96}$;

Concerning Eve's side (see caption of Table 3.1 for more details about how to read the tables):

- cells of type (1_i), with $i = u, v, w$ contain three elements. The terms that play a role in her discrimination are indicated by the same number and subindex letter. For example, consider the cell $X_1 = 0, Y_1 = 0, X_2 = 0, Y_2 = 0$. The label 1_u is used for this cell (the same one indicates $X_1 = 0, Y_1 = 0, X_2 = 1, Y_2 = 1$ and $X_1 = 0, Y_1 = 0, X_2 = 2, Y_2 = 2$). The three elements here are the three probability distributions:

$$P(0,0,0,0,\bar{z}_{00,00}), \quad P(0,0,0,0,\bar{z}_{00,11}), \quad P(0,0,0,0,\bar{z}_{00,22}).$$

  $P(0,0,0,0,\bar{z}_{00,00})$ refers to the probability that Eve guesses correctly, the remaining two $P(0,0,0,0,\bar{z}_{00,11})$, $P(0,0,0,0,\bar{z}_{00,22})$ refers to the probability she guesses wrongly.

- cells of type (2_i), with $i = u, v, w$, contain six elements;

- cells of type $*$, contain two elements distributed with probability one half (in this cases, she knows nothing about A and B symbols) ;

- cells of type + , contains only one term since in this case Eve's symbol is perfectly correlated with those of A and B;

A.2 Advantage distillation details

In this second appendix, we clarify why it is enough to consider six classes of distributions in the AD analysis of section 3.2.2. From Table 3.4 the

following relations hold:

$$
\begin{aligned}
P(E=[z_{ii},\tilde{z}_{ii00}]|X_2Y_2=00) &= P(E=[z_{ii},\tilde{z}_{ii11}]|X_2Y_2=11) = \bar{\delta}_1\\
P(E=[z_{ii},\tilde{z}_{ii11}]|X_2Y_2=00) &= P(E=[z_{ii},\tilde{z}_{ii00}]|X_2Y_2=11) = \bar{\eta}_1\\
P(E=[z_{ts},\tilde{z}_{st00}]|X_2Y_2=00) &= P(E=[z_{ts},\tilde{z}_{st11}]|X_2Y_2=11) = \bar{\delta}_2\\
P(E=[z_{ts},\tilde{z}_{st11}]|X_2Y_2=00) &= P(E=[z_{ts},\tilde{z}_{st00}]|X_2Y_2=11) = \bar{\eta}_2\\
P(E=[z_{ts},\tilde{z}_{ts00}]|X_2Y_2=00) &= P(E=[z_{ts},\tilde{z}_{ts11}]|X_2Y_2=11) = \bar{\delta}_3\\
P(E=[z_{ts},\tilde{z}_{ts11}]|X_2Y_2=00) &= P(E=[z_{ts},\tilde{z}_{ts00}]|X_2Y_2=11) = \bar{\eta}_3\\
P(E=[z_{st},\tilde{z}_{st00}]|X_2Y_2=00) &= P(E=[z_{st},\tilde{z}_{st11}]|X_2Y_2=11) = \bar{\delta}_4\\
P(E=[z_{st},\tilde{z}_{st11}]|X_2Y_2=00) &= P(E=[z_{st},\tilde{z}_{st00}]|X_2Y_2=11) = \bar{\eta}_4\\
P(E=[z_{st},\tilde{z}_{ts00}]|X_2Y_2=00) &= P(E=[z_{st},\tilde{z}_{ts11}]|X_2Y_2=11) = \bar{\delta}_5\\
P(E=[z_{st},\tilde{z}_{ts11}]|X_2Y_2=00) &= P(E=[z_{st},\tilde{z}_{ts00}]|X_2Y_2=11) = \bar{\eta}_5
\end{aligned}
$$

and $\bar{\delta}_6$ is the sum of all the $P(E=[z_{**},\tilde{z}_{**22}]|X_2=Y_2)$. As already stated in the caption of Table 3.4, $i,s,t=0,1,2$ with $s\neq t$ and $s<t$. In the computation, it is simpler to use Eve's probabilities conditioned on the fact that Alice and Bob have made no mistake after AD, so this means that we only need to consider the terms in the diagonal of Table 3.4. For this reason the δ_i,η_i appearing in eq. (3.10) are the previous ones but normalized. The complete expression is then derived according to the argument already presented at page 63.

Appendix B

Multipartite Bound Information

B.1 Derivation of (4.3.2)

By individual measurement to each copy of two Smolin states in (4.2), the five parties share measurement data such that Alice, Bob, and Clare possess two values labeled 1 and 2 and David and Elena keep single values. Both the first and the second distributions in the form in (4.5) can be written in a simpler form as follows. For the first copy,

A_1	C_1	B_1	D_1	$\mathcal{E}_1$	$P_{A_1B_1C_1D\mathcal{E}}$
i	i	i	i	ϵ_1	$1/8$
i	i	$i+1$	$i+1$	ϵ_2	$1/8$
i	$i+1$	i	$i+1$	ϵ_3	$1/8$
i	$i+1$	$i+1$	i	ϵ_4	$1/8$

(B.1)

where $i = 0, 1$, and for the second copy of A_2, B_2, C_2 and E, assuming Eve holding the second parameter f_k, $k = 1, 2, 3, 4$,

A_2	B_2	C_2	E	$\mathcal{E}_2$	$P_{A_2B_2C_2D\mathcal{E}}$
j	j	j	j	f_1	$1/8$
j	j	$j+1$	$j+1$	f_2	$1/8$
j	$j+1$	j	$j+1$	f_3	$1/8$
j	$j+1$	$j+1$	j	f_4	$1/8$

(B.2)

for $j = 1, 2$. The full probability obtained by measuring the state in (4.2) is then shown in (4.3.2).

B.2 The full distribution of (4.10)

The full distribution of (4.10) is explicitly shown as follows, for different values of $\mathcal{E}_1$,

$C_1^{'}$	C_2	$D^{'}$	E	$\mathcal{E}_1$	$\mathcal{E}_2$
j	j	j	j	ϵ_1	f_1
j	$j+1$	j	$j+1$	ϵ_1	f_2
j	j	$j+1$	$j+1$	ϵ_1	f_3
j	$j+1$	$j+1$	j	ϵ_1	f_4
j	j	j	j	ϵ_2	f_1
j	$j+1$	j	$j+1$	ϵ_2	f_2
j	j	$j+1$	$j+1$	ϵ_2	f_3
j	$j+1$	$j+1$	j	ϵ_2	f_4
$j+1$	j	$j+1$	j	ϵ_3	f_1
$j+1$	$j+1$	$j+1$	$j+1$	ϵ_3	f_2
$j+1$	j	j	$j+1$	ϵ_3	f_3
$j+1$	$j+1$	j	j	ϵ_3	f_4
$j+1$	j	$j+1$	j	ϵ_4	f_1
$j+1$	$j+1$	$j+1$	$j+1$	ϵ_4	f_2
$j+1$	j	j	$j+1$	ϵ_4	f_3
$j+1$	$j+1$	j	j	ϵ_4	f_4

(B.3)

For cases when Eve is with ϵ_3 or ϵ_4, the distribution in (4.10) can be obtained by replacing j with $j+1$ in (B.3).

Appendix C

Bell's inequalities for multipartite states

It is straightforward to construct a multipartite Bell's inequality that is violated by any pure multipartite entangled state. In the simplest case of three parties sharing a state Ψ_{ABC}, a measurement on, say, C projects the resulting bipartite state on $\tilde{\Psi}_{AB}$ with probability $P(\bar{c}|\bar{z})$. Thus, if the measurement on C is chosen such that the projected state on AB is entangled, the generalized Bell's inequality:

$$\sum_{abxy} c_{abxy} P(ab|xy, \bar{c}\bar{z}) \leq L \tag{C.1}$$

is violated by Ψ_{ABC} because of Gisin's theorem.

Using the following identity:

$$P(abc|xyz) = P(ab|xy, cz)P(c|xyz) = P(ab|xy, cz)P(c|z) \tag{C.2}$$

where the last term is obtained by imposing no-signalling between any party, the tripartite inequality is easily obtained multiplying both sides in (C.1) by $P(\bar{c}|\bar{z})$:

$$\sum_{abxy} c_{abxy} P(ab\bar{c}|xy\bar{z}) \leq LP(\bar{c}|\bar{z}) = \bar{L} \tag{C.3}$$

Note that, party C is just measuring one observable, namely $M_{\bar{z}}$, and that a violation of the obtained inequality does not provide information about the "type" of non locality in the state Ψ_{ABC}.

Appendix D

NS, Quantum and Local sets of correlations

The formulation adopted by Bell to show his famous theorem definitely inspired a new approach to discriminate between different kinds of possible correlations. A scenario constituted by two parties (A and B) which repeat a huge number of times the experiment of freely choose to "push a button" (x and y) between m possible ones[1] and which in every instance get an outcome (a and b) between d likely straightforwardly defines a probability distribution $P(ab|xy)$. In order for it to be a well defined probability distribution two conditions have to be satisfied:

Normalization

$$\sum_{ab} P(ab|xy) = 1 \quad \forall x, y \tag{D.1}$$

Positivity

$$P(ab|xy) \geq 0 \quad \forall a, b, x, y \tag{D.2}$$

[1] Note that, we are assuming here that the parties, have the same number m of settings, and the same number d of outcomes for each setting. The more general (asymmetrical) case can be tackled in the same way.

The set obtained in this way has an interesting structure. First, it is convex set: convex combinations of correlations are still legitimate correlations. Second, there are only a finite number of extremal correlations. Consequently, any correlation can be decomposed into a (not necessarily unique) convex combination of such extremal correlations.

For the case in exam, a total of $D = m^2d^2$ different probability distributions exists,which are labeled by the different $[abxy]$. When this probability distributions are considered as points in a $D-$dimensional real space, this set forms a convex polytope with a finite number of extremal vertices. This polytope is the convex hull of the extreme points. From the constraints (D.1) (D.2) imposed above the more general set of correlation is given, which comprise the set of probability distributions which allow instant communication (*signalling*) between the parties. More interesting from a physical point of view is the set of probability distributions which fulfil the no-signalling principle.

D.1 No-Signaling Set

The set of no-signaling distributions, is a subset of the previous one and consist of those probability distributions which do not allow instant communication between the parties. A compact way to define this constraint is through the following equation:

No-Signaling $B \to A$

$$P(a|xy) = \sum_b P(ab|xy) = \sum_{b'} P(ab'|xy') = P(a|xy') = P(a|x) \quad \forall a, x, y, y' \tag{D.3}$$

which imposes that a different input choice on Bob's side does not influence the local probability distribution on Alice's side. A similar condition holds for the opposite case:

No-Signaling $A \to B$

$$P(b|xy) = \sum_a P(ab|xy) = \sum_{a'} P(a'b|x'y) = P(b|x'y) = P(b|y) \quad \forall b, x, x', y \tag{D.4}$$

This conditions thus identify the no-signaling polytope to which we refer as $P_{NS}(ab|xy)$.

D.2 Quantum Set

Probability distributions which are obtained by general measurements on quantum states can be written, accordingly to Born's rule as follows:

$$P_Q(ab|xy)_\rho = tr(\rho_{AB} M_{a|x} \otimes M_{b|y}). \tag{D.5}$$

Here ρ is a quantum state (i.e. a unit trace semidefinite positive operator) on a Hilbert space $\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ where $\mathcal{H}_\mathcal{A}$ and $\mathcal{H}_\mathcal{B}$ are the state space of the system held by A and B respectively. The sets $\{M_{a|x}, and M_{b|y}\}$ define what is called a positive operator valued measure (POVM), i.e. a set of positive operators satisfying $\sum_a M_{a|x} = \mathbb{I}$ ($\sum_b M_{b|y} = \mathbb{I}$). POVM operator measurements include as a special case the ordinary Von Neumann measurements that use so-called projection valued measures (PVM) where all positive operators are orthogonal projection operators[2]. Quantum correlations are no-signaling thereby they are a subset of the no-signaling polytope before introduced. But in contrast while, the quantum set is still convex it is not a polytope since the number of extremal points is not finite.

[2]Note that in order to describe the full measurements process it is necessary to specify the set of so-called Kraus operators $\{K_{a|x}\}$ that correspond to the POVM element $\{M_{a|x}\}$, where $M_{a|x} = K_{a|x}(K_{a|x})^\dagger$. The reason for including the Kraus formalism, is due to the fact that the POVM description alone does not provide any answer about the state of the system after the measurement is performed.

D.3 Local Set

Finally, the set of local (classical) correlations consists of those probability distributions which are described by a model á la EPR:

$$P_L(ab|xy)_\rho = \int P^A(a|x,\lambda)P^B(b|y,\lambda)\sigma(\lambda)d\lambda, \tag{D.6}$$

where $\sigma(\lambda)$ refers to the probability measure according to which λ is distributed. The locality condition imposes that the local distributions $P^A(a|x,\lambda)$, $P^B(b|y,\lambda)$ can only depend on the chosen setting and on the hidden-variable λ, on which no restrictions are generally imposed. Furthermore, it is worth mentioning that the distribution σ does not depend neither on the outcomes nor on the settings of the remote parties. This is sometimes called the " free-will assumption", and in some way stress that the variable λ contains information about correlations between the two subsystem established in the past. Let us review what is known about the set of local correlations.

It is also a polytope whose vertices correspond to local deterministic distributions [WW01a], i.e. $P(ab|xy) = \delta_{a,f(x)}\delta_{b,g(y)}$ where the function $f(x)$ $(g(y))$ determines the outcome a (b) given the setting x (y). Thus for each set of settings (x, y) there is a unique set of outcomes $a = f(x)$, $b = g(y)$ for which $P(ab|xy) = 1$.

The local polytope is known to be constrained by two types of facets. The first are trivial facets and derive from the positivity condition (D.2). The second kind of facets are non trivial and separate correlations explainable by model (D.6) from those which cannot. Quantum correlations and more general no-signaling correlations fall on the other side of this facets, known as tight Bell's inequalities, thereby are termed non-local.

D.4 Bell's inequalities

As already said, in order to distinguish among the different kinds of correlations previously introduced, Bell's inequalities are shown to be a very powerful tool. From the previous geometrical explanation of the sets of

correlations it is straightforward to understand the role of a Bell's inequality. It is an hyperplane in the space of probabilities, which divides the no-signalling polytope in halves. If the inequality is a tight one then it divides local correlations from non-local ones. If it is not then it divides some non-local correlations from the rest. Any Bell's inequality in the bipartite scenario can be written as:

$$\sum_{abxy} c_{abxy} P(ab|xy) \leq \beta \tag{D.7}$$

where the coefficients c_{abxy} are reals and β represents the maximal bound achievable by the kind of correlations in exam. It is in principle possible to distinguish a different bound β for each of the different sets aforementioned. Sometimes, instead of dealing directly with probabilities, product expectation values are used which simplify the investigation considerably. These are defined in the usual way as the weighted sum of the products of the outcomes:

$$\langle A_x B_y \rangle = \sum_{ab} abP(ab|xy). \tag{D.8}$$

While projection (D.8) is a one-to-one mapping in the case of two outcomes per setting, it is not in general. This implies that even though it is easier to work with expectation values, some information about the structure of the correlations is unequivocally lost, when the scenario consist of more then two outcomes per setting..

It is worth mentioning that, as soon as the number of parties, settings and outcomes increase, determining whether a point lies within the local polytope, i.e. whether it does not violate a Bell's inequality is in general very hard to test. In '89 Pitowsky showed that this problem is related with another known problem in computational complexity which it is known to be NP-complete.

Local Correlations. One of the best known case so far is the simplest non trivial scenario of two parties with two dichotomic observables (2.19). As said, in an experiment where two separated parties measure one of

two possible observables, $\{A_1, A_2\}$ and $\{B_1, B_2\}$ with outcomes ± 1, the following inequality:

$$|\langle A_1 B_1\rangle + \langle A_1 B_2\rangle + \langle A_2 B_1\rangle - \langle A_2 B_2\rangle| \tag{D.9}$$

is bounded by 2 if their system is compatible with the predictions of a local realistic theory. The product expectation values are easily obtained, e.g. $\langle A_1 B_1\rangle = P(+1+1|11)+P(-1-1|11)-(P(+1-1|11)+P(-1+1|11))$, etc...

The local polytope is the convex hull in $\mathbb{R}^4$ of the 8 extreme points of the form:

$$\begin{aligned}&(1,1,1,1),(-1,-1,-1,-1),(1,1,-1,-1),(-1,-1,1,1),\\&(1,-1,1,-1),(-1,1,-1,1),(1,-1,-1,1),(-1,1,1,-1)\end{aligned} \tag{D.10}$$

This polytope is enclosed between 16 facets, 8 of which are trivial ones:

$$-1 \leq \langle A_1 B_1\rangle \leq 1, \quad -1 \leq \langle A_1 B_1\rangle \leq 1, \tag{D.11}$$

$$-1 \leq \langle A_2 B_1\rangle \leq 1, \quad -1 \leq \langle A_2 B_2\rangle \leq 1, \tag{D.12}$$

and 8 which are all equivalent to the CHSH inequality (D.9):

$$\begin{aligned}&|(-1)^{\gamma}\langle A_1 B_1\rangle + (-1)^{\gamma+\beta}\langle A_1 B_2\rangle+\\&\qquad (-1)^{\gamma+\alpha}\langle A_2 B_1\rangle + (-1)^{\gamma+\beta+\alpha+1}\langle A_2 B_2\rangle| \leq 2\end{aligned} \tag{D.13}$$

where $\alpha, \beta, \gamma \in \{0, 1\}$ Thereby correlations which satisfy the previous inequalities can be described by model (D.6).

Quantum Correlations. Given the previous inequalities, Tsirelson showed that for quantum mechanical systems the maximal achievable bound (*Tsirelson bound*) for (D.13) is equivalent to $2\sqrt{2}$. Interestingly, he proved that this bound is already reached by Pauli measurements on a singlet state so there is no advantage in considering quantum states on higher dimensional Hilbert spaces. As already shown by Bell, Tsirelson confirmed that

the space of local correlations is strictly contained in that of quantum correlations.

NS Correlations. In '94 Popescu and Rorlich [PR94] assuming relativistic causality and non-locality, in the sense of Bell's theorem, fund that quantum mechanics is not the more non-local theory (compatible with the no-signaling principle). No-signaling correlations can violate the Tsirelson bound and saturate the CHSH inequality up to its algebraic maximum, $|CHSH| = 4$. The probability distribution that achieves this reads:

$$\begin{aligned} &P(ab|x=1,y=1) = \frac{1}{2}\delta_{a,b}, \quad P(ab|x=1,y=1) = \frac{1}{2}\delta_{a,b}, \\ &P(ab|x=2,y=1) = \frac{1}{2}\delta_{a,b}, \quad P(ab|x=2,y=2) = \frac{1}{2} - \frac{1}{2}\delta_{a,b}. \end{aligned} \tag{D.14}$$

where $\delta_{a,b} = 1$ if $a = b$ and 0 otherwise. Distribution (D.14) , is termed PR box and is an extremal point of the no-signaling polytope for the case of two dichotomic observables per party. An interesting fact is given by the existence of a one-to-one correspondence between the non-local extreme points and the facets of the local polytope given by the CHSH inequalities (D.13). In terms of products expectations values these 8 boxes are given by:

$$\begin{aligned} &(-1,1,1,1),(1,-1,-1,-1),(1,-1,1,1),(-1,1,-1,-1), \\ &(1,1,-1,1),(-1,-1,1,-1),(1,1,1,-1),(-1,-1,-1,1). \end{aligned} \tag{D.15}$$

Bibliography

[ACM04] A. Acín, J. I. Cirac, and Ll Masanes, *Multipartite bound information exists and can be activated*, Phys. Rev. Lett. **92** (2004), 107903.

[AG05] Antonio Acín and Nicolas Gisin, *Quantum correlations and secret bits*, Phys. Rev. Lett. **94** (2005), 020501.

[AGS03] A. Acín, N. Gisin, and V. Scarani, *Security bounds in quantum cryptography using d-level systems*, Quant. Inf. Comp. **3** (2003), 563.

[AH09a] Remigiusz Augusiak and Paweł Horodecki, *Multipartite secret key distillation and bound entanglement*, Phys. Rev. A **80** (2009), 042307.

[AH09b] ———, *W-like bound entangled states and secure key distillation*, EPL **85** (2009), 50001.

[AMP12] Antonio Acín, Serge Massar, and Stefano Pironio, *Randomness versus nonlocality and entanglement*, Phys. Rev. Lett. **108** (2012), 100402.

[AVC03] A. Acín, G. Vidal, and J. I. Cirac, *On the structure of a reversible entanglement generating set for three–partite states*, Quant. Inf. Comp. **3** (2003), 55.

[Bar02] J. Barrett, *Nonsequential positive-operator-valued measurements on entangled mixed states do not always violate a bell inequality*, Phys. Rev. A **65** (2002), 042302.

[BB84] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India), 1984, p. 175.

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels*, Phys. Rev. Lett. **70** (1993), 1895.

[BBPS96] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher, *Concentrating partial entanglement by local operations*, Phys. Rev. A **53** (1996), 2046–2052.

[BC56] S.L. Braunstein and C.M. Caves, *Wringing out better bell inequalities*, Annals of Physics **202** (22-56), 1990.

[BDSW96] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters, *Mixed-state entanglement and quantum error correction*, Phys. Rev. A **54** (1996), 3824–3851.

[Bel64] J. Bell, *On the einstein-podolsky-rosen paradox*, Rev. Mod. Phys. **1** (1964), 195.

[Ben95] Charles Bennett, *Quantum information and computation*, Phys. Today **48** (1995), 24.

[BLM+05] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, *Nonlocal correlations as an information-theoretic resource*, Phys. Rev. A **71** (2005), 022101.

[BW92] Charles H. Bennett and Stephen J. Wiesner, *Communication via one- and two-particle operators on einstein-podolsky-rosen states*, Phys. Rev. Lett. **69** (1992), 2881–2884.

[CH74] John F. Clauser and Michael A. Horne, *Experimental consequences of objective local theories*, Phys. Rev. D **10** (1974), 526–535.

[Che04] Zeqian Chen, *Bell-klyshko inequalities to characterize maximally entangled statesof n qubits*, Phys. Rev. Lett. **93** (2004), 110403.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett. **23** (1969), no. 15, 880.

[CK78] I. Csiszár and J. Körner, *Broadcast channels with confidential messages*, IEEE Transactions on Information Theory **IT-24** (1978), 339■348.

[CLL04] Marcos Curty, Maciej Lewenstein, and Norbert Lütkenhaus, *Entanglement as a precondition for secure quantum key distribution*, Phys. Rev. Lett. **92** (2004), 217903.

[Col09] Roger Colbeck, *Quantum and relativistic protocols for secure multi-party computation*, arXiv **0911.3814v2** (2009), 150.

[CP02] Daniel Collins and Sandu Popescu, *Classical analog of entanglement*, Physical Review A **65** (2002), no. 3, 032321–.

[CRW03] M. Christandl, R. Renner, and S. Wolf, *A property of the intrinsic mutual information*, Proceedings of International Symposium on Information Theory (2003), 1.

[CT91] T. M. Cover and J. A. Thomas, *Elements of information theory*, Wiley, New York, 1991.

[DC00] W. W. Dür and J. I. Cirac, *Activating bound entanglement in multiparticle systems*, Physical Review A **62** (2000), no. 2, 022302–.

[DCLB00] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruß, *Distillability and partial transposition in bipartite systems*, Phys. Rev. A **61** (2000), 062313.

[DSS+00] David P. DiVincenzo, Peter W. Shor, John A. Smolin, Barbara M. Terhal, and Ashish V. Thapliyal, *Evidence for bound entangled states with negative partial transpose*, Phys. Rev. A **61** (2000), 062312.

[Ebe93] Philippe H. Eberhard, *Background level and counter efficiencies required for a loophole-free einstein-podolsky-rosen experiment*, Phys. Rev. A **47** (1993), R747–R750.

[EF01] Y. C. Eldar and J. D. Forney, *On quantum detection and the square-root measurement*, IEEE Trans. Inform. Theory **47** (2001), 858–872.

[Eke91] A. K. Ekert, *Quantum cryptography based on bell's theorem*, Phys. Rev. Lett. **67** (1991), 661.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Phys. Rev. **47** (1935), 777.

[FFW11] T. Franz, F. Furrer, and R. F. Werner, *Extremal quantum correlations and cryptographic security*, Phys. Rev. Lett. **106** (2011), 250502.

[Fin82] A. Fine, *Hidden variables, joint probability, and the bell inequalities*, Phys. Rev. Lett. **48** (1982), 291.

[GBP98] N. Gisin and Bechmann-Pasquinucci, *Bell inequality, bell states and maximally entangled states for n qubits*, Phys. Lett. A **246** (1998), 1.

[Gis91] N. Gisin, *Bell's inequality holds for all non-product states*, Phys. Lett. A **154** (1991), 201.

[GRW02] N. Gisin, R. Renner, and S. Wolf, *Linking classical and quantum key agreement: Is there a classical analog to bound entanglement?*, Algorithmica **34** (2002), 389–412.

[GW99] N. Gisin and S. Wolf, *Quantum cryptography on noisy channels: Quantum versus classical key-agreement protocols*, Phys. Rev. Lett. **83** (1999), 4200–4203.

[GW00] ———, *Linking classical and quantum key agreement: Is there bound information?*, Advances in Cryptology - Proceedings of Crypto 2000, Lecture Notes in Computer Science, **1880** (2000), 482–500.

[GWAN11] R. Gallego, L. E. W§rflinger, A. Acín, and M. Navascués, *An operational framework for nonlocality*, arXiv **1112.2647** (2011), 4.

[HA06] Paweł Horodecki and Remigiusz Augusiak, *Quantum states representing perfectly secure bits are always distillable*, Phys. Rev. A **74** (2006), 010302.

[Has09] M. B. Hastings, *Superadditivity of communication capacity using entangled inputs*, Nature Physics **5** (2009), 255.

[Hel76] C. W. Helstrom, *Quantum detection and estimation theory*, Academic Press, New York, 1976.

[HH99] M. Horodecki and P. Horodecki, *Reduction criterion of separability and limits for a class of distillation protocols*, Phys. Rev. A **59** (1999), 4206.

[HHH95] R. Horodecki, P. Horodecki, and M. Horodecki, *Violating bell inequality by mixed spin-1/2 states: necessary and sufficient condition*, Physics Letters A **200** (1995), 340–344.

[HHH96] Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki, *Separability of mixed states: necessary and sufficient conditions*, Physics Letters A **223** (1996), no. 1, 1 – 8.

[HHH98] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki, *Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?*, Phys. Rev. Lett. **80** (1998), 5239–5242.

[HHH99] PaweÅ? Horodecki, MichaÅ? Horodecki, and Ryszard Horodecki, *Bound entanglement can be activated*, Physical Review Letters **82** (1999), no. 5, 1056–1059.

[HHHO05] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim, *Secure key from bound entanglement*, Phys. Rev. Lett. **94** (2005), 160502.

[HHHO09] ———, *General paradigm for distilling classical key from quantum states*, IEEE Trans. Inform. Theory **55** (2009), 1898.

[HHT01] Patrick M. Hayden, Michal Horodecki, and Barbara M. Terhal, *The asymptotic entanglement cost of preparing a quantum state*, MATH.GEN. **34** (2001), 6891.

[HPHH08] K. Horodecki, L. Pankowski, M. Horodecki, and P. Horodecki, *Low-dimensional bound entanglement with one-way distillable cryptographic key*, Information Theory, IEEE Transactions on **54** (2008), no. 6, 2621–2625.

[idZHSL98] K. Życzkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, *Volume of the set of separable states*, Phys. Rev. A **58** (1998), 883.

[JM05] Nick S. Jones and Lluis Masanes, *Interconversion of nonlocal correlations*, Phys. Rev. A **72** (2005), 052312.

[Lan61] R. Landauer, *Irreversibility and heat generation in the computing process*, IBM Journal of Research and Development **5** (1961), 183–191.

[Lan92] ———, *Information is physical*, Physics and Computation, 1992. PhysComp '92., Workshop on, oct 1992, pp. 1 –4.

[LP99] Hoi-Kwong Lo and Sandu Popescu, *Classical communication cost of entanglement manipulation: Is entanglement an interconvertible resource?*, Phys. Rev. Lett. **83** (1999), 1459–1462.

[LPSW05] N. Linden, S. Popescu, B. Schumacher, and M. Westmoreland, *Reversibility of local transformations of multiparticle entanglement*, Quantum Information Processing **4** (2005), no. 3, 241–250.

[LWZG09] K. Li, A. Winter, X. Zou, and G. Guo, *Private capacity of quantum channels is not additive*, Phys. Rev. Lett. **103** (2009), 120501.

[Mas06] Lluis Masanes, *Asymptotic violation of bell inequalities and distillability*, Phys. Rev. Lett. **97** (2006), 050503.

[Mau93] U. M. Maurer, *Secret key agreement by public discussion from common information*, IEEE Transactions of Information Theory **39** (1993), 733–742.

[Mer90] N. D. Mermin, *Extreme quantum entanglement in a superposition of macroscopically distinct states*, Phys. Rev. Lett. **65** (1990), 1838.

[MW99] U. Maurer and S. Wolf, *Unconditionally secure key agreement and the intrinsic conditional information*, IEEE Transactions of Information Theory **45** (1999), 499–514.

[NC00] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.

[PAM+10] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, *Random numbers certified by bell's theorem*, Nature **464** (2010), 1021.

[PB11] Giuseppe Prettico and Joonwoo Bae, *Superactivation, unlockability, and secrecy distribution of bound information*, Phys. Rev. A **83** (2011), 042336.

[PBS11] S. Pironio, J. D. Bancl, and V. Scarani, *Extremal correlations of the tripartite no-signaling polytope*, J. Phys. A: Math. Theor. **44** (2011), 065303.

[Per96] Asher Peres, *Separability criterion for density matrices*, Phys. Rev. Lett. **77** (1996), 1413–1415.

[Per99] A. Peres, *All the bell inequalities*, Found. Phys. **29** (1999), 589.

[Pir05] S. Pironio, *Lifting bell inequalities*, Journal of Mathematical Physics **46** (2005), 062112.

[PR92] S. Popescu and D. Rohrlich, *Generic quantum nonlocality*, Phys. Lett. A **166** (1992), 293.

[PR94] S. Popescu and R. Rohrlich, *Quantum nonlocality as an axiom*, Found. Phys. **24** (1994), 379.

[RW03] R. Renner and S. Wolf, *New bounds in secret-key agreement: the gap between formation and secrecy extraction*, Advances in Cryptology, EUROCRYPT 2003, Lecture Notes in Computer Science **2656** (2003), 562.

[Sch35] E. Schrödinger, *Die gegenwä rtige situation in der quantenmechanik*, Naturwissenschaften **23** (1935), 807.

[SG01] V. Scarani and N. Gisin, *Spectral decomposition of bell's operators for qubits*, J. Phys. A: Math. Gen. **34** (2001), 6043.

[Sha48] C. E. Shannon, *A mathematical theory of communication*, Bell System Technical Journal **27** (1948), 379–423, 623–656.

[Sho94] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM J. Sci. Statist. Comput. **26** (1994), 1484.

[Smo01] J. A. Smolin, *Four-party unlockable bound entangled state*, Phys. Rev. A **63** (2001), 032306.

[SST01] Peter W. Shor, John A. Smolin, and Barbara M. Terhal, *Nonadditivity of bipartite distillable entanglement follows from a conjecture on bound entangled werner states*, Phys. Rev. Lett. **86** (2001), 2681–2684.

[SST03] P. W. Shor, J. A. Smolin, and A. V. Thapliyal, *Superactivation of bound entanglement*, Phys. Rev. Lett. **90** (2003), 107901.

[Sve87] G. Svetlichny, *Distinguishing three-body from two-body nonseparability by a bell-type inequality*, Phys. Rev. D **35** (1987), 3066.

[SY08] G. Smith and J. Yard, *Quantum communication with zero-capacity channels*, Science **321** (2008), 1812.

[TA06] Geza Toth and Antonio Acin, *Genuine tripartite entangled states with a local hidden-variable model*, Phys. Rev. A **74** (2006), 030306.

[Tsi80] Boris. S. Tsirelson, *Quantum generalization of bell's inequality*, Lett. Math. Phys. **4** (1980), 93.

[Tsi87] B.S. Tsirelson, *Quantum analogues of the bell inequalities. the case of two spatially separated domains.*, Journal of Soviet Mathematics **36** (1987), 557.

[VW01] K. G. H. Vollbrecht and R. F. Werner, *Entanglement measures under symmetry*, Phys. Rev. A **64** (2001), 062307.

[VW02] Karl Gerd H. Vollbrecht and Michael M. Wolf, *Activating distillation with an infinitesimal amount of bound entanglement*, Phys. Rev. Lett. **88** (2002), 247901.

[Wat04] John Watrous, *Many copies may be required for entanglement distillation*, Phys. Rev. Lett. **93** (2004), 010502.

[Wer89] Reinhard F. Werner, *Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model*, Phys. Rev. A **40** (1989), 4277–4281.

[WW00] R. F. Werner and M. M. Wolf, *Bell's inequalities for states with positive partial transpose*, Phys. Rev. A **61** (2000), 062102.

[WW01a] _____, *All-multipartite bell-correlation inequalities for two dichotomic observables per site*, Phys. Rev. A **64** (2001), 032112.

[WW01b] _____, *Bell inequalities and entanglement*, Quantum Information and Computation **1** (2001), 1–25.

[WZ82] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature **299** (1982), no. 5886, 802–803.