PhD Thesis

Impact of imperfections on correlation-based quantum information protocols

PhD Candidate:

Elsa Passaro

Thesis Supervisor:

Dr. Antonio Acín

ICFO - The Institute of Photonic Sciences

Acknowledgements

The research presented in this PhD Thesis is the result of more than four years of work at ICFO, and it would not have been possible without the support of many people. First of all, I would like to thank Toni for welcoming me in his extraordinary group, for his great scientific support and for all the things he taught me during these years. Then, I would like to thank all my collaborators, in particular Paul, Michele, Dani, Lorenzo and Olmo, with whom I learnt many interesting aspects of quantum information theory. Many thanks also to my officemates, Bogna, Markus, Belén and Lars, to the LIQUID team, to Marti, Alejandro, Senaida, Ariel, Ivan, Alexia, Marcus, Karen, Arnau, Jordi, Peter, Mafalda, Gonzalo, Jonatan, Janek... and to all the other current and former members of the group. Thank you all for the lunch breaks, the futbolín games, the hikes, the nice conferences, the dinners, and for all the stimulating (and often hilarious) discussions we shared.

I am very grateful also to the cooking team, for the effort of providing food for each other for almost one year, I really enjoyed it! Furthermore, I would like to thank all the friends I have met in these years at ICFO, in particular Noslen, Alberto, Miriam, Juan, Marc, Roland, Silvia, Fabian, Nadia, Philipp, and of course the group of "Los Italianos". Thanks to IT and the Human Resources staff at ICFO, for their efficiency and their effort for making things as easy as possible.

Many thanks to the Committee members for taking the time to read this Thesis and for coming to my defense.

Special thanks go to Adri, who has always been there when I needed her. Thank you for your lasting friendship and for our adventures together! Thanks also to all the wonderful friends I have met in Barcelona, above all Juanma, Cristina, Luca, Erica, Giuli, Oriol, but also many more. Furthermore, I would like to thank my old Italian friends: Lucia, Adriana, Fede, Matteo, Giandomenico, Claudia and Rita, who always make me feel like no time has passed between seeing them last.

Vorrei ringraziare particolarmente la mia famiglia, per avermi sempre appoggiata e per essermi stati sempre vicini nonostante la distanza che ci

separa. Grazie di cuore!

Y también quiero agradecerle a mi nueva familia española por haberme acogido tan amablemente: gracias a Paco, Ana, Esther, Dani, Carlos, María, Euge y Alberto.

Dulcis in fundo, I would like to thank Pablo, for his help and for cheering me up in the difficult moments. Thank you for your encouragement, your love and your great support during these years.

Abstract

Quantum information science is a rapidly evolving field both from the theoretical and the experimental viewpoint. The numerous studies in this field are motivated by the fact that protocols exploiting quantum resources can perform tasks that are unfeasible in classical information theory. Examples are the speed-up provided by quantum computation, the secure communication guaranteed by quantum cryptography, or the possibility of making highly sensitive measurements using quantum metrology. These protocols exploit quantum properties without classical analogues, namely entanglement and nonlocal correlations. Whereas these concepts caused severe criticism during the developing stage of quantum mechanics due to the counter-intuitive properties they give rise to, nowadays they are regarded as crucial resources for different technological applications. Moreover, their study is also relevant from a fundamental point of view.

Interestingly, the trustworthiness of quantum information protocols can be authenticated relying upon as few assumptions as possible, adopting the so-called "device-independent" framework. Indeed, this framework allows to perform information processing tasks without making any assumptions on the internal working of the involved devices, treating them as "black boxes". The quantum certification of device-independent protocols is guaranteed by the nonlocal character of the correlations between the inputs and outputs of those boxes. Unfortunately, demonstrating nonlocality is highly demanding from the implementation point of view, since low levels of experimental imperfections are tolerated. Those imperfections – *e.g.*noise and losses – may alter the input/output statistics, thus undermining the reliability of device-independent protocols. The experimental requirements for the security of device-independent protocols can be relaxed considering partly-device-independent scenarios, in which additional assumptions on the devices or the systems used in the protocols are made. Indeed, partly-device-independent protocols offer two main advantages: First, they are more secure than standard device-dependent protocols; second, they are in general more robust to experimental imperfections than their fully-device-independent counter-

parts. The general aim of this Thesis is to provide bounds on imperfections and losses arising in experimental implementations of device-independent and partly-device-independent protocols that are necessary or sufficient for security.

In the first part, we tackle the problem of secure implementation of quantum key distribution protocols in the device-independent and partly-device-independent scenarios. The goal is to establish conditions on the detection efficiency necessary for the security of those protocols. To this aim, we present a general attack on the detectors from which we derive bounds on the critical detection efficiency that do not depend on the number of measurements applied nor on the number of outcomes.

In the second part, we study randomness certification in the steering scenario and in the prepare-and-measure scenario. We devise an optimal method for quantifying the local and global randomness that can be extracted in both scenarios. Applying this method we provide sufficient conditions for randomness certification in presence of noise and losses. Moreover, we present a method that for any fixed state gives the optimal measurements and steering inequality that certify the most randomness.

The next question we address is the secure implementation of semi-device-independent protocols, whose quantum certification is provided by dimension witnesses. We study the problem of the robustness of device-independent dimension witnesses to loss, in the case in which shared randomness is allowed between the preparing and the measuring devices. The main result in this part is to provide thresholds for the critical detection efficiency necessary to perform reliable dimension witnessing. Furthermore, we study detection loophole attacks on semi-device-independent quantum and classical protocols in the case in which the preparing and measuring devices do not share pre-established correlations. We determine general conditions under which a potential eavesdropper cannot exploit the experimental losses to hack such protocols.

In the last part of the Thesis, we focus on a recently proposed quantum process and its inverse, namely the quantum state joining and splitting processes. In this context, we prove that a linear-optical realization of the quantum state joining of two photons relying only on post-selection – and thus simpler than the implementation originally proposed – is not possible, thus implying that such implementation requires at least one ancilla photon. Finally, we demonstrate that the quantum joining process is equivalent to the preparation of a particular class of three-qubit entangled states, showing that this process can also find application for generating complex cluster states of entangled photons.

List of publications

- A. Acín, D. Cavalcanti, E. Passaro, S. Pironio, and P. Skrzypczyk, "Necessary detection efficiencies for secure quantum key distribution and bound randomness".

  Physical Review A **93**, 012319 (2016)

- E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, "Optimal randomness certification in the quantum steering and prepare-and-measure scenarios".

  New Journal of Physics **17**, 113010 (2015)

- M. Dall'Arno, E. Passaro, R. Gallego, M. Pawłowski, and A. Acín, "Attacks on semi-device-independent quantum protocols".

  Quantum Information and Computation **15**, 0037 (2015)

- E. Passaro, C. Vitelli, N. Spagnolo, F. Sciarrino, E. Santamato, L. Marrucci, "Joining and splitting the quantum states of photons".

  Physical Review A **88**, 062321 (2013)

- M. Dall'Arno, E. Passaro, R. Gallego, and A. Acín, "Robustness of device-independent dimension witnesses".

  Physical Review A **86**, 042312 (2012)

Contents

List of acronyms

1SDI	One-Sided Device Independent
1SDIQKD	One-Sided-Device-Independent Quantum Key Distribution
CNOT	Controlled-NOT
r-CNOT	"reversed" Controlled-NOT
DI	Device Independent
DIDW	Device-Independent Dimension Witness
DIQKD	Device-Independent Quantum Key Distribution
DL	Detection Loophole
LHS	Local Hidden State
LHV	Local Hidden Variable
LOCC	Local Operations and Classical Communication
POVM	Positive Operator-Valued Measure
QKD	Quantum Key Distribution
QRAC	Quantum Random Access Code
QRG	Quantum Randomness Generation
RAC	Random Access Code
SDI	Semi-Device Independent
SDIQKD	Semi-Device-Independent Quantum Key Distribution
SDP	Semi-Definite Programme
TPES	Three-Photon Entangled State

Chapter 1

Introduction

In the last years, the distinguishing properties of quantum theory have been exploited to accomplish tasks which are unfeasible in classical theory. For example, protocols were proposed for secure quantum key distribution (QKD) [BB84, Eke91], quantum teleportation [BBC$^+$93, BPM$^+$97], and quantum randomness generation (QRG) [ROT94, FSS$^+$07, PAM$^+$10]. The first protocols to be proposed were device dependent, namely their success critically relies on the agreement between the description of the experimental setup and its implementation. But this hypothesis is never exactly fulfilled in practice, and a malicious adversary can exploit the mismatch between the theoretical description and the experimental implementation to hack the protocol.

Subsequently, device-independent (DI) protocols were proposed, in a framework where the devices are completely uncharacterized and the success of the protocol only depends on the statistics between inputs and outputs. This framework is highly suitable for adversarial scenarios, in which one would choose to adopt a paranoid attitude and avoid as many assumptions as possible, for instance in cryptographic protocols. But DI protocols, while extremely robust due to the fact that they rely on very few hypotheses, are very demanding from the experimental viewpoint. Indeed, realistic implementations of DI protocols are unavoidably subject to losses, and in this situation the given protocol is secure and reliable only when the so-called "detection loophole" is closed. In general, in order to close this loophole for DI quantum information protocols, the experimental devices need to exhibit very high detection efficiencies, which are too challenging for the current technology.

In order to overcome these problems, partly-DI protocols were recently introduced, which rely upon an intermediate level of trust between fully-DI and device-dependent protocols. Indeed, they depend on more hypotheses than fully DI protocols, but still do not assume a full characterization of the

involved devices and systems, as happens in device-dependent ones. Thus, partly-DI protocols constitute an opportunity to achieve a compromise between the assumptions under which they are valid and the level of losses they can tolerate.

1.1 Motivations and Results

In this Thesis we consider the problem of dealing with imperfections that are inevitably present in the implementation of DI and partly-DI quantum information protocols. Such imperfections, e.g. losses and noise, can tamper with the results of the given protocol causing misleading conclusions. For instance, in experimental implementations of quantum cryptographic protocols a malicious adversary can exploit the deviations from the theoretical model used to prove security. Therefore, it is crucial to ensure that those protocols cannot be sabotaged and to establish general conditions under which the imperfections arising in their experimental realizations are harmless. We examine this problem exploring different scenarios, such as the DI and partly-DI ones. Clearly, the optimal framework is the one that can guarantee the reliability of quantum information protocols making as few assumptions as possible. The requirements for the experimental implementation of DI protocols, which are very demanding for the current technology, can be relaxed considering partly-DI protocol, i.e. making some extra assumptions on the experimental devices. Recently, those scenarios have been investigated in order to look for the optimal trade-off between the assumptions made and the robustness of the protocol to experimental imperfections. This Thesis advances along these lines of research, investigating the amount of imperfections and losses that the implementation of DI and partly-DI quantum information protocols can tolerate.

1.1.1 Device-independent and partly-device-independent quantum key distribution protocols

Quantum key distribution (QKD) is one of the most remarkable applications of quantum physics. It allows secure communication between two distant parties guaranteed by the laws of quantum physics. Those laws ensure that the parties will be able to detect any attempt of eavesdropping by a potential external adversary. Unfortunately, when such protocols are implemented in the lab, due to unavoidable experimental imperfections they differ from the theoretical models used in the security proofs. An eavesdropper can then take advantage of the discrepancies to hack the cryptographic systems. Adopting

a device-independent (DI) framework, one can guarantee the security of a QKD protocol without relying on any assumptions about the internal working of the devices used in the protocol. The inconvenience is that, in order to exclude attacks on the detectors, DI QKD protocols require very high detection efficiencies. Indeed, especially in photonic implementations of DI and partly-DI QKD protocols the eavesdropper can exploit the losses to learn the key without being perceived. An example is the attack on the detectors recently demonstrated in [LWW$^+$10]. It is therefore necessary to establish experimental requirements for the implementation of secure QKD. More specifically, the issue we deal with is what amount of losses DI and partly-DI QKD protocols can tolerate. Another natural question is how much one can gain in terms of robustness to loss by considering partly-DI protocols with respect to their fully-DI counterparts.

Contributions

In Chapter 3 we present a general detection attack for QKD protocols. This attack applies to all protocols in which the key is constructed from the results of measurements performed by one of the parties on quantum particles that have propagated through an insecure channel. Therefore, it applies in particular to DI and partly-DI QKD protocols. From this attack we derive general bounds on the critical detection efficiencies needed for the security of this class of QKD protocols. Interestingly, the derived bounds do not depend on the dimension of the involved systems, nor on the number of performed measurements or the role of other parties in the protocol. They indicate that the implementation of partly-DI protocols are, in terms of detection efficiency, almost as demanding as fully-DI ones. The attack presented can be improved when considering specific protocols, as we illustrate for the case of two parties using untrusted measuring devices.

Moreover, we find out that this attack has a consequence also from a more fundamental point of view. Indeed, we show that it implies the existence of a very weak form of intrinsic randomness, which we name "bound randomness". This property emerges in nonlocal correlations for which a no-signalling eavesdropper cannot fix the results of all measurements in advance but she can find out a posteriori the results of any implemented measurements.

1.1.2 Randomness certification in the steering scenario

One of the most distinctive features of quantum mechanics is its intrinsically random character. While in classical mechanics lack of predictability can

always be attributed to ignorance or lack of control of the probed systems, the rules of quantum physics say that one cannot predict the outcome of a measurement even if all the variables of a system are known. This inherent unpredictability has been exploited in different applications such as quantum random number generation [ROT94] and quantum key distribution [SBPC$^+$09].

Recent results have shown that the randomness observed in quantum mechanics can be certified even without relying on any modelling of the quantum devices used for the generation of the random data - *i.e.* in a DI scenario - and therefore this is called DI randomness certification [Col06, PAM$^+$10]. In fact, by analyzing the data obtained in experiments involving local measurements on bipartite entangled systems one can prove that no one could have predicted this data in advance whenever a Bell inequality violation is observed [Bel64, BCP$^+$14]. Randomness certification has been studied also in partly-DI scenarios [LPY$^+$12, LTBS14], which involve some extra assumptions on the systems or the devices.

The so-called "steering" scenario is a partly-DI scenario that recently has been receiving lot of attention, since it allows for entanglement detection which is more robust to noise and experimental imperfections than Bell nonlocality [WJD07, QVC$^+$15]. It refers to the case where two parties apply local measurements on an unknown bipartite system. While one of them has complete knowledge of his measurement apparatuses, the other does not, and treats her measuring device as a black box with classical inputs and outputs. Indeed, quantum steering was initially introduced for entanglement certification when one of the parties is trusted but the other is not. Subsequently, it was shown to be useful for one-sided device independent quantum key distribution (1SDIQKD) [BCW$^+$12] and randomness certification [LTBS14].

The study of randomness certification in the steering scenario is important from a fundamental point of view in order to understand how much randomness can be maintained if we give up partial information about the specific description of the systems [LTBS14, BQB14, LPY$^+$12]. Furthermore, from a practical point of view the amount of randomness obtained in the steering scenario gives an upper bound to what would be obtained in a fully-DI setting, regardless of the number of measurements that the trusted party would apply.

Contributions

In Chapter 4 we provide a general and optimal method to quantify the amount of local or global randomness that can be certified from a single measurement in a steering experiment. Using this method we compute the

maximal amount of local and global randomness that can be certified by measuring systems subject to noise and losses. We show that local randomness can be certified from a single measurement if and only if the detectors used in the test have detection efficiency higher than 50%. These results can be easily extended beyond the steering scenario, namely to the prepare-and-measure scenario, where the state is also trusted, so that only the measuring device on one side is untrusted. In this case we show that even noisy states can perform very well for randomness certification.

Finally, we give a method to find the optimal steering inequality and the optimal measurements which obtain the most randomness from any fixed state. Using insight from this method, we demonstrate analytically that all pure partially entangled states lead to maximal randomness certification using only two fixed measurements.

1.1.3 Semi-device-independent protocols and device-independent dimension witnesses

The dimensionality of a system is regarded as a resource in quantum information processing. Indeed, higher-dimensional systems offer more degrees of freedom for the encoding of information. The Hilbert space dimension is usually intrinsic in the model considered for the description of the experimental setup. However, an interesting question in the DI framework is whether it is possible to derive some properties of non-characterized devices instead of assuming them, building only upon the knowledge of the correlations between preparations, measurements and outcomes. In general one could be interested in bounding the dimension of the systems prepared by a non-characterized device; one could also ask whether a source is intrinsically quantum or can be described classically. The framework of device-independent dimension witnesses (DIDWs) provides an effective answer to these questions, and is suitable for experimental implementation and for application in different contexts.

DIDWs are principally relevant for semi-device-independent (SDI) quantum protocols, which realize information tasks in a scenario where no assumption on the internal working of the devices used in the protocol is made, except their dimension. Those protocols are indeed based on the quantum certification provided by dimension witnesses for a fixed dimension. For instance, in [PB11] the authors present a quantum key distribution protocol whose security against individual attacks in a SDI scenario is based on DIDWs. Another example is given by quantum random access codes (QRACs), that make it possible to encode a sequence of qubits in a shorter

one in such a way that the receiver of the message can guess any of the original qubits with maximum probability of success. In [LPY+12, PZ10] QRACs were considered in the SDI scenario, with a view to their application in randomness expansion protocols. The classical analogous of SDI quantum protocols – namely, the case in which the exchanged system is classical – is known as the problem of random access codes (RACs) [ALMO08]. In the context of RACs, the aim of two distant parties is to optimally perform some one-sided communication task under a constraint on the amount of classical information exchanged.

Unavoidably, any implementation of protocols based on DIDWs is affected by experimental imperfections and losses. They can reduce the value of the dimension witness, thus making it impossible to witness the dimension of a system. In particular, in a cryptographic scenario a malicious provider could exploit the losses to skew the statistics of the experiment and ultimately fake its result. Therefore it is highly relevant to determine whether it is possible to perform reliable dimension witnessing in realistic scenarios and, in particular, with non-optimal detection efficiency.

Contributions

In Chapter 5 we tackle the problem of the robustness of DIDWs to losses. In particular, we consider the case where shared randomness between the preparing and the measuring device is allowed. First, we give a characterization of the sets of classical and quantum correlations obtained in this scenario with states of bounded dimension, which allow us to introduce DIDWs as tools to discriminate between these sets. Then, we provide the threshold for the detection efficiency that can be tolerated in dimension witnessing, both in the case where one is interested in lower bounding the dimension of the system as well as in the case where one is interested in discriminating between its quantum or classical nature.

In Chapter 6 we consider SDI classical and quantum protocols in the case in which the involved parties are not allowed to share pre-established correlations. In this case, the sets of d-dimensional classical correlations obtained are in general non-convex. We show that the exploitation of those non-convex sets allows dimension witnessing for an arbitrary non-zero value of the detection efficiency. Moreover, we provide general conditions under which a malicious provider cannot take advantage of the detection inefficiencies to fake the performance of SDI quantum protocols. For classical protocols, we provide conditions under which the worst case success probability of a RAC cannot be increased resorting to the exploitation of losses.

1.1.4 Joining and splitting the quantum states of photons

Quantum information technology promises a great enhancement of the computational power at our disposal, as well as perfectly secure transmission of information [BD00, Ser06, LJL+10]. To turn this vision into a reality, one of the greatest challenges today is to substantially increase the amount of information – the number of qubits – that can be processed simultaneously. In photonic approaches [KMN+07, OFV09, PCL+12], the number of qubits can be raised by increasing the number of photons. This is a fully scalable method, in principle, but in practice it is limited to 6-8 qubits by the present technology [YWX+12]. An alternative approach is that of using an enlarged quantum dimensionality within the same photon, for example by combining different degrees of freedom, such as polarization, time-bin, wavelength, propagation paths, or transverse modes such as orbital angular momentum [MVWZ01, BLPK05, MTTT07, LBA+09, CVDM+09, NSM+10, SK10, NGM+10]. Although not scalable, the latter approach may allow for a substantial increase in the number of qubits [GLY+10, Pil11, DLB+11, MSD+12]. Ideally, one would therefore like to combine these two methods and be able to dynamically switch from one to the other, depending on the specific needs, even during the computational process itself.

To this purpose, a quantum process called "quantum state joining" has been recently introduced and experimentally demonstrated [VSA+13]. This process consists in combining two arbitrary qubits initially encoded in separate input photons into a single output photon, within a four-dimensional quantum space. The inverse process was also proposed, in which the four-dimensional quantum information carried in a single input photon is split into two output photons, each carrying a qubit [VSA+13]. Both processes are in principle iterable, and hence may be used to realize an interface for converting a multi-photon encoding of quantum information into a single-photon higher-dimensional one and vice versa, thus enabling a full integration of the two encoding methods. These processes allow to multiplex and demultiplex the quantum information in photons, for instance to employ a smaller number of photons in lossy transmission channels. In addition, the quantum joining and splitting processes might also find application in the interfacing of multiple photonic qubits with a matter-based quantum register [JSC+04], another crucial element of future quantum information networks [Kim08]. For example, interfacing with multilevel quantum registers [GBR+06] may be facilitated by the quantum joining/splitting schemes.

The scheme used in [VSA+13] for the experimental demonstration of quantum joining is based on a double CNOT gate and a final projection.

In general, there exist other schemes for applying several CNOT gates in sequence [Ral04] which are experimentally less demanding than the one used in [VSA+13]. It is then natural to try an implementation exploiting these methods for the CNOT-based general scheme for quantum state joining. More generally, one might ask whether it is possible to implement the quantum joining process with a simpler linear-optical setup.

Contributions

In Chapter 7 we study the process of joining and splitting the states of photons from a theoretical point of view. We introduce some variants of the original schemes which do not need a projection and feed-forward mechanism to work (not considering the CNOT implementation), although at the price of using a doubled number of CNOT gates. We formally prove that quantum joining is impossible to achieve with an arbitrary linear optical scheme involving only two photons and a final postselection step. Hence, at least one ancilla photon is needed (or the presence of optical nonlinearity). Furthermore, we analyze the relationship between the joining process of two photonic qubits and a particular class of three-photon entangled states, in which two photons are separately entangled with a common "intermediate" photon. We show that the quantum joining process can be used to create such cluster states and that, conversely, the quantum joining of two photons can be immediately achieved by a teleportation scheme using a three-photon entangled state of this class.

Chapter 2

Background

In this Chapter we define some background notions and we analyze in detail the different scenarios studied in this Thesis.

First, we introduce the device-independent (DI) scenario, which allows to authenticate the trustworthiness of a protocol relying upon as few assumptions as possible. In this case, the quantum certification required to authenticate DI quantum protocols is provided by Bell inequalities. We furthermore describe the so-called "loopholes" arising in Bell experiments.Then, we define the "steering" scenario, in which one of the parties has a complete characterization of the behaviour of his devices, while the other is treated in a DI way, *i.e.* as a black box. The quantum certification in this case is provided by steering inequalities. Subsequently, we describe another partly-DI scenario that is the "semi-device-independent" (SDI) framework, in which one makes an assumption on the dimensionality of the physical systems shared by the parties while the devices are uncharacterized. The quantum certification needed for the reliability of SDI protocols is provided by dimension witnesses. We then introduce the notion of intrinsic randomness, which represents a crucial resource for several applications, such as quantum key distribution, gambling or numerical simulations. Finally, we describe the recently demonstrated processes of quantum state joining and splitting. These processes allow to transfer the quantum information initially encoded in two separate input systems into a single output system within a higher-dimensional quantum space, and vice versa.

2.1 Device-independent scenario

The device-independent (DI) scenario is a framework in which no assumptions are made on the internal working of the devices, nor on the physical

systems shared by the involved parties. In this scenario all the N measuring devices are treated as black boxes which receive some classical input $x_i \in \{1, \ldots, m\}$ and produce a classical output $a_i \in \{1, \ldots, d\}$, for $i = 1, \ldots, N$ (see Fig. 2.1). The relevant object in this scheme is the conditional probability distribution $P(a_1, \ldots, a_N | x_1, \ldots, x_N)$ of obtaining outcomes $a_1, \ldots, a_N$ when inputs $x_1, \ldots, x_N$ are provided. Although no assump-

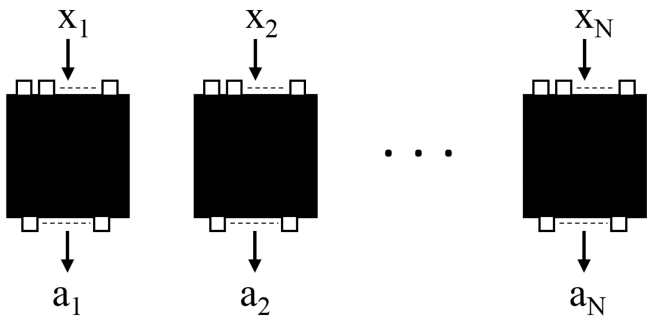

Figure 2.1: In the device-independent scenario the N measuring devices are treated as black boxes. Every box receives a classical input $x_i \in \{1, \ldots, m\}$ and produces a classical output $a_i \in \{1, \ldots, d\}$, for $i = 1, \ldots, N$.

tion is made on the devices, in the DI approach other assumptions are usually required, namely the measurement independence and no-signalling assumptions:

- **Measurement independence.**

  This assumption states that the choices of which measurements to perform have to be random and completely uncorrelated with any other variable. Mathematically, it implies that every input choice x_i is independent of any variable λ lying outside the future light cone of x_i, *i.e.* $p(x_i|\lambda) = p(x_i)$. This assumption is also commonly called *free will* assumption, since it states that the inputs $x_1, \ldots, x_N$ must be freely chosen by the parties. Conversely, if the measurement settings are determined in advance, the obtained correlations cannot provide a DI quantum certification. Recently, it was proved that in some contexts it is possible to relax the measurement independence assumption and still perform DI protocols considering only a small amount of measurement independence [PRB+14].

- **No-signalling principle.**

  This principle states that the input choice on one site cannot influence the statistics observed at a distant site. The no-signalling assumption is formally expressed by the following constraints on the conditional probability distribution:

$$\begin{aligned} &\sum_{a_i} P(a_1, \ldots, a_i, \ldots, a_N | x_1, \ldots, x_i, \ldots x_N) \\ =&\sum_{a_i} P(a_1, \ldots, a_i, \ldots, a_N | x_1, \ldots, x_i', \ldots x_N), \end{aligned} \tag{2.1}$$

  for all a_i, x_i for $i = 1, \ldots, N$. The constraints (2.1) allow the definition of the marginal probability distributions observed by the N parties. The no-signalling assumption is physically motivated by special relativity, which prevents faster-than-light communication. Indeed, if the measurements performed by two distant observers are space-like separated, then the no-signalling constraints (2.1) guarantee that the observers cannot use their black boxes for sending information instantaneously.

In the following of this Thesis, we assume that measurement independence and the no-signalling principle hold.

2.1.1 Bell nonlocality

Here we introduce the concepts of nonlocality and nonlocal correlations. For this purpose, let us consider the following setup. Consider a source which sends a physical system to each of two observers, called Alice and Bob, located far apart from each other. The observers perform measurements on the received systems adopting the DI scenario: they randomly choose a measurement – labeled x for Alice, y for Bob – and register their outcome, denoted a for Alice and b for Bob, as depicted in Fig. 2.2. We suppose that Alice and Bob cannot communicate to each other during the measurement stage. The validity of this assumption can be ensured by shielding their devices or by placing their laboratories sufficiently far away such that the events corresponding to their measurements are space-like separated (therefore signalling is impossible according to the no-signalling principle). Nevertheless, we assume that their boxes are allowed to share a predetermined strategy.

The aim of the two parties is to construct the conditional probability distribution $P(a, b|x, y)$ of obtaining outcomes a and b when measurements x and y are chosen. This distribution can be computed in a frequentist

manner from the statistics of inputs and outputs collected in different runs of the experiment under the *i.i.d.* assumption, i.e. that one can reproduce independent and identically distributed copies of the experiment. The whole procedure is called a Bell experiment.

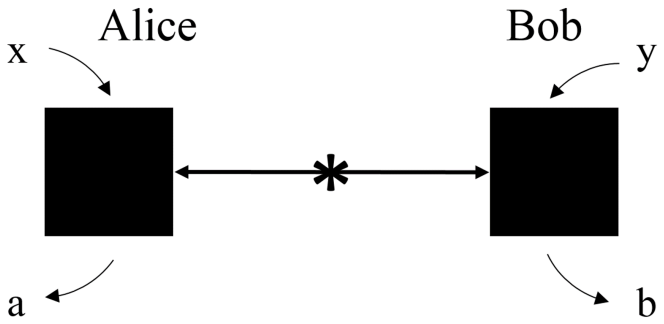

Figure 2.2: Bell experiment: Alice and Bob have two black boxes which perform measurements x and y on the received systems obtaining outcomes a and b, respectively. After repeating this procedure a large number of times, they collect the statistics to construct the conditional probability distribution $P(a, b|x, y)$.

If Alice and Bob had previously agreed on a common strategy, then all the possible conditional probability distributions that they can achieve classically can be written as

$$P(a, b|x, y) = \int d\lambda \, \rho(\lambda) P(a|x, \lambda) P(b|y, \lambda). \tag{2.2}$$

In (2.2) the variable λ (usually called "hidden variable") takes into account the shared randomness between Alice and Bob, $\rho(\lambda)$ is the probability distribution from which λ is drawn, and $P(a|x, \lambda)$ $[P(b|y, \lambda)]$ is the probability of obtaining outcome a (b) given input x (y) and hidden variable λ. A bipartite probability distribution that can be written as in (2.2) is said to have a local hidden variable (LHV) model. Conversely, if $P(a, b|x, y)$ cannot be written as in (2.2) the correlations measured cannot be explained by a LHV model and therefore they are called "nonlocal".

In general, a Bell experiment can be extended to more than two parties and it is defined by the triple (N, m, d), where N denotes the number of parties, m is the number of possible inputs for each party, and d is the number of outcomes. From a geometrical point of view, the conditional probability distributions $P(a_1, \ldots, a_N|x_1, \ldots, x_N)$ that can be observed in a

(N, m, d) Bell experiment can be considered as vectors in the Euclidean space $\mathbb{R}^{md^N}$. In this space, the set of all local conditional probability distributions obtainable in a (N, m, d) Bell experiment is characterized by a finite set of linear inequalities and is represented with a polytope – i.e. a convex set with a finite number of extreme points – which is usually referred to as *local polytope* (see Fig.2.3).

Another interesting set in this space is the set of quantum correlations achievable in a (N, m, d) Bell experiment. A conditional probability distribution $P(a_1, \ldots, a_N|x_1, \ldots, x_N)$ is quantum if there exist a quantum state and quantum measurements that reproduce it, according to the Born rule [NC00]:

$$P(a_1, \ldots, a_N|x_1, \ldots, x_N) = \mathrm{Tr}[\rho\, M_{x_1}^{a_1} \otimes \ldots \otimes M_{x_N}^{a_N}]. \tag{2.3}$$

In the last equation, ρ is a positive operator of unit trace acting on a Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_\mathcal{N}$. The measurement operators $M_{x_i}^{a_i}$ represent Positive Operator-Valued Measure (POVM) elements [NC00], *i.e.* positive operators acting on $\mathcal{H}_i$, fulfilling $\sum_{a_i} M_{x_i}^{a_i} = \mathbb{1} \quad \forall x_i,\, i \in 1, \ldots, N$. These conditions guarantee that the conditional probability distribution is positive and normalized. Geometrically, the set of quantum correlations is represented by a convex set with infinite extreme points. Therefore, unlike the local set, the quantum set is not a polytope and cannot be characterized with a finite set of linear inequalities.

In general, since every well-defined probability distribution has to be positive and normalized, a conditional probability distribution arising in a (N, m, d) Bell experiment must satisfy the following constraints:

- Positivity

$$P(a_1, \ldots, a_N|x_1, \ldots, x_N) \geq 0 \qquad \forall a_1, \ldots, a_N, x_1, \ldots, x_N$$

- Normalization

$$\sum_{a_1, \ldots, a_N} P(a_1, \ldots, a_N|x_1, \ldots, x_N) = 1 \qquad \forall x_1, \ldots, x_N$$

The set that includes all the correlations satisfying those constraints and the no-signalling conditions (2.1) is a polytope called *no-signalling* polytope (see Fig. 2.3).

Geometrically, the non-trivial facets of the local polytope L are described by the so-called *Bell inequalities* and divide the local set from the nonlocal one. It can be proved that quantum correlations described by (2.3) can violate a Bell inequality and therefore can exhibit nonlocality. An example of

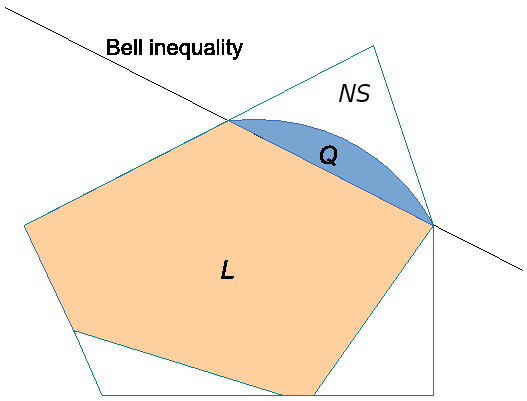

Figure 2.3: Geometrical representation of the probability space arising from a Bell experiment. The local polytope L is strictly contained in the quantum set Q, which is a convex set with infinite extreme points. The facets dividing the sets of local and nonlocal correlations correspond to tight Bell inequalities. The no-signalling polytope NS strictly contains the quantum set Q.

quantum correlations which are nonlocal will be given in 2.1.3. This means that the local polytope L is strictly contained in the set Q of quantum correlations. Thence, there exist correlations arising from quantum physics which do not admit a LHV model. Precisely, the quantum certification needed in the DI scenario to guarantee the "quantumness" of the correlations is given by the violation of a Bell inequality. Since quantum theory is no-signalling, the set Q of quantum correlations is contained in the no-signalling polytope. In [PR94] Popescu and Rohrlich identified the existence of no-signalling correlations which are super-quantum (*i.e.* , they are not in the quantum set), thus proving the strict inclusion of the quantum set Q into the no-signalling polytope.

2.1.2 Entanglement

Let us consider a system made up of N subsystems. The quantum state $\rho \in \mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_\mathcal{N}$ describing such a system is said to be *entangled* if it cannot be written as a convex combination of product states, i.e.

$$\rho = \sum_i p_i \, \rho_1^{(i)} \otimes \rho_2^{(i)} \otimes \cdots \otimes \rho_N^{(i)}, \tag{2.4}$$

where $\rho_i \in \mathcal{H}_i$ is the quantum state of the i-th subsystem. Conversely, if the state ρ can be written as (2.4), it is said to be *separable*. The operational meaning of this definition is that a multipartite state is separable if and only if it can be prepared by the parties using only local operations and classical communication (LOCC). Therefore, the preparation of entangled states requires global operations due to interactions between subsystems. For instance, entanglement can arise when two quantum states are produced from a common source.

It is worth mentioning that some entangled states can lead to nonlocal correlations when submitted to a Bell experiment. More precisely, while entanglement is necessary to give rise to nonlocal correlations the converse is not true, i.e. not all entangled states are nonlocal [Wer89].

2.1.3 CHSH inequality

In the simplest bipartite Bell scenario, *i.e.* the one where each of the two parties can perform two measurements with two possible outcomes, the only non-trivial facet of the local polytope is described by the so-called Clauser-Horne-Shimony-Holt (CHSH) inequality [CHSH69]. The CHSH scenario is the standard example to demonstrate that there are quantum correlations that are nonlocal. Let us denote by $x, y \in \{0, 1\}$ the measurement choice of the parties Alice and Bob, respectively. The corresponding outcomes are labelled $a_x, b_y \in \{-1, 1\}$. We consider now the correlator defined as

$$\langle A_x B_y \rangle = \sum_{a,b} abP(ab|xy).$$

It can be easily checked that the following inequality

$$\langle A_0 B_0 \rangle + \langle A_1 B_0 \rangle + \langle A_0 B_1 \rangle - \langle A_1 B_1 \rangle \leq 2,$$

which is the famous CHSH inequality, must hold for any local correlations satisfying (2.2).

It can be proved that the CHSH inequality is violated by the correlations obtained performing measurements $\{M_x^a\}$ for Alice and $\{N_y^b\}$ for Bob, where

$$M_0^a = \frac{\mathbb{1}_2 + a\sigma_x}{2}, \quad M_1^a = \frac{\mathbb{1}_2 + a\sigma_z}{2},$$
$$N_0^b = \frac{\mathbb{1}_2 + b\sigma_+}{2}, \quad N_1^b = \frac{\mathbb{1}_2 + b\sigma_-}{2},$$

and $\sigma_\pm = (\sigma_x \pm \sigma_z)/\sqrt{2}$, on the two-qubit maximally entangled state

$$|\Phi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Indeed, calculating the corresponding conditional probability distribution $P(ab|xy)$ according to the quantum theory prescription (2.3), one finds for the CHSH expression the value $2\sqrt{2}$. Therefore, this proves the existence of quantum correlations that cannot be described by a LHV model.

In 1983, it was shown by Cirel'son [Cir80] that the maximal value achievable by quantum mechanics for the CHSH expression is given by $2\sqrt{2}$, for all states and measurements in any possible Hilbert space.

2.1.4 Loopholes in Bell experiments

In any implementation of DI quantum protocols one cannot avoid technical imperfections that can affect the validity of the results of the Bell test, which is required as quantum certification in a DI scenario. Indeed, there can be unintended circumstances that open the possibility to reproduce an observed violation of a Bell inequality with a LHV models. These situations are usually referred to as "loopholes". In the following we introduce briefly the main loopholes arising in the implementation of a Bell test.

Locality loophole

One of the assumptions of the Bell test is the absence of communication between the two measurement sites. In practice, this is usually ensured by forbidding any light-speed communication, positioning the two sites at a distance such that the measurement events are space-like separated. This means that the measurement duration has to be shorter than the time it would take for a light-speed signal to travel from one site to the other. When this requirement is not satisfied, the so-called *locality loophole* arise. In this case nothing prevents a signal in carrying influence from the remote setting to the local outcome, which provides a LHV explanation for the results of the Bell experiment.

Moreover, according to the measurement independence assumption, the choices of which measurements to perform have to be random and uncorrelated with the hypothetical hidden strategy. Thence, in order to draw correct conclusions on the nonlocal nature of the observed correlations, one has also to exclude that the choice of measurement settings on one side is influenced by an earlier event that could be correlated to the choice on the other side. This means that the measurement choices must be free of any potential influence by the event which created the two entangled systems in the first place. For this reason, the loophole that occurs when this condition cannot be ensured is commonly called *freedom of choice loophole*.

Detection loophole

In realistic implementations of Bell experiments it is common that some particles emitted by the source will not be detected, especially in photonic experiments. Hence, in Bell-based protocols the subset of detected particles might display correlations that violate a Bell inequality although the entire ensemble can be actually described by a LHV model. Then a malicious adversary may exploit the inefficiencies of the untrusted devices to produce a Bell inequality violation with local correlations, thus faking the success of the protocol. This circumstance, arising when the efficiency of the detectors is not perfect, is commonly referred to as *detection loophole*.

Due to experimental limitations, often the *fair sampling* assumption has been invoked to justify the results of a Bell test performed with inefficient detectors. This assumption states that the sample of the detected events accurately represents the entire ensemble. Making the fair sampling assumption, the experimenters are therefore allowed to discard the rounds in which they observed undetected events. In DI cryptographic protocols this assumption is generally avoided, since it opens the possibility of malicious attacks [LWW$^+$10].

To achieve a conclusive Bell violation without assuming that the detected particles are a "fair" sample, a highly efficient experimental setup is necessary. For instance, in order to demonstrate a conclusive violation of the CHSH inequality with a two-qubit maximally entangled state the detection efficiency has to be higher than 82.8% [GM87], which makes Bell-based protocols very demanding experimentally. In 1993, Eberhard [Ebe93] showed that this critical efficiency can be lowered by considering non-maximally entangled states, reaching the lowest critical efficiency of 66.7% for slightly entangled states. Hence, if the experimenters do not want to rely on the fair sampling assumption, they cannot simply post-process the obtained statistics discarding all the events in which one or both detectors did not click. It is required instead that the efficiency of their detectors must be higher than a certain threshold, depending on the particular scenario, in order to prevent the detection loophole.

One approach to deal with the losses in the experiment is to map every no-click event into one of the possible outcomes of the measuring device. However, if the parties have access to the full statistics it is more convenient to model the experimental losses keeping track of the non-detected events by adding another output to the statistics - the no-click outcome $\emptyset$ - in order to exploit all the available information.

In the following of this Thesis we will address the problem of experimental losses for different DI and partly-DI protocols, deriving bounds on the critical

detection efficiencies necessary for their reliability.

2.2 Steering scenario

The steering scenario [Sch35] is a framework with an intermediate level of trust between the device-dependent and the fully-DI scenario. The scenario considered is the following [WJD07]: two parties, Alice and Bob, are located in distant laboratories and receive an unknown bipartite system from a common source. One of the two parties, say Alice, does not trust her measuring devices, which are treated as "black boxes", *i.e.* in a DI way. She can, nevertheless, choose which measurement to perform, which she labels by $x \in \{1, \ldots, m\}$, each of which provides an outcomes, which she labels $a \in \{1, \ldots, d\}$. The other party, Bob, has complete knowledge of his measuring devices, which allow him to perform quantum state tomography on his part of the system, and thus to obtain a complete description of his subsystem (see Fig.2.4). Therefore, in addition to the assumptions of the DI scenario, in the steering scenario we assume furthermore that Bob has a complete characterization of his quantum devices.

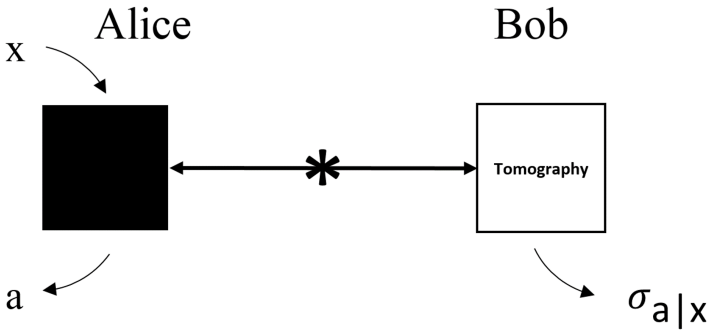

Figure 2.4: Steering scenario: Alice and Bob measure an unknown bipartite system received by an untrusted source. Alice treats her measurement device as a black box with inputs $x \in \{1, \ldots, m\}$ and outputs $a \in \{1, \ldots, d\}$. On the other hand, Bob trusts his device and performs quantum state tomography on his subsystem, obtaining a complete characterization of the assemblage $\sigma_{a|x}$.

Quantum steering was first introduced in the context of entanglement certification with an untrusted party [WJD07]. In the original scheme the aim of the untrusted party Alice is to convince Bob that their systems are

entangled by showing him that she can affect – or steer – the state of Bob's subsystem by making measurements on her part of the system. We notice that the scenario considered in this Thesis differs from the original "steering game" of [WJD07], where Bob tells Alice which measurement he wants her to perform. In fact, the present context is closer to the Bell scenario, with the only difference that Bob now trusts his devices. For this reason, quantum information protocols adopting this scenario are called one-sided device independent (1SDI).

The states reconstructed by Bob will usually depend on Alice's input and output as $\rho_{a|x} = \mathrm{Tr}_{\mathrm{A}}[(M_{a|x} \otimes \mathbb{1}_{\mathrm{B}})\rho_{\mathrm{AB}}]/P(a|x)$, where ρ_{AB} is the unknown state of the system shared with Alice, $P(a|x)$ is the probability that Alice observes outcome a given she chose x, and $M_{a|x}$ is the corresponding (unknown) element of Alice's measurement. The set of unnormalized states

$$\sigma_{a|x} = \mathrm{Tr}_{\mathrm{A}}[(M_{a|x} \otimes \mathbb{1}_{\mathrm{B}})\rho_{\mathrm{AB}}] = \rho_{a|x}P(a|x) \tag{2.5}$$

is called an *assemblage* and can be completely determined by Bob through tomographic measurements.

As noticed in [WJD07], Bob can determine if ρ_{AB} is entangled by looking at the form of the assemblage $\{\sigma_{a|x}\}_{a,x}$. This is because separable states can only lead to assemblages with the specific form

$$\sigma_{a|x} = \sum_{\lambda} q(\lambda)P(a|x,\lambda)\sigma_{\lambda}, \tag{2.6}$$

where λ is a hidden variable distributed according to $q(\lambda)$, which determines both Alice's response $P(a|x,\lambda)$, and the states sent to Bob, σ_{λ}. Assemblages of this form are said to have a Local Hidden State (LHS) model. On the contrary, quantum states leading to assemblages that cannot be decomposed as in (2.6) are said to be steerable. In [WJD07] the authors proved that steerable states are a strict subset of entangled states. Moreover, they proved that all the states that can exhibit Bell nonlocality are steerable, but the converse is not true. Any assemblage which cannot be decomposed as (2.6) can be detected through the violation of a steering inequality [CJWR09] (similar to a Bell inequality or an entanglement witness) or a simple semidefinite program [Pus13]. A steering inequality is of the form

$$\sum_{a,x} \mathrm{Tr}[F_{a|x}\,\sigma_{a|x}] \leq B_{\mathrm{LHS}}, \tag{2.7}$$

where $F_{a|x}$ denotes the observable measured by Bob when Alice performs measurement x and announces outcome a, and B_{LHS} is the bound that can

be attained with assemblages admitting a LHS model. Therefore, the quantum certification required for protocols adopting the steering framework is the violation of a steering inequality which not only guarantees that the shared state is entangled, but also that Alice is performing incompatible measurements [QVB14, UMG14].

Moreover, quantum steering was shown to be useful for one-sided device independent quantum key distribution (1SDIQKD) [BCW$^+$12] and randomness certification [LTBS14]. We investigate randomness certification in the steering scenario in presence of noise and losses in Chapter 4, where we additionally consider a prepare-and-measure version of this scenario, namely in which Bob holds the source and therefore knows the state ρ_{AB} of the shared system.

2.3 Semi-device-independent scenario

Recently, the semi-device-independent (SDI) scenario was introduced as an intermediate solution between the device-dependent and the fully-DI scenario. In the SDI scenario no assumption on the internal working of the devices used in the protocol is made, except their dimension.

The general structure of a SDI protocol is given by a preparing device (let us say on Alice's side) and a measuring device (on Bob's side) as in Fig. 2.5. In the most general scenario, the devices may share a priori correlated information, classical and quantum. However, in many realistic situations, one can assume that the preparing and measuring devices are uncorrelated and that all the correlations observed between the preparation and the measurement are due to the mediating particle connecting the two devices. An intermediate and also valid possibility is to assume that the devices only share classical correlations. In this case, the value of a random variable λ distributed according to the distribution q_λ is accessible to preparing and measuring devices. In this Section we focus on this last possibility, leaving the discussion of the case in which the preparing and measuring devices are uncorrelated to Chapter 6.

Alice chooses input $x \in \{1, \ldots, M\}$ and sends a fixed state $\rho_{x,\lambda} \in \mathcal{B}(\mathcal{H})$ to Bob, where $\mathcal{B}(\mathcal{H})$ denotes the space of linear operators $X : \mathcal{H} \to \mathcal{H}$. The assumption made in a SDI scenario is that the Hilbert space $\mathcal{H}$ on which $\rho_{x,\lambda}$ acts has a fixed dimension $d = d^*$ (or its dimension is assumed to be bounded by a given value d^*). Bob chooses the value of index $y \in \{1, \ldots, K\}$ and performs a fixed POVM $\Pi_{y,\lambda}$ on the received state, obtaining outcome $b \in \{1, \ldots, N\}$. After repeating the experiment several times (we consider the asymptotic case), they collect the statistics about indexes x, y, b obtaining

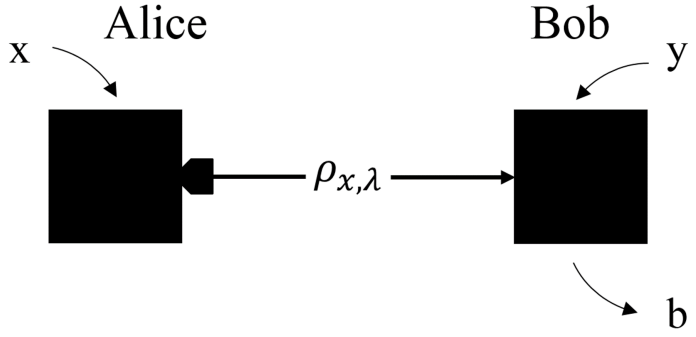

Figure 2.5: Setup for a generic SDI protocol. Two distant parties Alice and Bob are provided a black box each. Alice's box is a preparing device which sends the state $\rho_{x,\lambda}$ to Bob whenever Alice presses button $x \in \{1, \ldots, M\}$. Bob owns a measuring device that performs measurement $\Pi_{y,\lambda}$ on the received state whenever Bob presses button $y \in \{1, \ldots, K\}$, giving the outcome $b \in \{1, \ldots, N\}$. In the most general scenario, the preparing and measuring devices share a hidden random variable λ.

the conditional probabilities $P(b|x, y)$. The goal of a SDI protocol is to exploit the correlations between the two parties, encapsulated by $P(b|x, y)$, to accomplish an information task, e.g. to distribute a secure key or generate random numbers.

The quantum certification required to ensure the reliability of SDI protocols is provided by device-independent dimension witnesses (DIDWs) for a fixed dimension [GBHA10]. Indeed, DIDWs provide a tool to distinguish between classical and quantum systems of the same dimension. These witnesses were first introduced in [BPA$^+$08] in order to characterize the dimensionality of an unknown physical system building only on the knowledge of the observed correlations $P(b|x, y)$.

Let us denote with $\mathcal{C}_{d^*}$ the set of correlations that can be obtained by measuring classical states of dimension $d = d^*$ in a scenario with M preparations and K measurements with N outcomes. We say that a set $R = \{\rho_i\}$ of states is classical when the states commute pairwise, $[\rho_i, \rho_k] = 0$ for any i, k [HGM$^+$12, ZPWL11, LLF11, HSS07, HHHP06]. We notice that, when shared randomness is allowed between preparations and measurements, the set of achievable correlations is convex. This is not true in the case in which the preparing and measuring devices are not allowed to share pre-established correlations. We will analyze both cases in Chapter 5 and 6, respectively.

A DIDW $W_{\mathcal{C}_{d^*}}(P)$ is defined as a function of the conditional probability distribution $P = \{P(b|x,y)\}$ such that

$$W_{\mathcal{C}_{d^*}}(P) \leq L_{d^*} \qquad \forall\, P \in \mathcal{C}_{d^*}, \tag{2.8}$$

for some L_{d^*} depending on $W_{\mathcal{C}_{d^*}}$. This means that, once the dimensionality of the shared systems is assumed in a SDI protocol, a violation of (2.8) certifies that the observed correlations $P(b|x,y)$ cannot have been produced with classical systems.

SDI protocols based on DIDWs have been introduced recently, such as SDI quantum key distribution [PB11] and SDI randomness expansion [LPY$^+$12].

2.4 Randomness

Quantum mechanics predicts the existence of intrinsically random processes. Contrary to classical randomness, this lack of predictability cannot be attributed to ignorance or lack of control. It turns out that the notions of randomness and nonlocality are connected to each other: It can be proved [MAG06] that all no-signalling deterministic distributions are local. Indeed, a deterministic conditional probability distribution $P_{\mathrm{DET}}(a,b|x,y)$ can be written as a mixture of deterministic correlations $D(a,b|x,y)$, *i.e.* in which a and b are deterministic functions of x and y:

$$P_{\mathrm{DET}}(a,b|x,y) = \sum_{\lambda} p(\lambda) D_\lambda(a,b|x,y).$$

Imposing the no-signalling conditions on $D_\lambda(a,b|x,y)$, one has that a is a deterministic function of x only, and respectively b is a deterministic function of y only: $D_\lambda(a,b|x,y) = D_\lambda(a|x)D_\lambda(b|y)$. This implies that

$$P_{\mathrm{DET}}(a,b|x,y) = \sum_{\lambda} p(\lambda) D_\lambda(a|x) D_\lambda(b|y),$$

which shows that $P_{\mathrm{DET}}(a,b|x,y)$ admits a LHV model. Therefore, all no-signalling nonlocal correlations are intrinsically random.

Using this relation between randomness and nonlocality, recent results have shown that by analyzing the data obtained in experiments involving local measurements on bipartite entangled systems one can prove that no one could have predicted this data in advance whenever a Bell inequality violation is observed [Bel64, BCP$^+$14]. This protocol is called DI randomness certification [Col06, PAM$^+$10], since randomness can be certified without

relying on any modelling of the quantum devices used for the generation of the random data - *i.e.* in a DI scenario.

Here we introduce the framework used for DI randomness certification [NSPS14, BSS14]. Let us consider a Bell scenario in which two distant parties Alice and Bob want to extract private randomness from the outcomes obtained performing untrusted measurements on their shared system. We deal with the adversarial scenario – which is relevant for cryptographic tasks – where a potential eavesdropper, Eve, wants to predict the boxes' outcomes.

In the most general case, we do not make any assumption on the measurement devices, so that they could even have been provided by Eve. We also consider that the state ρ_{AB} of the system shared by the honest parties is the reduced state of a tripartite entangled state ρ_{ABE} shared by Alice, Bob and Eve, *i.e.* $\rho_{\mathrm{AB}} = \mathrm{Tr}_{\mathrm{E}}[\rho_{\mathrm{ABE}}]$. Hence, by applying measurements to her subsystem Eve can in principle obtain information about Alice and Bob's outcomes (a, b). For any quantum realization of the conditional probability distribution observed by the parties, any strategy of Eve can be seen as a POVM measurement [NC00] with elements $\{M_z^e\}$ that she applies on her reduced state $\rho_E = \mathrm{Tr}_{\mathrm{AB}}[\rho_{\mathrm{ABE}}]$.

Local randomness

We describe in the following how to quantify the local randomness associated with Alice's output a when a certain input $x = x^*$ is used. The amount of local randomness in Alice's outcome can be quantified by the *guessing probability*, that is the probability that Eve can guess correctly the outcome a of the measurement x^* of Alice using an optimal strategy. This quantity, denoted $P_{\mathrm{guess}}(x^*)$, is the probability that Eve's guess e is equal to the outcome a that Alice obtained, whenever Alice performs the specific measurement $x = x^*$, *i.e.*

$$P_{\mathrm{guess}}(x^*) = \sum_e P_{\mathrm{A}}(a = e|x^*)\, P_{\mathrm{E}}(e|a = e, z, x = x^*).$$

Applying Bayes theorem and the no-signalling constraints, namely that the marginal probability distribution for Alice do not depend on Eve's input z, this is equivalent to the joint probability that Alice and Eve give the same outcome whenever Alice performs measurement $x = x^*$:

$$P_{\mathrm{guess}}(x^*) = \sum_e P_{\mathrm{AE}}(a = e, e|z, x = x^*). \tag{2.9}$$

One can also express the guessing probability as as an average over Alice's probabilities conditioned on Eve's outcomes, *i.e.*

$$P_{\text{guess}}(x^*) = \sum_e P_{\text{E}}(e|z)\, P_{\text{A}}(a = e|e, z, x = x^*).$$

Conditioning on Eve's outcome defines a family of unnormalized conditional probability distributions, given by

$$\widetilde{P}_{e,z}(a, b|x, y) = P_{\text{E}}(e|z) P_{\text{AB}}(a, b|x, y, e, z),$$

such that averaging over these distributions one recovers the conditional probability distribution for Alice and Bob: $\sum_e \widetilde{P}_{e,z}(a, b|x, y) = P_{\text{AB}}(a, b|x, y)$.

In order to compute the optimal strategy for Eve, one has to maximize her guessing probability $P_{\text{guess}}(x^*)$ over all possible strategies (given by Eve's POVM elements $\{M_z^e\}$) and all possible quantum realizations compatible with the conditional probability distribution observed in the experiment. This would appear to consist in optimizing the set $\{\rho_{\text{ABE}}, M_x^a, M_y^b, M_z^e\}$ of state and measurements for Alice, Bob and Eve, which is a non-linear optimization problem. However, it has been showed [NSPS14, BSS14] that one can instead replace this by an equivalent linear optimization over all unnormalized quantum distributions $\widetilde{P}_e(a, b|x, y)$ that lead to the conditional probability distribution $P^{\text{obs}}(a, b|x, y)$ observed by Alice and Bob. More precisely, the maximization problem can be formulated as the following semidefinite programme (SDP) [BV04]:

$$\begin{aligned} \max_{\widetilde{P}_e} \quad & P_{\text{guess}}(x^*) = \textstyle\sum_e \widetilde{P}_a(a|x^*) \\ \text{subject to} \quad & \textstyle\sum_e \widetilde{P}_e(a, b|x, y) = P^{\text{obs}}(a, b|x, y) \quad \forall\, a, b, x, y \\ & \widetilde{P}_e(a, b|x, y) \text{ is quantum} \qquad \forall e. \end{aligned} \tag{2.10}$$

Randomness is certified whenever the guessing probability is strictly less than 1, in which case Eve cannot predict Alice's outcome with certainty.

Global randomness

One can also be interested in the DI guessing probability that quantifies the global randomness of the outcome pair (a, b) obtained measuring inputs $x = x^*$ and $y = y^*$. When the correlations $P(a, b|x, y)$ are extremal, *i.e.* they cannot be decomposed as a convex mixture of other correlations, the guessing probability is given by

$$G(P, x^*, y^*) = \max_{a,b} P(a, b|x, y).$$

In general, however, if the conditional probability distribution can be decomposed as $P(a,b|x,y) = \sum_\lambda q_\lambda P_\lambda(a,b|x,y)$, the guessing probability is given by the maximum of

$$G(P, x^*, y^*|\{q_\lambda, P_\lambda\}_\lambda) = \sum_\lambda q_\lambda \max_{a,b} P_\lambda(a,b|x,y)$$

over all convex decompositions of the observed correlations $P(a,b|x,y)$. As proved in [BSS14], this problem is equivalent to the following SDP:

$$\begin{aligned} \max_{P_{\alpha\beta}} \quad & \textstyle\sum_{\alpha\beta} P_{\alpha\beta}(\alpha,\beta|x^*,y^*) & \\ \text{subject to} \quad & \textstyle\sum_{\alpha\beta} P_{\alpha\beta}(a,b|x,y) = P^{\text{obs}}(a,b|x,y) & \forall\, a,b,x,y \\ & P_{\alpha\beta}(a,b|x,y) \text{ is quantum} & \forall \alpha,\beta. \end{aligned} \tag{2.11}$$

where $\alpha = \{1, \dots |a|\}$ and $\beta = \{1, \dots |b|\}$.

The guessing probability is related to the min-entropy $H_{min}(P, x^*, y^*) = -\log_2 G(P, x^*, y^*)$, which quantifies the number of random bits that can be certified in a DI protocol.

2.5 Quantum state joining and splitting

In this Section we recall the main definitions of two recently demonstrated processes, the "quantum state joining" process and its inverse, called "quantum state splitting" [VSA+13]. These processes allow to integrate two different approaches to increase the amount of information that can be processed simultaneously: First, raising the number of systems in which the information is encoded; second, exploiting an enlarged dimensionality within the same system by using different degrees of freedom of such system. The quantum state joining and splitting processes combine these two methods for photons and enable to switch from one to the other. In particular, in the quantum state joining process two arbitrary qubits initially encoded in separate input photons are combined into a single output photon, within a four-dimensional quantum space. Conversely, in the quantum state splitting process the four-dimensional quantum information carried in a single input photon is split into two output photons, each carrying a qubit.

To describe these processes with a simpler language we will refer to the polarization encoding of the qubits, although there is no general requirement on the choice of encoding at input and output. Let us then assume that two incoming photons, labeled 1 and 2, carry two polarization-encoded qubits,

namely

$$|\psi\rangle_1 = \alpha|H\rangle_1 + \beta|V\rangle_1,$$
$$|\phi\rangle_2 = \gamma|H\rangle_2 + \delta|V\rangle_2, \tag{2.12}$$

where $|H\rangle$ and $|V\rangle$ denote the states of horizontal and vertical linear polarization, corresponding to the logical 0 and 1, respectively. The two photons together form a (separable) quantum system, whose overall quantum state is given by the tensor product

$$\begin{aligned}|\psi\rangle_1 \otimes |\phi\rangle_2 = \alpha\gamma|H\rangle_1|H\rangle_2 + \alpha\delta|H\rangle_1|V\rangle_2 \\ + \beta\gamma|V\rangle_1|H\rangle_2 + \beta\delta|V\rangle_1|V\rangle_2\end{aligned} \tag{2.13}$$

The physical process of quantum state joining corresponds to transforming this two-photon system into a single-photon one, i.e., in an outcoming photon 3 having the following quantum state:

$$|\Psi\rangle_3 = \alpha\gamma|0\rangle_3 + \alpha\delta|1\rangle_3 + \beta\gamma|2\rangle_3 + \beta\delta|3\rangle_3, \tag{2.14}$$

where $|n\rangle$ with $n = 0, 1, 2, 3$ are four arbitrary single-photon orthogonal states, defining a four-dimensional logical basis of a ququart. Of course we cannot use only the two-dimensional polarization encoding for the outgoing photon. One possibility is to use four independent spatial modes. Another option, adopted in [VSA+13], is to use two spatial modes combined with the two polarizations. In the latter case, in the words of Neergaard-Nielsen [NN13], "the information is transferred from a Hilbert space of size 2 (photons) $\times$ 2 (polarizations) to a Hilbert space of size 1 (photon) $\times$ 2 (polarizations) $\times$ 2 (paths)". Although mathematically the quantum state joining process described in (2.14) is a simple change of basis, its physical implementation is much more complicated.

More generally, the joining process should work even for entangled qubits, both internally entangled (i.e., the two photons are entangled with each other) and externally entangled (the two photons are entangled with other particles outside the system). In the first case, the four coefficients obtained in the tensor product $\alpha\gamma, \alpha\delta, \beta\gamma, \beta\delta$ are replaced with four arbitrary coefficients $\alpha_0, \alpha_1, \alpha_2, \alpha_3$. In the second case, the four coefficients are replaced with four kets representing different quantum states of the external entangled system.

The quantum state splitting process is defined as the inverse process of quantum joining, transforming the ququart encoded in the input photon 3

$$|\Psi\rangle_3 = \alpha|0\rangle_3 + \beta|1\rangle_3 + \gamma|2\rangle_3 + \delta|3\rangle_3,$$

into a two-qubit state encoded in two output photons 1 and 2:

$$|\psi\rangle_{12} = \alpha|H\rangle_1|H\rangle_2 + \beta|H\rangle_1|V\rangle_2 + \gamma|V\rangle_1|H\rangle_2 + \delta|V\rangle_1|V\rangle_2.$$

Chapter 3

Necessary detection efficiencies for secure quantum key distribution

Quantum key distribution (QKD) allows two distant parties to produce a shared secret key that can be used for cryptographic tasks. While conventional cryptographic methods can be broken by a quantum adversary, in QKD protocols the security of the generated key is guaranteed by the laws of quantum physics.

Over the past few decades the problem of bridging the gap between realistic implementation of QKD protocols and their theoretical security proofs has attracted a lot of attention. The security of standard QKD protocols [BB84, Eke91] relies on a very detailed modelling of the preparing and measuring devices. However, unavoidable imperfections of the devices or unnoticed failures lead in practice to deviations from the model used to prove security – deviations that can be taken advantage of by a potential eavesdropper. Indeed, standard QKD protocols, being dependent on the accuracy with which the devices are described, can typically suffer attacks, for instance on the detectors [LWW$^+$10, GLLL$^+$11].

To overcome these problems one can shift to the DI paradigm [ABG$^+$07, PAB$^+$09]. In this context the only object one relies on is the statistics of inputs and outputs, and the security of a DI quantum key distribution (DIQKD) protocol is guaranteed by the nonlocal character of these statistics [BCP$^+$14]. The DI scenario allows for the most general and powerful quantum certification protocols as it depends on very few assumptions. Nevertheless, their implementations are demanding because they require very high detection efficiencies to close the detection loophole (e.g. with photonic implementations [BCP$^+$14, GMR$^+$13, CMA$^+$13]).

In order to make the experimental implementations less demanding intermediate scenarios have been introduced, in which the parties involved add some extra assumptions to the fully-DI scheme. The focus is still on the input/output statistics but with an intermediate level of trust between the fully-DI framework and the device-dependent one. Examples are the semi-device-independent (SDI) scenario [PB11] introduced in Section 2.3 or the one-sided device-independent (1SDI) one [TR11, TLGR12, BCW$^+$12] introduced in Section 2.2.

All these different QKD solutions are based on different assumptions and, thus, offer different levels of security. Although different QKD protocols use different strategies, most of them share the property that the key is constructed from the results of measurements performed by one of the end-users on quantum particles that have propagated through an insecure channel. This is the case, for instance, of the famous Bennett-Brassard-84 [BB84] and Ekert [Eke91] protocols, and standard DIQKD protocols, such as those introduced in [AMP06, ABG$^+$07, PAB$^+$09]. Notice however that not every QKD protocol is of this form, a paradigmatic example being measurement-device-independent QKD [LCQ12, BP12].

In this Chapter, we consider the above scenario and therefore we focus on an end-user in a cryptographic protocol who performs measurements on some quantum systems received through an insecure channel. In Section 3.1 we introduce a simple detection attack that allows an eavesdropper to learn the results of any subset of the measurements (including possibly all measurements). The only requirement is that the eavesdropper has to be able to control the detection efficiency of the measurements – which is a natural assumption in the adversary model of cryptographic protocols based on untrusted measurements, such as 1SDI, SDI, and DI protocols. The attack also applies to standard prepare-and-measure protocols if one cannot guarantee that the eavesdropper is unable to tune the detection efficiencies. In fact recent hacking attacks on standard QKD protocols have exploited the ability to manipulate detection efficiencies [LWW$^+$10, GLLL$^+$11]. Our attack defines detection efficiencies necessary for secure quantum key distribution using the previous protocols. We then discuss how our attack can also be applied to schemes for randomness generation. From a practical point of view, our results imply that the implementation of partly-DI protocols are, in terms of detection efficiency, almost as demanding as fully DI ones. Moreover, our attack has also implications from a fundamental point of view: in Section 3.2 we show that, as also observed independently in [Woo14, WPS], it implies the existence of a very weak form of intrinsic randomness in which an eavesdropper limited only by the no-signalling principle [BHK05] cannot a priori fix the outputs of the measurements in a Bell test, but she can later

find out the result of any implemented measurement. In analogy with results in thermodynamics and entanglement theory [HHH98] we name this effect *bound randomness*.

3.1 Detection attack to QKD protocols

The considered scenario consists of a party, say Bob, who measures quantum systems received through an insecure channel (see Fig.3.1). The received systems may have been prepared by another honest party, say Alice, or by an untrusted source. In particular, they may be entangled with other quantum systems. Bob performs on them one of M_B possible measurements with D possible outcomes. We label the measurement choice and result by $y = 1, \ldots, M_B$ and $b = 1, \ldots, D$ respectively. In the absence of loss, let Bob's device give the outcome b with probability $Q(b|y, \rho)$, where ρ is the state of the system received by Bob and which may be correlated with classical or quantum variables of other parties in the protocol. For simplicity in the notation, we omit ρ in what follows, as our results are independent of it.

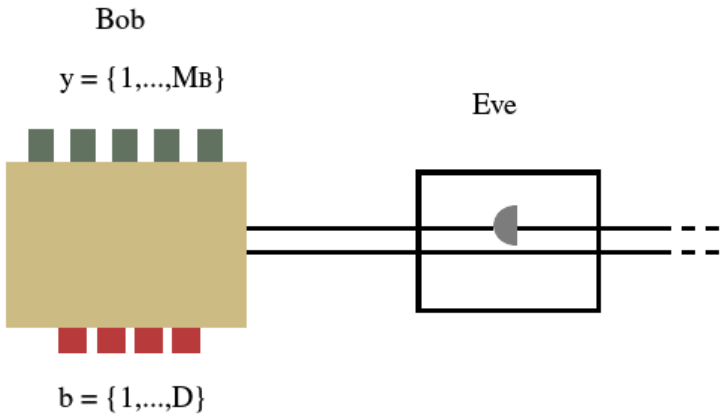

Figure 3.1: DI or partially DI QKD scenario: Bob performs measurement $y \in \{1, \ldots, M_{\mathrm{B}}\}$ on an unknown system delivered by an untrusted source and receives output $b \in \{1, \ldots, D\}$.

In a realistic implementation with losses and inefficient detectors, each measurement of Bob will have a detection efficiency η_y, and one more outcome is observed, corresponding to the no-click events which we denote by $b = \emptyset$. That different measurements may have different efficiencies naturally arises in certain situations, e.g. in [CBS+11]. In such a situation, Bob's device then

produces outcomes with probabilities $P(b|y) = \eta_y Q(b|y)$ for $b = 1, \ldots, D$, and $P(\emptyset|y) = 1 - \eta_y$.

Here we exhibit a simple attack which allows Eve to learn the output of any subset $G \in \{1, \ldots, M_B\}$ of Bob's measurements. This attack does not modify any of Bob's outcome probabilities, i.e., it reproduces the full lossy behavior of Bob's device. In particular, it does not rely on Bob performing any kind of post-selection. The attack only requires that Eve is able to tune arbitrarily the detection efficiency of Bob's detectors depending on the implemented measurement.

Let us now explain in detail how the attack works. Eve randomly selects with probability η_y one of the measurement $y \in G$ whose outcomes she wants to guess and with probability $1 - \sum_{y \in G} \eta_y$ she does not select any particular measurement. Depending on her choice, she then applies one of the two following strategies.

(i) If she picked measurements $\bar{y} \in G$, she performs this measurement on the incoming state. She obtains outcome b with probability $Q(b|\bar{y})$, she reads the outcome, and forwards the corresponding reduced state to Bob. On Bob's side, she forces Bob's detector to click if he performs measurement $y = \bar{y}$, in which case he obtains the same outcome b. If otherwise $y \neq \bar{y}$, she instructs Bob's device not to click, i.e., to output $b = \emptyset$.

(ii) If she did not select any particular measurement, she directly forwards the state to Bob without intervention. However, she instructs Bob's device not to click ($b = \emptyset$) if $y \in G$. If on the other hand $y \notin G$, she allows his detector to click with probability τ_y. Bob then obtains a proper result b with probability $\tau_y Q(b|y)$ and a no-click result with probability $1 - \tau_y$.

Obviously, Eve can always correctly guess Bob's output when $y \in G$ since when Bob's measuring device clicks, it always coincides with Eve's previous measurement result, and she always knows when his detector does not click (gives outcome $b = \emptyset$). Moreover, defining the τ_y such that $\eta_y = (1 - \sum_{y \in G} \eta_y)\tau_y$ for $y \notin G$, it is straightforward that the strategy yields the overall outcome probabilities $P(b|y) = \eta_y Q(b|y)$ if $b \neq \emptyset$ and $P(\emptyset|y) = 1 - \eta_y$, which correspond to lossy devices characterized by detection efficiencies η_y. The only requirement for the τ_ys to be well-defined is that $\sum_{y \in G} \eta_y \leq 1 - \eta'$, where $\eta' = \max_{y \notin G} \eta_y$.

Therefore, the attack works as long as Bob's observed detector efficiencies satisfy $\sum_{y \in G} \eta_y \leq 1 - \eta'$, where $\eta' = \max_{y \notin G} \eta_y$ is the maximum detection efficiency over the set of measurements complementary to G, i.e., those that Eve is not interested in guessing (if this complementary set of measurements is empty, i.e. when Eve wants to guess the output of all of Bob's measurement, we define $\eta' = 0$).

In the simple case where all detectors have the same efficiency $\eta_y = \eta$,

the attack works whenever $\eta \leq 1/(|G|+1)$ if $|G| < M_B$ or when $\eta \leq 1/M_B$ if $|G| = M_B$. In particular, when Eve is interested in guessing a single measurement of Bob, say $\bar{y}$, then $|G| = 1$ and the attack works as long as $\eta \leq 1/2$. Furthermore, if the detectors are not all equally efficient, Eve can use the inefficiency of the measurements $y \neq \bar{y}$ that she is not interested in to raise the critical efficiency of the measurement $\bar{y}$ that she wants to guess above $\eta_{\bar{y}} = 1/2$, as long as $\eta_{\bar{y}} \leq 1 - \max_{y \neq \bar{y}} \eta_y$.

3.1.1 Application to QKD protocols

The above attack applies to any cryptographic protocol in which the key is constructed from the results of measurements performed by one of the end-users on quantum particles received through an insecure channel. It thus applies to any Bell based DI protocol, but also to SDI approaches where the dimension is fixed, protocols based on steering, or prepare-and-measure protocols, unless the eavesdropper cannot tune Bob's detection efficiencies. In fact, in many of these protocols, the key is constructed from a single measurement, which means that in the best case scenario (that of equal detection efficiencies) they become insecure at $\eta = 1/2$. It is important to notice that the obtained critical detection efficiencies apply to any scenario, independently of the number of measurements M_B, outputs D, or the role of other parties in the protocol.

By using many measurements for the key generation, one increases the number of measurements that Eve needs to guess and the critical detection efficiency for our attack decreases. However, this solution is demanding from Alice's and Bob's point of view as many more symbols are sacrificed after basis reconciliation, and also more statistics needs to be collected to have a proper estimation of the protocol parameters. In fact the advantage of using more measurements is limited when considering two distant parties connected by a lossy channel. Take for instance a rather idealized situation in which all losses come from the channel, denoted by η_C and are equal to $\eta_C = 10^{\frac{-\alpha L}{10}}$, where L is the distance in km. Thus, the improvement in distance with the number of bases is only logarithmic. For instance, assuming a typical value for the losses of α of the order of 0.2 dB/km, one has that in order to compensate for the channel losses at 100 km Alice and Bob need to employ 100 bases (see Fig. 3.2).

A possible solution to overcome channel losses is to use heralded schemes [GPS10, MBA13] or quantum repeaters based on entanglement swapping [HKO$^+$12]. Using such schemes, which are technologically more demanding, the only relevant losses for security are those on the honest parties' labs. Alice and Bob can then decide which cryptographic solution to adopt, from

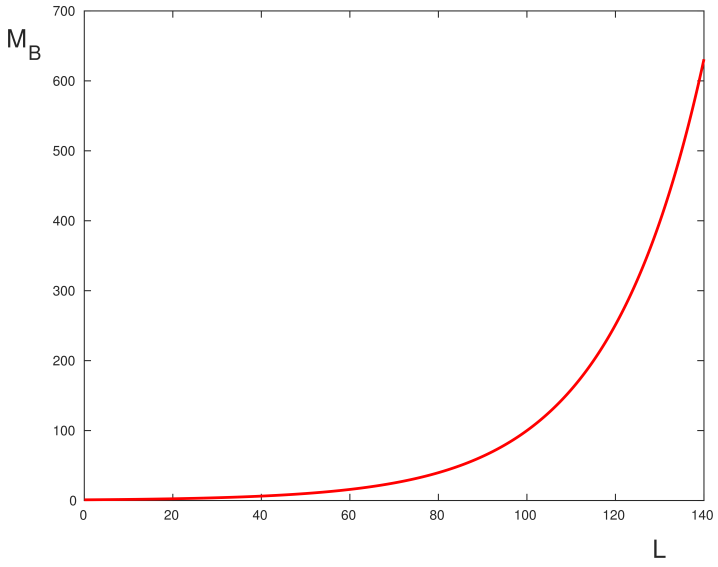

Figure 3.2: Number of bases required M_B versus the channel length L (in km), assuming a typical value of losses of 0.2 dB/km. Notice that Bob needs to measure in 100 bases to compensate for the losses on a 100 km channel.

standard to fully device-independent, depending on the observed detection inefficiencies and the plausibility of the assumptions needed for security.

Our attack also applies to randomness generation schemes based on correlations between measurements on two different devices. In these schemes, randomness is certified by the observed quantumness of the correlations, certified for instance by means of steering (see [LTBS14] and Chapter 4) or Bell inequalities [Col06, PAM+10]. As the particles come from an untrusted source, one cannot exclude that the attack has been implemented on each of the particles sent to the untrusted parties in the protocol (one in the case of steering and two for Bell-based schemes).

In the case of Bell-based protocols, for instance, it is possible to guess the result of one measurement on each device when their detection efficiency is 1/2. Note that in the context of randomness expansion, it is usually the case that one of the possible combinations of measurements is implemented most of the time, as this requires much less initial randomness to run the Bell test [PAM+10]. For all these protocols, randomness expansion is lost when the critical detection efficiency is 1/2.

3.1.2 Improved attacks

The previous attack applies to many cryptographic scenarios because it is independent of the number of measurements, outputs and actions by other parties. Improvements however may be expected for concrete protocols. For instance, we show in what follows how for two untrusted measuring devices, Eve can improve the attack by exploiting the detection efficiency of the second party too. Note though that the attack needs more operations from Eve's side on the untrusted devices than just varying the detection efficiency of the implemented measurements. This improved attack is inspired by the local models exploiting detection inefficiencies introduced in [MP03].

We thus consider a second party in the protocol, Alice, who performs M_A measurements of D outputs. Her measurement choice and result are labeled by x and a (see Fig.3.3). Again, in the presence of loss, the output probability distribution has one more result because of the no-click events and is of the form

$$\begin{aligned} P(ab|xy) &= \eta^2 Q(ab|xy), \\ P(\emptyset b|xy) &= \eta(1-\eta) Q(b|y), \\ P(a\emptyset|xy) &= \eta(1-\eta) Q(a|x), \\ P(\emptyset\emptyset|xy) &= (1-\eta)^2, \end{aligned} \tag{3.1}$$

where the detection efficiencies have for simplicity all been taken to be equal to η.

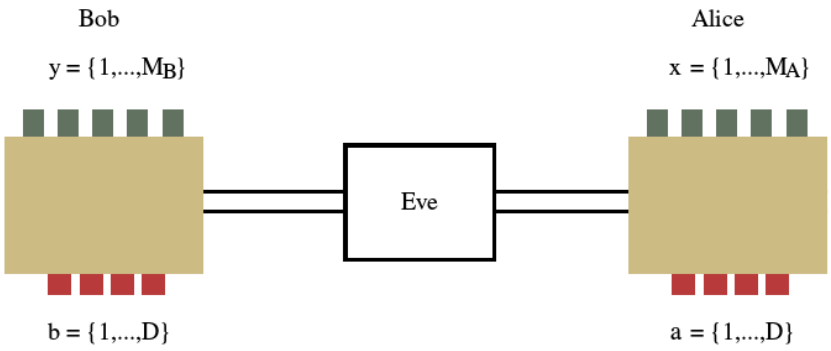

Figure 3.3: Eve can improve the bound on the critical detection efficiency in case of a DI scenario in which Alice and Bob want to extract a private key from two untrusted devices: here Bob inputs measurement $y \in \{1, \ldots, M_{\mathrm{B}}\}$ and receives output $b \in \{1, \ldots, D\}$, while Alice inputs measurement $x \in \{1, \ldots, M_{\mathrm{A}}\}$ and receives output $a \in \{1, \ldots, D\}$.

In the improved attack, Eve's goal is again to guess G measurements

on Bob's side. With probability q Eve uses the previous attack and does nothing on Alice's side. With probability $1-q$ the attack works in the reverse direction: Eve fixes the output of one of Alice's measurements (even though she is still guessing Bob's result), namely she picks one of Alice's measurements, say $\bar{x}$, with probability $1/M_A$, and decides an output for this measurement following the quantum probability $Q(a|\bar{x})$. If Alice happens to implement measurement $\bar{x}$ she will obtain this outcome, otherwise she observes a no-click. On Bob's side, Eve computes the reduced state corresponding to Alice's result and, for each measurement by Bob, selects one possible outcome following the probability $Q(b|y,ax)$ predicted by this state. This defines Bob's result, whose detector always clicks. The intuition behind the attack is that for those cases in which Eve fixes Alice's result, she can allow any measurement on Bob to give a result, as Alice effectively implements one single measurement and a hidden-variable model is enough to describe the observed correlations.

So far the model never gives two no-click events, which does not correspond to the expected behavior of actual lossy devices. To correct this, with probability r, Eve runs the above protocol and with probability $1-r$, she instructs both detectors not to click. We finally get

$$\begin{aligned} P(ab|xy) &= r\left(\frac{q}{|G|'}+\frac{1-q}{M_A}\right)Q(ab|xy) \\ P(a\emptyset|xy) &= r\,q\left(1-\frac{1}{|G|'}\right)Q(a|x) \\ P(\emptyset b|xy) &= r(1-q)\left(1-\frac{1}{M_A}\right)Q(b|y) \\ P(\emptyset\emptyset|xy) &= 1-r=(1-\eta)^2, \end{aligned} \tag{3.2}$$

where $|G|' = |G|+1$ when $|G| < M_B$ and $|G|' = |G|$ when $|G| = M_B$, as in the previous attack. Tuning the parameters so that the above probabilities correspond to those of lossy devices with equal efficiencies η as in (3.1), one finds

$$\eta = \frac{|G|' + M_A - 2}{|G|' M_A - 1}. \tag{3.3}$$

It is easy to see that this attack improves over the previous one, as the corresponding critical detection efficiency is always larger than $1/|G|'$. For example, in the simplest case where Alice performs 3 measurements, Bob performs two, and Eve guesses a single outcome, $(M_A, M_B, |G|) = (3,2,1)$, $\eta = 3/5$, increasing the critical efficiency by a further 10%. In the opposite limit, when $M_A \to \infty$, $\eta \to 1/|G|'$, showing that the advantage of attack-

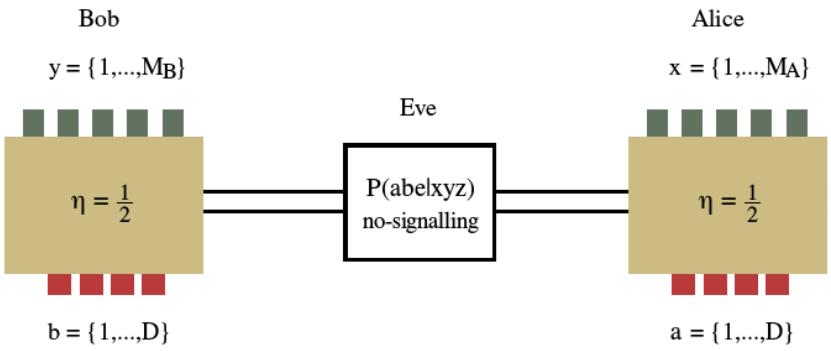

Figure 3.4: Setting for bound randomness: Alice and Bob wants to extract private randomness from their untrusted devices with detection efficiency $\eta = 1/2$; a no-signaling eavesdropper Eve performs the attack described in Section 3.1 to learn Alice and Bob's outputs.

ing Alice's measurements decreases with the number of measurements she performs.

3.2 Bound randomness

The results of this Chapter are not only limited to practical aspects of cryptographic protocol implementations, but also have implications from a more fundamental point of view. Our motivation in this scope is to understand how the predictability on the outcomes of a Bell experiment is limited by the no-signalling principle. In fact, as mentioned in Section 2.4, deterministic and no-signalling models can only lead to local correlations. Thus, the presence of non-locality, under the assumption of no-signalling, implies the existence of intrinsic randomness. Our main result in this ambit is to show that in some cases, this intrinsic Bell-certified randomness may appear in a very weak form: there are non-local correlations for which a no-signalling eavesdropper (i) cannot obviously fix the results of all measurements in advance but (ii) can later find out with certainty the outcome of any measurement. As mentioned, we dub this effect bound randomness (see also [Woo14, WPS]).

The construction of bound randomness relies on a couple of simple observations. First, in a randomness scenario consisting of two untrusted devices with uniform detection efficiency $\eta = 1/2$, our (primary) attack can be applied to both parties, so that the eavesdropper learns the result of one measurement each for Alice and Bob, $\bar{x}$ and $\bar{y}$ (see Fig. 3.4). Let $e = (e_a, e_b)$ be Eve's prediction for Alice and Bob's outcomes for measurements $\bar{x}$ and

$\bar{y}$. This variable can take $(D+1)^2$ possible values corresponding to the ideal D-valued measurement outcomes plus the no-detection event. Eve obtains outcome e with a certain probability $P_{\bar{x}\bar{y}}(e)$ and given e, her attack defines a joint probability $P_{\bar{x}\bar{y}}(ab|xy,e)$ for Alice and Bob. Since the attack does not change the expected probabilities $P(ab|xy)$ from Alice and Bob's perspective, we have that

$$\sum_e P_{\bar{x}\bar{y}}(abe|xy) = P(ab|xy), \tag{3.4}$$

where we have defined the tripartite conditional probability distribution $P_{\bar{x}\bar{y}}(abe|xy) = P_{\bar{x}\bar{y}}(e)P_{\bar{x}\bar{y}}(ab|xy,e)$. Note that the previous attack is nothing but the preparation by Eve of the observed correlations $p(ab|xy)$ as a mixture of the correlations $p_{\bar{x}\bar{y}}(ab|xye)$ with probabilities $p(e) = p_{\bar{x}\bar{y}}(abe|xy)/p_{\bar{x}\bar{y}}(ab|xye)$.

The second observation consists of noticing that the $M_A M_B$ different attacks defined by each combination of measurement settings $z = (\bar{x}, \bar{y})$ can be combined into a single tripartite conditional probability distribution

$$P(abe|xyz) \equiv P_z(abe|xy) \tag{3.5}$$

by adding an input z on Eve's, where z defines the combination of settings Eve wants to predict. It is easily verified that this tripartite distribution is no-signalling, see also [HRW13], and thus represents a valid attack by a no-signalling eavesdropper. By choosing her input z, Eve can steer the ensemble of no-signalling correlations prepared between Alice and Bob. The honest parties however cannot notice this because their observed mixed correlations after summing over Eve's measurement output are the same for any value of z. Thus, Eve can choose a posteriori the attack that allows her to predict the result of any given pair z of implemented measurements. The effect is similar to what happens in the quantum case when predicting the result of non-commuting variables on half of a maximally entangled state.

Note now that there exist correlations that are non-local – hence whose outcomes cannot all be fixed in advance – even when the detection efficiency is smaller than $1/2$ – hence whose outcomes can all be perfectly guessed by Eve a posteriori using the above construction. Examples of such correlations were given in [Mas02], where it was shown that the critical detection efficiency required to close the detection loophole decreases exponentially with the dimension of the measured quantum state in a scenario in which the number of measurements by Alice and Bob is exponentially large. For these distributions, Eve cannot fix the measurement results, otherwise the correlations would be local, but she can later predict the output of any implemented measurements by choosing her input, as the previous attack applied. More generally, any non-local correlations obtained for detection efficiencies

$\eta \leq 1/2$ constitute examples of bound randomness. Finally, it can be explicitly checked that both the all-versus nothing example of [Cab01] and the Peres-Mermin magic square [Ara04] exhibit bound randomness.

3.3 Discussion

We have provided a simple and general detection attack that allows an eavesdropper to guess some of (or all) the measurement results in a cryptographic protocol. It applies basically to any protocol with untrusted detectors in which she is able to tune the detection efficiency of untrusted devices, such as DI and partly-DI protocols. From our attack we have derived bounds on the critical detection efficiencies necessary for secure implementation of a large class of QKD protocols. The derived bounds only depend on the number of measurements that Eve wants to learn, and show that the implementation of most partly-DI solutions is, from the point of view of detection efficiency, almost as demanding as fully DI ones.

We also showed that the attack can be improved when considering specific protocols. Indeed, when considering two parties with untrusted detectors, Eve can exploit the detection inefficiencies of one party to improve her attack on the other. We present an analysis of the tightness of our attack in steering scenarios in Chapter 4.

From a more fundamental point of view, we have also showed how our attack implies the existence of non-local correlations with a very weak form of randomness in which an eavesdropper cannot obviously fix the results of all measurements in advance but she can later find out with certainty the result of any implemented measurement. In particular, we proved the existence of bound randomness in the case of eavesdroppers limited only by the no-signalling principle [BHK05].

Chapter 4

Optimal randomness certification in the quantum steering and prepare-and-measure scenarios

Quantum theory, unlike classical physics, implies the existence of intrinsic randomness that cannot be explained with our ignorance of underlying physical variables. Genuine random numbers constitute a useful resource for many applications, such as cryptography or gambling. Randomness certification protocols have been studied in the DI scenario, where the random character of the outputs obtained by the parties is guaranteed by the violation of a Bell inequality. However, DI protocols require low levels of losses [BCP$^+$14], which make them very demanding experimentally. In this Chapter we will focus on the steering scenario [Sch35, WJD07], a bipartite framework in which one of the parties has complete knowledge of his measurement apparatuses, while the other does not, and treats her measuring device as a black box (see Section 2.2). Quantum steering allows for entanglement detection which is more robust to noise and experimental imperfections than the DI scenario [WJD07, QVC$^+$15] and is relevant for one-sided device independent quantum key distribution (1SDIQKD) [BCW$^+$12] and randomness certification [LTBS14]. Several experimental groups have recently observed steering, including in continuous-variable systems [OPKP92, BSLR03], using entangled states with a local model [SJWP10], using inefficient detectors [SGA$^+$12, BES$^+$12, WRS$^+$12], asymmetric states [HES$^+$12], and multipartite systems [AWT$^+$15, CSA$^+$15, LCC$^+$15].

The main result of this Chapter is a general and optimal method to quantify the amount of local or global randomness that can be certified from

a single measurement in the steering scenario. We apply this method to compute the maximal amount of local and global randomness that can be certified in presence of noise and losses. Using this method and the results derived in Chapter 3 we show that local randomness can be certified from a single measurement if and only if the detectors used in the test have detection efficiency higher than 50%. Our method can be seen as the analogue of the approach of [NSPS14, BSS14] for the fully-DI scenario applied to a partly-DI scenario. We compare the results obtained there to those obtained here, in terms of the amount of randomness that can be obtained by measuring systems subjected to white noise, and find that substantial benefits can be obtained in the present setting.

We furthermore show that the results can be easily extended beyond the steering scenario, namely to the prepare-and-measure scenario, where the state is also trusted, so that only Alice's measuring device is untrusted. We show that in this case even noisy states can perform very well for randomness certification.

Finally, we give a method to find the optimal measurements which attain the most randomness from any fixed state. We use insight from this method to demonstrate analytically that maximal randomness can be extracted from all pure partially entangled states using only two fixed measurements.

4.1 Randomness and steering

The scenario considered in this Section is the steering scenario described in Section 2.2 and illustrated in Fig.4.1(a). In this scenario the relevant object is the assemblage (2.5) that is determined by Bob through tomographic measurements. The confirmation of steering, which is authenticated by the violation of a steering inequality (2.7), not only guarantees that the shared state is entangled but also that Alice is performing incompatible measurements [QVB14, UMG14]. It is thus very intuitive to expect a relation between steering and randomness: first, the correlations (entanglement) shared between Alice and Bob allows Bob to certify steering, and consequently the incompatibility of Alice's measurements. Second, since Alice's measurements are incompatible not all the outcomes she receives are predictable, and thus they are random.

There are several motivations to quantify the amount of randomness in the steering scenario. From a fundamental point of view, it is important to understand how much randomness can be maintained if we renounce partial information about the specific description of the involved systems [LTBS14, BQB14, LPY$^+$12]. From a practical point of view, the amount of

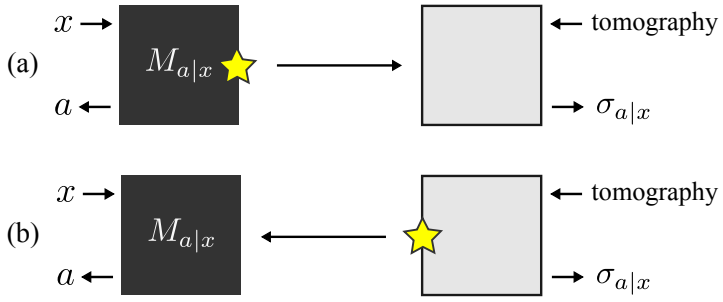

Figure 4.1: Setup for randomness certification in the quantum steering and prepare-and-measure scenarios. (a) Steering scenario: Alice and Bob measure an unknown bipartite system delivered by an untrusted source. Alice treats her measurement device as a black box with inputs $x \in \{1, \ldots, m_{\mathrm{A}}\}$ and outputs $a \in \{1, \ldots, d_{\mathrm{A}}\}$ and Bob performs tomography on his subsystem. (b) Prepare-and-measure scenario: similar to the previous scenario, but now Bob holds the source and then knows the bipartite state ρ_{AB}.

randomness certified in the steering scenario gives an upper bound to what Alice and Bob would obtain in a fully-DI setting, regardless of the number of Bob's measurements. Furthermore, it is a scenario that appears naturally in some asymmetric applications. For instance the present results give a way of quantifying the amount of randomness in remote untrusted stations. This is relevant, for instance, when the provider of a quantum random number generator wants to remotely check if the devices they provided are still functioning properly.

4.1.1 Local randomness certification

In order to certify the local randomness of Alice's outcomes we work in the adversarial scenario, where a potential eavesdropper, Eve, wants to predict them. This framework is relevant for cryptographic tasks, namely for one-sided device-independent quantum key distribution (1SDIQKD). In the most general case, we do not make any assumption on Alice's measurement device, so that it could even have been provided by Eve. As commented in Section 2.4 in the context of DI randomness certification, the bipartite state ρ_{AB} is considered as the reduced state of a tripartite entangled state ρ_{ABE} shared by Alice, Bob and Eve, *i.e.* $\rho_{\mathrm{AB}} = \mathrm{Tr}_{\mathrm{E}}[\rho_{\mathrm{ABE}}]$. Hence, by applying measurements to her subsystem Eve can in principle obtain information about Alice's outcome.

In this Section we will focus on the case where Alice and Bob want to

extract randomness from the outcomes of a single given measurement of Alice, let us say $x^* \in \{1, \ldots, m_{\mathrm{A}}\}$. We consider the case where Eve also knows from which measurement x^* Alice is going to extract randomness, so she can optimize her attack to obtain information about this measurement setting. The figure of merit we use to evaluate the amount of randomness in Alice's outcomes is Eve's guessing probability $P_{\mathrm{guess}}(x^*)$, *i.e.* the probability that Eve's guess e is equal to the outcome a that Alice obtained, whenever Alice performs the specific measurement $x = x^*$. The definition given by Eq. (2.9) for the guessing probability in the DI scenario (see Section 2.4) is used in this Chapter. This quantity is equal to the joint probability that Alice and Eve give the same outcome whenever Alice measurements $x = x^*$. One can certify randomness whenever $P_{\mathrm{guess}}(x^*)$ is strictly less than 1, otherwise Eve would be able to predict Alice's outcome with certainty.

After Alice and Eve have applied their measurements, the assemblage prepared will be

$$\sigma^e_{a|x} = \mathrm{Tr}_{\mathrm{AE}}[(M_{a|x} \otimes \mathbb{1}_{\mathrm{B}} \otimes M_e)\, \rho_{\mathrm{ABE}}], \tag{4.1}$$

where M_e is the element of Eve's (optimal) measurement which yields outcome $e \in \{1, \ldots, d_{\mathrm{A}}\}$. However, since Alice and Bob do not have access to Eve's outcomes, the assemblage they will reconstruct will be given by

$$\sigma^{\mathrm{obs}}_{a|x} = \sum_e \sigma^e_{a|x}. \tag{4.2}$$

In order to compute the optimal strategy for Eve we need to maximize her guessing probability (for a given input x^* of Alice), over all strategies. Naively, this would appear to constitute optimizing the triple $\{\rho_{\mathrm{ABE}}, M_{a|x}, M_e\}$, of state, measurements for Alice, and measurement for Eve, which is a non-linear optimization problem. However, just as in the DI case considered in Section 2.4, we can instead replace this by an equivalent linear optimization over all physical assemblages $\{\sigma^e_{a|x}\}_{a,e,x}$ that are compatible with the no-signalling principle and the observed assemblage $\{\sigma^{\mathrm{obs}}_{a|x}\}_{a,x}$. More precisely, the maximization problem can be formulated as the following semidefinite programme (SDP) [BV04]:

$$\begin{aligned}
\max_{\{\sigma^e_{a|x}\}_{a,e,x}} \quad & P_{\mathrm{guess}}(x^*) = \textstyle\sum_e \mathrm{Tr}(\sigma^e_{a=e|x^*}) & & \\
\text{subject to} \quad & \textstyle\sum_e \sigma^e_{a|x} = \sigma^{\mathrm{obs}}_{a|x} & & \forall\, a, x \\
& \textstyle\sum_a \sigma^e_{a|x} = \sum_a \sigma^e_{a|x'} & & \forall\, e,\ x \neq x' \\
& \sigma^e_{a|x} \succeq 0 & & \forall a, x, e.
\end{aligned} \tag{4.3}$$

In the objective function we used $P_{\mathrm{E}}(e)P_{\mathrm{A}}(a|x,e) = P(ae|x) = \mathrm{Tr}[\sigma^e_{a|x}]$ to re-express $P_{\mathrm{guess}}(x^*)$. The first constraint assures that the decomposition for Eve is compatible with the assemblage Alice and Bob observe. The second constraint is the no-signalling condition – i.e. Alice cannot signal to Bob and to Eve. The last one is the requirement for every $\sigma^e_{a|x}$ to be a valid (unnormalized) quantum state. We defer to the appendix the full proof that this optimization problem is equivalent to optimizing over states and measurements, which follows from the Gisin-Hughston-Jozsa-Wootters (GHJW) theorem [Gis89, HJW93] (which shows that all bipartite no-signalling assemblages have quantum realizations), combined with the fact that Eve, making only one measurement, also cannot signal.

Notice that the SDP (4.3) can be seen as the steering analogue of the SDP provided in (2.10) in Section 2.4, which bounds the amount of randomness given an observed nonlocal probability distribution $P^{\mathrm{obs}}(ab|xy)$. As mentioned before, the SDP (4.3) provides an upper bound on the amount of randomness (*i.e.* a lower bound on the P_{guess}) that can be found using the SDP given in Section 2.4. This follows because (4.3) does not allow Eve to attack the measurements of Bob. Thus, our SDP bounds the maximal amount of randomness that could be obtained if Bob were to perform any number of measurements (that Eve can attack) and compute the randomness based on the obtained probability distribution. The number of random bits is quantified by the min-entropy $H_{\min}(A|X) = -\log_2 P^*_{\mathrm{guess}}(x^*)$, where $P^*_{\mathrm{guess}}(x^*)$ is the result of the maximization (4.3).

In Fig. 4.2 we plot the amount of randomness certified in the case that Alice applies two mutually unbiased Pauli spin measurements on a two-qubit Werner state $\rho_{\mathrm{AB}} = v|\Phi_+\rangle\langle\Phi_+| + (1-v)\mathbb{1}/4$, where $|\Phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and compare it with the amount of randomness obtained in the case Bob also treats his measuring device as a black box (i.e. the fully device-independent case). In both cases randomness can be certified as long as $v > 1/\sqrt{2}$, which is the critical amount of noise for demonstrating either steering or nonlocality with only two measurements [CJWR09]. All numerical SDP calculations were performed using the CVX package for MATLAB [GB13, GB08], along with the library QETLAB [Joh15].

In Fig. 4.3 we also compute the amount of randomness that can be obtained by measuring the same spin measurements with detection efficiency η (for visibility $v = 1$ and $v = 0.9$), again comparing to the case where Bob treats his measuring device as a black box. That is, (for steering) instead of ideal measurements, with elements $M_{a|x}$, we consider inefficient measure-

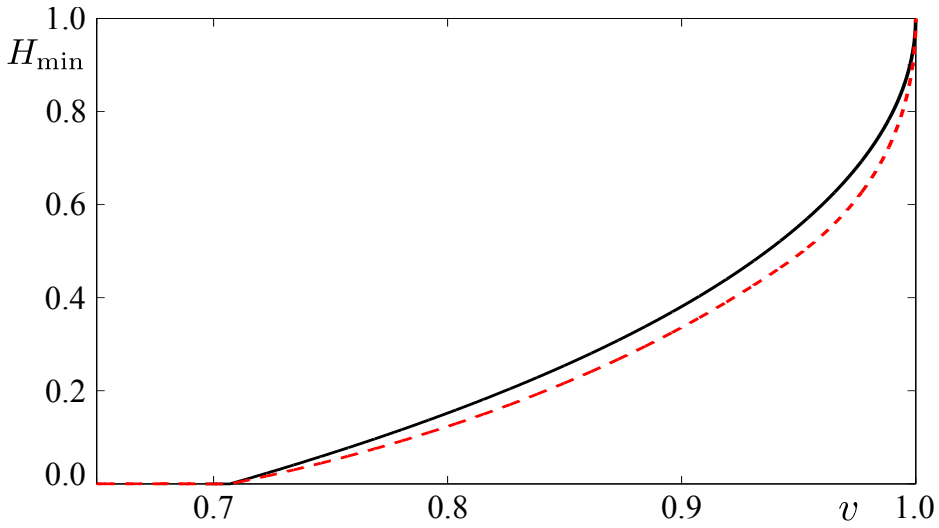

Figure 4.2: Random bits certified $H_{\min}$ versus the visibility v of the two-qubit Werner state. We compare the randomness obtained with our method in the steering scenario (solid line) with the fully-DI case as in Section 2.4 (dashed line).

ments $M_{a|x}^{(\eta)}$, with one additional outcome $a = \emptyset$, given by

$$M_{a|x}^{(\eta)} = \begin{cases} \eta M_{a|x}, & a \neq \emptyset \\ (1-\eta)\mathbb{1}, & a = \emptyset \end{cases} \tag{4.4}$$

(the measurements of Bob are similarly made inefficient in the nonlocality scenario).

In this case, two comparisons are made: (i) the case where Bob's detection efficiency is 1; and (ii) where Bob also has detection efficiency η. As one can see, for $v = 1$ randomness can be certified in the steering scenario whenever the detection efficiency is higher than 50%, matching the threshold below which no randomness can be obtained (derived in Chapter 3). Therefore, by bringing together the results shown in Fig 4.3 and the bounds on critical detection efficiencies derived in Chapter 3, we prove that randomness certification in the steering scenario can be achieved in presence of losses if and only if the detection efficiency is higher than 50%.

Moreover, we see that due to the much larger detection efficiencies for the CHSH inequality (82.8%) and for the DI case where Bob's measuring device is perfectly efficient (70.7%), the steering scenario offers a significant advantage when using the maximally entangled state over the nonlocality

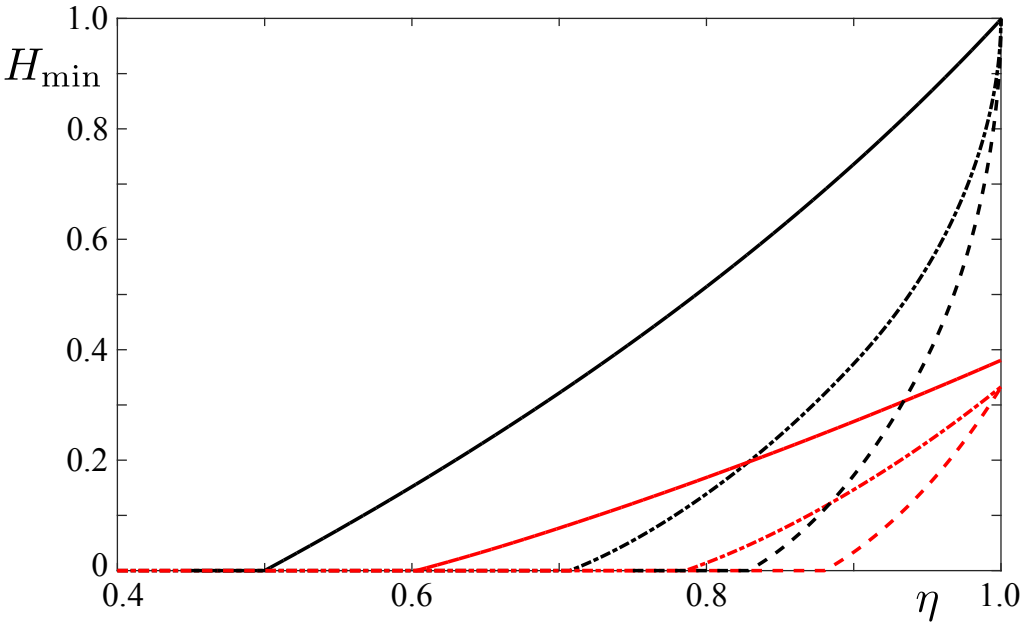

Figure 4.3: Random bits certified $H_{\min}$ versus the detection efficiency η for the two-qubit Werner state. Black lines: $v = 1$; Red lines: $v = 0.9$. Solid lines: our steering method; Dot-dashed lines: DI method in the case where Bob's detection efficiency is 1; Dashed lines: DI method where both Alice and Bob's detectors have efficiency η.

scenario, for the entire range of visibility which is experimentally significant (i.e. for $v = 0.9$ and above).

Finally, in Fig. 4.4 we plot the number of random bits certified in the case that Alice performs measurements in four mutually unbiased bases on her half of the entangled two-qutrit state $(|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$ in the presence of losses. Again, we see that whenever the detection efficiency is above 50% Alice is able to certify local randomness. Moreover, for efficiency $\eta = 1$ she certifies $H_{\min} = \log_2 3$ bits of randomness.

4.1.2 Global randomness certification

In the steering scenario one can also consider global randomness extraction from both the untrusted and trusted devices. Indeed, even though Bob trusts his devices, and knows which measurement he performs, there is still an optimal state that Eve can distribute which allows her to predict the outcome of Bob's measurement. This is because although Eve is not able to change

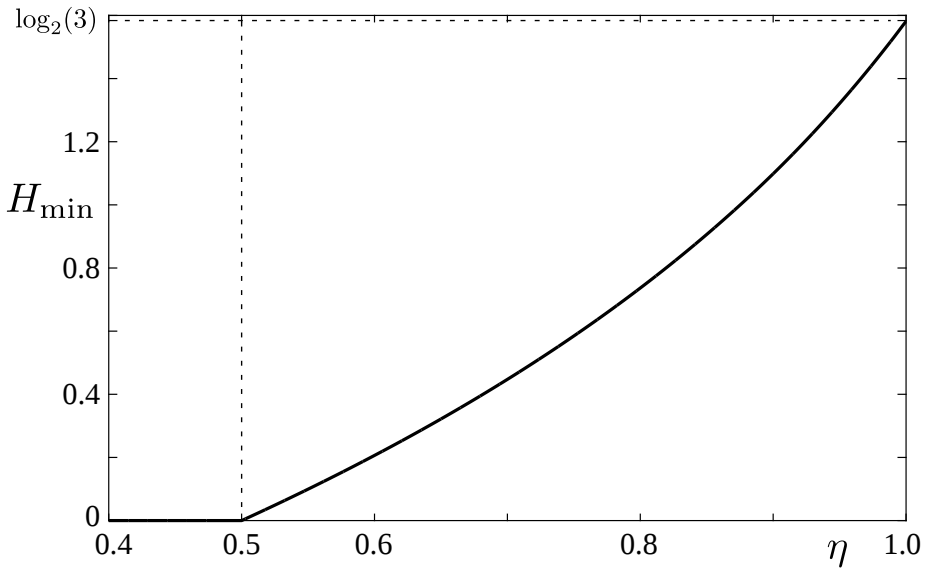

Figure 4.4: Random bits certified $H_{\min}$ versus the detection efficiency η for the two-qutrit maximally entangled state $|\Phi_+^{(3)}\rangle = (|00\rangle + |11\rangle + |22\rangle)/\sqrt{3}$.

the measurements performed by Bob, nor his reduced state, she still has additional classical side information that she can use to help her in guessing the result of Bob (since she holds the source).

Consider that, additionally to the outcomes of Alice's measurement $x = x^*$, Eve wants to guess the outcomes of a measurement M_b performed by Bob. Eve now has a pair of guesses (e, e'), which will be her guess for the pair (a, b). She will thus perform a measurement with elements $M_{ee'}$ on her share of the state, which after Alice also measures will lead to the assemblage for Bob $\sigma_{a|x}^{ee'} = \mathrm{Tr}_{\mathrm{AE}}[(M_{a|x} \otimes \mathbb{1}_{\mathrm{B}} \otimes M_{ee'})\rho_{\mathrm{ABE}}]$. Similarly to the case of local randomness, the global guessing probability P_{g} (defined in (2.11) in the DI scenario) can straightforwardly be shown to be the solution to the following SDP

$$\begin{aligned} P_{\mathrm{g}} \quad = \quad & \max_{\{\sigma_{a|x}^{ee'}\}_{a,e,e',x}} \quad \sum_{ee'} \mathrm{Tr}[M_{b=e'} \sigma_{a=e|x^*}^{ee'}] \\ & \text{s.t.} \quad \sum_{ee'} \sigma_{a|x}^{ee'} = \sigma_{a|x}^{\mathrm{obs}}, \qquad \forall a, x \\ & \qquad \sum_{a} \sigma_{a|x}^{ee'} = \sum_{a} \sigma_{a|x'}^{ee'}, \quad \forall x \neq x', a, e, e' \\ & \qquad \sigma_{a|x}^{ee'} \succeq 0, \qquad\qquad \forall a, x, e, e' \end{aligned} \tag{4.5}$$

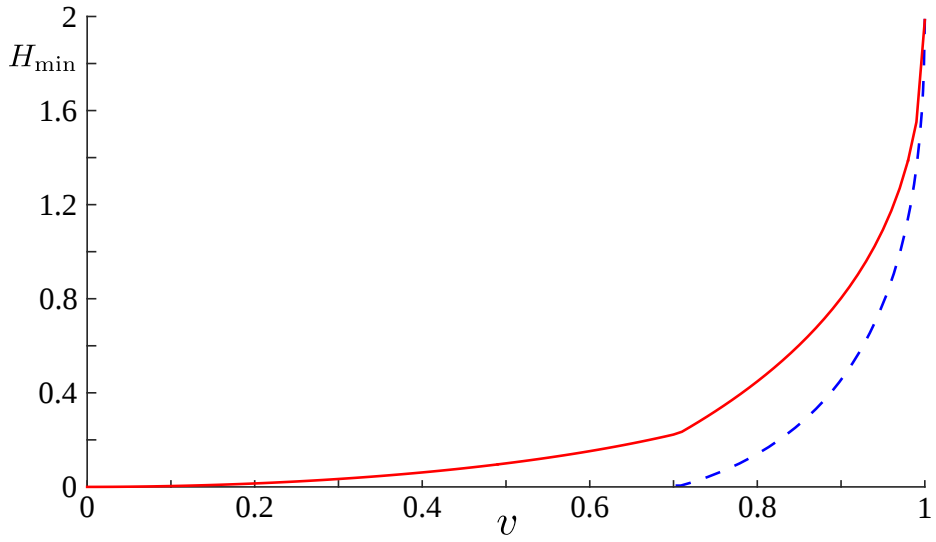

Figure 4.5: Global randomness obtained by measuring a two-qubit Werner state (with visibility v), with X and Z measurements for Alice, and X measurement for Bob, computed using Eq. (4.5) (red solid curve). As a matter of comparison we also plot the amount of global randomness obtained in the device-independent scenario, using the SDP given in (2.11) (blue dashed curve).

We again require consistency with the observed assemblage $\sigma_{a|x}^{\text{obs}}$, and demand positivity and no-signalling.

We computed the global randomness which can be certified without losses assuming X and Z measurements for Alice, and an X measurement for Bob, on two-qubit Werner states. The results can be seen in Fig. 4.5, alongside the corresponding curve calculated using the method described in Section 2.4 for the nonlocality scenario. As one can see, randomness can be certified in the device-independent scenario only when the observed correlations cannot be reproduced by a LHV model. Indeed, the visibility threshold for randomness certification in this scenario matches with the visibility required for the violation of the CHSH inequality, which is $v = 1/\sqrt{2}$. In the steering scenario, however, one can certify global randomness also from states that lead to a LHS model, *i.e.* from Werner states with visibility $v < 1/2$, as was noted also in [LTBS14]. In this case, Bob can always extract some randomness from states with visibility $v > 0$, as he owns a complete characterization of his system. As a result, we observe that the lower bound on the amount of global randomness that can be extracted in the steering scenario presented

in [LTBS14] is tight.

4.2 Prepare-and-measure scenario

Up to now we have considered the steering scenario, where Alice and Bob receive an unknown state ρ_{AB} from an untrusted source. It turns out that the results on local randomness straightforwardly apply to the case where Bob prepares a known state and sends half of it to Alice (see Fig.4.1(b)). In this case, since the global state ρ_{AB} is known, the assemblages reconstructed by Bob have to come from unknown measurements on this state, *i.e.* $\sigma_{a|x} = \sum_e \mathrm{Tr}_{\mathrm{A}}[(M^e_{a|x} \otimes \mathbb{1}_{\mathrm{B}})\rho_{\mathrm{AB}}]$. Thus the SDP (4.3) can be replaced by

$$\begin{aligned} \max_{\{M^e_{a|x}\}_{a,e,x}} \quad & P_{\mathrm{guess}}(x^*) = \textstyle\sum_e \mathrm{Tr}[(M^e_{a=e|x^*} \otimes \mathbb{1}_{\mathrm{B}})\rho_{\mathrm{AB}}] & \\ \text{subject to} \quad & \textstyle\sum_e \mathrm{Tr}_{\mathrm{A}}[(M^e_{a|x} \otimes \mathbb{1}_{\mathrm{B}})\rho_{\mathrm{AB}}] = \sigma^{\mathrm{obs}}_{a|x} & \forall\, a, x \\ & \textstyle\sum_a M^e_{a|x} = \sum_a M^e_{a|x'} & \forall x' \neq x, e \quad (4.6) \\ & \textstyle\sum_{a,e} M^e_{a|x} = \mathbb{1} & \forall x \\ & M^e_{a|x} \succeq 0 & \forall a, x, e. \end{aligned}$$

This SDP can be understood as the maximization of Eve's guessing probability over all possible POVM measurements (where the outcome e goes to Eve and the outcome a goes to Alice), with Eve oblivious of x, that can be applied to the state ρ_{AB}, given the observation of the assemblage $\{\sigma^{\mathrm{obs}}_{a|x}\}_{a,x}$. A derivation of this SDP can be found in A.2.

We used the above program to calculate the amount of randomness that can be obtained from the two qubit Werner state, and from the isotropic two-qutrit state $\rho_{\mathrm{AB}} = v|\Phi^{(3)}_+\rangle\langle\Phi^{(3)}_+| + (1-v)\mathbb{1}/9$, where $|\Phi^{(3)}_+\rangle = (|00\rangle + |11\rangle = |22\rangle)/\sqrt{3}$. In both cases we consider that Alice performs two mutually unbiased measurements (Pauli X and Z for qubits, and their generalization for qutrits).

For the case of no-losses, we observe that the amount of randomness that can be extracted in the prepare-and-measure scenario is *independent of the visibility* v, and equal to 1 bit and 1 trit $= \log_2(3)$ bits respectively. More precisely, for all $v \geq 0.05$ we observed numerically that $P_{\mathrm{guess}} \leq 0.339$. This coincides with the amount which is obtained in the steering scenario for $v = 1$, i.e. the ideal case. Therefore, this demonstrates that if knowledge of the state is assumed, then the lack of visibility cannot be used by Eve to guess the outcomes of Alice's measurements.

Turning to the case of losses, consistently with the above, we observe that, independent of the visibility, the dependence of the randomness on the

loss coincides with that found in the steering scenario for perfect visibility. That is, the solid black curves in Figs. 4.3 and 4.4 are obtained, for any fixed value of the visibility v.

This shows that the prepare-and-measure scenario greatly improves over the steering scenario when considering lack of visibility (i.e. noise) on the state.

4.3 Improving the randomness extraction

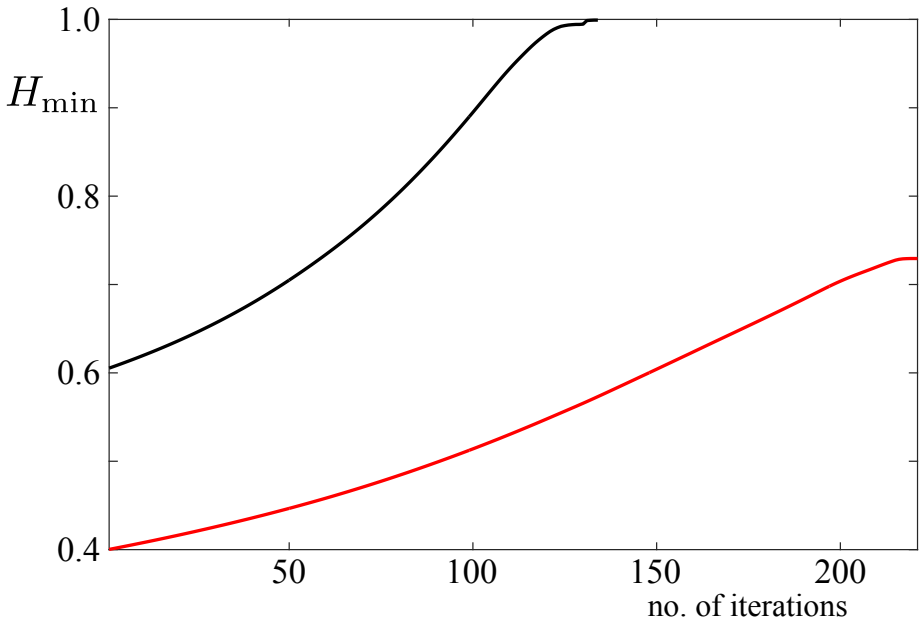

Figure 4.6: Plot of the random bits certified versus the number of steps of the see-saw iteration for a two-qubit partially entangled state $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with $\theta = \pi/7$ and starting with random measurements with $\eta = 1$ (black curve) and $\eta = 0.9$ (red curve).

The SDP (4.3) provides a way of quantifying the randomness in Alice's outcomes given the observation of a given assemblage. A natural question is, given a fixed state distributed between Alice and Bob and a fixed number of measurements for Alice, what is the best scheme they can implement (i.e. the best choice of measurements) which allows for the certification of the most randomness.

Here we propose a numerical see-saw method that, starting from an initial

amount of certified randomness, seeks for measurement schemes that lead to higher randomness certification. We focus on the case of local randomness; a similar scheme can also be implemented for global randomness.

Every SDP has a dual program, also an SDP, that can be obtained through the theory of Lagrange multipliers [BV04]. The dual of (4.3) is equivalent to

$$\begin{aligned} \min_{\{F_{a|x}\}_{a,x}} \quad & \textstyle\sum_{a,x} \mathrm{Tr}(F_{a|x}\, \sigma^{\mathrm{obs}}_{a|x}) \\ \text{subject to} \quad & \mathrm{Tr}[\sigma_{a'|x^*}] \leq \textstyle\sum_{a,x} \mathrm{Tr}(F_{a|x}\sigma_{a|x}) \qquad \forall\, a', \sigma_{a|x} \end{aligned} \tag{4.7}$$

where in the constraint, $\forall \sigma_{a|x}$ should be understood as for all no-signalling assemblages, i.e. those satisfying $\sum_a \sigma_{a|x} = \sum_a \sigma_{a|x'}$ for all $x' \neq x$. This problem is not in the form of an SDP; however, in Appendix A.3 we derive the dual SDP and show its equivalence to (4.7), which is easier to interpret. Since strong duality holds, the optimal value of this optimization problem is equal to the optimal value of (4.3), i.e. $P^*_{\mathrm{guess}}(x^*) = \sum_{a,x} \mathrm{Tr}(F^*_{a|x}\, \sigma^{\mathrm{obs}}_{a|x})$. Moreover, it outputs the coefficients $F^*_{a|x}$ of the optimal steering inequality that gives the tight upper bound on $P^*_{\mathrm{guess}}(x^*)$.

Once we have solved the dual problem (4.7) we can run a second SDP that optimizes the violation of the steering inequality $\sum_{a,x} \mathrm{Tr}(F^*_{a|x}\, \sigma_{a|x})$ over Alice's measurements $\{M_{a|x}\}_{ax}$:

$$\begin{aligned} \min_{\{M_{a|x}\}_{ax}} \quad & \textstyle\sum_{ax} \mathrm{Tr}[(M_{a|x} \otimes F_{a|x})\rho_{AB}] \\ \text{subject to} \quad & \textstyle\sum_a M_{a|x} = \mathbb{1} \qquad \forall\, x \\ & M_{a|x} \succeq 0 \qquad \forall\, a, x \end{aligned} \tag{4.8}$$

The solution of this optimization problem provides the measurements for Alice that allow for the certification of the most randomness using the steering inequality provided by the first SDP.

At this point, one can perform a see-saw iteration of the two SDPs in order to obtain the maximal randomness that can be certified from a given state, along with the optimal steering inequality and measurements $M_{a|x}$. The algorithm acts according to the scheme depicted in (4.9): given a state ρ_{AB} and a set of measurements $\{M^{(i)}_{a|x}\}_{a,x}$ for Alice, they lead to the assemblage $\{\sigma^{\mathrm{obs},(i)}_{a|x}\}_{a,x}$ using Eq. (2.5). This assemblage is input in the dual SDP (4.7) which provides the optimal steering inequality $\{F^{*\,(i)}_{a|x}\}_{a,x}$. This steering inequality is in turn used in the SDP (4.8) to obtain the optimal set of measurements $\{M^{*\,(i)}_{a|x}\}_{a,x}$, *i.e.* the measurements attaining the maximal violation.

At this point, we set $\{M_{a|x}^{(i+1)}\}_{a,x} = \{M_{a|x}^{*\,(i)}\}_{a,x}$ and repeat the iteration.

$$\begin{array}{ccc} \rho_{AB}, \{M_{a|x}^{(i)}\}_{a,x} & \xrightarrow{\text{Eq.(2.5)}} & \{\sigma_{a|x}^{\text{obs},(i+1)}\}_{a,x} \\ \uparrow & & \downarrow \text{SDP(4.7)} \\ \{M_{a|x}^{(i+1)}\}_{a,x} & \xleftarrow{\text{SDP(4.8)}} & \{F_{a|x}^{(i+1)}\}_{a,x} \end{array} \tag{4.9}$$

Hence, for every given initial state, the SDP (4.3) and its dual (4.7) give the best inequality to certify randomness from an assemblage, while the SDP (4.8) gives the best set of measurements – and therefore the best assemblage – for a given steering inequality.

In Fig. 4.6 we plot the result of this see-saw iteration, starting from two randomly chosen projective measurements, for $\eta = 1$ and $\eta = 0.9$, for the two-qubit partially entangled state $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$. When there are no losses, one bit of randomness is already known to be possible from any partially entangled state in the fully device-independent scenario [AMP12]. Since this scenario is more demanding, it implies one bit can also be obtained from any partially entangled state of two qubits in the steering scenario. If the method works it should be able to reproduce this result and, as can be seen, 1 bit of randomness is indeed found, thus demonstrating the utility of the method.

Further exploration showed numerically that contrary to the fully-DI case, here the measurements which achieve 1 bit of randomness from any partially entangled state can always be taken to be X and Z measurements (with the randomness obtained from the X measurement).

In Appendix B we show that this numerical evidence can in fact be turned into an analytic construction, which proves that 1 random bit can be obtained from any partially entangled state of two qubits (which is notably completely different to the approach used in [AMP12] for nonlocality). Moreover, the construction generalizes to qudits in a straightforward manner, showing that 1 dit of randomness can be obtained by performing two generalized Pauli measurements on any Schmidt-rank d state.

4.4 Discussion

We presented a method that certifies the optimal amount of local or global randomness that can be extracted in a steering experiment. Our method relies on optimization techniques that quantify the amount of certified randomness and provide the optimal steering inequality for randomness certification. Applying this method to realistic implementations - *i.e.* in presence of noise and losses - we have shown that a detection efficiency above 50%

is sufficient to achieve reliable local randomness certification in the steering scenario. Moreover, recalling the results derived in Chapter 3, we can conclude that having a detection efficiency higher than 50% is also a necessary condition to certify randomness in this scenario.

We also considered the case where additionally the source is trusted (prepare-and-measure scenario), and showed that in this scenario even states with low visibility are useful for randomness certification.

Finally, we have introduced a method which produces, for any given initial state, the optimal measurements which in turn give the optimal assemblage from which maximal randomness can be certified. Using this method as a starting point, we have shown analytically that 1 dit of randomness can be obtained from any pure entangled Schmidt-rank d state.

Chapter 5

Robustness of device-independent dimension witnesses

Device-independent dimension witnesses (DIDWs) provide a tool to test the dimensionality of an unknown physical system in a DI way.

DIDWs were first introduced in [BPA$^+$08] in the context of nonlocal correlations for multipartite systems. Later, the authors of [GBHA10] developed a general formalism for tackling the problem of DIDWs in a prepare-and-measure scenario. The derived formalism allows one to establish lower bounds on the classical and quantum dimension necessary to reproduce the observed correlations. Shortly after, the photon experimental implementations followed, making use of polarization and orbital angular momentum degrees of freedom [HGM$^+$12] or polarization and spatial modes [ABCB12] to generate ensembles of classical and quantum states, and certifying their dimensionality as well as their quantum nature.

The framework of DIDWs is suitable for experimental implementation and for application in different contexts, such as quantum key distribution [PB11] or quantum random access codes [LPY$^+$12, PZ10]. Indeed, apart from the fundamental interest of characterizing the Hilbert space dimension, it turns out that DIDWs can also distinguish between classical and quantum systems of the same dimension. Therefore, they provide a quantum certification for semi-device-independent (SDI) protocols, where no assumption is made on the devices used by the honest parties, except that they prepare and measure systems of a given dimension.

Clearly any experimental implementation of DIDWs is unavoidably affected by losses - that can be modelled as a constraint on the measurements - and can reduce the value of the dimension witness, thus making it impos-

sible to witness the dimension of a system. In this Chapter we tackle the problem of robustness of DIDWs to loss, *i.e.* the problem of whether it is possible to perform reliable dimension witnessing with non-optimal detection efficiency. We study this problem in the case where shared randomness between preparations and measurements is allowed (we will analyze the case in which no shared correlations are allowed between the parties in Chapter 6). The main result is to provide the threshold in the detection efficiency that can be tolerated in dimension witnessing, in the case where one is interested in the dimension of the system as well as in the case where the goal is to discriminate between its quantum or classical nature.

In Section 5.1 we discuss some relevant properties of the sets of quantum and classical correlations. Then, in Section 5.2 we introduce the concept of dimension witness as a tool to discriminate whether a given correlation matrix belongs to these sets. The main result we provide here is a bound on the critical detection efficiency necessary for reliable dimension witnessing as a function of the dimension of the system. We summarize our results and discuss some further developments in Section 5.3.

5.1 Sets of classical and quantum correlations

The general setup for performing DI dimension witnessing (introduced in [GBHA10]) is given by a preparing device (let us say on Alice's side) and a measuring device (on Bob's side) as in Fig. 5.1.

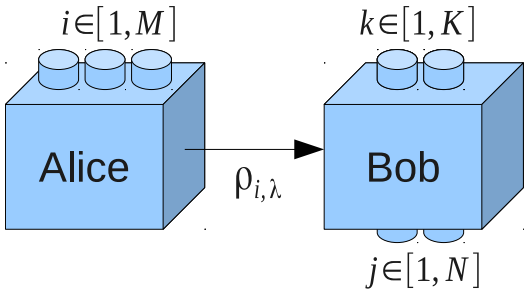

Figure 5.1: Setup for witnessing the dimension of a quantum or classical system. In the most general scenario considered here, Alice and Bob share a hidden random variable λ. Alice (on the left hand side) owns a preparing device which sends the state $\rho_{i,\lambda}$ to Bob whenever Alice presses button $i \in [1, M]$. Bob owns a measuring device that performs measurement $\Pi_{k,\lambda}$ on the received state whenever Bob presses button $k \in [1, K]$, giving the outcome $j \in [1, N]$.

In the most general scenario, the devices may share a priori correlated information, classical and quantum. In this Chapter we focus on the case in which the devices share a random variable λ distributed according to the distribution q_λ (the case in which the preparing and measuring devices are uncorrelated is considered in Chapter 6).

We notice that the notation used here is slightly different from the one used in Section 2.3. In the scenario considered in this Chapter, Alice chooses the value of index $i \in [1, M]$ and sends a fixed state $\rho_{i,\lambda} \in \mathcal{B}(\mathcal{H})$ to Bob, where $\mathcal{B}(\mathcal{H})$ denotes the space of linear operators $X : \mathcal{H} \to \mathcal{H}$. Bob chooses the value of index $k \in [1, K]$ and performs a fixed POVM $\Pi_{k,\lambda}$ on the received state, obtaining outcome $j \in [1, N]$. After repeating the experiment several times (we consider the asymptotic case), they collect the statistics about indexes i, j, k obtaining the conditional probabilities $p_{j|i,k}$.

We now introduce the set $\mathcal{Q}$ (the set $\mathcal{C}$) of correlations achievable with quantum (classical) preparations. In the following, we say that a set $R = \{\rho_i\}$ of states is classical when the states commute pairwise, $[\rho_i, \rho_k] = 0$ for any i, k [HGM+12, ZPWL11, LLF11, HSS07, HHHP06]. Likewise, a POVM $\Pi = \{\Pi^j\}$ is said to be classical when $[\Pi^j, \Pi^l] = 0$ for any j, l.

Formally, for any $M, K, N, d \in \mathbb{N}$ we define the *set of quantum correlations* $\mathcal{Q}(M, K, N, d)$ as the set of correlations $p_{j|i,k}$ with $i \in [1, M]$, $k \in [1, K]$ and $j \in [1, N]$ such that there exist a Hilbert space $\mathcal{H}$ with $\dim \mathcal{H} = d$, a quantum set $R = \{\rho_i \in \mathcal{H}\}_1^M$ of states and a set $P = \{\Pi_k\}_1^K$ of POVMs $\Pi_k = \{\Pi_k^j \in \mathcal{B}(\mathcal{H})\}_1^N$ for which $p_{j|i,k} = \mathrm{Tr}[\rho_i \Pi_k^j]$, namely

$$\begin{aligned}\mathcal{Q} := \{p \mid\ & \exists\ d\text{-dimensional Hilbert space } \mathcal{H}, \\ & \exists \text{ quantum set } \{\rho_i \in \mathcal{B}(\mathcal{H})\}_1^M \text{ of states}, \\ & \exists \text{ set } \{\Pi_k\}_1^K \text{ of POVMs } \Pi_k = \{\Pi_k^j \in \mathcal{B}(\mathcal{H})\}_1^N \\ & \text{such that } p_{j|i,k} = \mathrm{Tr}[\rho_i \Pi_k^j]\}.\end{aligned}$$

Analogously, for any $M, K, N, d \in \mathbb{N}$ we define the *set of classical correlations* $\mathcal{C}(M, K, N, d)$ as the set of correlations $p_{j|i,k}$ with $i \in [1, M]$, $k \in [1, K]$ and $j \in [1, N]$ such that there exist a Hilbert space $\mathcal{H}$ with $\dim \mathcal{H} = d$, a classical set $R = \{\rho_i \in \mathcal{B}(\mathcal{H})\}_1^M$ of states and a set $P = \{\Pi_k\}_1^K$ of POVMs $\Pi_k = \{\Pi_k^j \in \mathcal{B}(\mathcal{H})\}_1^N$ for which $p_{j|i,k} = \mathrm{Tr}[\rho_i \Pi_k^j]$, namely

$$\begin{aligned}\mathcal{C} := \{p \mid\ & \exists\ d\text{-dimensional Hilbert space } \mathcal{H}, \\ & \exists \text{ classical set } \{\rho_i \in \mathcal{B}(\mathcal{H})\}_1^M \text{ of states}, \\ & \exists \text{ set } \{\Pi_k\}_1^K \text{ of POVMs } \Pi_k = \{\Pi_k^j \in \mathcal{B}(\mathcal{H})\}_1^N \\ & \text{such that } p_{j|i,k} = \mathrm{Tr}[\rho_i \Pi_k^j]\}.\end{aligned}$$

We write $\mathcal{Q}$ and $\mathcal{C}$ omitting the parameters M, K, N, d whenever they are clear from the context.

We notice that, when shared randomness is allowed between quantum (classical) preparations and measurements, the set of achievable correlations is given by $\mathrm{Conv}\,\mathcal{Q}$ ($\mathrm{Conv}\,\mathcal{C}$), where for any set $\mathcal{X}$ we denote with $\mathrm{Conv}\,\mathcal{X}$ the convex hull of $\mathcal{X}$.

Here we show that it is not restrictive to consider only classical POVMs in the definitions of classical correlations. Concretely, we prove that for any correlation $p = \{p_{j|i,k}\} \in \mathcal{C}$ there exist a classical set $R = \{\rho_i\}$ of states and a set $Q = \{\Lambda_k\}$ of classical POVMs $\Lambda_k = \{\Lambda_k^j\}$ such that $p_{j|i,k} = \mathrm{Tr}[\rho_i \Lambda_k^j]$. Indeed, if $p = \{p_{j|i,k}\} \in \mathcal{C}$, by hypothesis there exist a classical set $R = \{\rho_i\}$ of states and a set $P = \{\Pi_k\}$ of POVMs $\Pi_k = \{\Pi_k^j\}$ such that $p_{j|i,k} = \mathrm{Tr}[\rho_i \Pi_k^j]$ for any i, j, k. Take $\Lambda_k^j = \sum_i \langle i|\Pi_k^j|i\rangle |i\rangle\langle i|$ where $\{|i\rangle\}$ is an orthonormal basis with respect to which the ρ_i's are diagonal (it is straightforward to verify that $\Lambda_k^j \geq 0$ for any k, j and $\sum_j \Lambda_k^j = \mathbb{1}$ for any k). Therefore we have $p_{j|i,k} = \mathrm{Tr}[\rho_i \Lambda_k^j]$ for any i, j, k which proves the previous statement, *i.e.* that every set of probabilities obtained with commuting states can be performed with classical states and classical POVMs. This clearly implies that commuting states may be equally regarded as classical variables, and the measurements as read-out of those classical variables.

Since classical correlations can always be reproduced by quantum ones, we immediately have $\mathcal{C} \subseteq \mathcal{Q}$ and $\mathrm{Conv}\,\mathcal{C} \subseteq \mathrm{Conv}\,\mathcal{Q}$. Moreover, by definition we have $\mathcal{C} \subseteq \mathrm{Conv}\,\mathcal{C}$ and $\mathcal{Q} \subseteq \mathrm{Conv}\,\mathcal{Q}$. In Appendix C we show an example where $\mathcal{C}$ is non-convex (namely $\mathcal{C} \subset \mathrm{Conv}\,\mathcal{C}$) and $\mathcal{C} \subset \mathcal{Q}$. Therefore, when the preparing and the measuring device are not allowed to share pre-established correlations, the sets of interest are non-convex and cannot be represented by a polytope. We postpone the analysis of this case to Chapter 6.

The relations between the sets of quantum and classical correlations are schematically depicted in Fig. 5.2.

5.2 Device-independent dimension witnesses

Building only on the knowledge of $p_{j|i,k}$, the task of a DIDW is to provide a lower bound on the dimension d of $\mathcal{H}$ or to certify that the states ρ_i must be quantum if their dimension is assumed to be smaller than a given value.

For any set of correlations $\mathcal{X}$ between M preparations and K measurements with N outcomes, a DIDW $W_{\mathcal{X}}(p)$ is a function of the conditional probability distribution $p = \{p_{j|i,k}\}$ with $i \in [1, M]$, $k \in [1, K]$, and $j \in [1, N]$

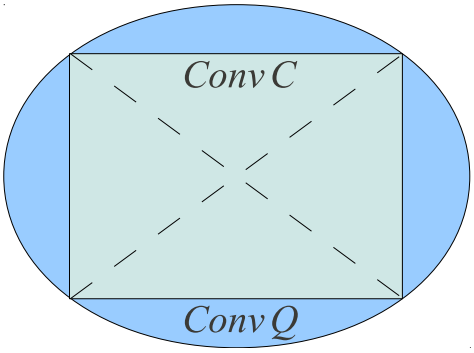

Figure 5.2: Schematic representation of the sets of classical and quantum correlations between preparations, measurements and outcomes. Dashed line represents the (non-convex) set $\mathcal{C}$ of classical correlations without shared randomness; the rectangle represents the set $\mathrm{Conv}\,\mathcal{C}$ of classical correlations with shared randomness; the ellipsoid represents the set $\mathrm{Conv}\,\mathcal{Q}$ of quantum correlations with shared randomness.

such that

$$W_{\mathcal{X}}(p) > L \Rightarrow p \notin \mathcal{X}, \tag{5.1}$$

for some L which depends on $W_{\mathcal{X}}$.

For any $M, N, K, d \in \mathbb{N}$ when $\mathcal{X} = \mathrm{Conv}\,\mathcal{C}(M, N, K, d)$ [when $\mathcal{X} = \mathrm{Conv}\,\mathcal{Q}(M, N, K, d)$] we say that $W_{\mathcal{X}}(p)$ is a classical (quantum) dimension witness for dimension d in the presence of shared randomness, since in this case the convex hulls of the correlation sets are involved. Given a set $R = \{\rho_{i,\lambda}\}$ of states and a set $P = \{\Pi_{k,\lambda}\}$ of POVMs $\Pi_{k,\lambda} = \{\Pi^j_{k,\lambda}\}$, we define $W_{\mathrm{Conv}\,\mathcal{C}}(R, P) := W_{\mathrm{Conv}\,\mathcal{C}}(p)$ with $p = \{p_{j|i,k}\}$ and $p_{j|i,k} = \sum_\lambda q_\lambda \,\mathrm{Tr}[\rho_{i,\lambda}\Pi^j_{k,\lambda}]$, and analogously for $W_{\mathrm{Conv}\,\mathcal{Q}}$.

Here we will consider only linear DIDWs, namely inequalities of the form of Eq. (5.1) such that

$$W(p) := \vec{c} \cdot \vec{p} = \sum_{i,j,k} c_{i,j,k} p_{j|i,k}, \tag{5.2}$$

where $\vec{c}$ is a constant vector.

Notice that for any function $W(p)$ and constant L, the witness $W(p) > L$ is only a representative of a class of equivalent witnesses such that if $W'(p) > L'$ is a member of the class, then $W(p) > L$ if and only if $W'(p) > L'$ for any conditional distribution p. The following Lemma provides a transformation that preserves this equivalence.

Lemma 1. *Given a function* $W(p) = \sum_{i,j,k} c_{i,j,k} p_{j|i,k}$ *and a constant* L*, take* $W'(p) = \sum_{i,j,k} c'_{i,j,k} p_{j|i,k}$ *with* $c'_{i,j,k} = c_{i,j,k} + \alpha_{i,k}$ *and* $L' = L + \sum_{i,k} \alpha_{i,k}$ *for any* $\alpha_{i,k}$ *that does not depend on outcome* j*. Then one has* $W(p) > L$ *if and only if* $W'(p) > L'$ *for any* p*.*

Proof. It follows immediately by direct computation. □

In the following our task is to find a set R of quantum states and a set P of POVMs such that a linear witness $W(R, P)$ maximally violates inequality (5.1). In order to simplify the optimization problem, we notice that due to linearity the maximum of any linear dimension witness $W(R, P)$ is achieved by an ensemble R of pure states and without shared randomness. Therefore, the maximization of Eq. (5.2) is equivalent to the maximization of

$$W(R, P) = \sum_{i,j,k} c_{i,j,k} \langle \psi_i | \Pi_k^j | \psi_i \rangle,$$

over the sets $R = \{\psi_i\}$ of pure states and the sets $P = \{\Pi_k\}$ of POVMs $\Pi_k = \{\Pi_k^j\}$, where $\psi := |\psi\rangle\langle\psi|$ denotes the projector corresponding to the pure state $|\psi\rangle \in \mathcal{H}$.

5.2.1 Robustness of DIDWs to loss

In practical applications, losses (due to imperfections in the experimental implementations or artificially introduced by a malicious provider) can noticeably affect the effectiveness of dimension witnessing. The main result of this Section is to provide a threshold value for the detection efficiency which allows to witness the dimension of the systems prepared by a source or to discriminate between its quantum or classical nature, when shared randomness between preparing and measuring devices is allowed. The task is to determine whether a given conditional probability distribution belongs to $\mathrm{Conv}\,\mathcal{C}$ or $\mathrm{Conv}\,\mathcal{Q}$. The situation is illustrated in Figure 5.3.

The experimental implementation is lossy and it can be modelled considering an ideal preparing device followed by a measurement device with non-ideal detection efficiency. This means that any POVM $\Pi_{k,\lambda}$ on Bob's side is replaced by a POVM $\Pi_{k,\lambda}^{(\eta)}$ with detection efficiency η, namely

$$\Pi_{k,\lambda}^{(\eta)} := \{\eta \Pi_{k,\lambda}, (1 - \eta)\mathbb{1}\}. \tag{5.3}$$

We notice that each lossy POVM has one outcome more than the ideal one, corresponding to the no-click event. In a general model, the detection efficiency η may be different for any POVM $\Pi_{k,\lambda}$. Nevertheless, in the following

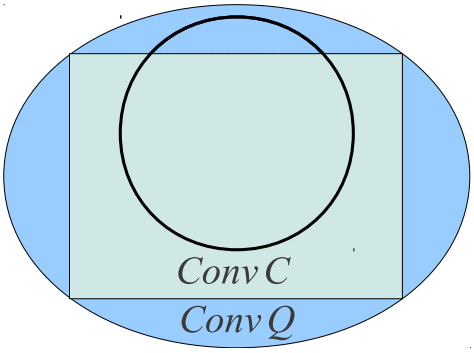

Figure 5.3: The Figure illustrates the problem of the robustness of device independent dimension witness. The convex hulls Conv $\mathcal{Q}$ and Conv $\mathcal{C}$ of the sets of quantum and classical correlations are represented as in Fig.5.2. In the presence of loss, only a subset of the possible correlations is attainable. The subset, surrounded by bold line in the figure, is parametrised by detection efficiency η. The task is to find the threshold value in η such that dimension witnessing is still possible. For example, when the task is to discriminate between the quantum or classical nature of a source, one is interested in achieving correlations in the dashed region, and our goal is to determine the values of η such that this area is not null.

we assume that they have the same detection efficiency, which is a reasonable assumption if the detectors have the same physical implementation [1]. Analogously given a set $P = \{\Pi_{k,\lambda}\}$ of POVMs we will denote with $P^{(\eta)} = \{\Pi^{(\eta)}_{k,\lambda}\}$ the corresponding set of lossy POVMs. Upon defining $p^{(\eta)} := \{p^{(\eta)}_{j|i,k}\}$ with $p^{(\eta)}_{j|i,k} = \sum_\lambda q_\lambda \operatorname{Tr}[\rho_{i,\lambda}\Pi^{j,(\eta)}_{k,\lambda}]$, one clearly has

$$p^{(\eta)} = \eta p^{(1)} + (1-\eta)p^{(0)}. \tag{5.4}$$

To attain our task we maximize a given dimension witness over the set of lossy POVMs as given by Eq. (5.3). Due to the model of loss introduced in Eq. (5.3) and to the freedom in the normalization of dimension witnesses given by Lemma 1, in the following without loss of generality for any dimension witness W as given in Eq. (5.2) it is convenient to take

$$c_{i,N,k} = 0, \quad \forall i,k. \tag{5.5}$$

[1] This is not the case in the hybrid scenario where different types of detectors (e.g. photodetectors and homodyne measurements) are used. A similar scenario was proposed for example in the context of Bell inequalities [CBS+11].

Here we prove that, given a set $R = \{\rho_{i,\lambda}\}_{i=1}^{M}$ of states and a set $P = \{\Pi_{k,\lambda}\}_{k=1}^{K}$ of POVMs $\Pi_{k,\lambda} = \{\Pi_{k,\lambda}^{j}\}_{j=1}^{N-1}$, for any linear dimension witness $W(p) = \sum_{i,j,k} c_{i,j,k} p_{j|i,k}$ with $i \in [1, M]$, $j \in [1, N]$, and $k \in [1, K]$ normalized as in Eq. (5.5) one has

$$W(R, P^{(\eta)}) = \eta W(R, P^{(1)}). \tag{5.6}$$

Indeed, one has

$$W(R, P^{(\eta)}) = \sum_{i,j,k} c_{i,j,k} \left[\eta p_{j|i,k}^{(1)} + (1-\eta) p_{j|i,k}^{(0)}\right] = \eta\, W(R, P^{(1)}),$$

where the first equality follows from Eq. (5.4) and the second from the fact that $W(p^{(0)}) = 0$ due to the normalization given in Eq. (5.5).

In particular from (5.6) it follows that for any linear dimension witness W one has

$$\max_{R,P} W(R, P^{(\eta)}) = \eta \max_{R,P} W(R, P^{(1)}),$$
$$\arg\max_{R,P} W(R, P^{(\eta)}) = \arg\max_{R,P} W(R, P^{(1)}).$$

Therefore, it is possible to recast the optimization of dimension witnesses in the presence of loss to the optimization in the ideal case. Then due to linearity we have noticed that it is not restrictive to carry out the optimization with pure states and no shared randomness. Consider the case where $M = d + 1$, $K = d$, and $N = 3$. Using the technique discussed in Appendix D.1 one can verify that the witness given by Eq. (5.2) with the following coefficients

$$c_{i,j,k} = \begin{cases} -1 & \text{if } i + k \leq M,\ j = 1 \\ +1 & \text{if } i + k = M + 1,\ j = 1 \\ 0 & \text{otherwise} \end{cases}, \tag{5.7}$$

is the most robust to non-ideal detection efficiency. This fact should not be surprising, as we notice that this witness relies on only 2 out of 3 outcomes. According to [GBHA10], we denote it I_{d+1}. In [GBHA10] (see also [Mas03]) it was conjectured that for any dimension d the dimension witness I_{d+1} is tight in the absence of loss.

Here we provide upper and lower bounds for the maximal value $I_{d+1}^{*} := \max_{R,P} I_{d+1}$ where the maximization is over any set $R = \{\rho_i \in \mathcal{B}(\mathcal{H})\}$ of states and any set $P = \{\Pi_k\}$ of POVMs $\Pi_k = \{\Pi_k^j \in \mathcal{B}(\mathcal{H})\}$ with $\dim \mathcal{H} = d$. We prove that for any dimension d we have

$$I_{d+1}^{*} \geq I_{d}^{*} + 1. \tag{5.8}$$

This follows from the recursive expression $I_{d+1} = I_d + C$, where

$$C := -\sum_{i=1}^{d} \langle \psi_i | \Pi_1^1 | \psi_i \rangle + \langle \psi_{d+1} | \Pi_1^1 | \psi_{d+1} \rangle,$$

and noticing that I_d and C can be optimized independently.

A tight upper bound for I_3 was provided in [GBHA10]. In the following we provide a constructive proof suitable for generalization to higher dimensions. We notice that for dimension $d = 2$ we have

$$I_3^* = \sqrt{2}. \tag{5.9}$$

The previous statement follows from standard optimization with Lagrange multipliers method and from the straightforward observation that given two normalized pure states $|v_0\rangle$ and $|v_1\rangle$, if a pure state $|u\rangle$ can be decomposed as follows

$$|u\rangle = \langle v_0|u\rangle |v_0\rangle + \langle v_1|u\rangle |v_1\rangle,$$

then $|\langle v_0|u\rangle| = |\langle v_1|u\rangle|$.

Making use of (5.8) and (5.9), we provide upper and lower bounds on I_{d+1}^* as follows

$$d - 2 + \sqrt{2} \leq I_{d+1}^* \leq d, \tag{5.10}$$

where the second inequality follows from the non discriminability of $d + 1$ states in dimension d (see [GBHA10]).

We now make use of these facts to provide our main result, namely a lower threshold for the detection efficiency required to reliably dimension witnessing. We consider the problem of lower bounding the dimension of a system prepared by a non-characterized source in Proposition 1, as well as the problem of discriminating between the quantum or classical nature of a source in Proposition 2.

Proposition 1. *For any d there exists a dimension witnessing setup such that it is possible to discriminate between the quantum and classical nature of a d-dimensional system using POVMs with detection efficiency η whenever*

$$\eta \geq \eta_{qc} := (d-1)/I_{d+1}. \tag{5.11}$$

Furthermore one has

$$\frac{d-1}{d} \leq \eta_{qc} \leq \frac{d-1}{d-2+\sqrt{2}}. \tag{5.12}$$

Proof. We provide a constructive proof of the statement. Take $M = d + 1$, $K = d$, and $N = 3$, and we show that I_{d+1} satisfies the thesis.

We notice that the maximum value of I_{d+1} attainable with classical states is given by $d - 1$ [GBHA10]. Then η_{qc} is the minimum value of the detection efficiency such that I_{d+1} can discriminate a quantum system from a classical one. Due to Eq. (5.6) we have Eq. (5.11). From Eq. (5.10) the lower and upper bounds for η_{qc} given in Eq. (5.12) straightforwardly follow. □

Notice that I_{d+1} in Eq. (5.11) can be numerically evaluated with the techniques discussed in Appendix D.2. Figure 5.4 plots the value of η_{qc} for different values of the dimension d of the Hilbert space $\mathcal{H}$. The threshold in the detection efficiency when $d = 2$ is $\eta_{\text{qc}} = 1/\sqrt{2}$, going asymptotically to 1 with d as $\sim 1 + 1/d$.

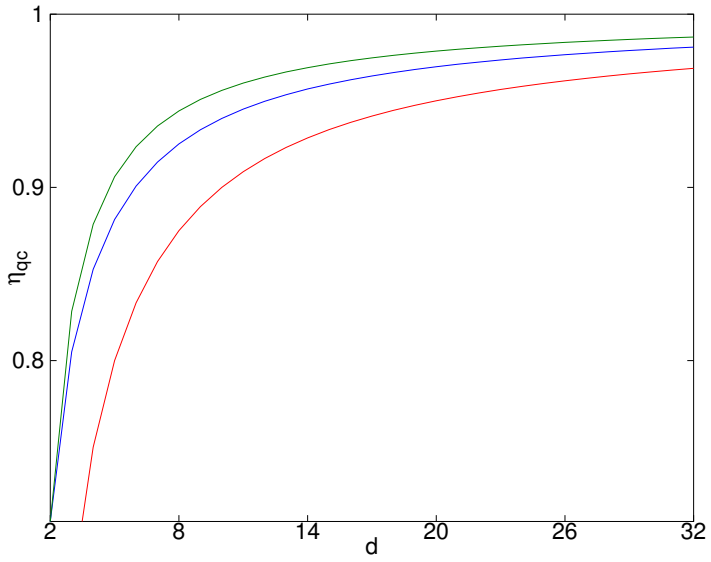

Figure 5.4: Threshold value (middle line) of the detection efficiency η_{qc} as in Eq. (5.11) as a function of the dimension d, obtained through numerical optimization of I_{d+1} with Algorithm 2. The lower bound (lower line) and upper bound (upper line) given by Eq. (5.12) are also plotted. As expected, the upper bound is tight for $d = 2$. The detection efficiency η_{qc} asymptotically goes to 1 as $d \to \infty$ since its upper and lower bound do the same.

Proposition 2. *For any d there exists a dimension witnessing setup such that it is possible to lower bound the dimension of a $d+1$-dimensional system*

using POVMs with detection efficiency η whenever

$$\eta \geq \eta_{dim} := I_{d+1}/d. \tag{5.13}$$

Furthermore one has

$$\eta_{dim} \geq 1 - \frac{2-\sqrt{2}}{d}. \tag{5.14}$$

Proof. We provide a constructive proof of the statement. Take $M = d + 1$, $K = d$, and $N = 3$, and we show that I_{d+1} satisfies the thesis.

We notice that the maximum value of I_{d+1} attainable in any dimension $> d$ is given by d [GBHA10]. Then η_{dim} is the minimum value of the detection efficiency such that I_{d+1} can lower bound the dimension of a $d+1$ dimensional system. Due to Eq. (5.6) we have Eq. (5.13). From Eq. (5.10) the lower bound to η_{dim} given by Eq. (5.14) straightforwardly follows. □

Notice that I_{d+1} in Eq. (5.13) can be numerically evaluated with the techniques discussed in Appendix D.2. Figure 5.5 plots the value of η_{dim} for different values of the dimension d of the Hilbert space $\mathcal{H}$. The threshold in the detection efficiency when $d = 2$ is $\eta_{\text{qc}} = 1/\sqrt{2}$, going asymptotically to 1 with d as $\sim 1 + 1/d$. We notice that η_{dim} grows faster than η_{qc}, thus showing that for fixed dimension, the discrimination between the quantum or classical nature of the source is more robust to loss than lower bounding the dimension of the prepared states.

5.3 Discussion

In this Chapter we addressed the problem whether a lossy setup can provide a reliable lower bound on the dimension of a classical or quantum system. First we provided some relevant properties of the sets of classical and quantum correlations attainable in a dimension witnessing setup. Then we introduced analytical and numerical tools to address the problem of the robustness of DIDWs, and we provided the amount of loss that can be tolerated in dimension witnessing. The presented results are highly relevant for experimental implementations of DIDWs, and can be naturally applied to SDIQKD and QRACs.

We notice that, while we provided analytical proofs of our main results, i.e. Propositions 1 and 2, their optimality as a bound relies on numerical evidences. In particular, they are optimal if the dimension witness I_{d+1} is indeed the most robust to loss for any d, which is suggested by numerical evidence obtained with the techniques of Appendix D.1 and Appendix D.2.

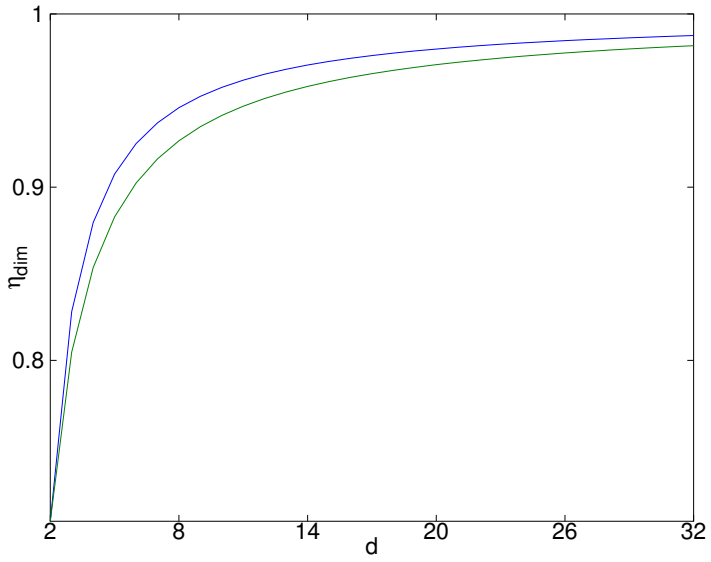

Figure 5.5: Threshold value (upper line) of the detection efficiency η_{dim} as in Eq. (5.13) as a function of the dimension d, obtained through numerical optimization of I_{d+1} with Algorithm 2. The lower bound (lower line) given by Eq. (5.14) is also plotted. As expected, the lower bound is tight for $d = 2$. The detection efficiency η_{dim} asymptotically goes to 1 as $d \to \infty$ since its lower bound does the same (and $\eta_{\text{dim}} \leq 1$ is a trivial upper bound).

Thus, a legitimate question is whether the bounds provided in Propositions 1 and 2 are indeed optimal. Moreover, it is possible to consider models of loss more general than the one considered in this Chapter, e.g. one in which a different detection efficiency is associated to any POVM.

A natural generalization of the problem of DIDWs, in the ideal as well as in the lossy scenario, is that in the absence of correlations between the preparations and the measurements. In this case, as discussed above, the relevant sets of correlations are $\mathcal{Q}$ and $\mathcal{C}$, which are non-convex as shown in Section 5.2. The non-convexity of the relevant sets allows the exploitation of non-linear witnesses [BQB14] - as opposed to what we did in the present Chapter. We address the problem to investigate the conditions under which this exploitation allows to dimension witness for any non-null value of the detection efficiency in Chapter 6.

Another natural generalization is that of entangled assisted DIDWs, namely when entanglement is allowed to be shared between the preparing device on

Alice's side and the measuring device on Bob's side. This problem is similar to that of super-dense coding [BW92]. Indeed, consider again Fig. 5.1; In the simplest super-dense coding scenario, Alice presses one button out of $M = 4$, while Bob always performs the same POVM ($K = 1$) obtaining one out of $N = 4$ outcomes. The dimension of the Hilbert space $\mathcal{H}$ is $\dim(\mathcal{H}) = 2$, but a pair of maximally entangled qubits is shared between the parties. In this case, the results of [BW92] imply that a classical system of dimension 4 (quart) can be sent from Alice to Bob by sending a qubit (corresponding to half of the entangled pair).

Consider the general scenario where now the two parties are allowed to share entangled particles. The super-dense coding protocol automatically ensures that by sending a qubit Alice and Bob can always achieve the same value of any DIDW as attained by a classical quart. Remarkably, the super-dense coding protocol turns out not to be optimal, as we identified more complex protocols beating it. In particular, we found a ($M = 4, K = 2, N = 4$) situation for which, upon performing unitary operations on her part of the entangled pair and subsequently sending it to Bob, Alice can achieve correlations that cannot be reproduced upon sending a quart. This thus proves the existence of communication contexts in which sending half of a maximally entangled pair is a more powerful resource than a classical quart. This observation is analogous to that done in [PZ10], where it was shown that entangled assisted QRACs (where an entangled pair of qubits is shared between the parties) outperform the best of known QRACs.

Chapter 6

Detection loophole attacks on semi-device-independent quantum and classical protocols

Recently, semi-device-independent (SDI) quantum protocols were proposed, in order to realize information tasks – e.g. secure key distribution, random access coding, and randomness generation – in a scenario where no assumption on the internal working of the devices used in the protocol is made, except their dimension. Those partly-DI protocols offer two main advantages: on the one hand, their implementation is often less demanding than fully-DI protocols; on the other hand, they are more secure than their device-dependent counterparts. The security of SDI protocols is based on the quantum certification provided by dimension witnesses for a fixed dimension [GBHA10].

SDI classical protocols – in which the exchanged system is classical – have also been proposed, and they are known as random access codes (RACs) [ALMO08]. In this context, the aim of two distant parties is to optimally perform some one-sided communication task under a constraint on the amount of classical information exchanged.

Despite their security, real world implementations of SDI (quantum or classical) protocols are subject to detection loophole (DL) attacks – as happens for any fully DI protocol. In a DL attack, a malicious provider exploits non-ideal detection efficiencies to skew the statistics of the experiment and ultimately fake its result. The main result of this Chapter is to provide conditions under which DL attacks are harmless in faking the result of a SDI (quantum or classical) protocol.

The problem of DL attack on SDI protocols shares analogies with the problem of the robustness to loss of device-independent dimension witness (DIDWs) [GBHA10, HGM$^+$12, ABCB12], addressed in Chapter 5. Nev-

ertheless, while in the latter the task is to devise conditions under which dimension witnessing is possible even in the presence of loss, in the present Chapter we consider an adversarial scenario, and the task is to prevent the exploitation of non-ideal detection efficiencies by a malicious eavesdropper to produce input/output statistics which would be forbidden in the absence of DL. Moreover, oppositely to what we do in Chapter 5, where no assumption is made about the functioning of the devices apart from their dimension, here we consider protocols in which the preparing and measuring devices do not share pre-established correlations, but only local randomness is allowed. In this case the set of d-dimensional classical correlations is in general non-convex (see Section 5.2 and Appendix C) and its characterization is a complex problem. Yet, we show that these non-convex sets of correlations are interesting when considering scenarios with inefficient detectors since their exploitation allows dimension witnessing for an arbitrary non-zero value of the detection efficiency.

In Section 6.1 we introduce DL attacks and present our main results. In Section 6.2 we derive conditions under which DL attacks on SDI quantum protocol are harmless, in the general framework where only the statistics of the protocol is taken into account. We address the problem of the certification of SDI classical protocols, in the framework of RACs, in Section 6.3. Finally, we summarize and discuss our results in Section 6.4.

6.1 Detection loophole attack

The general structure of SDI (quantum and classical) protocols is the one introduced in Section 2.3. The existing quantum protocols for QKD [PB11] and QRG [LPY$^+$12], as well as classical RACs, are examples of this structure. In this Chapter we consider SDI protocols in which the two parties, Alice and Bob, have access to uncorrelated random number generators. Notice that the assumption of uncorrelation is fulfilled by a broad class of protocols. Indeed, in any SDI setup one necessarily has to assume that the devices are shielded – namely they cannot communicate except through message A. Then to have shared (classical or quantum) randomness one is forced to introduce a trusted third party random generator, or to allow for infinite local memory on each device storing previously distributed randomness.

For each round, we denote by j (i) the random variable generated by Alice's (Bob's) generator and with q_j (p_i) its probability distribution. As said, these probability distributions are independent. Random variables j and i represent the strategy that Alice and Bob apply, respectively. This scheme is depicted in Fig. 6.1.

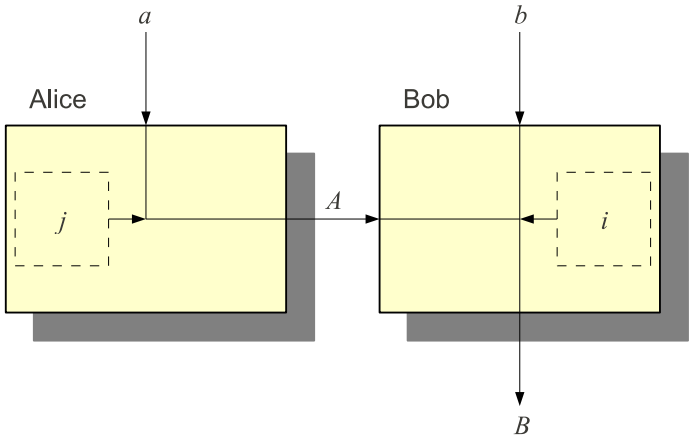

Figure 6.1: Scheme of a generic SDI (quantum or classical) protocol in which no shared randomness is allowed between the preparing and the measuring device. In this case, Alice and Bob's boxes are allowed to use a classical random generator (dashed-line boxes), which outcome – j for Alice's box and i for Bob's – is not accessible to the parties but can influence the outcome of the box.

In each run, Alice and Bob get classical inputs x and y respectively. Alice sends a message A – which may be classical or quantum – to Bob, who then returns a classical value b. Finally, collecting the statistics of several runs (the asymptotic case is always considered), they obtain the conditional probability distribution $P(b|x,y)$ of outcome b given inputs x and y, namely

$$P(b|x,y) := \sum_{i,j,A} p_i q_j P_i(b|A,y) P_j(A|x). \tag{6.1}$$

It is important to stress that – as Eq. (6.1) clearly shows – access is granted only to the inputs x, y and the output b, while no knowledge of the internal behavior of the black boxes (including the random variables i, j) and of the message A is provided. The goal is to exploit the correlations between the two parties, encapsulated by $P(b|x,y)$ to accomplish an information task, e.g. to distribute a secure key or generate random numbers.

When studying DL attacks, we assume that for each round of the experiment Alice or Bob can claim that their detector did not click, and in this case this round of the experiment is discarded from the statistics. In general, Alice's box can decide whether to click after receiving her input x and random variable j, while Bob's box after receiving his input y, the message A and random variable i. Thus, the detection efficiencies, i.e. the probabilities

that the detector clicks, are denoted with $\eta_j(x)$ for Alice and $\eta_i(A,y)$ for Bob. We notice that these probabilities cannot be estimated as they depend on the variables i and j internal to the devices. The conditional probability distribution of outcome b given inputs x and y in the presence of a DL attack is given by

$$P_{DL}(b|x,y) := \frac{\sum_{i,j,A} p_i q_j \eta_i(A,y)\eta_j(x)P_i(b|A,y)P_j(A|x)}{\sum_{i,j,A} p_i q_j \eta_i(A,y)\eta_j(x)P_j(A|x)}. \tag{6.2}$$

We use the subscript DL whenever a distribution is obtained resorting to DL attack, *i.e.* discarding the no-click events. We are assuming that for every input x, y there is a non-zero probability of click, namely denominator in Eq. (6.2) is strictly larger than 0 for any x and y.

Notice that whether Alice uses DL is not relevant[a], since any settings that she can prepare with DL can also clearly be achieved without resorting to it, so Eq. (6.2) can be simplified as

$$P_{DL}(b|x,y) = \frac{\sum_{i,A} p_i \eta_i(A,y)P_i(b|A,y)P(A|x)}{\sum_{i,A} p_i \eta_i(A,y)P(A|x)}, \tag{6.3}$$

where $P(A|x) := \sum_j q_j \eta_j(x)P_j(A|x)/\sum_j q_j\eta_j(x)$.

Independently of the task to be realized, all the known examples of SDI quantum protocols are based on the quantum certification provided by dimension witnesses [GBHA10] or, in other words, on the fact that, for a fixed dimension of the exchanged system A, there are quantum distributions $P(b|x,y)$ that cannot be attained when system A is classical - a system is classical if the states in which it can be prepared are pairwise commuting. This quantum certification plays here the same role as Bell violations for fully DI protocols. Our purpose is then to understand how a DL attack can mimic correlations that are intrinsically quantum exploiting the losses in the implementation. That is, rather than analyzing the effect of losses for a given quantum protocol, we study situations in which the observed correlations are useless for any quantum protocol. This is analogous to what is done when studying the detection loophole for Bell inequalities.

On the other hand, for classical protocols such a general approach is obviously not possible. However, when addressing the problem of classical

[a]This may be no more true if other constraints are introduced, since in this case the sets of distributions $P(A|x)$ and $P_{DL}(A|x)$ attainable by Alice can be different. For example, suppose that Alice is computationally constrained to prepare message A in time polynomial in the size of x. On the one hand, without resorting to DL it is impossible to obtain the distribution $P(A|x) = \delta_{A,f(x)}$, with $f(x)$ some NP-hard function (as long as we assume that $P \neq NP$). On the other hand, exploiting DL Alice can randomly choose A and check in polynomial time whether $A = f(x)$, clicking only in this case.

RACS, one is usually interested in maximizing some figure of merit related to the particular communication task, such as the worst case or average probability of correct detection. Here we will focus on the former - being the latter related by Yao's principle [ALMO08, Yao77] – and we will devise conditions under which it cannot be improved resorting to DL attack.

6.2 Certification of semi-device-independent quantum protocols

In this Section, we focus on SDI quantum protocols, namely where the exchanged system A is quantum. As mentioned, the success of SDI quantum protocols depends on the generated statistics. Usually, for a given protocol, a large enough value of a particular function of such statistics ensure the success of the protocol. For instance, the protocol in [PB11] is secure only when it is assumed that the dimension of the measured systems is two and a large value of a dimension witness is observed. Yet, in general, a necessary condition for the successful performance of any protocol is the ability to discriminate whether the source is intrinsically quantum or it can be described as a classical distribution, building only on the knowledge of the conditional probability distribution $P(b|x,y)$. That is, it is necessary to certify that the observed correlations cannot be explained classically and, therefore, are potentially useful for quantum protocols without classical analogue. The advantage of this approach is that it allows one to evaluate necessary conditions for security irrespectively of the particular protocol considered. Indeed, finding a DL attack able to fake an intrinsically quantum distribution by exploiting detection inefficiencies makes the observed correlations useless for any protocol. In this Section we provide conditions under which DL attack can by no means recast a classical $P(b|x,y)$ into an intrinsically quantum $P_{DL}(b|x,y)$ thus faking the result of the protocol.

We say that a conditional probability distribution $P(b|x,y)$ of outcome b given inputs x on Alice's side and y on Bob's side admits a classical (quantum) d-dimensional model if it can be written as

$$P(b|x,y) = \sum_{A,i} p_i P_i(b|A,y) P(A|x),$$

where

$$\sum_A P(A|x) = 1,\ \forall x, \quad \sum_b P_i(b|A,y) = 1,\ \forall A,y,i, \tag{6.4}$$
$$P(A|x) \geq 0\ \forall A,x, \quad P_i(b|A,y) \geq 0\ \forall b,A,y,i$$

for some probability p_i and where A is a classical (quantum) d-dimensional system. Given some correlations with losses, we say that DL attacks are harmless whenever there is no classical attack faking the correlations.

The probability of click on Bob's side given he received message A from Alice and input y is given by

$$Q(b \neq \emptyset|A, y) := \sum_i p_i \eta_i(A, y),$$

where $\emptyset$ denotes the no-click event. Now we show that whenever

$$Q(b{\neq}\emptyset|A, y) = Q(b{\neq}\emptyset|y), \tag{6.5}$$

DL attacks are harmless. Formally, we want to prove that if $Q(b{\neq}\emptyset|A, y) = Q(b{\neq}\emptyset|y)$ for any A, y, then if $P_{DL}(b|x, y)$ does not admit a d-dimensional classical (quantum) model then neither $P(b|x, y)$ does. To show this, we prove that under the hypothesis (6.5), if $P(b|x, y)$ admits a d-dimensional classical (quantum) model then also $P_{DL}(b|x, y)$ admits a d-dimensional classical (quantum) model.

Let us then assume that $P(b|x, y)$ admits a classical (quantum) model, namely it can be written as

$$P(b|x, y) = \sum_{A,i} p_i P_i(b|A, y) P(A|x),$$

with $P_i(b|A, y), P(A|x)$ satisfying Eq. (6.4) and for some probability p_i. Then by definition

$$P_{DL}(b|x, y) = \frac{\sum_{i,A} p_i \eta_i(A, y) P_i(b|A, y) P(A|x)}{\sum_{i,A} p_i \eta_i(A, y) P(A|x)}.$$

Upon introducing the hypothesis $Q(b{\neq}\emptyset|A, y) = Q(b{\neq}\emptyset|y)$ one has

$$P_{DL}(b|x, y) = \frac{\sum_{i,A} p_i \eta_i(A, y) P_i(b|A, y) P(A|x)}{Q(b{\neq}\emptyset|y)}.$$

Thus, setting

$$P_{DL}(b|A, y) = \frac{\sum_i p_i \eta_i(A, y) P_i(b|A, y)}{Q(b{\neq}\emptyset|y)},$$

one clearly has $\sum_b P_{DL}(b|A, y) = 1$ and $P_{DL}(b|A, y) \geq 0$ for any b, A, y. Then $P_{DL}(b|x, y)$ admits the d-dimensional classical (quantum) model

$$P_{DL}(b|x, y) = \sum_A P_{DL}(b|A, y) P(A|x).$$

Then, whenever $P_{DL}(b|x,y)$ does not admit a d-dimensional classical (quantum) model, also $P(b|x,y)$ does not.

At this point it is convenient to discuss condition (6.5) in relation with the fair sampling assumption. As we have seen above, the latter states that the set of events in which the detectors clicked is a randomly chosen sample from the total set of events that one would have obtained with perfect detectors, *i.e.*

$$P_{DL}(b|x,y) = P(b|x,y). \tag{6.6}$$

One can clearly see by using Eq. (6.3), that (6.5) does not necessarily imply the fair sampling assumption. Indeed, in order to fulfill the fair sampling assumption for every choice of $\{p_i, P(A|x), P_i(b|A,y)\}$, one needs that $\eta_i(A,y) = \eta(y)$. On the other hand, in order to fulfill (6.5) for every function p_i it suffices that $\eta_i(A,y) = \eta_i(y)$. In this sense, the condition (6.5) generalizes the fair sampling assumption, providing strictly weaker hypothesis under which DL-attacks are harmless.

Nonetheless, the fair sampling assumption and our slightly more general condition (6.5) have in common that they refer to properties of the internal working of the devices. In particular, condition $\eta_i(A,y) = \eta_i(y)$ – or the more constraining fair sampling assumption – cannot be verified solely from the statistics, since the message A sent by Alice is not directly accessible to the parties.

Here we provide a much stronger condition for DL attacks to be harmless, as it is stated only in terms of the probability $Q(b{\neq}\emptyset|x,y)$ of click given inputs x on Alice's side and y on Bob's side, namely

$$Q(b{\neq}\emptyset|x,y) := \sum_{i,A} p_i \eta_i(A,y) P(A|x). \tag{6.7}$$

Notice that this probability is accessible to the parties, being a function of the inputs x, y which are in turn accessible. In the following we show that whenever statistics of bidimensional systems fulfill

$$Q(b{\neq}\emptyset|x,y) = Q(b{\neq}\emptyset|y) \;\; \forall x,y \tag{6.8}$$

DL-attacks are harmless.

Specifically, we want to show that if Eq. 6.8 holds, then if $P_{DL}(b|x,y)$ does not admit a 2-dimensional classical model then neither $P(b|x,y)$ does. Let us prove a converse equivalent statement, *i.e.* that if condition 6.8 holds, then whenever $P(b|x,y)$ admits a 2-dimensional classical model then also $P_{DL}(b|x,y)$ admits a 2-dimensional classical model. We notice that by hy-

pothesis [Eq. (6.8)], for any pair of inputs x_0, x_1 on Alice's side one has

$$\sum_A Q(b{\neq}\emptyset|A, y)\,[P(A|x{=}x_0) - P(A|x{=}x_1)] = 0,$$

where the sum is over $A = 0, 1$.

Rearranging explicitly the terms in previous Equation and using the fact $P(A = 1|x) = 1 - P(A = 0|x)$ for any x, one obtains that either

$$P(A{=}0|x{=}x_0) = P(A{=}0|x{=}x_1),$$

for any x_0, x_1, namely the message A sent by Alice is independent on her input x, or

$$Q(b{\neq}\emptyset|A{=}0, y) = Q(b{\neq}\emptyset|A{=}1, y),$$

for any y, namely the detection probability on Bob's side is independent on the message A received from Alice.

In the former case $P(b|x, y)$ clearly admits a classical local model, namely one in which no message is sent from Alice to Bob, and the same holds true for $P_{DL}(b|x, y)$ due to Eq. (6.3). In the latter case the hypothesis (6.5) of the previous statement is satisfied, and accordingly to what we proved the thesis follows.□

As said, contrary to the previous proof that used the hypothesis (6.5), this result is much stronger, as it is proven under an assumption that can be verified only from the observed statistics. The price to pay is that it only holds for systems of dimension two. Condition (6.8) is, therefore, highly inequivalent to (6.5) or the fair sampling assumption. In fact, the attack presented in [LWW$^+$10, GLLL$^+$11] fulfills condition (6.8), however clearly violates the fair sampling assumption (but also violates the assumption on the dimension).

Recalling the definition of the sets of classical correlations given in Section 5.1 for DIDWs, we have just proved that if condition (6.8) holds, then if $P_{DL}(b|x, y) \notin \mathcal{C}(M, K, N, 2)$ also $P(b|x, y) \notin \mathcal{C}(M, K, N, 2)$, for any non-null value of the overall detection efficiency. Thus, adding an additional constraint to the devices, namely that they do not share correlations, one can exploit the non-convexity of the set $\mathcal{C}(M, K, N, 2)$ to perform detection-loophole-free dimension witnessing (for dimension 2) for any value of the detection efficiency. This is very useful for experimental implementation of dimension witnessing in presence of loss, where the task is to determine whether the observed conditional probability distribution $P_{DL}(b|x, y)$ belongs to the set $\mathcal{C}$ of classical correlations. Indeed, if $P_{DL}(b|x, y)$ violates a DIDW for dimension 2, and therefore does not admit a bidimensional classical model,

then the experimenter can deduce that the ideal conditional probability distribution $P(b|x,y)$ (without post-processing) also cannot be described by a bidimensional classical model, as long as condition (6.8) is met.

6.3 Certification of semi-device-independent classical protocols

In this Section, we focus on SDI classical protocols, namely where the exchanged system A is classical. We devise functions of the input/output statistics that cannot be altered by DL attacks. Thus, any certification for SDI classical protocols building only on the value of these functions will be immune to DL attacks. Again, the main advantage is that, as above, these functions can be verified only from the observed statistics.

A SDI classical protocol can be viewed as a random access code [ANTSV02, HIN$^+$06] (RAC), and in the following it will be convenient to work in the framework of RACs. In this framework, the aim of the two distant parties Alice and Bob is to optimally perform some communication task by means of one-sided communication of classical information. RACs are usually denoted with the notation $n \to m$. Here n is the number of input bits of Alice, namely the dimension of input x is $\dim(x) = 2^n$, while m is the number of bits sent by Alice, namely the dimension of message A is $\dim(A) = 2^m$ (see Fig. 6.1).

In this scenario, the relevant figures of merit usually considered are the worst case or the average success probability to have that $b = f(x,y)$ for a specific Boolean function $f(x,y) \in \{0,1\}$. Here we will focus on the former, being the latter related through Yao's principle [Yao77]. The worst case probability of success P^{wc} is defined as

$$P^{wc} := \min_{x,y} P(B{=}f(x,y)|x,y).$$

The probability that $b = f(x,y)$ with the DL exploit is given by

$$P_{DL}(b{=}f(x,y)|x,y) = \frac{\sum_{i,A} w_i(A,x,y) P_i(b{=}f(x,y)|A,y)}{\sum_{i,A} w_i(A,a,y)}, \tag{6.9}$$

where $w_i(A,x,y) = p_i \eta_i(A,y) P(A|x)$ and the worst case probability that $b = f(x,y)$ is given by

$$P^{wc}_{DL} := \min_{x,y} P_{DL}(b{=}f(x,y)|x,y).$$

Here we provide conditions under which the worst case success probability of a RAC cannot be increased resorting to DL exploitation. When these hypotheses are satisfied, a protocol relying on the worst case success probability may not be affected by DL attack.

Specifically, we prove that given a RAC, if the worst case success probability without resorting to DL attack is P^{wc}=1/2, then the worst case probability of success resorting to DL attack is P^{wc}_{DL}=1/2.

The proof proceeds by absurd assuming $P^{wc} = 1/2$ and $P^{wc}_{DL} > 1/2$. Equation (6.9) is the weighted sum over indices i and A of the numbers $P_i(b = f(x,y)|A,y)$ with weights $w_i(A,x,y)/\sum_{i,A} w_i(A,x,y)$ and therefore is upper bounded by

$$P_{DL}(b{=}f(x,y)|x,y) \leq \max_{A,i}\{P_i(b{=}f(x,y)|A,y)\},$$

and one has

$$P^{wc}_{DL} \leq \min_{x,y}\max_{A,i}\{P_i(b{=}f(x,y)|A,y)\}.$$

Since we are assuming $P^{wc}_{DL} > 1/2$ there exists a strategy i_0 of Bob and a message A_0 of Alice such that for all x, y one has $P_{i_0}(b = f(x,y)|A_0,y) > 1/2$. Then Bob can exploit a new strategy where he applies strategy i_0 whenever he gets A_0 and returns a random number otherwise, for which the probability $\tilde{P}(b{=}f(x,y)|x,y)$ of $b{=}f(x,y)$ given inputs x and y is given by

$$\tilde{P}(b{=}f(x,y)|x,y) = \left[P_{i_0}(b{=}f(x,y)|A_0,y) - \frac{1}{2}\right] P(A_0|x) + \frac{1}{2}.$$

This new strategy does not resort to DL and since $P_{i_0}(b = f(x,y)|A_0,y) > 1/2$ it has the worst case success probability greater than

$$\tilde{P}^{wc} = \min_{x,y}\{\tilde{P}(b{=}f(x,y)|x,y)\} > \frac{1}{2}$$

which contradicts the assumptions.□

Now we show that for any $n \to 1$ RAC, the worst case success probability resorting to DL attack is P^{wc}_{DL}=1/2, *i.e.* DL attacks are harmless. Indeed, in [ANTSV99] it was shown that for any $n \to 1$ RAC the hypothesis $P^{wc} = 1/2$ is fulfilled, so the statement follows.

One may ask whether it is possible to relax this hypothesis, namely if also RACs with $P^{wc} > 1/2$ cannot be affected by DL attack. We provide here an example of RAC with worst case success probability larger than 1/2, and show that this probability can be increased using DL attack. Consider

the $3 \to \log 6$ RAC. Alice is given three independent bits x_0, x_1, x_2, namely $x = x_0 \otimes x_1 \otimes x_2$, and she can send to Bob a 6-dimensional message or, equivalently, one bit A_0 and one trit A_1, namely $A = A_0 \otimes A_1$. Bob's input is the trit $y = 0, 1, 2$ and the function to be computed is $f(x, y) = x_y$. Here we show that the worst case success probability P^{wc} without resorting to DL of $3 \to \log 6$ RAC is $P^{wc} < 0.981$, while there exists a DL attack such that the worst case success probability is $P^{wc}_{DL} = 1$.

First, we prove that for the $3 \to \log 6$ RAC one has $P^{wc} < 0.981$. An explicit upper bound for the worst case quantum success probability – which is clearly at least as large as the classical one P^{wc} – was derived in [Nay99] in the context of quantum finite automata, namely

$$(1 - h(P^{wc}))n \leq m,$$

where $h(.)$ is the Shannon binary entropy function. Setting $n = 3$ and $m = \log 6$ we get $P^{wc} < 0.981$.

Now we provide a protocol using DL which achieves the worst case success probability $P^{wc}_{DL} = 1$. The idea is to use part of the communicated message to distribute randomness. Alice can choose the trit A_1 at random and encode $A_0 = x_{A_1}$, in other words she sends one of her bits randomly to Bob but also sends him information regarding which bit it is. If $y = A_1$ then Bob returns $y = A_0$ which is equal to x_y. If $y \neq A_1$ his detector does not click. The detection efficiency of Bob's device with this protocol is given by $\eta_i(A, y) = \delta_{y,A_1}$, and the worst case success probability is given by $P^{wc}_{DL} = 1$.

6.4 Discussion

In this Chapter we addressed the problem of how non-ideal detection efficiencies can be exploited to fake the result of SDI quantum and classical protocols through DL attacks. For quantum protocols, we discussed general conditions under which DL attacks are harmless in terms of the detection probability. Furthermore we showed that an extra assumption on the functioning of the devices - namely that they do not share correlations - allows one to bound the dimension for an arbitrary non-zero value of the detection efficiency. In this case, we presented the requirements to answer the question whether the ideal conditional probability distribution $P(b|x, y) \in \mathcal{C}$ from the knowledge of $P_{DL}(b|x, y)$ only. These results are thus of relevance for the quantum certification of the devices. For classical protocols, we provided conditions under which DL attacks cannot increase the worst case success probability of a RAC. Our main results can be used as a general guideline to

devise quantum and classical protocols resistant to attacks that take advantage of detection inefficiencies, being thus of relevance for applications such as quantum key distribution, quantum randomness generation, and RACs. A natural follow-up question is to understand how DL attacks apply to specific examples of SDI protocols.

Chapter 7

Joining and splitting the quantum states of photons

In order to exploit the enhanced computational power provided by quantum information technology, one major challenge nowadays is to significantly increase the amount of information that can be processed simultaneously. In photonic approaches [KMN+07, OFV09, PCL+12], one can raise the number of qubits by increasing the number of photons in which information is encoded. Alternatively, one can exploit an enlarged quantum dimensionality within the same photon by combining different degrees of freedom, such as polarization, time-bin, wavelength, propagation paths, or transverse modes such as orbital angular momentum [MVWZ01, BLPK05, MTTT07, LBA+09, CVDM+09, NSM+10, SK10, NGM+10].

In this Chapter we study the recently demonstrated processes of quantum state joining and splitting [VSA+13], which combine these two methods and enable to dynamically switch from one to the other even during the computational process itself. More precisely, in the quantum state joining process two arbitrary qubits initially encoded in separate input photons are combined into a single output photon, within a four-dimensional quantum space. The quantum state splitting process consists in the inverse process, namely in which the four-dimensional quantum information carried in a single input photon is split into two output photons, each carrying a qubit. Since both processes are in principle iterable [VSA+13], they provide a useful interface for converting multiparticle quantum information protocols into protocols that exploit many degrees of freedom of one particle and vice versa, thus allowing to integrate the two encoding methods. These processes can be used to multiplex and demultiplex the quantum information across photons in quantum communication networks, for example with the purpose of using a smaller number of photons in lossy transmission channels. The idea of mul-

tiplexing/demultiplexing the quantum information in photons was proposed for example in [GECP08], but a complete implementation scheme had not been developed (in particular, the proposal reported in [GECP08] relies on the existence of a hypothetical CNOT gate in polarization encoding between photons which is independent of the spatial mode of the photons, but the proposal does not include a discussion on how to realize this gate in practice) and had not been experimentally demonstrated. In addition, the quantum joining and splitting schemes might also find application in the storing of multiple incoming photonic qubits in a smaller number of multilevel matter registers [JSC$^+$04].

This Chapter is structured as follows. In Section 7.1, the joining/splitting schemes are revisited by adopting the more general photon occupation-number formalism and some variants of the original schemes are introduced which do not need a projection and feed-forward mechanism to work (not considering the CNOT implementation), although at the price of using a doubled number of CNOT gates. In Section 7.2, we then develop a formal proof of the fact that quantum joining is impossible for an arbitrary linear optical scheme involving only two photons and a final post-selection step. Hence, at least one ancilla photon is needed (or the presence of optical nonlinearity). In Section 7.3, we analyze the relationship between the joining process of two photonic qubits and a particular class of three-photon entangled states, in which two photons are separately entangled with a common "intermediate" photon. We show that the quantum joining process can be used to create such cluster states and that, conversely, having at one's disposal one of these states, the quantum joining of two other photons can be immediately achieved by a teleportation scheme. We also note that these three-photon entangled states are of the same kind as the "linked" multiphoton states first introduced by Yoran and Reznik to perform deterministic quantum computation with linear optics [YR03]. Finally, in Section 7.4, we draw some concluding remarks.

7.1 Joining and splitting schemes in a photon-number notation

In this Section, we revisit the joining and splitting schemes introduced in [VSA$^+$13] adopting the more general photon-number notation, as opposed to the polarization-ket notation used in [VSA$^+$13] and in Section 2.5. In particular, photonic qubits will be represented as pairs of modes, with one photon that can occupy either one, as in the "dual-rail" qubit encoding. Of course, the two modes can also correspond to two orthogonal polarizations

of a single spatial mode, thus reproducing the polarization-encoding case.

Given two modes forming a qubit, the $|10\rangle$ ket, where the 0's and 1's refer here to the photon numbers, corresponds to having a photon in the first mode, encoding the logical 0 of the qubit. The $|01\rangle$ ket will then represent the photon in the second path, encoding the logical 1 of the qubit. For our schemes, we will however also need the $|00\rangle$ ket, representing a vacuum state, i.e. the "empty" qubit.

The basic difficulty with implementing the quantum state joining/splitting processes is that a form of interaction between photons is needed. But photons do not interact in vacuum and exhibit exceedingly weak interactions in ordinary nonlinear media. A way to introduce an effective interaction, known as the Knill-Laflamme-Milburn (KLM) method [KLM01], is based on exploiting two-photon interferences and a subsequent "wavefunction collapse" occurring on measurement. This idea allowed for example the first experimental demonstrations of controlled-NOT (CNOT) quantum logical gates among qubits carried by different photons [OPW$^+$03, PFJF03, GPW$^+$04, ZZC$^+$05], and is at the basis of the implementation of the quantum joining and splitting processes described in this Section.

To get the main idea of the quantum joining implementation, consider again the two input photons given in Eq. (2.12). A single CNOT gate using one photon qubit as "target" and the other as "control" may be used to transfer a qubit from a photon to another, if the receiving photon initially carried a zeroed qubit. In order to obtain the state joining, we might then try for example to transfer the qubit ϕ from photon 2 to photon 1, while preserving the other qubit ψ by storing it into a different degree of freedom of photon 1 (for example spatial modes). However, the interference processes utilized in the KLM CNOT require the two photons to be indistinguishable in everything, except for the qubit ϕ involved in the transfer. So, they are disrupted by the presence of the second qubit ψ carried by the target photon, even if stored in different degrees of freedom.

To get around this obstacle, the authors of [VSA$^+$13] proposed a scheme that is based on the following three main subsequent steps: (i) "unfold" the target qubit ψ (carried by input photon 1) initially travelling in mode t, by turning it into the superposition $\alpha|H\rangle_{t_1} + \beta|H\rangle_{t_2}$ of two zeroed polarization qubits, travelling in separate optical modes t_1 and t_2; (ii) duplicate the control qubit ϕ (carried by input photon 2) travelling in mode c on an ancillary photon travelling in mode a, thus creating the entangled state $\gamma|H\rangle_c|H\rangle_a + \delta|V\rangle_c|V\rangle_a$; (iii) execute two KLM-like CNOT operations (of the Pittman kind [PJF01, PFJF03]), one with modes c and t_1, the other with modes a and t_2. In this way, each CNOT operates with a target photon that carries a zeroed qubit and no additional information, but the target photon is always

interacting with either the control qubit or its entangled copy.

To complete the process, the photons travelling in modes c and a must be finally measured. For certain outcomes of this measurement, occurring with probability 1/32, the outgoing target photon is then collapsed in the final "joined" state $|\psi \otimes \phi\rangle = \alpha\gamma|H\rangle_{t_1} + \alpha\delta|V\rangle_{t_1} + \beta\gamma|H\rangle_{t_2} + \beta\delta|V\rangle_{t_2}$, which contains all the quantum information of the two input photons. The success probability can be raised to 1/8 by exploiting a feed-forward scheme and using other measurement outcomes. This probabilistic feature of the setup is common to all KLM-based implementations of CNOT gates (although, in principle, the success probability could be raised arbitrarily close to 100% by using a large number of ancilla photons).

7.1.1 Quantum state joining scheme

Let us first consider the joining process, schematically illustrated in Fig. 7.1a. Labelling as c (for control) and t (for target) the travelling modes of the two input photons, the input state is taken to be the following:

$$\begin{aligned} |\Psi\rangle_i &= \alpha_0|10\rangle_t|10\rangle_c + \alpha_1|10\rangle_t|01\rangle_c \\ &\quad +\alpha_2|01\rangle_t|10\rangle_c + \alpha_3|01\rangle_t|01\rangle_c, \end{aligned} \tag{7.1}$$

which may represent both separable and non-separable two-photon states.

The qubit "unfolding" step corresponds to adding two empty modes for photon t and rearranging the four modes so as to obtain the following state:

$$\begin{aligned} |\Psi\rangle_u &= \alpha_0|1000\rangle_t|10\rangle_c + \alpha_1|1000\rangle_t|01\rangle_c \\ &\quad +\alpha_2|0010\rangle_t|10\rangle_c + \alpha_3|0010\rangle_t|01\rangle_c \\ &= \alpha_0|10\rangle_{t_1}|00\rangle_{t_2}|10\rangle_c + \alpha_1|10\rangle_{t_1}|00\rangle_{t_2}|01\rangle_c \\ &\quad +\alpha_2|00\rangle_{t_1}|10\rangle_{t_2}|10\rangle_c + \alpha_3|00\rangle_{t_1}|10\rangle_{t_2}|01\rangle_c, \end{aligned} \tag{7.2}$$

where in the second expression we have split the four t modes, so as to treat the first two as one qubit (t_1) and the final two as a second qubit (t_2). Notice that both of them are initialized to logical zero, but with the possibility for each of them to be actually empty.

Each of these qubits must now be subject to a CNOT gate, using the same c qubit as control. The action of the CNOT gate in the photon-number notation is described by the following equations:

$$\begin{aligned} \hat{U}_{\rm CNOT}|10\rangle_c|10\rangle_t &= |10\rangle_c|10\rangle_t \\ \hat{U}_{\rm CNOT}|01\rangle_c|10\rangle_t &= |01\rangle_c|01\rangle_t \\ \hat{U}_{\rm CNOT}|10\rangle_c|01\rangle_t &= |10\rangle_c|01\rangle_t \\ \hat{U}_{\rm CNOT}|01\rangle_c|01\rangle_t &= |01\rangle_c|10\rangle_t \end{aligned} \tag{7.3}$$

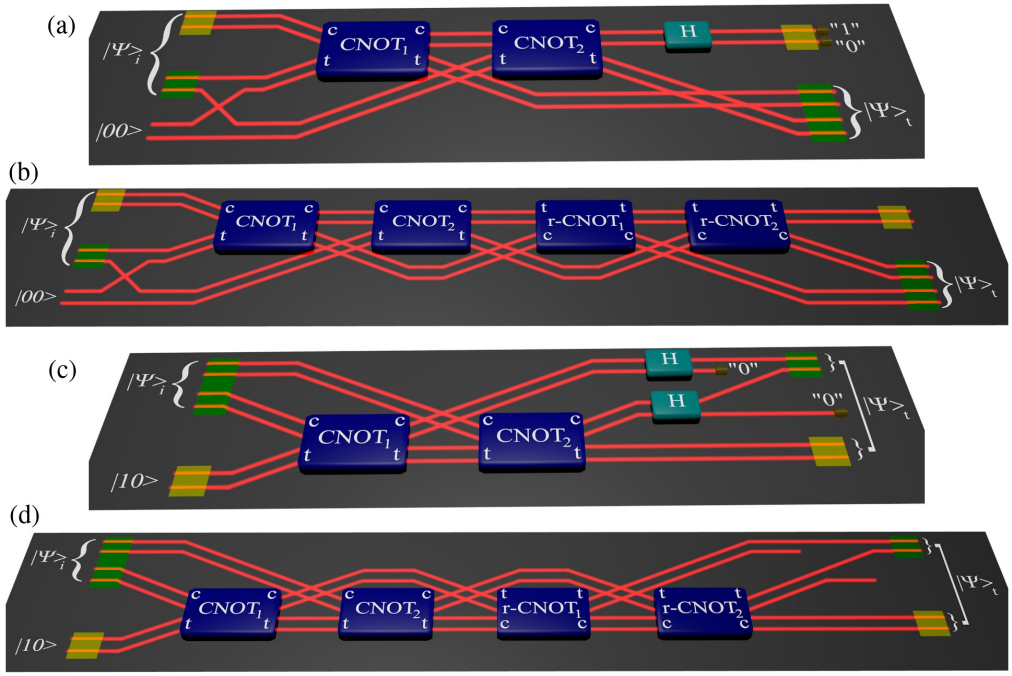

Figure 7.1: Optical schemes for quantum state joining and splitting. Each line represents a separate photonic mode (either spatial or of polarization). A qubit is represented by a double parallel line, as in a dual-rail implementation. A single-photon ququart, as obtained after the quantum joining, is represented by four parallel lines. H stands for a Hadamard quantum gate, CNOT for a controlled NOT quantum gate and r-CNOT for a CNOT gate in which the control and target ports have been reversed. The "0" sign corresponds to a vacuum detection (no photons). $|\Psi\rangle_i$ is the input state and $|\Psi\rangle_t$ the final (target) state. (a) Scheme for quantum joining based on a double CNOT gate and final projection. Feed-forward is needed to obtain deterministic behavior (not considering the CNOT contribution). (b) Alternative scheme for deterministic quantum joining, using four CNOT gates, with the second two gates having inverted control and target ports. This leads to a deterministic behavior without projection and feed-forward (not considering the CNOT success probability). (c) Scheme for quantum splitting, with double CNOT gate and final projection. This scheme is probabilistic (with a 50% success probability, not considering the CNOT gates contribution) and could be made deterministic only by combining quantum non-demolition measurements and feed-forward. (d) Alternative scheme for deterministic quantum splitting by using four CNOT gates (not considering the CNOT success probability).

However, in the present implementation of the quantum fusion we need to have the CNOT act also on "empty target qubits", that is vacuum states. For these we assume the following behavior:

$$\begin{aligned} \hat{U}_{\mathrm{CNOT}}|10\rangle_c|00\rangle_t &= \mu|10\rangle_c|00\rangle_t \\ \hat{U}_{\mathrm{CNOT}}|01\rangle_c|00\rangle_t &= \mu|01\rangle_c|00\rangle_t \end{aligned} \tag{7.4}$$

where μ is a possible complex amplitude rescaling relative to the non-vacuum case. A unitary CNOT must have $|\mu| = 1$, but probabilistic implementations do not have this requirement. The quantum joining scheme works if the two CNOTs have the same μ. In particular the CNOTs implementation proposed by Pittman *et al.* and used in [VSA+13] have $\mu = 1$, so for brevity we will remove μ in the following expressions.

Let us then consider the action of these two CNOT gates to the unfolded state given in Eq. (7.2):

$$\begin{aligned} |\Psi\rangle_f &= \hat{U}_{\mathrm{CNOT}_2}\hat{U}_{\mathrm{CNOT}_1}|\Psi\rangle_u \\ &= \alpha_0|10\rangle_{t1}|00\rangle_{t2}|10\rangle_c + \alpha_1|01\rangle_{t1}|00\rangle_{t2}|01\rangle_c \\ &\quad +\alpha_2|00\rangle_{t1}|10\rangle_{t2}|10\rangle_c + \alpha_3|00\rangle_{t1}|01\rangle_{t2}|01\rangle_c \end{aligned} \tag{7.5}$$

If now we project the c photon state on $|+\rangle = (|10\rangle + |01\rangle)/\sqrt{2}$, so as to erase the c qubit, and reunite the t_1 and t_2 kets, we obtain

$$|\Psi\rangle_t = \alpha_0|1000\rangle_t + \alpha_1|0100\rangle_t + \alpha_2|0010\rangle_t + \alpha_3|0001\rangle_t, \tag{7.6}$$

which is the desired joined state. Since the c qubit measurement has a probability of 50% of obtaining $|+\rangle$, without feed-forward the described method has a success probability of 50% not considering the CNOT success probability.

If the outcome of the c measurement is $|-\rangle = (|10\rangle - |01\rangle)/\sqrt{2}$, we obtain the following target state:

$$|\Psi'\rangle_t = \alpha_0|1000\rangle_t - \alpha_1|0100\rangle_t + \alpha_2|0010\rangle_t - \alpha_3|0001\rangle_t. \tag{7.7}$$

This state can be transformed back into $|\Psi\rangle_t$, as given in Eq. (7.6), by a suitable unitary transformation. Therefore, the success probability of the joining scheme can be raised to 100% (again not considering CNOTs success probabilities) by a simple feed-forward mechanism.

Alternative to this feed-forward scheme, one might recover a deterministic behavior for the joining step (not considering the CNOT) by avoiding the c-photon projection and applying two additional CNOT gates in which control and target qubits have swapped roles, so as to "disentangle" the c and t

photons. This alternative is illustrated in Fig. 7.1b. In other words, after the first two CNOTs, we must apply a third CNOT with t_1 used as control and c as target and a fourth CNOT with t_2 as control and c as target. This time, for a proper working of the scheme, we must consider the possibility that the control port of the CNOT is empty. As for the previous case of empty target qubit, the CNOT outcome in this case is taken to be simply identical to the input except for a possible amplitude rescaling, i.e.

$$\begin{aligned} \hat{U}_{\rm CNOT}|00\rangle_c|10\rangle_t &= \mu'|00\rangle_c|10\rangle_t \\ \hat{U}_{\rm CNOT}|00\rangle_c|01\rangle_t &= \mu'|00\rangle_c|01\rangle_t \end{aligned} \tag{7.8}$$

which is what occurs indeed in most CNOT implementations. Moreover, we again assume $\mu' = 1$ in the following, for simplicity. Let us then take the state given in Eq. (7.5) and apply the two "reversed" CNOT gates, denoted as r-CNOT:

$$\begin{aligned} |\Psi\rangle_{f2} &= \hat{U}_{\text{r-CNOT}_2}\hat{U}_{\text{r-CNOT}_1}|\Psi\rangle_f \\ &= |10\rangle_c\,(\alpha_0|10\rangle_{t1}|00\rangle_{t2} + \alpha_1|01\rangle_{t1}|00\rangle_{t2} \\ &\quad +\alpha_2|00\rangle_{t1}|10\rangle_{t2} + \alpha_3|00\rangle_{t1}|01\rangle_{t2}) \\ &= |10\rangle_c \otimes |\Psi\rangle_t \end{aligned} \tag{7.9}$$

where $|\Psi\rangle_t$ is given in Eq. (7.6). After this step, one can just discard photon c and photon t will continue to hold the entire initial quantum information. We notice that this second implementation method does not require the feed-forward, which is an advantage in terms of resources, but it needs four CNOTs instead of two. Since CNOT implementations based on linear optics are actually probabilistic, the final success probability will be significantly smaller than the first method without feed-forward, so this scheme is not convenient at the present stage.

7.1.2 Quantum state splitting scheme

Let us now move to the quantum state splitting process, illustrated in Fig. 7.1c. We assume to have an input photon encoding two qubits (i.e., a ququart) in the four-path state

$$|\psi\rangle_i = \alpha_0|1000\rangle + \alpha_1|0100\rangle + \alpha_2|0010\rangle + \alpha_3|0001\rangle \tag{7.10}$$

We label this input photon as c (for control). We also label the first two modes as c_1 and the last two modes as c_2. We then take another photon,

labeled as t (for target), that is initialized in the logical zero state of two other modes, so that the initial two-photon state is the following:

$$\begin{aligned} |\Psi\rangle_i &= (\alpha_0|10\rangle_{c_1}|00\rangle_{c_2} + \alpha_1|01\rangle_{c_1}|00\rangle_{c_2} \\ &\quad +\alpha_2|00\rangle_{c_1}|10\rangle_{c_2} + \alpha_3|00\rangle_{c_1}|01\rangle_{c_2})|10\rangle_t \end{aligned}$$

We now apply the two CNOT gates in sequence, using the t photon as target qubit in both cases and the c_1 and c_2 modes of the c photon as control qubit in the first and second CNOT, respectively. In order to do these operations properly, we need to define the CNOT operation also for the case when the control qubit is empty, as already discussed above. Hence, we obtain

$$\begin{aligned} &\hat{U}_{\mathrm{CNOT}_1}\hat{U}_{\mathrm{CNOT}_2}|\Psi\rangle_i = \alpha_0|10\rangle_{c_1}|00\rangle_{c_2}|10\rangle_t \\ &+\alpha_1|01\rangle_{c_1}|00\rangle_{c_2}|01\rangle_t + \alpha_2|00\rangle_{c_1}|10\rangle_{c_2}|10\rangle_t \\ &+\alpha_3|00\rangle_{c_1}|01\rangle_{c_2}|01\rangle_t \end{aligned}$$

Now we need to erase part of the information contained in the control photon. This is accomplished by projecting onto $|+\rangle_{c_i} = (|10\rangle_{c_i} + |01\rangle_{c_i})/\sqrt{2}$ combinations of the first and second pairs of modes, while keeping unaffected their relative amplitudes. In other words, we must apply an Hadamard transformation on each pair of modes, and take as successful outcome only the logical-zero output (corresponding to the $|+\rangle$ combination of the inputs). The projection is actually performed by checking that no photon comes out of the $|-\rangle$ (i.e., logical one) output ports of the Hadamard. The two surviving output modes are then combined into a single output c-photon qubit, which together with the t-photon qubit form the desired split-qubit output. Indeed, we obtain the following projected output:

$$\begin{aligned} |\Psi\rangle_f &= \alpha_0|10\rangle_c|10\rangle_t + \alpha_1|10\rangle_c|01\rangle_t \\ &\quad +\alpha_2|01\rangle_c|10\rangle_t + \alpha_3|01\rangle_c|01\rangle_t \end{aligned} \tag{7.11}$$

which describes the same two-qubit state as the input, but encoded in two photons instead of one. The proposed scheme for splitting has a 50% probability of success, not considering the CNOT contribution. It might be again possible to bring the probability to 100% (not considering CNOTs) by detecting the actual c-photon output mode pair after the Hadamard gates by a quantum non-demolition approach or in post-selection, and then applying an appropriate unitary transformation to the t photon.

Also in this case, we can replace the projection and feed-forward scheme by the action of a third and fourth CNOT gates in which the target and control roles are reversed, that is, using the t photon as control and c_1 and c_2

as targets of the third and fourth CNOT gates, respectively. This is shown in Fig. 7.1d. After the four CNOTs, one obtains the following state:

$$\begin{aligned}
&\alpha_0|10\rangle_{c_1}|00\rangle_{c_2}|10\rangle_t + \alpha_1|10\rangle_{c_1}|00\rangle_{c_2}|01\rangle_t + \\
&\alpha_2|00\rangle_{c_1}|10\rangle_{c_2}|10\rangle_t + \alpha_3|00\rangle_{c_1}|10\rangle_{c_2}|01\rangle_t \\
&= \alpha_0|1000\rangle_c|10\rangle_t + \alpha_1|1000\rangle_c|01\rangle_t + \\
&\alpha_2|0010\rangle_c|10\rangle_t + \alpha_3|0010\rangle_c|01\rangle_t, \qquad (7.12)
\end{aligned}$$

where in the second equality we have regrouped the four c modes. Then, an inverse unfolding step, that is simply discarding the second and fourth mode of the c photon, which are always empty, will lead to final state $|\Psi\rangle_f$ given in Eq. (7.11) with 100% probability. In this splitting case, the advantage of using this alternative scheme is more marked, as it is the only possibility to avoid post-selection or quantum nondemolition steps.

The CNOT gates utilized in the joining and splitting processes described in this Section can be implemented using different methods. In particular, since the photons being processed in each CNOT stage have no additional information, linear-optics KLM-like schemes based on two-photon interference can be used. It is for this reason that our schemes require the unfolding step and a double CNOT, rather than using a single CNOT for transferring the qubit from one photon to the other (if nonlinear-optical CNOT gates will ever be realized, they might possibly allow for a CNOT operation to be performed while another degree of freedom is present and remains unaffected, thus making the joining/splitting schemes much simpler). The only requirement for these CNOT gates is that they must be applicable also to the case when one of the input qubits is empty, i.e., there is a vacuum state at one input port. As we show in the next Section, this is a nontrivial requirement.

7.2 Unfeasibility of the quantum joining with two photons and post-selection

There exist different linear-optical based implementations of CNOT gates. The simplest are those based on post-selection and not requiring ancillary photons, such as the scheme first proposed by Ralph et al. [RLBW02] and Hofmann and Takeuchi [HT02] and later experimentally demonstrated by O'Brien et al. [OPW$^+$03]. Although such CNOT gates are based on post-selection and hence require destroying the output photons, there exist also schemes for applying several CNOT gates in sequence, with only one final post-selection step [Ral04]. These schemes require only the two photons to be combined and a final post-selection step based on photon detection.

Given the CNOT-based general scheme for quantum joining described in the previous Section, it is then natural to try an implementation exploiting these schemes.

More generally, one might ask whether a proper mixing of the two photon modes in a suitable linear-optical setup, followed by a filtering step on one of the two photons might suffice to obtain the joining onto the remaining photon. In this Section we prove that this is not possible: In particular, we show that no possible unitary evolution of the two photons as resulting from propagation through an arbitrary linear optical system, followed by an arbitrary projection for one of the two photons can lead to the quantum joining. This in turn shows that the joining scheme cannot be based on the CNOT gates of Ralph's kind and requires at least one ancilla photon. With one ancilla photon, it is possible to implement for example the CNOT gates proposed by Pittman [PJF01] and thus successfully obtain the quantum joining of two photon states, as demonstrated in [VSA$^+$13]. Of course the demonstrated implementation is probabilistic, because the CNOT gates are implemented in a probabilistic way.

We notice that the two-photon input state can be written in full generality as follows:

$$\begin{aligned} |\Psi\rangle_i &= \alpha_0|1010\rangle + \alpha_1|1001\rangle + \alpha_2|0110\rangle + \alpha_3|0101\rangle \\ &= \left(\alpha_0\hat{a}_1^+\hat{a}_3^+ + \alpha_1\hat{a}_1^+\hat{a}_4^+ + \alpha_2\hat{a}_2^+\hat{a}_3^+ + \alpha_3\hat{a}_2^+\hat{a}_4^+\right)|\emptyset\rangle \end{aligned} \tag{7.13}$$

where the four coefficients $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ define the input quantum information, $\hat{a}_i^+$ denote the creation operators for an arbitrary orthonormal set of input modes $|\psi\rangle_i$, and $|\emptyset\rangle$ denotes the global vacuum state. The mode-indices i here can be taken to include also the polarization degree of freedom, and we have selected four arbitrary modes 1-4 to encode the input information, with modes 1-2 used for one qubit and modes 3-4 for the other (possibly entangled with each other).

The propagation through an arbitrary linear-optical system can be described by the following transformation of the creation operators:

$$\hat{a}_i^+ \to \hat{b}_i^+ = \sum_j u_{ij}\hat{a}_j^+ \tag{7.14}$$

where u_{ij} are the coefficients of a unitary matrix describing the propagation and the operators $\hat{b}_j^+$ create the propagated (output) modes $|\chi\rangle_j$. Applying this transformation to the input state Eq. (7.13) we obtain the following propagated two-photon state (here we are using the Schrödinger representation,

in which the evolution acts on the state):

$$|\Psi\rangle_p = \left(\alpha_0 \hat{b}_1^+ \hat{b}_3^+ + \alpha_1 \hat{b}_1^+ \hat{b}_4^+ + \alpha_2 \hat{b}_2^+ \hat{b}_3^+ + \alpha_3 \hat{b}_2^+ \hat{b}_4^+\right) |\emptyset\rangle \tag{7.15}$$

Now, let us act on this state with a projector $\hat{\Pi}$ corresponding to the detection of a single photon in the arbitrary mode $|\phi\rangle = \sum_h \phi_h |\chi\rangle_h$, as given by the following:

$$\hat{\Pi} = \sum_h \phi_h^* \hat{b}_h. \tag{7.16}$$

Thus, we obtain the following projected one-photon state

$$\begin{aligned} |\Psi\rangle_f &= \hat{\Pi}|\Psi\rangle_p \\ &= \sum_h \phi_h^* \hat{b}_h \left(\alpha_0 \hat{b}_1^+ \hat{b}_3^+ + \alpha_1 \hat{b}_1^+ \hat{b}_4^+ + \alpha_2 \hat{b}_2^+ \hat{b}_3^+ + \alpha_3 \hat{b}_2^+ \hat{b}_4^+\right) |\emptyset\rangle \\ &= \alpha_0 \left(\phi_3^* |\chi\rangle_1 + \phi_1^* |\chi\rangle_3\right) + \alpha_1 \left(\phi_4^* |\chi\rangle_1 + \phi_1^* |\chi\rangle_4\right) \\ &\quad + \alpha_2 \left(\phi_3^* |\chi\rangle_2 + \phi_2^* |\chi\rangle_3\right) + \alpha_3 \left(\phi_4^* |\chi\rangle_2 + \phi_2^* |\chi\rangle_4\right). \end{aligned} \tag{7.17}$$

Hence, due to the bosonic nature of the photons, the final state results to be a linear combination of the following four "symmetrized" optical modes

$$\begin{aligned} |u\rangle_0 &= \phi_3^* |\chi\rangle_1 + \phi_1^* |\chi\rangle_3, \\ |u\rangle_1 &= \phi_4^* |\chi\rangle_1 + \phi_1^* |\chi\rangle_4, \\ |u\rangle_2 &= \phi_3^* |\chi\rangle_2 + \phi_2^* |\chi\rangle_3, \\ |u\rangle_3 &= \phi_4^* |\chi\rangle_2 + \phi_2^* |\chi\rangle_4. \end{aligned} \tag{7.18}$$

The input quantum information will be preserved if and only if the four modes $|u\rangle_i$ form a linearly independent set. This in turn will depend on the determinant of the following matrix $\mathcal{M}$ of coefficients, expressing the linear dependence of the four $|u\rangle_i$ modes on the propagated modes $|\chi\rangle_i$:

$$\mathcal{M} = \begin{pmatrix} \phi_3^* & 0 & \phi_1^* & 0 \\ \phi_4^* & 0 & 0 & \phi_1^* \\ 0 & \phi_3^* & \phi_2^* & 0 \\ 0 & \phi_4^* & 0 & \phi_2^* \end{pmatrix}, \tag{7.19}$$

A simple calculation shows that the determinant of this matrix is identically nil, thus proving the statement. If the optical system includes losses from media absorption, these can be included in the treatment as additional non-optical excitation modes in which the input optical modes can be transformed in the course of propagation. In other words, Eq. (7.14) will include also the creation operators of material excitations, although the latter will not

contribute to the $|u\rangle_i$ and $|\phi\rangle$ modes. Thus the proof remains valid even in lossy optical systems.

As a consequence of our proof, we can state that in general the mixing of two photons in a linear optical scheme followed by a final post-selection step can only lead to a loss of some information, e.g., ending up with a qutrit instead of a ququart. Alternatively, one may somehow preserve the initial information conditioned on the fact that there is "less information to start with", because the input two-photon state is properly constrained, for example, to a separable state [GW03, BvF$^+$06].

Beside this mathematical proof, one might be interested in seeking a more physical explanation for why the joining scheme using two CNOT in series following the concept of [Ral04] fails. To this purpose, we carried out a detailed analysis, of which we report here only the main conclusions. The problem is that the scheme given in [Ral04] is conceived for executing multiple CNOT in series, with the assumption that each control or target port of all the gates is occupied by a photon carrying the corresponding qubit. In the case of quantum joining, instead, the target ports may see the presence of "empty" qubits (or vacuum states), which open up new possible photonic evolution channels in the setup that are not excluded in the final post-selection step and which are instead absent in the standard case. These channels alter the final probabilities and disrupt the CNOT proper workings.

7.3 Three-photon entangled states

In this Section, we explore the relationship between the joining process of two photonic qubits and a particular class of three-photon entangled states (TPES), in which two photons are separately entangled with a common "intermediate" photon. This intermediate doubly-entangled photon must clearly hold two separate qubits, as defined by exploiting four orthogonal optical modes. A schematic diagram of this particular form of entangled cluster is given in Fig. 7.2.

An example of such three-photon entangled states can be defined as follows:

$$|\psi\rangle_{123} = \frac{1}{2}\left(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2\right)|H\rangle_3 \otimes \left(|u\rangle_1|d\rangle_3 - |d\rangle_1|u\rangle_3\right)|u\rangle_2, \quad (7.20)$$

where photon 1 is the intermediate photon, entangled with photons 2 and 3, and we introduced $|u\rangle$ and $|d\rangle$, to refer to the "up" and "down" paths of a dual-rail qubit encoding. It is understood that the three photons are identified by a further label associated with propagation modes. Other possible

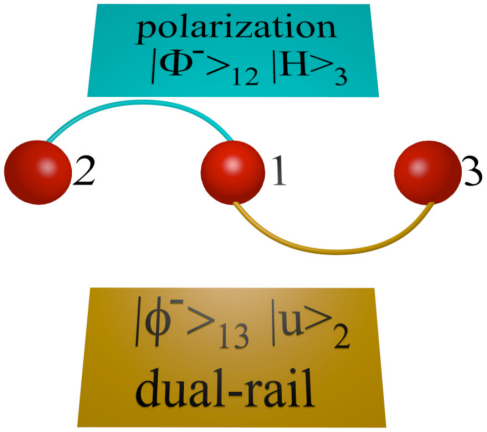

Figure 7.2: Schematic representation of the TPES state given in Eq. (7.20) of the main text. The three red spheres represent the three photons, with photon 1 separately entangled with photons 2 and 3. Each line correspond to an entanglement link. In the specific example, the upper (green) line corresponds to a polarization maximal entanglement in Bell state $|\Phi^-\rangle$, while the lower (yellow) line indicates a spatial-mode maximal entanglement (in a dual-rail basis) in Bell state $|\phi^-\rangle$. Other TPES states can be obtained by changing the specific Bell states used for the two entanglement links.

pair-wise maximally-entangled TPES are obtained from (7.20) by exchanging H and V and/or u and d in photon 1, or by changing the $-$ sign into a $+$ in one or both the factors, for a total of 16 possible independent combinations. These can be also written more compactly in terms of the Bell basis of maximally entangled qubit pairs, defined as follows

$$|\Psi^{\pm}\rangle_{ij} = \frac{1}{\sqrt{2}}(|H\rangle_i|H\rangle_j \pm |V\rangle_i|V\rangle_j)|u\rangle_i|u\rangle_j, \tag{7.21a}$$

$$|\Phi^{\pm}\rangle_{ij} = \frac{1}{\sqrt{2}}(|H\rangle_i|V\rangle_j \pm |V\rangle_i|H\rangle_j)|u\rangle_i|u\rangle_j, \tag{7.21b}$$

$$|\psi^{\pm}\rangle_{ij} = \frac{1}{\sqrt{2}}(|u\rangle_i|u\rangle_j \pm |d\rangle_i|d\rangle_j)|H\rangle_i|H\rangle_j, \tag{7.21c}$$

$$|\phi^{\pm}\rangle_{ij} = \frac{1}{\sqrt{2}}(|u\rangle_i|d\rangle_j \pm |d\rangle_i|u\rangle_j)|H\rangle_i|H\rangle_j. \tag{7.21d}$$

Using this notation, Eq. (7.20) can be for example rewritten as $|\psi\rangle_{123} = |\Phi^{-}\rangle_{12}|H\rangle_3 \otimes |\phi^{-}\rangle_{13}|u\rangle_2$, and the other TPES are obtained by replacing one or both the Bell states with another one. Notice that states (7.21a) and (7.21b) are Bell states with respect to the polarization degree of freedom of the pair, while states (7.21c) and (7.21d) are Bell states with respect to the spatial-mode (or propagation path) degree of freedom of the pair.

Here and in the following discussion, for the sake of definiteness, we have adopted a notation referring to the specific case in which the double entanglement exploits two separate degrees of freedom, that is the polarization and a pair of spatial modes. We stress, however, that there is no actual requirement of using this specific choice of degrees of freedom for the validity of our analysis. There is even no need of using two separate degrees of freedom, as all qubit entanglements could for example also be encoded using a set of four spatial modes, e.g., four parallel paths, or four eigenmodes of the orbital angular momentum of light.

The state (7.20), or anyone of the other TPES, can be used as a resource for carrying out a two-in-one qubit teleportation of the quantum state, i.e., the teleportation of the four-dimensional quantum state initially encoded in two input photons in a single output photon. Actually, the problem of preparing three-photon entangled states such as (7.20) is essentially equivalent to that of realizing the quantum joining. Indeed, quantum state joining can be used to prepare the three-photon entangled state (7.20) and, conversely, state (7.20) can be used to carry out the quantum state joining of two photonic qubits via teleportation. We prove this in detail in Appendix E.

Following the same ideas, one may use the state joining protocol to create even more complex entanglement clusters of photons, exploiting multiple

degrees of freedom per photon. In particular, we notice that the TPES introduced above belong to the family of "linked" states first proposed by Yoran and Reznik in order to perform deterministic quantum computation with linear optics [YR03]. Not surprisingly, the optical scheme proposed in [YR03] to create such linked states is also very similar to that used for quantum-state joining (but it did not include explicitly the KLM gate implementations).

7.4 Discussion

In summary, we have revisited the quantum-state joining and splitting processes recently introduced in [VSA+13] from a theoretical point of view. After casting the associated formalism in the more general photon-number notation, we have introduced some modified schemes that do not require feed-forward or post-selection. Next, we have provided a formal proof that the quantum joining of two photon states with linear optics cannot be accomplished using only post-selection and requires the use of at least one ancilla photon, despite the existence of linear-optical implementations of CNOT gates which do not require ancillary photons. Finally, we have investigated the relationship between the state-joining scheme and the generation of clusters of three-photon entangled states involving more than one qubit per particle. This shows that the joining/splitting processes find application for the generation of complex cluster states of entangled photons, which is of fundamental interest and might open the way to novel quantum protocols.

Chapter 8

Conclusions

In this Thesis we analyzed several aspects of the problem of experimental imperfections, such as noise and losses, occurring in realistic implementations of different quantum information protocols, both in the DI framework and in partly-DI scenarios. We showed the general importance of deriving conditions for having a trustworthy quantum certification of such protocols. Indeed, since the DI and partly-DI scenarios do not rely on a complete characterization of the involved devices, one has to rule out the interference of malicious adversaries exploiting the experimental losses in order to authenticate the reliability of the given protocol. In this Chapter we summarize the main results obtained and discuss open problems and further developments.

Necessary detection efficiencies for secure implementation of QKD protocols

In recent years, several hacking attacks have broken the security of quantum cryptography implementations by exploiting the presence of losses and the ability of the eavesdropper to tune detection efficiencies. In Chapter 3 we have presented a simple attack of this form that applies to any protocol in which the key is constructed from the results of untrusted measurements performed on particles coming from an insecure source or channel. Because of its generality, this attack applies to a large class of protocols, from standard prepare-and-measure to DI schemes. Obviously our attack cannot be applied to protocols in which the key is not constructed from measurement results, such as in measurement-device-independent schemes [LCQ12, BP12]. These protocols, almost by definition, are only sensitive to attacks on the devices that prepare the quantum states. The generality of our attack also implies that the implementation of partly DI solutions is, from the point of view of detection efficiency, almost as demanding as DI ones, which, in turn, offer

stronger security.

Interestingly, the critical detection efficiency corresponding to our attack only depends on the number of measurements that Eve wants to learn, but is independent of the total number of measurements M_B, number of outputs D, or dimension of the quantum systems used.

We have also presented an improved attack that applies to protocols with two untrusted detectors. In this attack, the eavesdropper exploits the detection inefficiencies of one of the parties to improve her attack on the other party. More generally, it would be interesting to derive a formalism to study the robustness of concrete protocols to detection attacks, as these are the most advanced at the moment. This will allow us to understand for which protocols the detection bounds for security derived in Chapter 3 are tight. An analysis of the tightness of our attack in the steering scenario has been presented in Chapter 4, showing that the derived bound is tight for certifying randomness from a single measurement.

Finally, our results imply also the existence of an intriguing and weak form of certified randomness, that we named bound randomness. In a scenario in which an eavesdropper is limited only by the no-signalling principle, there exist non-local correlations for which she can find out a posteriori the results of any implemented measurements. A final open question is to understand if this form of randomness exists in the quantum case, that is, when the eavesdropper is limited by the quantum formalism.

Randomness certification in the steering and prepare-and measure scenarios

The study of randomness certification in scenarios with intermediate levels of trust such as the steering and prepare-and-measure scenarios is motivated by the fundamental question of how much randomness can be kept if we give up partial information about the description of the devices and systems used in the protocol. Moreover, from a more practical point of view, the amount of randomness obtained in the steering scenario gives an upper bound to what would be obtained in a fully-DI setting, regardless of the number of measurements performed.

Our main result in this area is a general and optimal method to quantify the amount of local or global randomness that can be extracted from a single measurement in two scenarios: (i) the quantum steering scenario, where two parties measure a bipartite system in an unknown state but one of them does not trust his measurement apparatus, and (ii) the prepare-and-measure scenario, where additionally the quantum state is known. We used this method to compute the maximal amount of local and global randomness that can be

certified by measuring systems subject to noise and losses in those two scenarios. Using also the results of Chapter 3, we proved that local randomness can be certified from a single measurement if and only if the detectors used in the test have detection efficiency higher than 50%. Furthermore, we showed that the results obtained for the steering scenario can easily be extended to the prepare-and-measure scenario. In this case we showed that even noisy states can perform very well for randomness certification. Finally, we presented a method to find the best measurements which can certify the most randomness from any fixed state. Using insight from this method, we showed analytically that one can certify maximal randomness from all pure partially entangled states using only two fixed measurements. Since local randomness certification is of fundamental importance for one-sided-device-independent and DI quantum key distribution, the results presented in Chapter 4 have a natural application in cryptographic protocols.

Device-independent dimension witnesses and semi-device-independent protocols

A DIDW is a tool for bounding the dimension of the Hilbert space of an unknown classical or quantum system in a DI framework, *i.e.* adopting as few assumptions as possible. Furthermore, when the dimension is assumed, DIDWs can be used to distinguish between the classical and quantum nature of a source. Thus, they provide a quantum certification for SDI protocols, in a scenario in which only the dimension of the exchanged system is assumed while the devices are uncharacterized. In Chapter 5 we have given a characterization of the sets of classical and quantum correlations achievable in the framework of DIDWs with local and shared randomness, and we have provided analytical and numerical tools for the optimization of DIDWs in the realistic case in which the implementation is affected by loss. Using these tools, we have derived upper and lower bounds for the critical detection efficiency necessary for performing reliable dimension witnessing. The presented results are of fundamental importance for experimental implementations of DIDWs and SDI protocols based on DIDWs.

A natural generalization of the problem of DIDWs is that of entangled assisted DIDWs, namely when entanglement is allowed to be shared between the preparing device on Alice's side and the measuring device on Bob's side. We compared entangled assisted DIDWs with super-dense coding, finding that in some communication contexts the former outperform the latter. This indicates that the problem of entangled assisted DIDWs deserves further investigation.

Another development of this problem is to study the robustness of DIDWs

considering models of loss more general than the one considered in Chapter 5, e.g. one in which a different detection efficiency is associated to each POVM.

Finally, a further generalization of the problem of DIDWs is the case in which no shared randomness is allowed between the preparations and the measurements. In this case, the non-convexity of the relevant sets enables the exploitation of non-linear witnesses which allow to dimension witness for arbitrarily low values of the detection efficiency [BQB14]. We have addressed this problem in Chapter 6, investigating the conditions under which one can perform dimension witnessing for any non-null value of the detection efficiency with independent devices.

Chapter 6 tackles the problem of DL attacks to SDI quantum and classical protocols. SDI classical protocols are represented by random access codes, which provide a general framework for describing one-sided classical communication tasks. In this context, we have provided general conditions under which detection inefficiencies can be exploited by a malicious provider to fake the performance of SDI quantum and classical protocols – and discussed how to prevent it. Some of the presented results hold in the hypothesis that the message sent by Alice is 2-dimensional. For the classical case, we showed through the example of $3 \to \log 6$ RAC that this assumption cannot be relaxed trivially. Thus, it remains an open problem how to devise more general conditions under which DL attacks are harmless.

Joining and splitting the quantum states of photons

Recently, a photonic process named quantum state joining has been experimentally demonstrated [VSA$^+$13], which consists in the transfer of the internal two-dimensional quantum states of two input photons, i.e., two photonic qubits, into the four-dimensional quantum state of a single photon, i.e., a photonic ququart. A scheme for the inverse process, namely quantum state splitting, has also been theoretically proposed. Both processes can be iterated in a cascaded layout, to obtain the joining and/or splitting of more than two qubits, thus leading to a general scheme for varying the number of photons in the system while preserving its total quantum information content.

In Chapter 7 we revisited these processes from a theoretical point of view. We introduced some modified schemes that are in principle unitary (not considering the implementation of the CNOT gates) and do not require projection and feed-forward steps. This can be particularly important in the quantum state splitting case, to obtain a scheme that does not rely on post-selection. These schemes for multiplexing the quantum information across photons, despite having a relatively low success probability, may already find application in quantum communication or in interfacing with atomic mem-

ories, when high losses are involved. In this context, a possible advantage could be in the overall rate of decoherence of the stored quantum information, which for entangled states will scale with the number of involved registers. Moreover, we formally proved that it is impossible to transfer all the quantum information encoded in two input photons into one output photon using linear optics and post-selection, without including ancillary photons in the process. Therefore, the quantum joining of two photon states with linear optics requires the use of at least one ancilla photon. This is somewhat unexpected, given that the demonstrated joining scheme involves the sequential application of two CNOT quantum gates, for which a linear optical scheme with just two photons and post-selection is known to exist. Furthermore, we explored the relationship between the joining scheme and the generation of clusters of multi-particle entangled states involving more than one qubit per particle. This shows that the joining/splitting processes can be interestingly applied to the study of fundamental issues in quantum physics, such as for generating qudit cluster states or for converting the local properties of a particle into nonlocal ones by splitting them among separable particles. Finally, we notice that if the recent attempts at achieving gigantic nonlinear interactions among photons will succeed [SKFP11, PFL$^+$12], deterministic schemes for quantum state joining and splitting should also become possible, likely making the associated photon multiplexing/demultiplexing an important resource for future quantum communication networks.

Appendix A

Derivation of the SDPs presented in Chapter 4

A.1 Obtaining the SDP for the guessing probability in the steering scenario

In this Appendix we will show how to arrive at the SDP (4.3) for Eve's guessing probability.

The most general attack that Eve can implement in the case that she is interested in guessing the result of a single measurement ($x = x^*$) of Alice, is to distribute a state ρ_{ABE} to Alice and Bob (keeping a part for herself) on which she will perform a measurement with POVM elements M_e, for $e = 1, \ldots, d_{\mathrm{A}}$, and distribute to Alice a set of measuring devices which implement the POVMs with elements $M_{a|x}$, for $x = 1, \ldots, m_{\mathrm{A}}$ and $a = 1, \ldots, d_{\mathrm{A}}$. When Eve obtains outcome e from her measurement she will give this as her guess for the outcome of Alice. Thus, the guessing probability of Eve is given by

$$P_{\mathrm{guess}}(x^*) = \sum_e \mathrm{Tr}[(M_{a=e|x^*} \otimes M_e)\rho_{\mathrm{AE}}] \tag{A.1}$$

Alice and Bob can however determine the assemblage $\sigma^{\mathrm{obs}}_{a|x}$ that they hold, (i.e. the set of conditional states prepared for Bob, along with the corresponding

probabilities). Thus the optimization problem we need to solve is given by

$$\begin{aligned} \max_{\rho_{\mathrm{ABE}},\{M_{a|x}\}_{a,x},\{M_e\}_e} \quad & \textstyle\sum_e \mathrm{Tr}[(M_{a=e|x^*} \otimes M_e)\rho_{\mathrm{AE}}] \\ \text{subject to} \quad & \mathrm{Tr}_{\mathrm{A}}[(M_{a|x} \otimes \mathbb{1}_{\mathrm{B}})\,\rho_{\mathrm{AB}}] = \sigma^{\mathrm{obs}}_{a|x}, \forall a, x \\ & \rho_{\mathrm{ABE}} \succeq 0, \quad \mathrm{Tr}\,\rho_{\mathrm{ABE}} = 1 \\ & M_{a|x} \succeq 0, \forall a, x \quad \textstyle\sum_a M_{a|x} = \mathbb{1}, \forall x \\ & M_e \succeq 0, \forall e \quad \textstyle\sum_e M_e = \mathbb{1}. \end{aligned} \tag{A.2}$$

Here, the first constraint is the consistency with the observed assemblage, the second constraints demand that ρ_{ABE} is a valid quantum state and the third and fourth constraints that the measurements $M_{a|x}$ and M_e are valid POVMs.

Defining now the joint assemblage for Alice, Bob and Eve,

$$\sigma^e_{a|x} = \mathrm{Tr}_{\mathrm{AE}}[(M_{a|x} \otimes \mathbb{1}_{\mathrm{B}} \otimes M_e)\,\rho_{\mathrm{ABE}}], \tag{A.3}$$

it is straightforward to see that all of the constraints appearing in (4.3) are satisfied whenever the constraints in (A.2) are satisfied, and that the objective functions match. Thus it is straightforward to see that the optimization problem (4.3) is at least a relaxation of (A.2). What we will show now is that they are in fact equivalent optimization problems by showing that any solution to (4.3) also implies a solution to (A.2).

First of all, consider an assemblage $\sigma^e_{a|x}$ satisfying all of the constraints in (4.3). For a fixed e, we can define $P_{\mathrm{E}}(e) = \sum_a \mathrm{Tr}\,\sigma^e_{a|x}$. Note that $P_{\mathrm{E}}(e)$ is indeed independent of x, since $\sum_a \sigma^e_{a|x} = \sum_e \sigma^e_{a|x'}$ is independent of x, due to no-signalling. Moreover, we define $\tilde{\sigma}^e_{a|x} = \sigma^e_{a|x}/P_{\mathrm{E}}(e)$, which has the following properties

$$\textstyle\sum_a \tilde{\sigma}^e_{a|x} = \sum_a \tilde{\sigma}^e_{a|x'} \quad \forall e, x \neq x', \qquad \mathrm{Tr}\sum_a \tilde{\sigma}^e_{a|x} = 1 \quad \forall e \tag{A.4}$$

which show that for each e, $\tilde{\sigma}^e_{a|x}$ is a valid assemblage [Pus13]. From the GHJW theorem [Gis89, HJW93] it therefore follows that there is a quantum state ρ^e_{AB} and POVM elements $M^e_{a|x}$ such that

$$\mathrm{Tr}_{\mathrm{A}}[(M^e_{a|x} \otimes \mathbb{1}_{\mathrm{B}})\rho^e_{\mathrm{AB}}] = \tilde{\sigma}^e_{a|x} \tag{A.5}$$

Now, we finally consider that Eve also sends an additional degree of freedom which is read by the measuring device of Alice – an auxiliary classical 'flag' system, which we label A'. This system has orthogonal states $|e\rangle$, for $e = 1, \ldots, d_{\mathrm{A}}$. This will be read by Alice's measuring device, and, conditioned

on the flag, the appropriate measurement will be made. We can thus now construct the complete strategy of Eve

$$\begin{aligned} \rho_{\mathrm{ABE}} &= \sum_e p_{\mathrm{E}}(e)|e\rangle\langle e|_{\mathrm{A}'} \otimes \rho^e_{\mathrm{AB}} \otimes |e\rangle\langle e|_{\mathrm{E}} \\ M_{a|x} &= \sum_e |e\rangle\langle e|_{\mathrm{A}'} \otimes M^e_{a|x} \\ M_e &= |e\rangle\langle e|_{\mathrm{E}} \end{aligned} \tag{A.6}$$

Clearly this defines a valid state and valid measurements, hence they satisfy the latter constraints of (A.2). Furthermore, by construction it also satisfies the first consistency constraint, which is straightforwardly verified.

In total, we thus conclude that the two optimization problems are equivalent, since the solution to either one implies a solution to the other, obtaining the same $P_{\mathrm{guess}}(x^*)$. We thus focus on the problem (4.3) which is easier to solve, being an SDP optimization, linear in the optimization variables $\sigma^e_{a|x}$.

A.2 Derivation of the Prepare-and-Measure SDP

In this Appendix we will show that the amount of randomness that can be certified in the prepare-and-measure scenario when Alice receives her share of the state through an untrusted channel, and does not trust her measuring device, is given by the SDP (4.6) in the main text.

Bob prepares a known bipartite state ρ_{AB} half of which is sent to Alice through the insecure quantum communication channel. Eve can intercept the state, and the most general operation she can perform (in the case that she is guessing only the outcome of a single measurement $x = x^*$) is a measurement with Kraus operators K_e, i.e. the POVM elements are $M_e = K_e^\dagger K_e$, and the state prepared by Eve after obtaining outcome e is

$$\rho^e_{\mathrm{AB}} = \frac{(K_e \otimes \mathbb{1})\rho_{\mathrm{AB}}(K_e^\dagger \otimes \mathbb{1})}{\mathrm{Tr}[K_e \rho_{\mathrm{A}} K_e^\dagger]} \tag{A.7}$$

which occurs with probability $P_{\mathrm{E}}(e) = \mathrm{Tr}[M_e \rho_{\mathrm{A}}]$. Eve will guess that the outcome of Alice's measurement is e. Eve now forwards the state onto Alice, and since she controls completely Alice's device, she will allow the device to perform the measurement $N^e_{a|x}$ when her outcome was e, and when Alice chooses to make measurement x (that is, Eve sends the classical information of which outcome she obtained along with the quantum state). Thus, the

probability for Alice to obtain outcome a, given that she made measurement x and Eve obtained outcome e is given by

$$P_{\mathrm{A}}(a|x,e) = \frac{\mathrm{Tr}[N^e_{a|x} K_e \rho_{\mathrm{A}} K_e^\dagger]}{\mathrm{Tr}[K_e \rho_{\mathrm{A}} K_e^\dagger]}. \tag{A.8}$$

Putting everything together, we see therefore that the guessing probability is obtained by allowing Eve to optimize over all available strategies, and is given by

$$\begin{aligned}
\max_{K_e, N^e_{a|x}} \quad & P_{\mathrm{guess}}(x^*) = \textstyle\sum_e \mathrm{Tr}[N^e_{a=e|x^*} K_e \rho_{\mathrm{A}} K_e^\dagger] && \\
\text{subject to} \quad & \textstyle\sum_e \mathrm{Tr}_{\mathrm{A}}[(N^e_{a|x} \otimes \mathbb{1})(K_e \otimes \mathbb{1}) \rho_{\mathrm{AB}} (K_e^\dagger \otimes \mathbb{1})] = \sigma^{\mathrm{obs}}_{a|x} && \forall\, a, x \\
& \textstyle\sum_a N^e_{a|x} = \mathbb{1} && \forall\, e, x \\
& \textstyle\sum_e K_e^\dagger K_e = \mathbb{1} && \\
& N^e_{a|x} \succeq 0 && \forall\, a, e, x
\end{aligned} \tag{A.9}$$

Currently, this optimization is not in the form of an SDP, due to the nonlinear nature of the objective function and the constraints. However, it can easily be written in the form of an SDP by introducing the new variable $M^e_{a|x} = K_e^\dagger N^e_{a|x} K_e$. The three final constraints on $N^e_{a|x}$ and K_e imply the following constraints on $M^e_{a|x}$,

$$\begin{aligned}
\textstyle\sum_a M^e_{a|x} = \textstyle\sum_a M^e_{a|x'}, \qquad & \forall\, e, x' \neq x, \\
\textstyle\sum_{ae} M^e_{a|x} = \mathbb{1}, \qquad & \forall\, x, \\
M^e_{a|x} \succeq 0, \qquad & \forall\, a, e, x.
\end{aligned} \tag{A.10}$$

However, we can see that whenever we have a set of $M^e_{a|x}$ satisfying the above constraints, it implies that there exist $N^e_{a|x}$ and K_e satisfying the original constraints – i.e. the two sets are equivalent. To see this, we denote first $M_e = \sum_a M^e_{a|x} \succeq 0$ (which is independent of x), and therefore we can write $M_e = K_e^\dagger K_e$, for some K_e, which is always possible for a positive semi-definite operator. Moreover, since $\sum_{ae} M^e_{a|x} = \sum_e K_e^\dagger K_e = \mathbb{1}$, the second constraint is satisfied. Finally, defining $N^e_{a|x} = (K_e^\dagger)^{-1} M^e_{a|x} (K_e)^{-1} \succeq 0$ (using the pseudo-inverse when necessary), we also have that

$$\sum_a N^e_{a|x} = (K_e^\dagger)^{-1} M_e (K_e)^{-1} = (K_e^\dagger)^{-1} K_e^\dagger K_e (K_e)^{-1} = \mathbb{1} \tag{A.11}$$

Thus, we can re-express the optimization problem (A.9) in the form of the

following SDP

$$\begin{aligned} \max_{M^e_{a|x}} \quad & P_{\text{guess}}(x^*) = \textstyle\sum_e \text{Tr}[M^e_{a=e|x^*}\rho_{\text{A}}] & \\ \text{subject to} \quad & \textstyle\sum_e \text{Tr}_{\text{A}}[(M^e_{a|x}\otimes \mathbb{1})\rho_{\text{AB}}] = \sigma^{\text{obs}}_{a|x} & \forall\, a,x \\ & \textstyle\sum_a M^e_{a|x} = \sum_a M^e_{a|x'} & \forall\, e, x\neq x' \\ & \textstyle\sum_{ae} M^e_{a|x} = \mathbb{1} & \forall\, x, \\ & M^e_{a|x} \succeq 0 & \forall\, a,e,x \end{aligned} \tag{A.12}$$

which is exactly the optimization problem given in the main text.

A.3 Deriving the dual of the SDP (4.3)

In this Appendix we show the explicit form of the dual of the SDP (4.3), and explain why Eq. (4.7) is an equivalent form, which is easier to interpret.

As a reminder, the primal problem is given by

$$\begin{aligned} \max_{\sigma^e_{a|x}} \quad & P_{\text{guess}}(x^*) = \textstyle\sum_e \text{Tr}[\sigma^e_{a=e|x^*}] & \\ \text{subject to} \quad & \textstyle\sum_e \sigma^e_{a|x} = \sigma^{\text{obs}}_{a|x} & \forall\, a,x \\ & \textstyle\sum_a \sigma^e_{a|x} = \sum_a \sigma^e_{a|x^*} & \forall\, e,\ x\neq x^* \\ & \sigma^e_{a|x} \succeq 0 & \forall a,x,e. \end{aligned} \tag{A.13}$$

Let us introduce dual variables $F_{a|x}$, G^e_x and $H^e_{a|x}$, with respect to the first, second and third set of constraints respectively, and form the Lagrangian for this problem,

$$\begin{aligned} \mathcal{L} \;=\; & \sum_e \text{Tr}[\sigma^e_{a=e|x^*}] + \sum_{ax} \text{Tr}[F_{a|x}(\sigma^{\text{obs}}_{a|x} - \sum_e \sigma^e_{a|x})] \\ & + \sum_{aex} \text{Tr}[G^e_x(\sigma^e_{a|x} - \sigma^e_{a|x^*})] + \sum_{aex} \text{Tr}[H^e_{a|x}\sigma^e_{a|x}] \end{aligned} \tag{A.14}$$

After re-arranging, and grouping terms, this is equivalent to

$$\begin{aligned} \mathcal{L} \;=\; & \sum_{ax} \text{Tr}[F_{a|x}\sigma^{\text{obs}}_{a|x}] \\ & + \sum_{aex} \text{Tr}[(\delta_{a,e}\delta_{x,x^*}\mathbb{1} - F_{a|x} + G^e_x - \delta_{x,x^*}\sum_{x'} G^e_{x'} + H^e_{a|x})\sigma^e_{a|x}] \end{aligned} \tag{A.15}$$

This Lagrangian provides an upper bound on the primal objective as long as $H^e_{a|x} \succeq 0$. Moreover, it provides a non-trivial upper bound only when the

inner bracket in the second line identically vanishes for each value of a, e, x. Thus, we arrive at the dual problem

$$\begin{aligned} \min_{F_{a|x}, G^e_x, H^e_{a|x}} \quad & \textstyle\sum_{ax} \mathrm{Tr}[F_{a|x}\sigma^{\mathrm{obs}}_{a|x}] && \text{(A.16)} \\ \text{subject to} \quad & \delta_{a,e}\delta_{x,x^*}\mathbb{1} - F_{a|x} + G^e_x - \delta_{x,x^*}\textstyle\sum_{x'} G^e_{x'} + H^e_{a|x} = 0 \qquad \forall\, a, e, x \\ & H^e_{a|x} \succeq 0 \qquad \forall\, a, e, x \end{aligned}$$

However, $H^e_{a|x}$ is playing the role of a slack variable, since it doesn't appear in the objective function, so we can finally simplify the dual to arrive at

$$\begin{aligned} \min_{F_{a|x}, G^e_x} \quad & \textstyle\sum_{ax} \mathrm{Tr}[F_{a|x}\sigma^{\mathrm{obs}}_{a|x}] && \text{(A.17)} \\ \text{subject to} \quad & F_{a|x} - \delta_{a,e}\delta_{x,x^*}\mathbb{1} - G^e_x + \delta_{x,x^*}\textstyle\sum_{x'} G^e_{x'} \succeq 0 \qquad \forall\, a, e, x \end{aligned}$$

The dual is easily seen to be strictly feasible, for example by taking $G^e_x = 0$ and $F_{a|x} = \alpha\mathbb{1}$ for $\alpha > 1$. Thus strong duality holds, and the optimal value of the dual is equal to the optimal value of the primal. In the form (A.17), the dual is seen manifestly to be an SDP, as expected. Finally, to understand the meaning of the constraint, we multiply by an arbitrary valid assemblage $\sigma_{a|x}$, and take the sum in a and x and the trace. We find

$$\sum_{ax} \mathrm{Tr}[F_{a|x}\sigma_{a|x}] \geq \mathrm{Tr}[\sigma_{e|x^*}] = P(e|x^*) \qquad \text{(A.18)}$$

must hold for all e. Since this condition also holds for all valid assemblages, we see that the second constraint enforces that the value of the inequality is a uniform upper bound on the probability that any individual outcome occurs for the measurement x^*, independent of the assemblage. Hence, one sees immediately why this bounds the guessing probability.

Appendix B

Maximal local randomness from all pure states

In this Appendix we will show analytically that appropriate measurements on all partially entangled qudit states necessarily lead to 1 dit of randomness.

Consider first the partially entangled two-qubit state in Schmidt form, $|\psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$, for $\theta \in (0, \pi/4]$, and that Alice's two measurements are X and Z measurements, that are labelled 0 and 1 respectively. The assemblage created for Bob is then

$$\begin{aligned} \sigma_{0|0} &= \frac{1}{2}|\uparrow_\theta\rangle\langle\uparrow_\theta|, \\ \sigma_{1|0} &= \frac{1}{2}|\uparrow_{-\theta}\rangle\langle\uparrow_{-\theta}|, \\ \sigma_{0|1} &= \cos^2\theta|0\rangle\langle 0|, \\ \sigma_{1|1} &= \sin^2\theta|1\rangle\langle 1|, \end{aligned} \tag{B.1}$$

where $|\uparrow_\theta\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$. Crucially, each element of the assemblage is pure, i.e. each element is of the form $\sigma_{a|x} = P(a|x)\Pi_{a|x}$, where $\Pi_{a|x}$ is a one-dimensional projector. The purity of Bob's assemblage substantially constrains Eve's possible strategies, such that

$$\sigma^e_{a|x} = q(ae|x)\Pi_{a|x} \tag{B.2}$$

where each $q(ae|x) \geq 0$. This says that Eve must prepare the same pure state for Bob in each instance, all she can vary is the probability of the two outcomes (which must still be positive). To be consistent with the observed assemblage, we must have that

$$\sum_e q(ae|x) = P(a|x). \tag{B.3}$$

The guessing probability also now becomes

$$P_{\text{guess}}(x^* = 0) = \sum_e \text{Tr}[\sigma^e_{a=e|0}] = q(00|0) + q(11|0). \tag{B.4}$$

Now, the no-signalling constraint says that $\sum_a \sigma^e_{a|0} = \sum_a \sigma^e_{a|1}$ for all e. Specifically, in the case at hand

$$q(0e|0)\Pi_{0|0} + q(1e|0)\Pi_{1|0} = q(0e|1)\Pi_{0|1} + q(1e|1)\Pi_{1|1}, \tag{B.5}$$

which must be true for all matrix elements. While the projectors on the right-hand-side, corresponding to measurements of Z, are diagonal, the left-hand-side, corresponding to X, are in general not diagonal. Thus, taking the trace with $|1\rangle\langle 0|$, we arrive at the condition

$$\cos\theta \sin\theta (q(0e|0) - q(1e|0)) = 0. \tag{B.6}$$

Since $\cos\theta \sin\theta \neq 0$ for $\theta \in (0, \pi/4]$, this implies that $q(0e|0) = q(1e|0)$. In particular, this says that $q(01|0) = q(11|0)$. However, to be consistent $q(00|0) + q(01|0) = p(0|0) = 1/2$, and thus we arrive at

$$1/2 = q(00|0) + q(01|0) = q(00|0) + q(11|0) = P_{\text{guess}}. \tag{B.7}$$

Thus, analytically it must be the case that $P_{\text{guess}} = 1/2$, and hence 1 bit of randomness is obtained by measuring X and Z on any partially entangled state of two qubits.

The above also extends to qudits; assuming that the state has Schmidt-rank d then 1 dit of randomness can always be obtained. Let us now write the state as

$$|\psi\rangle = \sum_{k=0}^{d-1} \sqrt{\lambda_k}|k\rangle|k\rangle \tag{B.8}$$

where $\sum_k \lambda_k = 1$, and $\lambda_k > 0$. Alice's first measurement will now be in the Fourier-transform basis, with eigenstates

$$|\tilde{a}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{ak}|k\rangle \tag{B.9}$$

and $\omega = e^{2\pi i/d}$ the corresponding root of unity. Her second measurement will be in the Z basis with eigenstates $\{|a\rangle\}$. For Alice's first measurement she obtains each outcome with equal probability $p(a|0) = 1/d$, and prepares the pure states for Bob $\Pi_{a|0}$, given by

$$\Pi_{a|0} = \sum_{kl} \sqrt{\lambda_k \lambda_l}\omega^{a(l-k)}|k\rangle\langle l|. \tag{B.10}$$

For Alice's second measurement, she obtains outcome a with probability $p(a|1) = \lambda_a$, and prepares the state $\Pi_{a|1} = |a\rangle\langle a|$. As above, the purity of Bob's assemblage means that Eve is again forced to use strategies of the form $\sigma^e_{a|x} = q(ae|x)\Pi_{a|x}$. For consistency we still have $\sum_e q(ae|x) = p(a|x)$, for the guessing probability $P_{\text{guess}}(x^* = 0) = \sum_e q(ee|0)$, and from no-signalling $\sum_a q(ae|0)\Pi_{a|0} = q(ae|1)\Pi_{a|1}$. Once again, the right-hand-side is diagonal, and hence by looking at the off-diagonal matrix elements, i.e. by taking the trace with $|k\rangle\langle l|$, we find that

$$\sum_a q(ae|0)\sqrt{\lambda_k\lambda_l}\omega^{a(l-k)} = 0 \tag{B.11}$$

Since, by assumption of being Schmidt-rank d, none of the Schmidt coefficients vanish, we therefore must have that

$$\sum_a q(ae|0)\omega^{a(l-k)} = 0. \tag{B.12}$$

Considering only the elements with $k = 0$ (and $l = 1, \ldots, d-1$), along with the equation $\sum_a q(ae|0) = P(e)$, which says that Eve's probability to output e is just the conditional distribution, we notice that this set of equations, when combined, has the familiar form of a discrete Fourier transform (up to normalization):

$$\begin{bmatrix} 1 & 1 & \ldots & 1 \\ 1 & \omega & \ldots & \omega^{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{d-1} & \ldots & \omega^{(d-1)^2} \end{bmatrix} \begin{bmatrix} q(0e|0) \\ q(1e|0) \\ \vdots \\ q(d-1,e|0) \end{bmatrix} = \begin{bmatrix} P(e) \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{B.13}$$

Thus, this equation is readily inverted, and we obtain as solution $q(ae|0) = P(e)/d$ for all a, e. In particular, this implies that Eve's guess is completely uncorrelated from Alice's, and her guessing probability is $P_{\text{guess}} = \sum_e q(ee|0) = \frac{1}{d}\sum_e P(e) = 1/d$. Thus 1 dit of randomness is obtained from Alice's measurement.

Appendix C

Non-convexity of the set of classical correlations $\mathcal{C}$

In this Appendix we show an example where the set of classical correlations $\mathcal{C}$ introduced in Section 5.1 in the framework of DIDWs is non-convex (namely $\mathcal{C} \subset \mathrm{Conv}\,\mathcal{C}$) and $\mathcal{C} \subset \mathcal{Q}$. Take $M = 3$, $K = 2$, $N = 2$, and $d = 2$ and consider the following conditional probability distribution of obtaining outcome j given i, k

$$p_{j|i,1} = \begin{pmatrix} 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \\ 0 & 1 \end{pmatrix}, \qquad p_{j|i,2} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}, \tag{C.1}$$

where the i's label the rows and the j's the columns.

First we show that $p \in \mathrm{Conv}\,\mathcal{C}$. Indeed p can be obtained when Alice and Bob share classical correlations represented by a uniformly distributed random variable λ taking values $1, 2$ making use of the classical set $R = \{\rho_{i,\lambda}\}$ of states and of the set $P = \{\Pi_{k,\lambda}\}$ of classical POVMs $\Pi_{k,\lambda} = \{\Pi^j_{k,\lambda}\}$, with

$$\begin{aligned} &\rho_{1,1} = |0\rangle\langle 0|, \quad \rho_{2,1} = |0\rangle\langle 0|, \quad \rho_{3,1} = |1\rangle\langle 1|, \\ &\rho_{1,2} = |0\rangle\langle 0|, \quad \rho_{2,2} = |1\rangle\langle 1|, \quad \rho_{3,2} = |1\rangle\langle 1|, \end{aligned}$$

and

$$\begin{aligned} &\Pi^1_{1,1} = |0\rangle\langle 0|, \quad \Pi^1_{2,1} = |0\rangle\langle 0|, \\ &\Pi^1_{1,2} = |0\rangle\langle 0|, \quad \Pi^1_{2,2} = |1\rangle\langle 1|, \end{aligned}$$

which proves that $p = \{p_{j|i,k} = \sum_\lambda q_\lambda \,\mathrm{Tr}[\rho_{i,\lambda}\Pi^j_{k,\lambda}]\} \in \mathrm{Conv}\,\mathcal{C}$.

Now we show that $p \in \mathcal{Q}$. Indeed p can be obtained by Alice and Bob making use of the quantum set $R = \{\rho_i\}$ of states and of the set $P = \{\Pi_k\}$

of quantum POVMs $\Pi_k = \{\Pi_k^j\}$, with

$$\rho_1 = |0\rangle\langle 0|, \quad \rho_2 = |+\rangle\langle +|, \quad \rho_3 = |1\rangle\langle 1|,$$

and

$$\Pi_1^1 = |0\rangle\langle 0|, \quad \Pi_2^1 = |+\rangle\langle +|,$$

which proves that $p \in \mathcal{Q}$.

Finally, we verify that if Alice and Bob make use of classical sets of states and POVMS and do not have access to shared randomness there is no way to achieve the probability distribution p given by (C.1). Indeed, to have perfect discrimination between ρ_1 and ρ_3 with POVM Π_1 (see (C.1)), one must take ρ_1 and ρ_3 orthogonal - let us say without loss of generality $\rho_1 = |0\rangle\langle 0|$ and $\rho_3 = |1\rangle\langle 1|$, and $\Pi_1^1 = |0\rangle\langle 0|$ and $\Pi_1^2 = |1\rangle\langle 1|$. Due to the hypothesis of classicality of the sets of states, ρ_2 must be a convex combination of ρ_1 and ρ_3. Then, in order to have $p_{j|2,1}$ as in (C.1), one has to choose $\rho_2 = (\rho_1 + \rho_3)/2 = \mathbb{1}/2$. Finally, the only possible choice for Π_2 is $\Pi_2^1 = \mathbb{1}$ and $\Pi_2^1 = 0$, which is incompatible with the remaining entries of $p_{j|i,2}$ in (C.1). This proves that $p \notin \mathcal{C}$.

Appendix D

Algorithms for numerical optimization of device-independent dimension witnesses

In this Appendix we show the algorithms used for numerical optimization of DIDWs. In Section D.1 we consider linear DIDWs and present the algorithm used to find, among all the tight classical DIDWs in the simplest non-trivial scenario, the most robust to loss, which is labeled I_{d+1}. In D.2 we prove an useful Lemma which allows us to simplify the algorithm presented in Section D.1, and we use the new algorithm to optimize I_{d+1}.

D.1 Numerical optimization of DIDWs

Given a linear dimension witness W the following algorithm converges to a local maximum of $W(R, P)$.

Algorithm 1. *For any set* $R^{(0)} = \{\psi_i^{(0)}\}$ *of pure states and any set* $P^{(0)} = \{\Pi_k^{(0)}\}$ *of POVMs* $\Pi_k^{(0)} = \{\Pi_k^{j,(0)}\}$,

1. *let* $|\bar{\psi}_i^{(n+1)}\rangle = \left[(1-\epsilon)\mathbb{1} + \epsilon \sum_{j,k} c_{i,j,k} \Pi_k^{j,(n)}\right] |\psi_i^{(n)}\rangle$,

2. *let* $\bar{\Pi}_k^{j,(n+1)} = \left\{\left[(1-\epsilon)\mathbb{1} + \epsilon \sum_i c_{i,j,k} \psi_i^{(n)}\right] \sqrt{\Pi_k^{j,(n)}}\right\}^2$,

3. *normalize* $|\psi_i^{(n+1)}\rangle = ||\bar{\psi}_i^{(n+1)}||^{-1/2} |\bar{\psi}_i^{(n+1)}\rangle$,

4. normalize $\Pi_k^{j,(n+1)} = S_k^{-\frac{1}{2}} \bar{\Pi}_k^{j,(n+1)} S_k^{-\frac{1}{2}}$ *with* $S_k = \sum_j \bar{\Pi}_k^{j,(n+1)}$.

As for all steepest-ascent algorithm, there is no protection against the possibility of convergence toward a local maximum, rather than the global one. Hence one should run the algorithm for different initial ensembles in order to get some confidence that the observed maximum is the global maximum (although this can never be guaranteed with certainty). Any initial set of states and any initial set of POVMs can be used as a starting point, except for a subset corresponding to minima of $W(R, P)$. These minima are unstable fix-points of the iteration, so even small perturbations let the iteration converge to some maxima. The parameter ϵ controls the length of each iterative step, so for ϵ too large, an overshooting can occur. This can be kept under control by evaluating $W(R, P)$ at the end of each step: if it decreases instead of increasing, we are warned that we have taken ϵ too large.

Referring to Fig. 5.1, the simplest non-trivial scenario one can consider is the one with $M = 3$ preparations and $K = 2$ POVMs each with $N = 3$ outcomes, one of which corresponding to no-click event. In this case one has several tight classical DIDWs. Applying Algorithm 1 we verified that among them the most robust to loss is given by Eq. (5.2) with coefficients given by Eq. (5.7).

D.2 Numerical optimization of I_{d+1}

The following Lemma proves that the POVMs maximizing I_{d+1} for any dimension d are such that one of their elements is a projector on a pure state, thus generalizing a result from [Mas05].

Lemma 2. *For any dimension d, the maximum of I_{d+1} is achieved by a set $P = \{\Pi_k\}$ of POVMs $\Pi_k = \{\Pi_k^j\}$ with Π_k^1 a projector with* $\operatorname{rank} \Pi_k^1 = 1$ *for any k.*

Proof. For any fixed set $R = \{\psi_i\}$ of pure states define $A_k := -\sum_{i \neq k} \psi_i$, $B := \psi_k$, and $X_k := A_k + B_k$. Then clearly $A_k \leq 0$, $B_k \geq 0$ and $\operatorname{rank} B_k = 1$ for any k. From Eq. (5.2) it follows immediately that the optimal set $P^* = \{\Pi_k^*\}$ of POVMs $\Pi_k^* = \{\Pi_k^{*j}\}$ is such that $\Pi_k^{*1} = \arg\min_{\Pi_k^1} \operatorname{Tr}[X \Pi_k^1]$. The optimum of I_{d+1} is achieved when Π_k^1 is the sum of the eigenvectors of X_k corresponding to positive eigenvalues.

Upon denoting with $\lambda_1(A_k) \geq \cdots \geq \lambda_n(A_k)$ the eigenvalues of A_k, the Weyl inequality (see for instance [Bha06]) $\lambda_1(X_k) \leq \lambda_1(A_k) + \lambda_n(B_k)$ holds for any n. Since $\lambda_1(A_k) \leq 0$ and $\lambda_n(B_k) = 0$ for any k and for any $n \neq 0$, the thesis follows immediately. □

Algorithm 1 can be simplified using Lemma 2. The following algorithm converges to a local maximum of I_{d+1}.

Algorithm 2. *For any set* $R^{(0)} = \{\psi_i^{(0)}\}$ *of pure states and any set* $P^{(0)} = \{\Pi_k^{(0)}\}$ *of POVMs* $\Pi_k^{(0)} = \{\Pi_k^{j,(0)}\}$,

1. *let* $|\bar{\psi}_i^{(n+1)}\rangle = |\psi_i^{(n)}\rangle + \epsilon \sum_{j,k} c_{i,j,k} \langle \pi_k^{(n)} | \psi_i^{(n)} \rangle |\pi_k^{(n)}\rangle$,
2. *let* $|\bar{\pi}_k^{(n+1)}\rangle = |\pi_k^{(n)}\rangle + \epsilon \sum_{i,k} c_{i,j,k} \langle \psi_i^{(n)} | \pi_k^{(n)} \rangle |\psi_i^{(n)}\rangle$,
3. *normalize* $|\psi_i^{(n+1)}\rangle = ||\bar{\psi}_i^{(n+1)}||^{-1/2} |\bar{\psi}_i^{(n+1)}\rangle$,
4. *normalize* $|\pi_k^{(n+1)}\rangle = ||\bar{\pi}_k^{(n+1)}||^{-1/2} |\bar{\pi}_k^{(n+1)}\rangle$.

The same remarks made about Algorithm 1 hold true for Algorithm 2. Nevertheless, we verified that in practical applications Algorithm 2 always seems to converge to a global, not a local maximum. This can be explained considering that without loss of generality it optimizes over a smaller set of POVMs when compared to Algorithm 1. Moreover, we noticed that the optimal sets of states and POVMs are real, namely there exists a basis with respect to which states and POVM elements have all real matrix entries. A similar observation was done in [FFW11] in the context of Bell's inequalities.

Appendix E

Equivalence of quantum state joining and the preparation of a TPES

In this Appendix we show that the problem of preparing a TPES such as (7.20):

$$|\psi\rangle_{123} = \frac{1}{2}\left(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2\right)|H\rangle_3 \otimes \left(|u\rangle_1|d\rangle_3 - |d\rangle_1|u\rangle_3\right)|u\rangle_2 \quad \text{(E.1)}$$

is essentially equivalent to that of realizing the quantum state joining. Precisely, we show that quantum state joining can be exploited to prepare the TPES (E.1) and, conversely, state (E.1) can be used to carry out the quantum state joining of two photonic qubits via teleportation.

Indeed, to obtain the three-photon state (E.1), or anyone of the other TPES, one must simply apply the quantum state joining protocol to two photons each taken from a separate entangled pair. In particular, one pair (say, photons 2 and 4) must be entangled in polarization and the other (photons 3 and 5) in the spatial degree of freedom defined by modes $|u\rangle$ and $|d\rangle$. Then photons 4 and 5 are state-joined into photon 1, so that their polarization and spatial modes properties are both transferred into this single photon. This leads immediately to state (E.1).

Conversely, let us assume that we have initially three photons (labeled 1, 2, 3) in state (E.1) and that the qubits we want to join are encoded in two other photons (labeled 4 and 5), as described by the states

$$|\psi\rangle_4 = (\alpha|H\rangle_4 + \beta|V\rangle_4) \otimes |u\rangle_4, \quad \text{(E.2)}$$

$$|\psi\rangle_5 = |H\rangle_5 \otimes (\gamma|u\rangle_5 + \delta|d\rangle_5). \quad \text{(E.3)}$$

Recasting the overall 5-photon initial state $|\psi\rangle_{12345} = |\psi\rangle_{123}|\psi\rangle_4|\psi\rangle_5$ in terms of the basis (7.21) for the states of the pairs 2, 4 and 3, 5, one obtains the following expression:

$$
\begin{aligned}
|\psi\rangle_{12345} = & \frac{1}{4}|\Phi^+\rangle_{24}|\phi^+\rangle_{35}(\alpha|H\rangle_1 - \beta|V\rangle_1)(\gamma|u\rangle_1 - \delta|d\rangle_1) \\
& - \frac{1}{4}|\Phi^+\rangle_{24}|\phi^-\rangle_{35}(\alpha|H\rangle_1 - \beta|V\rangle_1)(\gamma|u\rangle_1 + \delta|d\rangle_1) \\
& + \frac{1}{4}|\Phi^+\rangle_{24}|\psi^+\rangle_{35}(\alpha|H\rangle_1 - \beta|V\rangle_1)(\delta|u\rangle_1 - \gamma|d\rangle_1) \\
& - \frac{1}{4}|\Phi^+\rangle_{24}|\psi^-\rangle_{35}(\alpha|H\rangle_1 - \beta|V\rangle_1)(\delta|u\rangle_1 + \gamma|d\rangle_1) \\
& - \frac{1}{4}|\Phi^-\rangle_{24}|\phi^+\rangle_{35}(\alpha|H\rangle_1 + \beta|V\rangle_1)(\gamma|u\rangle_1 - \delta|d\rangle_1) \\
& + \frac{1}{4}|\Phi^-\rangle_{24}|\phi^-\rangle_{35}(\alpha|H\rangle_1 + \beta|V\rangle_1)(\gamma|u\rangle_1 + \delta|d\rangle_1) \\
& - \frac{1}{4}|\Phi^-\rangle_{24}|\psi^+\rangle_{35}(\alpha|H\rangle_1 + \beta|V\rangle_1)(\delta|u\rangle_1 - \gamma|d\rangle_1) \\
& + \frac{1}{4}|\Phi^-\rangle_{24}|\psi^-\rangle_{35}(\alpha|H\rangle_1 + \beta|V\rangle_1)(\delta|u\rangle_1 + \gamma|d\rangle_1) \\
& + \frac{1}{4}|\Psi^+\rangle_{24}|\phi^+\rangle_{35}(\beta|H\rangle_1 - \alpha|V\rangle_1)(\gamma|u\rangle_1 - \delta|d\rangle_1) \\
& - \frac{1}{4}|\Psi^+\rangle_{24}|\phi^-\rangle_{35}(\beta|H\rangle_1 - \alpha|V\rangle_1)(\gamma|u\rangle_1 + \delta|d\rangle_1) \\
& + \frac{1}{4}|\Psi^+\rangle_{24}|\psi^+\rangle_{35}(\beta|H\rangle_1 - \alpha|V\rangle_1)(\delta|u\rangle_1 - \gamma|d\rangle_1) \\
& - \frac{1}{4}|\Psi^+\rangle_{24}|\psi^-\rangle_{35}(\beta|H\rangle_1 - \alpha|V\rangle_1)(\delta|u\rangle_1 + \gamma|d\rangle_1) \\
& - \frac{1}{4}|\Psi^-\rangle_{24}|\phi^+\rangle_{35}(\beta|H\rangle_1 + \alpha|V\rangle_1)(\gamma|u\rangle_1 - \delta|d\rangle_1) \\
& + \frac{1}{4}|\Psi^-\rangle_{24}|\phi^-\rangle_{35}(\beta|H\rangle_1 + \alpha|V\rangle_1)(\gamma|u\rangle_1 + \delta|d\rangle_1) \\
& - \frac{1}{4}|\Psi^-\rangle_{24}|\psi^+\rangle_{35}(\beta|H\rangle_1 + \alpha|V\rangle_1)(\delta|u\rangle_1 - \gamma|d\rangle_1) \\
& + \frac{1}{4}|\Psi^-\rangle_{24}|\psi^-\rangle_{35}(\beta|H\rangle_1 + \alpha|V\rangle_1)(\delta|u\rangle_1 + \gamma|d\rangle_1). \qquad \text{(E.4)}
\end{aligned}
$$

Then, to obtain the state-joining one needs to perform a Bell measurement in polarization on the photons 2 and 4 and another Bell measurement in the modes u and d on the photons 3 and 5. Whatever the outcome of the two Bell measurements, one may carry out an appropriate unitary transformation in order to cast photon 1 in the desired "joined" state

$$|\Psi\rangle_1 = (\alpha|H\rangle_1 + \beta|V\rangle_1) \otimes (\delta|u\rangle_1 + \gamma|d\rangle_1).$$

The unitary transformation must be selected according to the result of the two Bell measurements, out of 16 possible results (and if a different TPES state is used in the process, it affects only the set of unitary transformations to be used).

It is interesting to note that, if a method for deterministic complete Bell state measurement is available, the quantum state joining obtained by this teleportation method can be also accomplished in a deterministic way. Indeed, one needs to prepare in advance a TPES using the probabilistic joining protocol by making as many attempts as needed. Then, one can complete the joining of the input photons deterministically by using the above described teleportation protocol.

Bibliography

[ABCB12] H. Ahrens, P. Badziąg, A. Cabello, and M. Bourennane. Experimental device-independent tests of classical and quantum dimensions. *Nature Physics*, 8:592–595, 2012.

[ABG+07] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98:230501, 2007.

[ALMO08] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols. Quantum random access codes with shared randomness. arXiv:0810.2937, 2008.

[AMP06] A. Acín, S. Massar, and S. Pironio. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, 8:126, 2006.

[AMP12] A. Acín, S. Massar, and S. Pironio. Randomness versus nonlocality and entanglement. *Physical Review Letters*, 108:100402, 2012.

[ANTSV99] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and a lower bound for 1-way quantum automata. In *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC'99)*, pages 376–383. ACM Press, 1999.

[ANTSV02] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense quantum coding and quantum finite automata. *Journal of the ACM*, 49(4):496–511, 2002.

[Ara04] P. K. Aravind. Quantum mysteries revisited again. *American Journal of Physics*, 72:1303, 2004.

[AWT+15] S. Armstrong, M. Wang, R. Y. Teh, Q. Gong, Q. He, J. Janousek, H.-A. Bachor, M. D. Reid, and P. K. Lam. Multipartite Einstein-Podolsky-Rosen steering and genuine tripartite entanglement with optical networks. *Nature Phisics*, 11:167–172, 2015.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179. IEEE Press, New York, 1984.

[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. *Physical Review Letters*, 70:1895–1899, 1993.

[BCP+14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86:419–478, 2014.

[BCW+12] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Physical Review A*, 85:010301, 2012.

[BD00] C. H. Bennett and D. P. DiVincenzo. Quantum information and computation. *Nature*, 404:247–255, 2000.

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1:195, 1964.

[BES+12] A. J. Bennet, D. A. Evans, D. J. Saunders, C. Branciard, E. G. Cavalcanti, H. M. Wiseman, and G. J. Pryde. Arbitrarily loss-tolerant Einstein-Podolsky-Rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole. *Physical Review X*, 2:031003, 2012.

[Bha06] R. Bhatia. *Positive Definite Matrices*. Princeton University Press, 2006.

[BHK05] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95:010503, 2005.

[BLPK05] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat. Generation of hyperentangled photon pairs. *Physical Review Letters*, 95:260501, 2005.

[BP12] S. L. Braunstein and S. Pirandola. Side-channel-free quantum key distribution. *Physical Review Letters*, 108:130502, 2012.

[BPA+08] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani. Testing the dimension of Hilbert spaces. *Physical Review Letters*, 100:210503, 2008.

[BPM+97] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature*, 390:575–579, 1997.

[BQB14] J. Bowles, M. T. Quintino, and N. Brunner. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. *Physical Review Letters*, 112:140407, 2014.

[BSLR03] W. P. Bowen, R. Schnabel, P. K. Lam, and T. C. Ralph. Experimental investigation of criteria for continuous variable entanglement. *Physical Review Letters*, 90:043601, 2003.

[BSS14] J.-D. Bancal, L. Sheridan, and V. Scarani. More randomness from the same data. *New Journal of Physics*, 16(3):033011, 2014.

[BV04] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[BvF+06] L. Bartůšková, A. Černoch, R. Filip, J. Fiurášek, J. Soubusta, and M. Dušek. Optical implementation of the encoding of two qubits to a single qutrit. *Physical Review A*, 74:022325, 2006.

[BW92] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Physical Review Letters*, 69:2881–2884, 1992.

[Cab01] A. Cabello. "All versus nothing" inseparability for two observers. *Physical Review Letters*, 87:010403, 2001.

[CBS+11] D. Cavalcanti, N. Brunner, P. Skrzypczyk, A. Salles, and V. Scarani. Large violation of Bell inequalities using both particle and wave measurements. *Physical Review A*, 84:022105, 2011.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.

[Cir80] B. S. Cirel'son. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[CJWR09] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. D. Reid. Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox. *Physical Review A*, 80:032112, 2009.

[CMA+13] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat. Detection-loophole-free test of quantum nonlocality, and applications. *Physical Review Letters*, 111:130406, 2013.

[Col06] R. Colbeck. *Quantum and relativistic protocols for secure multi-party computation*. PhD thesis, University of Cambridge, 2006. arXiv:0911.3814.

[CSA+15] D. Cavalcanti, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. Souto Ribeiro, and S. P. Walborn. Detection of entanglement in asymmetric quantum networks and multipartite quantum steering. *Nature Communications*, 6:7941, 2015.

[CVDM+09] R. Ceccarelli, G. Vallone, F. De Martini, P. Mataloni, and A. Cabello. Experimental entanglement and nonlocality of a two-photon six-qubit cluster state. *Physical Review Letters*, 103:160401, 2009.

[DLB+11] A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, and E. Andersson. Experimental high-dimensional two-photon entanglement and violations of generalized Bell inequalities. *Nature Physics*, 7:677–680, 2011.

[Ebe93] P. H. Eberhard. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Physical Review A*, 47:R747–R750, 1993.

[Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67:661, 1991.

[FFW11] T. Franz, F. Furrer, and R. F. Werner. Extremal quantum correlations and cryptographic security. *Physical Review Letters*, 106:250502, 2011.

[FSS+07] M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro. Secure self-calibrating quantum random-bit generator. *Physical Review A*, 75:032334, 2007.

[GB08] M. Grant and S. Boyd. Graph implementations for nonsmooth convex programs. In V. Blondel, S. Boyd, and H. Kimura, editors, *Recent Advances in Learning and Control*, Lecture Notes in Control and Information Sciences, pages 95–110. Springer-Verlag Limited, 2008. `http://stanford.edu/~boyd/graph_dcp.html`.

[GB13] M. Grant and S. Boyd. CVX: Matlab software for disciplined convex programming, version 2.0 beta. `http://cvxr.com/cvx`, 2013.

[GBHA10] R. Gallego, N. Brunner, C. Hadley, and A. Acín. Device-independent tests of classical and quantum dimensions. *Physical Review Letters*, 105:230501, 2010.

[GBR+06] M. Grace, C. Brif, H. Rabitz, I. Walmsley, R. Kosut, and D. Lidar. Encoding a qubit into multilevel subspaces. *New Journal of Physics*, 8(3):35, 2006.

[GECP08] J. C. García-Escartín and P. Chamorro-Posada. Quantum multiplexing with the orbital angular momentum of light. *Physical Review A*, 78:062320, 2008.

[Gis89] N. Gisin. Stochastic quantum dynamics and relativity. *Helvetica Physica Acta*, 62:363–371, 1989.

[GLLL+11] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications*, 2(349), 2011.

[GLY+10] W.-B. Gao, C.-Y. Lu, X.-C. Yao, P. Xu, O. Gühne, A. Goebel, Y.-A. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan. Experimental demonstration of a hyper-entangled ten-qubit Schrödinger cat state. *Nature Physics*, 6:331–335, 2010.

[GM87] A. Garg and N. D. Mermin. Detector inefficiencies in the Einstein-Podolsky-Rosen experiment. *Physical Review D*, 35:3831–3835, 1987.

[GMR+13] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam, R. Ursin, and A. Zeilinger. Bell violation using entangled photons without the fair-sampling assumption. *Nature*, 497:227–230, 2013.

[GPS10] N. Gisin, S. Pironio, and N. Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Physical Review Letters*, 105:070501, 2010.

[GPW+04] S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph, and A. Zeilinger. Realization of a photonic controlled-NOT gate sufficient for quantum computation. *Physical Review Letters*, 93:020504, 2004.

[GW03] A. Grudka and A. Wójcik. How to encode the states of two non-entangled qubits in one qutrit. *Physics Letters A*, 314:350–353, 2003.

[HES+12] V. Händchen, T. Eberle, S. Steinlechner, A. Samblowski, T. Franz, R. F. Werner, and R. Schnabel. Observation of one-way Einstein-Podolsky-Rosen steering. *Nature Photonics*, 6:596, 2012.

[HGM+12] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres. Experimental estimation of the dimension of classical and quantum systems. *Nature Physics*, 8:588–591, 2012.

[HHH98] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Physical Review Letters*, 80:5239–5242, 1998.

[HHHP06] M. Horodecki, P. Horodecki, R. Horodecki, and M. Piani. Quantumness of ensemble from no-broadcasting principle. *International Journal of Quantum Information*, 4:105–118, 2006.

[HIN+06] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita. (4,1)-Quantum random access coding does not exist – one qubit is not enough to recover one of four bits. *New Journal of Physics*, 8(8):129, 2006.

[HJW93] L. P. Hughston, R. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, 183:14–18, 1993.

[HKO+12] J. Hofmann, M. Krug, N. Ortegel, L. Gérard, M. Weber, W. Rosenfeld, and H. Weinfurter. Heralded entanglement between widely separated atoms. *Science*, 337:6090, 2012.

[HRW13] E. Hänggi, R. Renner, and S. Wolf. The impossibility of non-signaling privacy amplification. *Theoretical Computer Science*, 486:27–42, 2013.

[HSS07] M. Horodecki, A. Sen(De), and U. Sen. Quantification of quantum correlation of ensembles of states. *Physical Review A*, 75:062329, 2007.

[HT02] H. F. Hofmann and S. Takeuchi. Quantum phase gate for photonic qubits using only beam splitters and postselection. *Physical Review A*, 66:024308, 2002.

[Joh15] N. Johnston. QETLAB: A MATLAB toolbox for quantum entanglement, version 0.8. `http://qetlab.com`, 2015.

[JSC+04] B. Julsgaard, J. Sherson, J. I. Cirac, J. Fiurášek, and E. S. Polzik. Experimental demonstration of quantum memory for light. *Nature*, 432:482–486, 2004.

[Kim08] H. J. Kimble. The quantum internet. *Nature*, 453:1023–1030, 2008.

[KLM01] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409:46–52, 2001.

[KMN+07] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79:135–174, 2007.

[LBA+09] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White. Simplifying quantum logic using higher-dimensional Hilbert spaces. *Nature Physics*, 5:134–140, 2009.

[LCC+15] C.-M. Li, K. Chen, Y.-N. Chen, Q. Zhang, Y.-A. Chen, and J.-W. Pan. Genuine high-order Einstein-Podolsky-Rosen steering. *Physical Review Letters*, 115:010402, 2015.

[LCQ12] H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108:130503, 2012.

[LJL+10] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O'Brien. Quantum computers. *Nature*, 464:45–53, 2010.

[LLF11] S. Luo, N. Li, and S. Fu. Quantumness of quantum ensembles. *Theoretical and Mathematical Physics*, 169:1724–1739, 2011.

[LPY+12] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han. Semi-device-independent randomness certification using $n \to 1$ quantum random access codes. *Physical Review A*, 85:052308, 2012.

[LTBS14] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani. Quantum randomness extraction for various levels of characterization of the devices. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424028, 2014.

[LWW+10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4:686–689, 2010.

[MAG06] Ll. Masanes, A. Acin, and N. Gisin. General properties of nonsignaling theories. *Physical Review A*, 73:012112, 2006.

[Mas02] S. Massar. Nonlocality, closing the detection loophole, and communication complexity. *Physical Review A*, 65:032121, 2002.

[Mas03] Ll. Masanes. Tight Bell inequality for d-outcome measurements correlations. *Quantum Information and Computation*, 3(4):345–358, 2003.

[Mas05] Ll. Masanes. Extremal quantum correlations for N parties with two dichotomic observables per site. arXiv:quant-ph/0512100, 2005.

[MBA13] A. Máttar, J. B. Brask, and A. Acín. Device-independent quantum key distribution with spin-coupled cavities. *Physical Review A*, 88:062319, 2013.

[MP03] S. Massar and S. Pironio. Violation of local realism versus detection efficiency. *Physical Review A*, 68:062109, 2003.

[MSD+12] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto. Quantum communication without the necessity of quantum memories. *Nature Photonics*, 6:777–781, 2012.

[MTTT07] G. Molina-Terriza, J. P. Torres, and Ll. Torner. Twisted photons. *Nature Physics*, 3:305–310, 2007.

[MVWZ01] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412:313–316, 2001.

[Nay99] A. Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of the 40th Annual Symposium on Foundations of Computer Science (FOCS'99)*, pages 369–376. IEEE, 1999.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NGM+10] E. Nagali, D. Giovannini, L. Marrucci, S. Slussarenko, E. Santamato, and F. Sciarrino. Experimental optimal cloning of four-dimensional quantum states of photons. *Physical Review Letters*, 105:073602, 2010.

[NN13] J. S. Neergaard-Nielsen. Quantum information processing: Two become one. *Nature Photonics*, 7:512–513, 2013.

[NSM+10] E. Nagali, L. Sansoni, L. Marrucci, E. Santamato, and F. Sciarrino. Experimental generation and characterization of single-photon hybrid ququarts based on polarization and orbital angular momentum encoding. *Physical Review A*, 81:052317, 2010.

[NSPS14] O. Nieto-Silleras, S. Pironio, and J. Silman. Using complete measurement statistics for optimal device-independent randomness evaluation. *New Journal of Physics*, 16(1):013035, 2014.

[OFV09] J. L. O'Brien, A. Furusawa, and J. Vučković. Photonic quantum technologies. *Nature Photonics*, 3:687–695, 2009.

[OPKP92] Z. Y. Ou, S. F. Pereira, H. J. Kimble, and K. C. Peng. Realization of the Einstein-Podolsky-Rosen paradox for continuous variables. *Physical Review Letters*, 68:3663–3666, 1992.

[OPW+03] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning. Demonstration of an all-optical quantum controlled-NOT gate. *Nature*, 426:264–267, 2003.

[PAB+09] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[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*, 464:1021–1024, 2010.

[PB11] M. Pawłowski and N. Brunner. Semi-device-independent security of one-way quantum key distribution. *Physical Review A*, 84:010302, 2011.

[PCL+12] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Żukowski. Multiphoton entanglement and interferometry. *Reviews of Modern Physics*, 84:777–838, 2012.

[PFJF03] T. B. Pittman, M. J. Fitch, B. C. Jacobs, and J. D. Franson. Experimental controlled-NOT logic gate for single photons in the coincidence basis. *Physical Review A*, 68:032316, 2003.

[PFL+12] T. Peyronel, O. Firstenberg, Q.-Y. Liang, S. Hofferberth, A. V. Gorshkov, T. Pohl, M. D. Lukin, and V. Vuletić. Quantum

nonlinear optics with single photons enabled by strongly interacting atoms. *Nature*, 488:57–60, 2012.

[Pil11] D. Pile. View from... OSA Frontiers in Optics 2011: How many bits can a photon carry? *Nature Photonics*, 6:14–15, 2011.

[PJF01] T. B. Pittman, B. C. Jacobs, and J. D. Franson. Probabilistic quantum logic operations using polarizing beam splitters. *Physical Review A*, 64:062311, 2001.

[PR94] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.

[PRB+14] G. Pütz, D. Rosset, T. J. Barnea, Y.-C. Liang, and N. Gisin. Arbitrarily small amount of measurement independence is sufficient to manifest quantum nonlocality. *Physical Review Letters*, 113:190402, 2014.

[Pus13] M. F. Pusey. Negativity and steering: A stronger Peres conjecture. *Physical Review A*, 88:032313, 2013.

[PZ10] M. Pawłowski and M. Żukowski. Entanglement-assisted random access codes. *Physical Review A*, 81:042326, 2010.

[QVB14] M. T. Quintino, T. Vértesi, and N. Brunner. Joint measurability, Einstein-Podolsky-Rosen steering, and Bell nonlocality. *Physical Review Letters*, 113:160402, 2014.

[QVC+15] M. T. Quintino, T. Vértesi, D. Cavalcanti, R. Augusiak, M. Demianowicz, A. Acín, and N. Brunner. Inequivalence of entanglement, steering, and Bell nonlocality for general measurements. *Physical Review A*, 92:032107, 2015.

[Ral04] T. C. Ralph. Scaling of multiple postselected quantum gates in optics. *Physical Review A*, 70:012312, 2004.

[RLBW02] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White. Linear optical controlled-NOT gate in the coincidence basis. *Physical Review A*, 65:062324, 2002.

[ROT94] J. G. Rarity, P. C. M. Owens, and P. R. Tapster. Quantum random-number generation and key sharing. *Journal of Modern Optics*, 41(12):2435, 1994.

[SBPC+09] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81:1301–1350, 2009.

[Sch35] E. Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31:555–563, 1935.

[Ser06] A. V. Sergienko. *Quantum Communications and Cryptography*. CRC Press, Taylor & Francis Group, 2006.

[SGA+12] D. H. Smith, G. Gillett, M. P. Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, H. M. Wiseman, S. W. Nam, and A. G. White. Conclusive quantum steering with superconducting transition-edge sensors. *Nature Communications*, 3:625, 2012.

[SJWP10] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. J. Pryde. Experimental EPR-steering using Bell-local states. *Nature Physics*, 6:845–849, 2010.

[SK10] S. Straupe and S. Kulik. Quantum optics: The quest for higher dimensionality. *Nature Photonics*, 4:585–586, 2010.

[SKFP11] E. Shahmoon, G. Kurizki, M. Fleischhauer, and D. Petrosyan. Strongly interacting photons in hollow-core waveguides. *Physical Review A*, 83:033806, 2011.

[TLGR12] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3(634), 2012.

[TR11] M. Tomamichel and R. Renner. Uncertainty relation for smooth entropies. *Physical Review Letters*, 106:110506, 2011.

[UMG14] R. Uola, T. Moroder, and O. Gühne. Joint measurability of generalized measurements implies classicality. *Physical Review Letters*, 113:160403, 2014.

[VSA+13] C. Vitelli, N. Spagnolo, L. Aparo, F. Sciarrino, E. Santamato, and L. Marrucci. Joining the quantum state of two photons into one. *Nature Photonics*, 7:521–526, 2013.

[Wer89] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40:4277–4281, 1989.

[WJD07] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Physical Review Letters*, 98:140402, 2007.

[Woo14] E. Woodhead. *Imperfections and self testing in prepare-and-measure quantum key distribution.* PhD thesis, Université Libre de Bruxelles, 2014. `http://dipot.ulb.ac.be/dspace/bitstream/2013/209185/1/23388d86-c59c-449c-b88a-1e97a45f1ad8.txt`.

[WPS] E. Woodhead, S. Pironio, and J. Silman. Partially deterministic polytopes. Unpublished.

[WRS+12] B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. M. Wiseman, R. Ursin, and A. Zeilinger. Loophole-free Einstein-Podolsky-Rosen experiment via quantum steering. *New Journal of Physics*, 14(5):053030, 2012.

[Yao77] A. C.-C. Yao. Probabilistic computations: Toward a unified measure of complexity. In *Proceedings of the 18th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 222–227. IEEE, 1977.

[YR03] N. Yoran and B. Reznik. Deterministic linear optics quantum computation with single photon qubits. *Physical Review Letters*, 91:037903, 2003.

[YWX+12] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan. Observation of eight-photon entanglement. *Nature Photonics*, 6:225–228, 2012.

[ZPWL11] X. Zhu, S. Pang, S. Wu, and Q. Liu. The classicality and quantumness of a quantum ensemble. *Physics Letters A*, 375:1855–1859, 2011.

[ZZC+05] Z. Zhao, A.-N. Zhang, Y.-A. Chen, H. Zhang, J.-F. Du, T. Yang, and J.-W. Pan. Experimental demonstration of a nondestructive controlled-NOT quantum gate for two independent photon qubits. *Physical Review Letters*, 94:030501, 2005.