UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

Quantum information with black boxes : lifting protocols from theory to implementation

Alejandro Máttar Flores

PhD thesis

Quantum information with black boxes

Lifting protocols from theory to implementation

Alejandro Máttar Flores

Advisor: Prof. Antonio Acín

ICFO - The Institute of Photonic Sciences

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

July 26, 2017

To my parents and brothers.

The thing that differentiates scientists is purely an artistic ability to discern what is a good idea, what is a beautiful idea, what is worth spending time on, and most importantly: what is a problem that is sufficiently interesting, yet sufficiently difficult that it hasn't yet been solved, but, the time for solving it has come now.

-Prof. S. Dimopoulos *(Particle Fever, 2013)*

Acknowledgments

Many thanks to Toni, for hosting me in his group, being the best supervisor I could think of, and always advising me wisely in this project.

To Dani, who apart from co-supervising this project has been a great friend and a true mentor during all these years in Barcelona.

To Paul, from who I learned to understand Science, and to who I owe so much for all the friendship and support that he and his family have given me.

To my dear brother Osvaldo, for sharing with me the importance of experiments, quantum wise but also with congas, djembés and agogos.

To Alexia, Boris and Flavio, for helping me to *find a stable position* and to organise the best conference ever *#YQIS*2016.

To Janek, Jonatan and Matty, who supported me and walked me through important steps of my PhD, including mountain trips, skiing lessons and pub nights.

Special thanks to Gustavo Lima and Konrad Banaszek, who I deeply appreciate for receiving me in Chile and Poland, and from whom I have learned so much.

To Flo and Martí, from who I learned a lot and shared great (football) moments.

To Maciek and Karen for their friendship, especially during my first steps.

To Victoria, Peter, Senaida and Elisa, for the greatest Salsa nights in Barcelona.

To Alex and Gonzalo, for being true counselors. #Office368.

Many thanks to Nicolas Brunner, Huges de Riedmatten and Anna Sanpera for joining this project by forming the Committee to evaluate and review this Thesis.

Special thanks also to Ariel, Arnau, Bogna, Dario, Eric, Ivan, Joe, Jordi, Lars, Leo, Mafalda, Matteo, Michal and Zahra with whom I spent great times in this trip.

I also thank the Human Resources crew of ICFO for their invaluable support.

Resumen

De acuerdo con estimaciones recientes, 10^{18} bytes de datos se generan diariamente alrededor del mundo. Nuestra sociedad necesita urgentemente soluciones efectivas para lidiar con este diluvio de datos. Utilizando elementos fundamentales de la teoría cuántica —la teoría más explorada de la física moderna, posiblemente— la información cuántica está revolucionando la forma en la que adquirimos, procesamos, almacenamos y transmitimos información. En plena era de la información, el sector industrial reconoce cada vez más el potencial de las tecnologías cuánticas, y a su vez nuevos desarrollos en el procesamiento de la información cuántica continúan impulsando descubrimientos prominentes relacionados con aspectos científicos de carácter más fundamental.

Existen varios programas de investigación alrededor del mundo desarrollando y comercializando tecnologías cuánticas, principalmente para aplicaciones de criptografía y generación de números aleatorios. Así, las limitaciones que hoy nos separan de la era de la información cuántica están siendo gradualmente superadas. Sin embargo, existe un problema fundamental que aún necesita ser enfrentado: la imposibilidad de saber lo que *realmente sucede* en un experimento cuántico, debido a sus dimensiones de tamaño atómico. En efecto, ¿cómo podrá un usuario garantizar el funcionamiento adecuado de un dispositivo cuántico que ha sido adquirido a través de una compañía externa? A sus ojos el dispositivo será una verdadera caja negra. Incluso si el usuario contara con un Doctorado en ciencia cuántica, el problema prevalecería insoluble debido a la imposibilidad de controlar a la perfección, es decir monitorear, todos los procesos físicos que ocurren en cualquier experimento cuántico. Además, la situación se vuelve aún más dramática si se piensa en aplicaciones en donde un agente maligno pudiese hackear los dispositivos y manipular su funcionamiento interno, volviendo así el protocolo en cuestión inseguro y por ende también irrelevante.

El propósito de esta Tesis es entonces contribuir al desarrollo experimental de protocolos de información cuántica con dispositivos sin caracterizar, llamados *device-independent*. Estos protocolos son, por naturaleza, immunes a cualquier ataque o falla relacionada con desajustes entre la teoría y la implementación del protocolo. Esto se logra a lo largo de los diferentes Capítulos prosiguiendo las siguientes tres tareas que en ocasiones se traslapan: *(i)* Ampliar las capacidades teóricas estableciendo un entendimiento mayor de los recursos fundamentales de

la teoría de la información cuántica con dispositivos sin caracterizar. *(ii)* Desarrollar protocolos de información cuántica competitivos, encontrando un intercambio adecuado entre alto rendimiento y practicabilidad; entre el poder del marco de trabajo *device-independent* y sus menos demandantes versiones, dichas *semi-device-independent*. *(iii)* Analizar y mejorar las condiciones experimentales de diversas plataformas para llevar a cabo implementaciones en experimentos de prueba de principio, demostrando la realización de protocolos de información cuántica con cajas negras.

Nuestro objetivo de convertir la teoría de la información cuántica en una tecnología tangible para nuestra sociedad a través del uso de dispositivos sin caracterizar contribuye no solamente al desarrollo tecnológico de estos protocolos, sino que también ofrece una visión valiosa de aspectos más fundamental. En este sentido, contribuimos a la caracterización y cuantificación del *entrelazamiento* —el recurso cuántico fundamental de muchos fenómenos sin contraparte clásica— en escenarios de interés práctico en dónde se consideran dispositivos sin caracterizar. Desde la perspectiva más aplicada, contribuimos al desarrollo de dos tareas específicas: la certificación de números genuinamente aleatorios en escenarios *device-independent* y *semi-device-independent*, y la generación de una llave secreta entre dos partes de manera *device-independent*.

Abstract

According to recent estimates, 10^{18} bytes of data are generated on a daily basis around the globe. Our information society urges for radical solutions to treat such data deluge. By exploiting fundamental key elements of quantum theory —arguably the most probed theory of modern physics— quantum information science is nowadays revolutionizing the way in which we acquire, process, store and transmit information. In the midst of the information era, the potential of quantum technologies is being recognized by the industry sector, and in turn, new capabilities for quantum information processing keep driving exciting discoveries related to more fundamental aspects of science.

There are several research programs all around the world fostering the development and commercialization of quantum technologies, mostly for cryptographic and randomness generation duties. Thus, the technological limitations that today step us aside from the quantum information era are gradually being overcome. But there is a fundamental issue that still needs to be faced: the impossibility to know *what is really going on* in quantum experiments, due to their atomic-scale dimensions. Indeed, how will an average user guarantee the proper functioning of a quantum device that has been purchased from an external company? To his eyes, the device will merely look like a black box. Even if the customer holds a PhD in quantum science, the issue will remain fundamentally cumbersome because of the impossibility to fully control, *i.e.* monitor, all the physical processes occurring in any quantum experiment. Furthermore, the situation turns even more dramatic when considering adversarial applications, where a malicious eavesdropper could break the devices to manipulate their internal working, turning the protocol insecure and hence irrelevant as well.

Therefore, it is the purpose of this Thesis to contribute to the experimental development of quantum information protocols with uncharacterized devices, namely, *device-independent* quantum information protocols. These protocols are naturally immune to any attack or failure related to mismatches between protocol theory and its actual implementation. This is achieved throughout the different Chapters by pursuing the following three overlapping duties: *(i)* To broaden theoretic capabilities by establishing a richer understanding of relevant fundamental resources lying at the basis of the theory of quantum information with uncharacterized devices. *(ii)* To develop competitive quantum information protocols by find-

ing an adequate trade-off between high-performance and practicability; between the power of the device-independent framework and its less demanding, so-called *semi-device-independent*, relaxations. *(iii)* To analyze and improve experimental conditions of diverse physical setups in order to carry out implementations in proof-of-principle experiments demonstrating quantum information protocols with black boxes.

Our objective of turning the theory of quantum information into a graspable technology for our society through the development and implementation of protocols based on the minimalist, user-friendly, black-box paradigm contributes not only to the technological development of these protocols, but it also offers valuable insights on more fundamental aspects of quantum theory. In this sense, we contribute to the characterization and quantification of *entanglement*—the pivotal quantum resource at the basis of most testable phenomena without classical account— in scenarios of practical interest where uncharacterized devices are used. From the more applied perspective, we contribute to the development of two specific information tasks: the certification of genuinely random numbers in device-independent and semi-device-independent scenarios, and the generation of a shared secret key among two parties in a full device-independent manner.

List of Publications

This PhD Thesis is based on the following Publications:

- A. Máttar, J. Bohr-Brask and A. Acín. Device-independent quantum key distribution with spin-coupled cavities. *Phys. Rev. A* **88** 062319 (2013)
- A. Máttar, P. Skrzypczyk, J. Bohr-Brask, D. Cavalcanti and A. Acín. Optimal randomness generation from optical Bell experiments. *New J. Phys.* **17** 022003 (2015)
- A. Máttar and A. Acín. Implementations for device-independent quantum key distribution. *Phys. Scr.* **91**, 043003 (2016)
- A. Máttar, P. Skrzypczyk, G. Aguilar, R. Nery, P. Souto-Ribeiro, S. Walborn, and D. Cavalcanti. Experimental multipartite entanglement and randomness certification of the W state in the quantum steering scenario. *Quantum Sci. Technol.* **2** 015011 (2017)
- A. Máttar, P. Skrzypczyk, D. Cavalcanti, J. Kolodynski, K. Banaszek and A. Acín. Device-independent quantum key distribution with single-photon sources. *In preparation*.
- E. Gómez, A. Máttar, S. Gómez, D. Cavalcanti, O. Jiménez, A. Acín and G. Lima. Experimental nonlocality-based randomness generation with non-projective measurements. *Submitted to Nature Photonics*.
- V. Lipinska, F. Curchod, A. Máttar and A. Acín . A measure of nonlocality without anomalies. *In preparation*.

Other Publications not included in this Thesis:

- D. Rielander, A. Lenhard, O. Jimenez, A. Máttar, D. Cavalcanti, M. Mazzera, A. Acín and H. de Riedmatten. Frequency-bin entanglement of ultra-narrow band non-degenerate photon pairs. *Submitted to Quantum Sci. Technol.* Pre-print avilable at: *ArXiv* **quant-ph** 1707.02837 (2017).

Contents

1. Introduction

1.1. Brief overview

Quantum information science exploits fundamental key elements of quantum theory —arguably the most probed theory of modern physics— to dramatically improve the acquisition, transmission and processing of information. Over the last three decades, the field has experienced tremendous growth as a consequence of the following converging stimuli: *(i)* the development of quantum algorithms and quantum information protocols largely outperforming their classical counterparts, *(ii)* the urgent demand for radical changes in technology due to the fact that the miniaturization of information, dictated by Moore's law, has reached the quantum scale and *(iii)* the development of efficient experimental techniques to create, store and manipulate quantum systems within a wide range of physical implementations. In the midst of the information era, the potential of quantum technologies is nowadays recognized by enterprises from the industry sector, and in turn, new capabilities for quantum information processing keep driving exciting discoveries related to more fundamental aspects of science.

Quantum Key Distribution (QKD), that is, the distribution of a secret key between two honest parties whose security is exclusively guaranteed from the laws of quantum physics [BB84, Eke91], is possibly the most mature quantum information technology today. Originally introduced by Bennett and Brassard in the eighties [BB84], QKD fundamentally changes and improves the way in which we assess crypto-security, as QKD security is no longer based on assumptions on the eavesdropper's computational power, but on the fact that her actions must obey the laws of quantum physics. With the subsequent development of optic fibre technology, entangled photon sources and decoy state pulses, QKD became experimentally reachable by the beginning of the 21st century [HMP00, ZQM$^+$06]. Up to date, QKD has been extensively implemented and allows two honest users to exchange secure keys at a rate of kilobits per second over hundreds of kilometers with optic fibers [KLH$^+$15] and on free-space as well [SMWF$^+$07]. In fact, there are currently four companies offering commercial QKD systems (ID Quantique, MagiQ, QuintessenceLabs and SeQureNet) and several others — including Toshiba, HP and IBM— are also developing active research programs.

A few years ago, however, several publications reported on the hacking of some of the above-mentioned QKD commercial products [ZFQ+08, LWW+10, GLLL+11a]. At first sight, this seemed to suggest that the mathematical proofs of QKD security were flawed, or even worse, that quantum theory itself was incorrect. But a closer examination revealed that *in reality* the hacking attacks had not broken any principle at all: instead, they had exploited mismatches —hitherto unidentified— between the theoretical description and the physical implementation of the protocol in question. In fact, the success and security of existing QKD products is built upon assumptions about the quantum states and measurements used which are crucial, though actually difficult to meet in practice [SK14]. If the parties cannot legitimately guarantee that the states that they receive and the measurements that they perform correspond to those required by QKD theory, security breaches are opened and protocols become unreliable and insecure.

Of course, a patch closing the loophole exploited in the attacks was immediately put in place by the company distributing the QKD products. This is in fact a possible solution to the quantum hacking problem: to patch all mismatches occurring between theoretical modeling and real implementation by improving experimental conditions to guarantee that the states and measurements required in the protocol are correctly implemented. However, this approach seems out of reach, due to the near-to-perfect implementation demands from QKD theory [SK14], and to the unavoidable presence of noise sources that will never be fully characterized and thoroughly accounted for in any experiment.

A radically different solution to this fundamental problem would be to completely ignore the internal working of all devices and attempt to establish security exclusively from the observed statistics, that is, without making any assumption about the states and measurements used in the QKD protocol. This approach was introduced by Acín and collaborators ten years ago [ABG+07], under the name of device-independent quantum key distribution (DIQKD). Inspired from previous results on self-testing [MY98] and non-signaling key distribution [BHK05], DIQKD proposes a minimalist paradigm to design protocols whose security is exclusively guaranteed from the observed (classical) data, without any reference to the shape of the (quantum) states and measurements used to obtain it.

Generally speaking, the device-independent (DI) approach provides protocols naturally immune to hacking attacks exploiting experimental imperfections, and thus has emerged as an engaging formalism for the development of new-generation quantum information technologies. The DI approach has in fact been proven fruitful over the past decade for QKD [ABG+07, MPA11, PMLA13, VV14, MS16] and beyond, yielding protocols also for random number generation (RNG) [Col07, PAM+10, GMDLT+13, NSBSP16], entanglement detection [BGLP11, BBS+13] and other tasks as well [GBHA10, CBB15, CS16].

Experimentally, however, implementing DI quantum information protocols remains hitherto difficult because the uncharacterized devices used must produce statistics exhibiting Bell nonlocality [Bel64, BCP+14] —a strong form of correlations achievable by means of quantum resources but with no classical counterpart— in a loophole-free manner. In particular, loophole-free implementations in the context of Bell experiments crucially rely on high overall efficiencies for the collection of the observed statistics, making the certification of genuine nonlocality difficult —though not impossible [HBD+15, GVW+15, SMSC+15]— to be implemented from state-of-the-art quantum technologies.

A midpoint among the scenario in which all quantum devices are trusted and the full DI paradigm is the semi-DI approach (see Fig. 1.1). This is a hybrid combination which takes the best of the two worlds, as it provides high performance from less experimental requirements by moderating ultra-security claims through protocols based on partial elements of trust. The semi-DI approach delivers a very competitive edge because it offers a more practical framework than the DI formalism to implement quantum information protocols with uncharacterized devices. For instance, in Measurement-DIQKD [LCQ12], the two parties willing to share a secret key prepare specific quantum states which are sent to a measurement station in between them. The state preparation is device-dependent, but the measurement process in the middle remains, indeed, device-independent. Measurement-DIQKD has been experimentally demonstrated lately at high rates with continuous variable systems [POS+15]. Generally speaking, relaxing DI quantum information protocols consists of assuming that some of the parties trust their measurement apparatuses while the devices of the other parties remain uncharacterised. This relaxation, which is often experimentally justified, is often based on the observation of Einstein-Podolsky-Rosen (EPR) steering correlations [WJD07, SNC14], and in particular has been proven effective for one-sided DIQKD [BCW+12] and for one-sided DIRNG [PCSA15, MSA+17].

This Thesis contributes to the experimental development of quantum information protocols with uncharacterized devices, namely, "black boxes". It aims at reducing the breach between quantum information theory and implementation. This is achieved throughout the different Chapters of this Thesis by pursuing the following three overlapping duties: *(i)* To Broaden theoretic capabilities by establishing a richer understanding of relevant fundamental resources lying at the basis of the theory of DI and semi-DI quantum information. *(ii)* To develop competitive quantum information protocols by finding an adequate trade-off between high-performance and practicability; between the power of the DI framework and its less demanding semi-DI relaxations. *(iii)* To analyse and improve experimental conditions of diverse physical setups in order to carry out state-of-the-art implementations of quantum information protocols with black boxes.

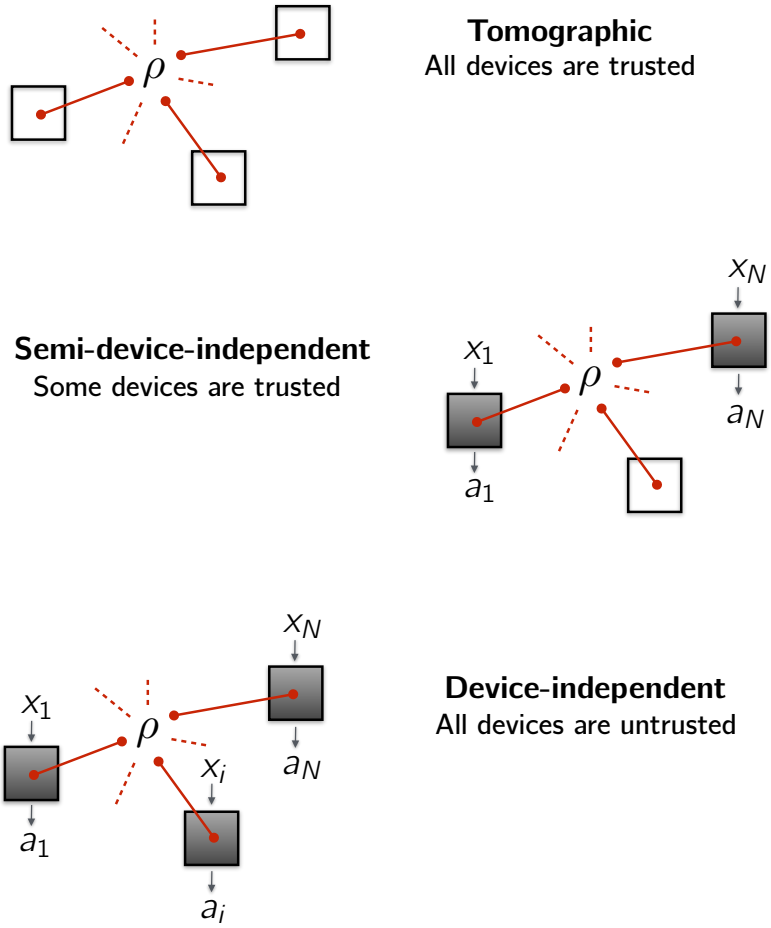

Figure 1.1.: **Operational approaches to quantum information processing.** An unknown quantum state ρ is distributed among N parties holding each a measurement device. *Top:* In the standard approach, all devices behave as white boxes, in the sense that their internal working is fully trusted. The parties can therefore apply tomography techniques to reconstruct the state ρ. Quantum information processing under this approach relies on the certification of entanglement among the different devices. *Middle:* The semi-DI approach is hybrid as certain devices are uncharacterized and may be treated as black boxes, producing an outcome labeled a_i for some possible input choice labeled x_i for the i-th party. Quantum information processing in this approach relies on the observation of steering correlations in the network. *Bottom:* The full DI approach treates all devices as black boxes. This minimalist framework provides the strongest form of security in these scenarios since both the state and measurement devices can, to some extent, be provided by a malicious agent. The DI approach is based on the observation of nonlocal correlations.

1.2. Motivation and main contributions

This Thesis focuses on turning the theory of quantum information into a graspable technology for our society through the development and implementation of prominent protocols based on the minimalist, user-friendly, black-box paradigm. From the fundamental standpoint, it contributes to the characterization and quantification of *entanglement* [Sch35, HHHH09] —the pivotal quantum resource at the basis of most testable phenomena without classical account— in scenarios of practical interest where uncharacterised devices are used. From the more applied perspective, it contributes to the development of two specific information tasks: the certification of genuinely random numbers in DI and semi-DI scenarios, and the generation of a shared secret key among two parties in a full DI manner.

1.2.1. Entanglement with uncharacterised devices

Entanglement is the key resource at the heart of quantum mechanics to assess information processing with black boxes. From the practical side, it is highly desirable to count with experimental techniques to detect the presence of entanglement in networks buit from uncharacterized devices. From the more fundamental side, it is crucial to enlighten the subtle relation that exists between entanglement, nonlocality, and steering, which are known to be inequivalent types of correlations.

Experimental detection of multipartite entanglement over steering networks. We develop and implement semi-definite programming (SDP) techniques to experimentally certify the presence of all kinds of entanglement on a three-qubit photonic W state in the steering scenario. The W state displays both genuine multipartite entanglement (GME) and entanglement in all of its reduced states, being therefore a flexible resource for quantum networks. We show that all types of entanglement of the W state can in fact be certified in all tripartite steering scenarios in a scheme where each party applies the same set of measurements. In this way, each party can certify all types of entanglement without the need to rely on any characterisation of the measurement devices used by the others. Our techniques can be readily adapted to other states in larger networks.

Quantifying nonlocality without anomalies. We introduce a natural measure of nonlocality based on the probability for a quantum state to produce nonlocal correlations from uniformly random sampled measurements. Our measure is operational and has the crucial advantage of encompassing all Bell inequalities for a given scenario at the same time. With this measure, we show that no *anomalies*

of nonlocality —-cases in which maximal entanglement does not yield maximal nonlocality— occur for two-qubit states for a large class of situations.

1.2.2. Genuine random number generation

Entangled quantum systems have the potential to provide *genuine* randomness, that is, randomness which cannot be attributed to incomplete knowledge of any classical variable of the system. At the basis of such genuine, device-independent, randomness lies a quantitative relation between the amount of nonclassicality — nonlocality or steering— observed, and the degree of predictability of the results produced by the uncharacterised devices. What is the maximal amount of randomness that a given quantum state allows for? What is the maximal amount of randomness that a given physical setup allows for? What are the experimental challenges encountered in the certification of genuine randomness? We assess these questions, both within theory and experiment, by focusing our attention on optical polarization-based schemes.

Optimal randomness generation in Bell experiments. We construct a general framework and methods for optimal randomness certification in Bell experiments. The idea is to keep as much information as possible by avoiding any post-processing of outcomes, then to estimate randomness by constructing a device-independent guessing probability optimized over all possible Bell inequalities, and finally to optimize the latter quantity over all the tunable physical parameters of the experiment. We then focus on entirely optical polarization-based implementations, for which we certify four times more randomness than what a standard analysis, based on a binning of the outcomes and on the use of a single Bell inequality, can achieve.

Experimental one-sided device-independent randomness certification. We implement for the first time methods for one-sided device independent randomness certification on a three-qubit W state. The W state is created at each round of the experiment from pairs of entangled photons, using both their polarization and spatial degrees of freedom in order to produce three qubits. First, we show that any reduction of the W state is steerable but does not allow for one-sided randomness certification: this constitutes the discovery of a form of steerable correlations for which an eavesdropper can predict the result of any of the measurements performed on the untrusted side. We verify that the experimental data of each of the the reduced states does not reveal any amount of one-sided randomness, as predicted by the theory. Second, we analyze the amount of randomness retrieved when untrusted measurements are performed on both the polarization

and path degrees of freedom of one of the two photons produced. In fact, a physical bipartition of the state naturally stems between the two photons produced in the experimental implementation of the photonic W state. We manage to certify 0.26 ± 0.04 bits from the bipartitions of the W state. This value falls far from the theoretical value of $-\log_2(2/3) \approx 1.58$ bits. This discrepancy is due to the fact that the amount of randomness is extremely sensitive to the visibility of the pure W state with respect to white noise. For instance, we observe that for visibility of 99.4% the number of one-sided random bits that can be certified is already less than unity.

Certifying more than one random bit from one entangled bit is possible. Motivated by the extreme sensitivity of randomness towards visibility encountered with the W state, we consider a refined scheme based on Sagnac interferometry to certify more than one bit of randomness from one of the parts of an entangled bit, that is, a maximally entangled state of two qubits. From the fundamental perspective, this probes the ultimate limits for randomness certification using quantum resources. From the practical perspective our scheme offers an advantage over standard Bell experiments based on projective measurements of up to 30% in the number of bits certified. Upon optimization of the physical parameters and of all possible Bell inequalities, our optical experiment based on polarization-entangled photons certifies 1.17 ± 0.08 full DI random bits. We further increase this number by assuming that the other qubit is trusted; in this case, we certify 1.27 ± 0.15 semi-DI random bits.

1.2.3. Device-independent quantum key distribution

Implementing DIQKD is similar than certifying genuine random numbers in the sense that the parties willing to exchange the secret key need to produce statistical data exhibiting violation of a Bell inequality free from the detection loophole. This demands high efficiencies for the collection of the experimental data, but in the DIQKD case this is far more difficult to achieve as the parties are far from each other and loss increases exponentially with distance over channels. Is it possible to circumvent this problem and close the detection loophole at long distances? If so, which are the remaining experimental challenges for DIQKD? Which experimental setups could make DIQKD a technological reality?

Theoretic solutions for experimental DIQKD. We provide solutions based on heralded-state-preparation to overcome the crucial problem of channel loss in the frame of DIQKD physical implementations. By means of SDP techniques, we

also develop an efficient method which allows one to assume that spurious contributions not accounted for in the modelling of an experiment are fully controlled by the eavesdropper to her benefit. Last but not least, we introduce a method based on data post-processing to deal with the negative impact of loss on the information reconciliation part of QKD protocols, a crucial issue unaddressed until now. The post-processing method in fact provides much greater robustness against noise and loss, and significantly higher key-generation rates.

Implementation proposals. We propose the first implementation for DIQKD based on light-matter interaction. The scheme relies on a heralded mapping of polarization entanglement of light onto matter spins which can be subsequently read-out with near-to-unit efficiency. We also introduce and analyze improved versions of existing optical DIQKD schemes based on spontaneous parametric down-conversion (SPDC) sources, and present a DIQKD implementation which does not rely on SPDC processes, but instead, is based on single-photon sources —a new-generation resource for scalable photonic quantum technologies whose development has grown extensively in the recent times. Our DIQKD scheme based on single-photon sources largely outperforms previous proposals when physical imperfections are taken into account.

2. Preliminaries

In this Chapter we introduce the concepts and tools necessary for the development of quantum information protocols with black boxes. We narrow our focus to the bipartite case, the situation mostly —though not exclusively— encountered along this Thesis (in Chap. 3 the tripartite case is also broadly considered). We begin by formally defining the concepts of *entanglement, steering* and *nonlocality* in Sec. 2.1. These three resources enable quantum information tasks when all devices are trusted, when some devices are trusted, and when no device is trusted, respectively, as explained already in Fig. 1.1. Then, in Sec. 2.2 we characterize the sets of *assemblages* and *correlations* attainable by quantum theory. Such characterization is indispensable for implementing semi-DI and DI quantum information programs, whose general architecture is also described. In Sec. 2.3 we introduce the problem of quantifying nonlocality and steering, which typically is assessed by constructing witnesses known as *Bell inequalities* and *steering inequalities*. We then make use of these tools in Sec. 2.4 to recall methods to certify *genuine randomness* from quantum systems. This intrinsic randomness cannot be attributed to a lack of knowledge of the underlying system, and thus it is certified in a DI or semi-DI manner. Finally, in Sec. 2.5 we review how such genuine randomness can further be used to establish a secret key among two honest users in a full DI way, in a task known as *device-independent quantum key distribution* (DIQKD).

2.1. The impossibility for local descriptions

Quantum entanglement. In 1935, Einstein, Podolsky and Rosen [EPR35] and Schrödinger [Sch35] discovered a "spooky" feature of the quantum mechanical description of Nature with no classical counterpart, and which, since then, has lied at the center of interest of modern physics. This feature, called *entanglement*, is the impossibility for the state of a composite system to be written as a convex sum of products of local states of the individual subparts. To be precise, the quantum state ρ describing a bipartite system AB is *separable* if it can be written as a convex combination of product states [HHHH09]:

$$\rho^{\mathrm{SEP}} = \sum_{\lambda} p_{\lambda} \rho_{\lambda}^{\mathrm{A}} \otimes \rho_{\lambda}^{\mathrm{A}}. \tag{2.1}$$

On the contrary, if the quantum state ρ does not admit a decomposition in terms of local states of A and B, it is said to be *entangled*. Deciding if a state ρ is entangled or not amounts to check its membership to the set $\mathcal{S}$ of all separable states (see top of Fig. 2.1), *i.e.* those admitting a decomposition of the form (2.1). Up to date, this so-called separability problem remains a cumbersome task, beyond the scope of this Thesis and which can only be efficiently pursued for qubit-qubit and qubit-qutrit systems [HHHH09]. Still, the certification of entanglement of any state is possible to achieve by performing specific measurements on the quantum state one is willing to test. These specific measurements stem from a necessary and sufficient entanglement criterion formulated in terms of directly measurable observables W known as *entanglement witnesses* [GT09]. In fact, these witnesses are observables such that their expectation value $\mathrm{Tr}[W\rho]$ is strictly negative only if the state ρ is entangled.

In practice, however, the construction of such entanglement witnesses relies on a prior knowledge of ρ, and furthermore assumes trustworthiness on the measurement apparatuses to perform the desired measurements and estimate the expectation value of W. Such assumptions are often not justifiable, especially since slight mismatches between either the state or the measurements and their actual physical implementation may lead to false-positive conclusions about the presence of entanglement in the state [RFSB$^+$12].

Quantum steering. In contrast, if the bipartite scenario is semi-DI (see the middle of Fig. 2.1) no assumption about the shape of the states and measurements implemented is made for one of the parties. Concretely, the scenario is composed by Alice and Bob sharing an unknown quantum state ρ, with Bob trusting his measurement apparatus, but Alice is not. Alice performs m_A measurements on her subsystem labeled by $x = 0, ..., m_A - 1$, each having o_A outcomes $a = 0, ..., o_A - 1$. No characterisation of Alice's measurements is assumed, while Bob has full control of his measurements and can thus access the assemblage of unnormalized states given by:

$$\sigma_{a|x} = \mathrm{Tr}_{\mathsf{A}}\left[M_{a|x} \otimes \mathbb{1}^{\mathsf{B}}\ \rho\right]. \tag{2.2}$$

The measurements of Alice are defined by *positive-operator valued measures* (POVMs), satisfying $\sum_a M_{a|x} = \mathbb{1}^{\mathsf{A}}$ and $M_{a|x} \geq 0\ \forall a, x$. The collection of all quantum assemblages —those arising from any quantum state ρ and any set of POVM measurements $\{M_{a|x}\}_{a|x}$— forms the set $\mathcal{Q}_\sigma$ shown in Fig. 2.1 and defined as:

$$\begin{aligned}\mathcal{Q}_\sigma = \Big\{\ \sigma^{\mathsf{B}}_{a|x} \mid \sigma^{\mathsf{B}}_{a|x} &= \mathrm{Tr}_{\mathsf{A}}\left[M_{a|x} \otimes \mathbb{1}^{\mathsf{B}}\ \rho\right], \\ &\rho \geq 0,\ \ M_{a|x} \geq 0,\ \ \textstyle\sum_a M_{a|x} = \mathbb{1}^{\mathsf{A}}\Big\}.\end{aligned} \tag{2.3}$$

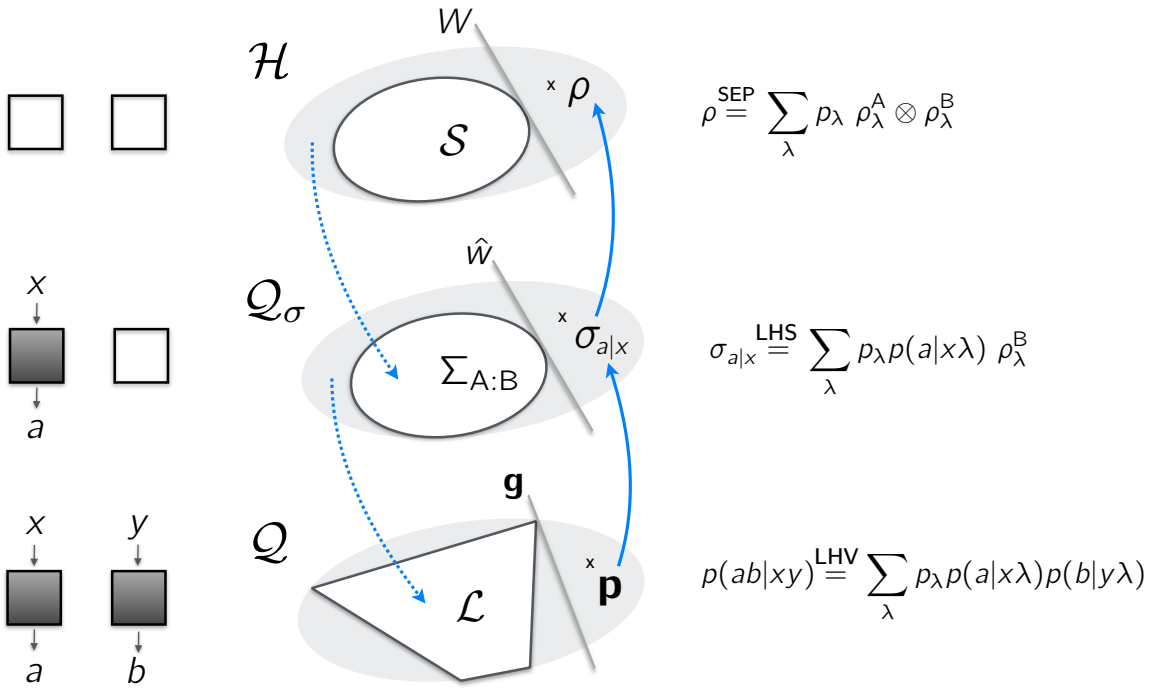

Figure 2.1.: **Quantum resources.** *Top:* Membership of a quantum state ρ to the space of separable states $\mathcal{S}$ is in practice observed with an entanglement witness: a hyperplane W on the space of all states, $\mathcal{H}$. *Middle:* The semi-DI approach is based on the observation of assemblages which do not admit an LHS model, that is, not belonging to the convex set $\Sigma_{\text{A:B}}$. The steerability of an assemblage $\sigma_{a|x}$ is witnessed through the violation of a steering inequality: a linear functional $\hat{w}$ in the space of quantum assemblages $\mathcal{Q}_\sigma$. *Bottom:* In the DI case, Alice and Bob rely on the observation of a nonlocal behavior $\mathbf{p}$ lying outside from the polytope $\mathcal{L}$. This is witnessed in practice through the violation of a Bell inequality $\mathbf{g}$ acting on the space $\mathcal{Q}$ of all quantum behaviors. *Blue arrows* illustrate that entanglement is necessary to demonstrate steering, which in turn is necessary to demonstrate nonlocality. *Dashed blue arrows* illustrate that entanglement, steering and nonolocality are inequivalent resources: there exist entangled states which are unsteerable, and assemblages demonstrating steering but leading always to behaviors that admit an LHV model.

Steering is formally defined as the possibility of remotely generating ensembles that could not be produced by a *local hidden state* (LHS) model [WJD07]. An LHS model is a set of messages λ distributed according to some probability p_λ, instructing Alice's device to output a with probability $p(a|x\lambda)$ whenever she decided to apply measurement x, and providing Bob with the state ρ_λ. Bob does not have access to the classical variable λ, so the final assemblage he observes is composed by the elements:

$$\sigma_{a|x}^{\mathrm{LHS}} = \sum_\lambda p_\lambda p(a|x\lambda)\ \rho_\lambda^{\mathrm{B}}, \quad \forall\ a, x. \tag{2.4}$$

An assemblage is said to demonstrate steering if it does not admit an LHS model (2.4). Furthermore, a quantum state ρ is said to be *steerable* if there exists measurements $\{M_{a|x}\}_{a,x}$ which produce an assemblage that demonstrates steering. Note that assuming that ρ is separable implies the existence of an LHS model for $\sigma_{a|x}$. This shows that entanglement is a necessary condition to demonstrate steering. Interestingly, the converse statement does not hold, as shown in Fig. 2.1: there exist entangled states which cannot lead to steering, even when considering general (POVM) measurements [QVC+15]. The collection of all (unnormalized) assemblages admitting an LHS model for Bob forms the convex set:

$$\Sigma_{\mathrm{A:B}} = \left\{ \sigma_{a|x}^{\mathrm{B}} \mid \sigma_{a|x}^{\mathrm{B}} = \sum_\mu D_\mu(a|x)\sigma_\mu^{\mathrm{B}},\ \sigma_\mu^{\mathrm{B}} \geq 0 \right\} \tag{2.5}$$

where we have used the fact that any probability distribution $p(a|x\lambda)$ can always be written as a convex combination of deterministic strategies $D_\mu(a|x)$. Deciding whether an assemblage $\sigma_{a|x}$ demonstrates steering amounts to checking its membership to $\Sigma_{\mathrm{A:B}}$, which can be turned into an efficient SDP problem whose feasability we shall discuss in the next Sections [CS17].

Quantum nonlocality. In the DI case Bob is also "*untrusted*", in the sense that his measurement device remains uncharacterized. He performs m_B unknown measurements $\{M_{b|y}\}_{b,y}$ on his system, labeled by $y = 0, \ldots, m_B - 1$ and each having o_B outcomes $b = 0, \ldots, o_B - 1$. Since in this case everything (the state and all the measurements) is uncharacterised, all possible information is contained in the joint conditional probabilities given by Born's rule,

$$p(ab|xy) = \mathrm{Tr}\left[M_{a|x} \otimes M_{b|y}\ \rho\right]. \tag{2.6}$$

The $o_A o_B m_A m_B$ such probabilities are the components of a real vector $\mathbf{p} = \{p(ab|xy)\}$. $\mathbf{p}$ is the *behavior*, or the *correlations*, associated with the *quantum realization* defined by the state ρ and the measurements with elements $\{M_{a|x}\}$

and $\{M_{b|y}\}$. The ensemble of all possible quantum behaviors —those arising from any possible quantum realization— forms the convex *quantum* set $\mathcal{Q}$:

$$\mathcal{Q} = \Big\{ \mathbf{p} \mid p(ab|xy) = \mathrm{Tr}\left[M_{a|x} \otimes M_{b|y}\ \rho\right], \\ \rho \geq 0,\ M_{a|x} \geq 0,\ M_{b|y} \geq 0,\ \textstyle\sum_a M_{a|x} = \mathbb{1}^{\mathrm{A}},\ \sum_b M_{b|y} = \mathbb{1}^{\mathrm{B}} \Big\} \tag{2.7}$$

whose characterization is of paramount importance for DI quantum information protocols and will be discussed in detail in the next Section.

In an analogous way to steering, nonlocality is defined as the possibility to remotely generate behaviors that could not be prepared by a *local hidden variable* (LHV) model [Bel64, BCP+14]. An LHV model is again a set of classical instructions λ distributed according to some probability p_λ and providing local response functions $p(a|x\lambda)$ and $p(b|y\lambda)$ independent of the measurements made and of the outcomes observed by the opposite party. In this case, the components of $\mathbf{p}$ take the form:

$$p(ab|xy) = \sum_\lambda p_\lambda p(a|x\lambda)p(b|y\lambda), \quad \forall\ a, b, x, y. \tag{2.8}$$

A behavior is said to be *nonlocal* whenever it does not admit an LHV model (2.8). One can furthermore check that an assemblage $\sigma_{a|x}$ which is LHS immediately yields a behavior $\mathbf{p}$ which is LHV, or simpler said, local. In other terms, an LHS model is a special instance of an LHV model for which the response function on the trusted side is dictated by quantum theory. On the contrary, there exist assemblages demonstrating steering but always leading to local behaviors, even for the most general quantum measurements [QVC+15], as illustrated in Fig. 2.1. It can be shown that the collection of all local behaviors (2.8) forms a convex set [Fin82]:

$$\mathcal{L} = \left\{ \mathbf{p} \mid p(ab|xy) = \sum_{\mu,\nu} p_{\mu\nu} D_\mu(a|x) D_\nu(b|y),\ p_{\mu\nu} \geq 0,\ \sum p_{\mu\nu} = 1 \right\} \tag{2.9}$$

which is a polytope whose extremal vertices are the bipartite deterministic strategies $\{D_\mu(a|x)D_\nu(b|y)\}_{\mu\nu}$. Note that the two last conditions in (2.9) simply demand that $p_{\mu\nu}$ is a valid probability distribution. Hence, the local polytope $\mathcal{L}$ consists of all possible convex combinations of deterministic strategies.

One of the most prominent scientific achievements of the 20$^{\text{th}}$ is the discovery of quantum nonlocality by J. Bell [Bel64]. Bell's theorem proves the existence of quantum realizations yielding behaviors $\mathbf{p} \in \mathcal{Q}$ which are nonlocal $\mathbf{p} \notin \mathcal{L}$. This implies that the inclusion of sets $\mathcal{Q} \subset \mathcal{L}$ is strict, as the bottom of Fig. 2.1 shows. In fact, it turns out that all pure entangled states display nonlocality when applying appropriate measurements onto them [Gis91], which confirms the intimate relation existing among these two fundamental resources.

2.2. Characterization of quantum resources

Understanding which assemblages σ and which behaviors $\mathbf{p}$ can be recovered by quantum theory is a fundamental question of paramount importance for the development of semi-DI and DI quantum information protocols. The idea behind these protocols is to bound the actions of a third party Eve—the adversary who prepared the devices— by constraining her attacks on the devices. These atacks are remote preparations of quantum assemblages σ^e and behaviors $\mathbf{p}^e$.

Box 1. Architecture of programs based on nonclassical resources.

1. Program for semi-DI quantum information:

$$\begin{aligned} \max \quad & f\left(\{\sigma^e\}_e\right) \\ \text{s.t.} \quad & cons\left(\sigma, \{\sigma^e\}_e\right) \text{ and } \sigma^e \in \mathcal{Q}_\sigma \ \forall e \end{aligned}$$

2. Program for DI quantum information:

$$\begin{aligned} \max \quad & f\left(\{\mathbf{p}^e\}_e\right) \\ \text{s.t.} \quad & cons\left(\mathbf{p}, \{\mathbf{p}^e\}_e\right) \text{ and } \mathbf{p}^e \in \mathcal{Q} \ \forall e \end{aligned}$$

A sketch of typical optimization problems relevant for semi-DI and DI quantum information are presented in Box 1. f represents the objective function, the quantity to optimize. It is a function of the variables of the program labeled by e. For instance, when considering the task of certifying genuine random numbers, f is the probability for Eve to guess the outcomes of the black boxes. In the semi-DI case, the constraints *cons* relate the observed assemblage σ with the finite collection of quantum strategies $\{\sigma^e\}_e$ achievable by Eve. These strategies are the optimization variables of the program: the program looks for a worst-case for f given the observation of σ. In the DI case, the observed data is the behavior $\mathbf{p}$ and the strategies of Eve are quantum behaviors $\{\mathbf{p}^e\}_e$.

Imposing membership conditions $\sigma^e \in \mathcal{Q}_\sigma$ and $\mathbf{p}^e \in \mathcal{Q}$ for Eve's strategies requires to characterize in an efficient way those assemblages and behaviors that Eve can reach within quantum theory, or at least, that she can reach without supraluminal power if nonsignaling constraints are set [BCP+14]. When the objective function and the constraints are linear functions of the variables (for instance, when characterizing the LHV set, see Fig. 2.1) the programs presented in Box 1 become linear. When the programs involve matrix inequalities they become SDP.

Characterization of quantum assemblages. It turns out that in the bipartite case, every nonsignaling assemblage admits a quantum realization [SBC+15]. More precisely, given an assemblage of positive matrices satisfying the *nonsignaling condition* $\sum_a \sigma_{a|x} = \sum_a \sigma_{a|x'} = \rho^B$, it is always possible to find an explicit construction of a quantum state ρ and measurements $\{M_{a|x}\}$ satisfying (2.2). The multipartite case is much more subtle since there exist nonsignaling assemblages which do not admit a quantum realization. This phenomena known as *post-quantum steering* [SBC+15] falls beyond the scope of this Thesis, which mostly focuses on one-sided DI protocols. Note however that it is possible to apply hierarchical methods similar to the ones described next for nonlocality to efficiently approximate $\mathcal{Q}_\sigma$, at least for the tripartite case [CSA+15, SBC+15, MSA+17].

Characterization of quantum behaviors. Given a behavior $\mathbf{p}$, does there exist a quantum state ρ and local measurements $\{M_{a|x}\}$ and $\{M_{b|y}\}$ such that $p(ab|xy) = \mathrm{Tr}\left[M_{a|x} \otimes M_{b|y}\ \rho\right]$ (2.6)? The question is troublesome since the set $\mathcal{Q}$ (2.7) is hard to characterize. Still, it is possible to define a convergent hierarchy of convex sets characterized by valid SDP constraints and being such that $\mathcal{Q}^1 \supseteq \mathcal{Q}^2 \supseteq ... \supseteq \mathcal{Q}$ [NPA07]. This so-called Navascues-Pironio-Acin (NPA) hierarchy is infinite but converges to the quantum set $\mathcal{Q}$ from the outside, allowing to relax the difficulty of the problem (to the order k) by replacing $\mathcal{Q}$ by $\mathcal{Q}^k$. Such approximation from the outside for $\mathcal{Q}$ is highly relevant in DI applications, where the observed behavior $\mathbf{p}$ is assumed to be prepared by a malicious agent, Eve. Indeed, in this case it is safe to relax $\mathcal{Q}$ to $\mathcal{Q}^k$ since this amounts to give more power to Eve to tailor a *supra-quantum* behavior $\mathbf{p} \in \mathcal{Q}^k$ for her own benefit. Since the convergence of $\mathcal{Q}^k$ is heuristically fast, this approximation is not overpessimistic. Hence, unless otherwise specified and for computational purposes, in this Thesis we assume from now on that $\mathcal{Q}$ is always relaxed to $\mathcal{Q}^k$.

2.3. Quantifying steering and nonlocality

Membership problems. Deciding if a quantum assemblage demonstrates steering amounts to testing its membership to the set $\Sigma_{A:B}$ of assemblages having an LHS model. The set $\Sigma_{A:B}$ in (2.3) is characterized by linear and positive-semi-definite constraints, which allows one to write the membership problem into an efficient SDP that tests if a given assemblage $\sigma_{a|x}$ belongs to $\Sigma_{A:B}$:

$$\begin{aligned} &\text{find} \quad \{\sigma_\lambda\}_\lambda \\ &\text{s.t.} \quad \sum_\lambda D_\lambda(a|x)\sigma_\lambda = \sigma_{a|x} \quad \forall a, x \\ &\qquad \text{and} \quad \sigma_\lambda \geq 0 \quad \forall \lambda \end{aligned} \tag{2.10}$$

Equivalently, deciding if a quantum behavior $\mathbf{p}$ is nonlocal requires to test its membership to the LHV set $\mathcal{L}$, which is a polytope characterized by a finite number of linear constraints (2.9). In this case, the membership problem is translated to a linear program where $\lambda = (\mu, \nu)$ parametrizes the determinstic strategies $D_\lambda(ab|xy) = D_\mu(a|x)D_\nu(b|y)$ of the two parties:

$$\begin{aligned} &\text{find} \quad \{p_\lambda\}_\lambda \\ &\text{s.t.} \quad \begin{array}{l} \sum_\lambda p_\lambda D_\lambda(ab|xy) = p(ab|xy) \quad \forall a, b, x, y, \\ \sum_\lambda p_\lambda = 0 \quad \text{and} \quad p_\lambda \geq 0 \quad \forall \lambda \end{array} \end{aligned} \tag{2.11}$$

Strict feasability. Unfortunately, the membership programs (2.10) and (2.11) are not *strictly feasible*, in the sense that whenever $\sigma_{a|x} \notin \Sigma_{\text{A:B}}$ and $\mathbf{p} \notin \mathcal{L}$ the programs won't be able to find an LHS or LHV decomposition, respectively. It is highly advantageous —both from the computational and practical perspectives— to turn such programs into strictly feasible SDP versions. In analogy with entanglement detection techniques [HHHH09], this is typically achieved by ensuring that the decomposition of $\sigma_{a|x}$ and $\mathbf{p}$ exisits in terms of additional sets characterized by SDP constraints. For example, the steering weight [SNC14] and the EPR2 decomposition of nonlocality [EPR92] are quantifiers motivated by the best separable approximation of entanglement [LS98]. They look for the minimum weight v such that $\sigma_{a|x}$ and $\mathbf{p}$ can be decomposed in terms of generic nonsignaling (NS) resources and generic classical resources, namely:

$$\begin{aligned} v^* &= \min v \quad \text{s.t} \quad \sigma_{a|x} = v\sigma^{\text{NS}}_{a|x} + (1-v)\sigma^{\text{LHS}}_{a|x} \\ v^* &= \min v \quad \text{s.t} \quad \mathbf{p} = v\mathbf{p}^{\text{NS}} + (1-v)\mathbf{p}^{\text{LHV}} \end{aligned} \tag{2.12}$$

In particular whenever $v^* = 0$ the resource admits a classical model, while a strictly positive value $v^* > 0$ guarantees that $\sigma_{a|x} \notin \Sigma_{\text{A:B}}$ and $\mathbf{p} \notin \mathcal{L}$ respectively. A similar approach is to ask how much noise r one has to add to a given assemblage or behavior in order for it to have an LHS or LHV model. The noise can take different forms; for instance, it can be set to be a fixed point like the maximally mixed, so-called, *white noise*. In this case the SDP yields the *robustness*:

$$\begin{aligned} r^* &= \min r \quad \text{s.t} \quad (1-r)\sigma_{a|x} + r\mathsf{I}_{a|x} \in \Sigma_{\text{A:B}} \\ r^* &= \min r \quad \text{s.t} \quad (1-r)\mathbf{p} + r\mathbb{1}_{\mathbf{p}} \in \mathcal{L} \end{aligned} \tag{2.13}$$

where $\mathsf{I}_{a|x}$ and $\mathbb{1}_{\mathbf{p}}$ denote the maximally mixed assemblage and the maximally mixed behavior, the centers of the LHS and LHV sets. In particular, such white noise robustness r^* will be used as a steering quantifier for multipartite entanglement detection in Chap. 3.

Duality and optimal inequalities. Strict feasability is a crucial step because it enables the derivation of linear witnessses —inequalities— to quantify steering and nonlocality in a practical manner. In the semi-DI case, the *dual formulation* [BV04] of strictly feasible SDPs (2.12) and (2.13) provides operators $\{F_{a|x}\}_{ax}$, which are the optimal variables of the dual program, such that the linear functional:

$$\hat{w}: \ \sigma_{a|x} \ \mapsto \ \sum_{ax} \mathrm{Tr}\left[F_{a|x}\ \sigma_{a|x}\right] \tag{2.14}$$

yields the solution of the primal problem $\hat{w}\left(\sigma_{a|x}\right) = w^*$. In particular, the operators $\{F_{a|x}\}_{ax}$ are such that the *steering inequality* $\hat{w}\left(\sigma_{a|x}\right) > \beta$ is violated only if $\sigma_{a|x}$ demonstrates steering. β is a real number known as the classical bound of the inequality. (In the examples presented in (2.13) and (2.14), $\beta = 0$).

In the DI case, the dual variables are real numbers g_{abxy} acting linearly on $\mathbf{p}$:

$$\mathbf{g}\cdot\mathbf{p}: \ p(ab|xy) \ \mapsto \ \sum_{abxy} g_{abxy}p(ab|xy) \tag{2.15}$$

with $\mathbf{g}\cdot\mathbf{p} = g^*$ coinciding with the optimal solution of the primal problem. The quantity $\mathbf{g}\cdot\mathbf{p}$ is a real number; it is the *observed violation* of the Bell inequality [Bel64, BCP+14] $\mathbf{g}\cdot\mathbf{p} < g_{\mathrm{loc}}$. g_{loc} is the *local* bound of the inequality. In both the semi-DI and DI approaches, the witnesses $\hat{w}$ and $\mathbf{g}$ are optimal hyperplanes (see Fig. 2.1) which minimize the primal objective functions.

Box 2. Examples of inequalities with 2 measurements and 2 outcomes.

1. Steering inequality [CS17]:

$$\hat{w}\left(\sigma_{a|x}\right) = \sum_{ax} \mathrm{Tr}\left[(-1)^a\ \sigma_{a|x}B_x\right] \ < \ \sqrt{2} \tag{2.16}$$

2. Bell inequality (CHSH [CHSH69]):

$$\mathbf{g}\cdot\mathbf{p} = \sum_{abxy}(-1)^{a+b+xy}p(ab|xy) \ < \ 2 \tag{2.17}$$

In Box 2 we present inequalities being maximally violated by the two-qubit maximally entangled state $|\phi^+\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$. To obtain the maximal quantum violation, in the steering case Alice and Bob perform two Pauli measurements ($\hat{X}$ and $\hat{Z}$); in particular $B_0 = \hat{X}$ and $B_1 = \hat{Z}$. In the DI case (2.17), the maximal violation $2\sqrt{2}$ is obtained with $\hat{X}$ and $\hat{Z}$ for Alice and $1/\sqrt{2}(\hat{X} \pm \hat{Z})$ for Bob.

Measures of steering and nonlocality. Thus, the most practical way to quantify steering and nonlocality is through the amount of violation of steering and Bell inequalities: σ demonstrates more steering than σ' if $\hat{w}(\sigma) > \hat{w}(\sigma')$. Similarly, $\mathbf{p}$ is more nonlocal than $\mathbf{p}'$ if $\mathbf{g} \cdot \mathbf{p} > \mathbf{g} \cdot \mathbf{p}'$. As explained, such quantification of steering and nonlocality has practical advantages and, as we shall see later, it directly enables semi-DI and DI quantum information tasks. However, from a fundamental perspective this approach is problematic because in general there exist other inequalities $\hat{w}'$ and $\mathbf{g}'$ such that $\hat{w}'(\sigma') > \hat{w}'(\sigma)$ and $\mathbf{g}' \cdot \mathbf{p}' > \mathbf{g}' \cdot \mathbf{p}$. This fundamental problem can be circumvented by relating back the amount of violation of inequalities to operational measures of steering or nonlocality. In the examples analyzed in this Chapter, this is equivalent to return to the original, primal, problem. Indeed, notorious examples of operational measures based on inequality violations are the robustness to the addition of noise (2.13) [ADGL02, CS17] or losses [Ebe93], the nonclassical content (2.12) [SNC14, EPR92], the statistical strength of Bell tests [AGG05], the communication cost needed to reproduce the observed correlations [BT03, NV16] and the simulation of quantum correlations with nonclassical resources [BGS05]. As we shall see in Chap. 4, it may be valuable to consider measures of nonlocality and steering which are not linked to the violation of inequalities but instead operate directly at the level of the quantum state. As a final comment, note that Refs. [GWAN12, dV14, GA15], inspired by entanglement theory, introduced a more axiomatic approach to quantification by characterising the set of operations that cannot increase the amount of steering and nonlocality, respectively.

2.4. Genuine randomness from quantum systems

In this Section we review how to apply the machinery developed in the previous Sections of this Chapter to carry the quantum information task of certifying genuine random numbers in a DI and semi-DI manner. As explained in Chap. 1, device-independence is tremendously advantageous as it allows to ignore the internal working of the devices used and hence it provides immunity to hacking attacks exploiting experimental imperfections.

In classical mechanics, for every event there exist conditions that could cause no other event. For instance, knowing the location and momentum of all particles of a composite system is sufficient to determine its values at any given future time [Lap14]. In quantum mechanics, astonishingly, this so-called *scientific determinism* falls apart as the outcomes of quantum measurements can be intrinsically random. For example, detecting the path, 0 or 1, taken by single photons after a

50/50 beam-splitter results in a sequence:

$$01110101010100110101 \ldots \tag{2.18}$$

for which, the probability of observing each outcome is 50%. The sequence (2.18) is indeed random as the next value cannot be predetermined in advance, provided that the laws of quantum physics yield a correct description of the situation. Such randomness is in fact at the basis of quantum random number generators that are sold commercially.

But how can one be sure that there is not some hidden mechanism that would let someone else to predict the sequence? This is a serious problem because at the quantum level it is very difficult to have control over the processes that are being implemented, which in turn makes difficult to provide a fair assessment of the unpredictability of the sequence. Moreover, there could be a backdoor in our quantum random number generator secretly inserted by a malicious manufacturer to retrieve all the outcomes of the observed sequence (2.18) in a deterministic way. In this case randomness would be only apparent, as it would be related to an incomplete knowledge of the system.

Remarkably, over the past decade results have shown that certain quantum systems hold the potential to provide a strong form of randomness which cannot be attributed to incomplete knowledge of any classical variable of the system. At the basis of such genuine randomness lies a quantitative relation between the amount by which a Bell inequality or a steering inequality is violated, and the degree of predictability of the results of the test [PAM$^+$10, PCSA15]. Intuitively, the violation of such inequalities certifies the presence of nonlocal and steering correlations respectively, and in turn, this guarantees that the outcomes of the measurements cannot be determined in advance [Eke91, Col07]. Furthermore, this genuine randomness is certified without any characterisation of the devices used, that is, in a DI fashion. Device independence is advantageous since it provides immunity to attacks that exploit imperfections, and to which device-dependent protocols are susceptible [GLLL$^+$11a]. For this reason, DI and semi-DI randomness generation have recently received much attention [NSPS14, BSS14, DdlTA14, dlTHD$^+$15, PCSA15].

Indeed, an intense research effort has been devoted to the experimental realisation of genuine randomness generation. A few years ago, Pironio *et al.* [PAM$^+$10] implemented the first proof-of-principle experiment. It involved two entangled atomic ion qubits confined in two independent vacuum chambers separated by approximately one meter. This implementation, which was based on light-matter interaction, managed to certify 42 random bits over a period of one month.

The principal challenge for a DI randomness generation experiment is that it must close the *detection loophole* [Pea70, San92], *i.e.* it must provide a Bell

inequality violation without post-selection on the data, since otherwise violation can be faked by classical resources [GLLL$^+$11b] and no genuine randomness can be guaranteed. The detection loophole was first successfully closed on several systems relying on light-matter interaction [RKM$^+$01, ABW$^+$09, HKO$^+$12]. More recently it was closed in optical setups with polarization-entangled photons [CMA$^+$13, GMR$^+$13]. As we shall see, these optical implementations represent an important achievement as they enable much higher rates of genuine random bits per time unit.

Box 3. Fundamental assumptions for quantum DI and semi-DI protocols

(i) All the untrusted devices can be shielded: the parties holding them control all information leaks.

(ii) The choice of measurements made on the untrusted devices is independent of any external variable.

(iii) The parties have trusted classical memories and share an authenticated, but otherwise public, classical channel.

(iv) Quantum physics is correct.

Scenario and assumptions. To carry out the tasks of DI and semi-DI randomness generation, we must bound the predictability that an eavesdropper Eve can have about the outcomes produced by the black boxes (recall Fig. 1.1), only from the observation of an assemblage σ or a behavior $\mathbf{p}$, and from a minimal set of fundamental assumptions made explicit in Box 3.

For simplicity and following the line of the previous Chapter, we consider the case of two parties, Alice and Bob, holding quantum devices. In the DI case the two devices are black boxes, while in the semi-DI (also known as one-sided DI) case, only the device of Alice is untrusted. The black boxes are assumed to be manufactured by Eve with any *a priori* unknown quantum state ρ, possibly correlated with Eve through some other quantum system ρ^{ABE}, such that $\rho = \mathrm{Tr}_{\mathrm{E}}\left[\rho^{\mathrm{ABE}}\right]$. The measurements implemented by the untrusted parties are also unknown, described by positive operators summing to identity.

We consider that Eve is only interested in guessing the outcome a of Alice's box when a fixed measurement $x = x^*$ is chosen by Alice. In this case the quantum information task is known as *local* randomness certification. The case where Eve wishes to guess the output of the two boxes for fixed measurements x^* and y^*,

known as *global* randomness certification, can be straightforwardly obtained as a generalization of the local case [NSPS14, PCSA15].

The set of fundamental assumptions required for DI and semi-DI randomness generation is listed in Box 3. Without assumption *(i)*, the value of the output a can leak-out of Alice's shield and Eve can trivially guess it with certainty. Similarly, without assumption *(ii)* Eve can know if the measurement x^* is going to be implemented and attack the device only when this is the case. This attack would in fact remain undetected; from a fundamental perspective, this assumption is intimately related to the *freedom of choice and superdeterminism loopholes* in the context of Bell experiments [Lar14]. Assumption *(iii)* simply guarantees that the two parties are indeed interchanging information with each other and are correctly keeping track of the outcomes observed at each round. Finally, note that assumption *(iv)* could actually be relaxed by considering, instead, an eavesdropper with supra-quantum power, that is, being only limited by the non-signaling principle [BHK05, PMLA13].

It is important to mention that the set of fundamental assumptions presented in Box 3 are also the ones which are required for device-independent quantum key distribution (DIQKD), which will be the task of interest in the next Chapter. Indeed, we will see that DI random number generation is a primitive for DIQKD. Finally, all along this Thesis we also consider for simplicity that all the statistics are obtained from an infinite number of *independent and identically distributed* (i.i.d.) rounds. Note that this assumption is not fundamental: it can actually be alleviated by means of statistical analysis and hypothesis testing [Lar14].

Furthermore, additionally to the assumptions presented in Box 3, when we will report experimental results in the Sections which follow, we shall assume that fair-sampling is valid and that the experimental setup is not vulnerable to the detection loophole. This assumption is reasonable given that this loophole has already been closed in several Bell experiments. Moreover, it is not our intention to generate from our research genuine randomness for direct commercial applications; instead, we are interested in exploring and reveal the remarkable features and capabilities that genuine quantum randomness can potentially offer.

Quantifying Eve's guessing probability. The predictability of the outcome a when a given measurement x^* is chosen by Alice is quantified by the *guessing probability* $G(x^*)$ [Col07, NSPS14, PCSA15]: the probability that Eve guesses correctly the value of a, optimized over all of Eve's possible quantum strategies, and conditioned on the observation of an assemblage σ or a behavior $\mathbf{p}$ by Alice and Bob. In fact, the optimal number of random bits that can be certified per round from x^* can measured by the *min-entropy* of the guessing probability [NSPS14],

$-\log_2 G(x*)$. Note that whenever $G(x^*) = 1$, Eve has full knowledge about the next possible value of a and no randomness can be certified. On the contrary, as long as $G(x^*) < 1$ Eve cannot predict Alice's outcome with certainty, and a positive amount of random bits per round can be certified. In particular, when Eve has no knowledge at all about the string of outcomes of x^*, her best strategy is to give a random guess, which succeeds with probability $G(x^*) = \frac{1}{o_A}$ (recall that o_A is the number of outcomes of Alice's measurements). In this case, the maximal amount of randomness, $\log_2 o_A$ bits per round, is certified.

At each round of the experiment, Eve applies a measurement M_e with o_A outcomes on her share of the system, with the aim that her outcome e equals that of Alice's a, whenever Alice measures x^*, with the highest probability. In other words, Eve wants to maximize the objective function:

$$\sum_e p(e, a = e|x^*) = \sum_e \mathrm{Tr}\left[\left(M_{a=e|x^*} \otimes \mathbb{1} \otimes M_e\right) \rho^{\mathrm{ABE}}\right]. \tag{2.19}$$

In the one-sided-DI case, the states left for Bob after Alice and Eve's measurements are given by $\sigma^e_{a|x} = \mathrm{Tr}_{\mathrm{AE}}\left[\left(M_{a|x} \otimes \mathbb{1} \otimes M_e\right) \rho^{\mathrm{ABE}}\right]$. Furthermore, using the fact that $\sum_e M_e = \mathbb{1}$, the assemblage observed by Bob is recovered from $\sigma_{a|x} = \sum_e \sigma^e_{a|x}$. Thus, the collection of unnormalized assemblages $\{\sigma^e_{a|x}\}_e$ may be seen as preparations made by Eve's measurement, such that whenever Eve obtains the result $e = a$, she guesses that the outcome of the black box was a. Formally, the one-sided DI guessing probability $G_\sigma(x^*)$ conditioned on the observation of $\sigma = \{\sigma_{a|x}\}_{ax}$ by Alice and Bob is given by the solution of the SDP [PCSA15]:

$$\begin{aligned} G_\sigma(x^*) \;=\; \max_{\{\sigma^e\}} \;& \sum_e \mathrm{Tr}\left[\sigma^e_{a=e|x^*}\right] \\ \text{s.t.} \;& \sum_e \sigma^e = \sigma \\ & \sum_a \sigma^e_{a|x} = \textstyle\sum_a \sigma^e_{a|x'} \quad \forall e, x, x' \\ & \sigma^e_{a|x} \geq 0 \quad \forall a, x, e \end{aligned} \tag{2.20}$$

As expected, the objective function in (2.20) coincides with (2.19). The first constraint guarantees that Eve reproduces on average the assemblage observed by Bob, while the two last constraints guarantee that each of the assemblages prepared by Eve admits a quantum realization, as explained in Sec. 2.2. Note that the program presented in (2.20) has the architecture for semi-DI quantum information processing which was presented in the top of Box 1.

In the full DI case, there is no knowledge about the shape of the states or the measurements impemented by the parties. Still, the probabilities $p(e, a = e|x^*)$

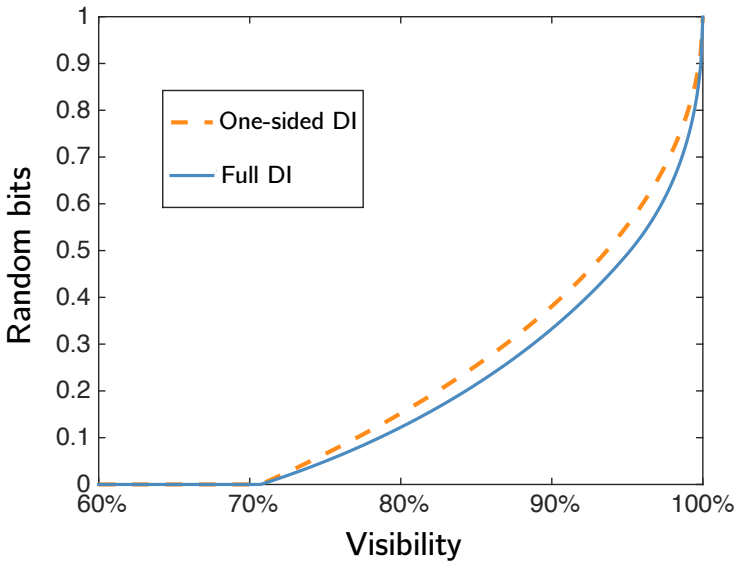

Figure 2.2.: **Genuine randomness versus visibility.** The semi-DI approach slightly outperforms the DI one, although no randomness can be certified below $v = \frac{1}{\sqrt{2}}$ for both approaches. But above $v = 1/\sqrt{2}$ the semi-DI approach provides higher performance as it is based on additional assumptions of trust. (See main text for details).

may be conceived as marginals of a collection of unnormalized behaviors $\{\mathbf{p}^e\}_e$ with elements $\mathbf{p}^e = \{p(eab|xy)\}_{abxy}$ prepared by Eve and reproducing on average the behavior observed by Alice and Bob, that is, $\sum_e \mathbf{p}^e = \mathbf{p}$. Thus, the DI guessing probability $G_{\mathbf{p}}(x^*)$ conditioned on the observation of $\mathbf{p}$ by Alice and Bob is given by the solution of the following SDP [NSPS14, BSS14]:

$$\begin{aligned} G_{\mathbf{p}}(x^*) \;=\; \max_{\{\mathbf{p}^e\}} \;\; & \sum_e p(e, a = e|x^*) \\ \text{s.t.} \;\; & \sum_e \mathbf{p}^e = \mathbf{p} \\ & \mathbf{p}^e \in \widetilde{\mathcal{Q}} \quad \forall e \end{aligned} \tag{2.21}$$

where $\widetilde{\mathcal{Q}}$ denotes the NPA relaxation (recall Sec. 2.2) of the set of unnormalized behaviors admitting a quantum realization. The program looks for the best possible quantum strategy for Eve to maximize the probability that her outcome is correlated to Alice's, and it has the same structure than the general program for DI quantum information presented in the bottom of Box 1.

In figure Fig. 2.2 we plotted the number of genuine random bits certified using programs (2.20) and (2.21). The assemblage σ was obtained from the two-qubit Werner state $v\,|\phi^+\rangle\langle\phi^+| + \frac{1-v}{4}\mathbb{1}$, were $\frac{1}{4}\mathbb{1}$ is the maximally mixed state, and $|\phi^+\rangle$ is the maximally entangled state encountered already in Chap. 4. The measurements made by Alice are the Pauli observables $\hat{X}$ and $\hat{Z}$. In the full DI case, the measurements made by Bob are $(\hat{X} \pm \hat{Z})/2$. Note that for perfect visibility $v = 1$, both approaches certify 1 genuine random bit. Below $v = 1/\sqrt{2}$, no randomness is certified in either case. Above $v = 1/\sqrt{2}$ the semi-DI approach provides higher performance as it is based on additional assumptions of trust.

Furthermore, from the dual formulation of programs (2.20) and (2.21), which are strictly feasible, it is possible to retrieve optimal steering and Bell inequalities, which are such that $\hat{w}\,(\sigma) = G_\sigma(x^*)$ and $\mathbf{g}\cdot\mathbf{p} = G_{\mathbf{p}}(x^*)$ respectively. Such linear witnesses are crucial for the quantification of randomness in practical situations, and we shall encounter them in the following Chapters.

2.5. Device-independent quantum key distribution

In this Section we recall how the task of distributing a secret key among two honest users, Alice and Bob, can be pursued in a DI manner. This so-called *device-independent quantum key distribution* (DIQKD) task is intimately related to the certification of genuine random numbers exposed in the previous Section. However, as we shall see later, DIQKD is more delicate to achieve in experimental situations, mostly due to the long distances separating the two parties [1].

DIQKD relies on a relaxation of the security assumptions that are usually made in QKD. While QKD relies on a near-to-perfect match between theory and implementation which is hard to meet in practice [SK14], DIQKD completely ignores the internal working of all devices used in the protocol, thus providing immunity against hacking attacks exploiting experimental imperfections. Inspired from previous results on self-testing [MY98] and non-signalling key distribution [BHK05], DIQKD [ABG+07, MPA11, PMLA13] introduces a minimalist paradigm to design protocols whose security is exclusively guaranteed from the observed statistics without any reference to the shape of the states and measurements used to obtain them.

Scenario. Concretely, the device-independent scenario [ABG+07] assumes the four fundamental assumptions for DI protocols, presented in Box 3, and encountered already in the previous Section: *(i)* Alice and Bob are located in se-

[1] Note that, although the randomness certification task requires two boxes, in practice it is considered as a single-user protocol.

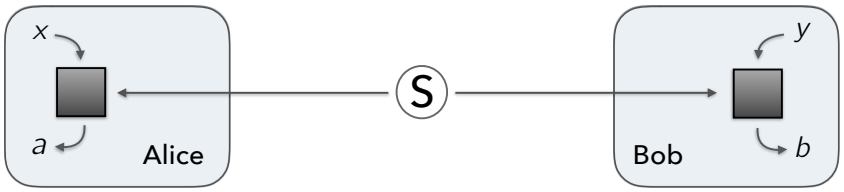

Figure 2.3.: **DIQKD scenario.** At each round, Alice and Bob receive from a source S the reduction of a quantum state ρ^{ABE} possibly prepared by an eavesdropper Eve, onto which they perform measurements labeled x and y producing outcomes a and b, respectively. The measurement devices are untrusted and to some extent could have been provided by Eve, which means that the measurement elements $M_{a|x}$ and $M_{b|y}$ remain uncharacterized. Hence, the only relevant object throughout the protocol is the observed behavior $P(a, b|x, y)$. Eve also performs a measurement (not shown) on her share of the state, designed to guess Alice's output a in the best possible way.

cure labooratories from which they can control information leaks (gray areas in Fig. 2.3), *(ii)* each of them has a trusted random number generator, *(iii)* they have trusted computing devices and an authenticated classical channel, and *(iv)* quantum physics is correct. Without assumptions *(i)* and *(iii)* cryptography - quantum or not- is inconceivable, while assumptions *(ii)* and *(iv)* arguably adhere to fundamental aspects of science. Note that no assumption is made about any implementation detail, such as the state produced or the internal working of the devices used by Alice and Bob during the entire protocol, for instance.

Protocol. For completeness, we recall the protocol for DIQKD from refs. [ABG+07, MPA11, PMLA13]. At each round, the parties perform measurements labeled $x \in \mathcal{X}$ and $y \in \mathcal{Y}$ on some unknown quantum state ρ^{AB}, and obtain outcomes $a \in \mathcal{O}_{\mathcal{A}}$ and $b \in \mathcal{O}_{\mathcal{B}}$, respectively, for some alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{O}_{\mathcal{A}}$ and $\mathcal{O}_{\mathcal{B}}$. No other assumption on ρ^{AB} is made, other than the fact that it is a quantum state. In fact, ρ^{AB} could be an operator of any dimension, and could even be correlated with another quantum system in the possession of a malicious eavesdropper E, such that $\rho^{\mathrm{AB}} = \mathrm{Tr}_{\mathrm{E}}\left[\rho^{\mathrm{ABE}}\right]$, as illustrated in Fig. 2.3.

The measurements made by Alice and Bob on ρ^{AB} remain also uncharacterized; the only restriction set is that they must obey Born's rule in order to reproduce the observed statistics, namely, the joint probability of outcomes a, b conditioned on the measurement choices x, y must read $P(a, b|x, y) = \mathrm{Tr}\left[\rho^{AB}\ M_{a|x} \otimes M_{b|y}\right]$, for all a, b, x and y within their respective alphabet. $M_{a|x}$ and $M_{b|y}$ are positive

operators describing measurement choices x and y, but nothing is specified about their actual shape, other than the fact that $\sum_a M_{a|x} = \mathbb{1}_A$ for all $x \in \mathcal{X}$ and $\sum_b M_{b|y} = \mathbb{1}_B$ for all $y \in \mathcal{Y}$. We denote the alphabet sizes $m_A = |\mathcal{X}|$ and $m_B = |\mathcal{Y}|$ for the measurement choices, and $o_A = |\mathcal{O}_A|$ and $o_B = |\mathcal{O}_B|$ for the possible outcomes. As before, we denote $\mathbf{p}$ the $o_A o_B m_A m_B$-sized behavior, or correlations, with components $P(a, b|x, y)$.

The protocol begins with Alice and Bob using the authenticated public channel to share a sample of their data in order to estimate the behavior $\mathbf{p}$. A Bell inequality, that is, a linear functional $\mathbf{g} = \{g_{abxy}\}$ pre-established by Alice and Bob, and possibly known to Eve, is then applied to the observed $\mathbf{p}$ (recall Sec. 2.3). In particular, the Bell inequality $\mathbf{g} \cdot \mathbf{p} < g_{\text{loc}}$ witnesses the nonlocality of $\mathbf{p}$ for some local bound g_{loc} [Bel64, BCP+14]. If $\mathbf{g} \cdot \mathbf{p}$ is found to be greater than the local bound g_{loc}, then Alice and Bob can use classical error correction and privacy amplification to distill a secret key from some fixed measurements x^* and y^* out of the remaining data [ABG+07, MPA11, PMLA13]. Concretely, we shall consider from now on that Alice can chose among 2 possible measurements ($m_A = 2$) labeled $x = 0, 1$, while Bob can choose among 3 possible ones ($m_B = 3$), although his third measurement labeled $y = 2$ is only used to extract the key [ABG+07, MPA11]. Hence, from now on, we assume $x^* = 0$ and $y^* = 2$.

Secret key. Security proofs in DIQKD are constructed from the following observation: under reasonable assumptions, the restrictions set on the observed correlations $\mathbf{p}$ by Born's rule and by the amount of observed violation $\mathbf{g} \cdot \mathbf{p}$ are sufficient to bound the predictability of Eve in such a way that the users certify that they have stronger correlations among them; if this is the case then their bit strings remain private, even after having published a (small) fraction of the outcomes to make the strings perfectly correlated. In [PMLA13], the only extra assumption required to prove security is that the quantum memory of the eavesdropper is bounded. This assumption is reasonable given the current status of quantum technologies, and is formally known as the bounded quantum storage (BQS) model. It is worth mentioning that a noise-tolerant proof of DIQKD security without any additional assumption has been given in [VV14]. A different and more robust proof has later been derived in [MS16].

Remember that, given the observation of $\mathbf{p}$ by the two users, the predictability that Eve can have on the outcome of Alice when input x^* is chosen can be quantified by the *guessing probability* $G_{\mathbf{p}}(x^*)$ defined in (2.21), the average probability that Eve correctly guesses the output of Alice using an optimal strategy [NSPS14, BSS14]. As explained in Sec. 2.4, from the dual formulation of the SDP program (2.21) one retrieves the Bell inequality $\mathbf{g}$ which is such that $\mathbf{g} \cdot \mathbf{p} = G_{\mathbf{p}}(x^*)$. Such a $\mathbf{g}$ is the optimal Bell inequality for bounding the degree

of predictability that Eve can have about the string of outcomes of Alice. Program (2.21) is hence relevant to retrieve the optimal Bell inequality to bound the predictability of Eve on a from an observed behavior $\mathbf{p}$. Nevertheless, these methods should not be considered to be part of the DIQKD protocol, since existing DIQKD security proofs assume that the inequality used in the protocol described above is pre-established and even publicly announced just as the protocol starts. Therefore, from this time forth we shall assume that such inequality $\mathbf{g}$ is fixed and publicly known.

After the success of the estimation phase of the DIQKD protocol, in which the data reveals violation of the Bell inequality $\mathbf{g}$, it turns out that Alice and Bob have to publish a fraction of bits to correlate their bit strings given by the conditional entroy $H(x^*|y^*)$ of the joint probability distribution $P(a, b|x^*, y^*)$; this is the information reconciliation step of the protocol. In fact, in the asymptotic limit of a large number N of causally independent rounds, it has been shown that the number of device-independent secret bits certified per round from the pair of settings (x^*, y^*) is given by [MPA11]:

$$r = -\log_2 G_{\mathbf{p}}(x^*) - H(x^*|y^*). \tag{2.22}$$

Formula (2.22) is quite intuitive. The first term $-\log_2 G_{\mathbf{p}}(x^*)$ has already been encountered; it corresponds to the min-entropy of the device-independent guessing probability [NSPS14, KRS09]. It quantifies the amount of private randomness left in the string of outcomes of Alice, given the best possible strategy used by Eve to attempt to learn such string. Note that whenever $G_{\mathbf{p}}(x^*) = 1$, Eve has full knowledge about the string and $r = 0$ (this occurs in particular when no Bell violation is observed). The second term in (2.22) is the conditional entropy of the joint probability distribution $P(a, b|x^*, y^*)$. It is incorporated in order to account for the information reconciliation step required by any QKD protocol. As explained, $NH(x^*|y^*)$ represents the number of key bits that have to be published by Alice and Bob for successful information reconciliation [MPA11].

Note that the key rate expression presented in (2.22) has also been proved to hold beyond the case where the rounds are causally independent; in particular, it remains valid in the more realistic DIQKD approach based on the BQS model previously mentioned [PMLA13], where the only additional assumption required is that the quantum memory of the eavesdropper is limited in time. Indeed, this assumption is reasonable given the current status of quantum technology. DIQKD security in the BQS model arises from the following fact: since Eve cannot hold quantum information about the state of Alice and Bob for too long, she is forced to readout her system, and her optimal strategy is to apply a generalized measurement optimized to correlate her result with the one of Alice at each round.

More recently, Ref. [AFRV16] realized that it is possible to establish a reduction

from the scenario in which the most general quantum adversary operates to the scenario in which the untrusted devices operate in an i.i.d. way in each round of the protocol. In other words, this implies that (2.22) is at least a lower bound on the number of secret key bits certified against any quantum adversary.

Experimental challenges. Experimentally, DIQKD remains hitherto challenging because the devices of Alice and Bob, which are a priori distant from each other, must produce correlations that exhibit nonlocal correlations —i.e. correlations which violate a Bell inequality [Bel64]— without post-selection on the data, since otherwise the violation can be faked by an eavesdropper with classical resources [GLLL$^+$11a]. This is difficult to achieve in real experiments due to typical exponential increase of loss in the optical channel separating the two parties. Channel loss can be eliminated by means of conditioning over an auxiliary measurement that allows to safely discard rounds for which the photon —the information carrier— did not arrive, without opening the *detection loophole* [Pea70, San92]. These methods based on safe conditioning have been proposed —and experimentally demonstrated in some cases— both within the framework of all-optical implementations [GPS10, CM11, KXRP13, BPM$^+$16], as well as with hybrid systems based on light-matter interaction [PAM$^+$10, HKO$^+$12, MBA13, BYHR13, HBD$^+$15].

Furthermore, loss also affects the *information reconciliation* [BB84, Eke91] part of the DIQKD protocol, a step crucial to ensure perfect correlation in the final string of secret bits. This is an issue that most DIQKD proposals [GPS10, CM11, MBA13], with the exception of Ref [PMW$^+$11], had not addressed so far. We will review and address this problem in Chap. 6 by evaluating the optimal amount of randomness from the post-processed data of conclusive rounds, which turns out to be a direct application of the methods recently exposed by ref. [TdlTB$^+$16] in the context of device-independent random number generation.

3. Entanglement detection with uncharacterized devices

The certification of entanglement is a crucial task for the near-future development of quantum networks composed by observers sharing multipartite quantum states. In this Chapter we derive and experimentally apply tools to certify all kinds of entanglement in asymmetric networks, where some users do not have control over the measurements they are performing. Such asymmetry naturally emerges in physical systems where certain degrees of freedom cannot be experimentally controlled. Furthermore, it arises in adversarial situtations, such as in semi-DI cryptographic applications in quantum networks.

3.1. Background

In Sec. 2.1 we overviewed that experimentally certifying the presence of entanglement is a difficult task since mismatches between either the state or the measurements and their actual physical implementation may lead to false-positive conclusions about the presence of entanglement in the network [RFSB+12]. Although such mismatches can in principle be patched, the situation becomes dramatic when considering applications, where the devices used are not trusted as they could have been provided and controlled by some adversary. As mentioned already, one solution to this problem is the use of DI techniques [BCP+14], for which no assumption is made on the devices that generate the state or perform the measurements. In this approach the devices are seen as black boxes, accessed only with classical inputs (corresponding to the measurement choices) and providing classical outputs (corresponding to the measurement outcomes). Although such *DI entanglement witnesses* have been soundly considered in the past years [BGLP11, BBS+13], their physical implementation turns out to be very demanding [GLLL+11a] for it requires one to observe a Bell inequality violation without the presence of loopholes [HBD+15, SMSC+15, GVW+15].

A midpoint among the aforementioned cases is the semi-DI approach based on the presence of quantum steering [WJD07] to certify entanglement in the

network. This is an asymmetric situation in the sense that only some of the parties in the network use trusted devices while others do not [CSA+15]. Trust should be understood in terms of full knowledge or characterisation of the devices used. More precisely, whenever a party's device is assumed untrusted all the analysis employed is only based on the statistics it produces, not on its internal working. The steering approach is less demanding experimentally than the DI case and it presents practical interest for adversarial situations; for instance, one could think of a practical semi-DI network composed by a single central provider using well characterised devices, while the remaining parties, the clients, hold untrusted, *i.e.* uncharacterized devices. For these reasons the study of quantum steering has increased substantively in recent years [BCP+14].

Methods to certify all kinds of multipartite entanglement in semi-DI networks were presented —and experimentally demonstrated— recently [CSA+15]. These methods rely on SDP techniques and represent an important achievement for the certification of entanglement in quantum networks. In fact, these techniques certify entanglement in networks with amounts of noise that make them undetectable by the existing fully DI techniques [BGLP11]. In this Chapter we apply such semi-DI entanglement certification techniques to the three-qubit W state. Crucially, this state displays both genuine multipartite entanglement (GME) and entanglement in all of its reduced states, being then a flexible resource for the implementation of quantum networks. Moreover, we show that all types of entanglement of the W state can be certified in all tripartite steering scenarios in a scheme where each party applies the same set of measurements.

3.2. Witnesses construction

We begin by constructing multipartite semi-DI entanglement witnesses [CSA+15, MSA+17] for the bipartite and tripartite cases. The construction can be generalized for a larger number of parties and the intuition behind it is the following. Assuming that the quantum state distributed in a steering network (recall the middle of Fig. 1.1) is separable according to some particular decomposition (*e.g* fully separable, separable across any bipartition, etc.) imposes constraints on the collection of all possibly observable set of post-measured states that the untrusted measurements create for the the parties holding trusted devices. From these constraints one can then determine if the original state could have the considered decomposition with SDP techniques in an efficient way. Crucially, this provides experimentally friendly entanglement witnesses, known as steering inequalities.

3.2.1. Bipartite case

In the bipartite case, presented already in Chap. 2, Alice and Bob share a state ρ^{AB}. The measurements performed by Alice are untrusted and therefore they are described by unknown positive operators $M_{a|x}$ summing to identity for each x, where x labels the measurement chosen by her and a the obtained outcome. On the other hand, the other party, Bob, trusts his measurement device and can thus perform quantum tomography on his system to observe an unnormalized conditional state $\sigma^{B}_{a|x} = \mathrm{Tr}_A \left[M_{a|x} \otimes \mathbb{1}^B \, \rho^{AB}\right]$, $\forall\, a, x$ as stated already in (2.2).

The statistics observed by Alice can be recovered from the relation (Born rule) $p(a|x) = \mathrm{Tr}\left[\sigma^{B}_{a|x}\right]$, and thus the quantum assemblage $\{\sigma^{B}_{a|x}\}_{a,x}$ contains all the information obtainable in this measurement scenario. If ρ^{AB} is not entangled, it has the form (2.1) and in this case, the assemblage takes the form (2.4), meaning that the assemblage admits an LHS model, a classical process explaining the observation of the assemblage $\{\sigma^{B}_{a|x}\}_{a,x}$ by the two parties. In particular, if $\sigma^{B}_{a|x}$ admits an LHS model it belongs to the convex set $\Sigma^{B}_{A:B}$ of all unnormalized LHS assemblages defined by (2.5).

Crucially, imposing membership in $\Sigma^{B}_{A:B}$ involves a finite number of linear matrix inequalities and positive-semidefinite constraints for the variables σ^{B}_{μ} in (2.5), which are all valid constraints to formulate the problem as an SDP [BV04]. By introducing the *maximally mixed assemblage* for Bob, $\mathsf{I}^{B}_{a|x} = \frac{1}{o_A}\mathrm{Tr}_A\left[\frac{\mathbb{1}_{AB}}{d_A d_B}\right]$, where o_A denotes the number of outcomes of Alice and d_A and d_B denote the dimension of the systems, we obtain the SDP test for bipartite entanglement with one party holding untrusted devices given by the first program of (2.13). This test provides the robustness r^* to white noise of the assemblage observed by Bob $\sigma^{B}_{a|x}$.

Since $\mathsf{I}^{B}_{a|x} \in \Sigma^{B}_{A:B}$, a sufficiently small value of r will always solve the constraint of (2.13), and hence this SDP is strictly feasible. The solution of the test, denoted by r^*, quantifies how much maximally mixed noise has to be added to the assemblage such that the mixture becomes LHS: if $r^* = 0$, then $\sigma^{B}_{a|x} \in \Sigma^{B}_{A:B}$ and no steering can be demonstrated. Conversely, if $r^* > 0$, some amount of noise has to be added to the assemblage to make it LHS, so we certify entanglement in ρ^{AB}.

As explained in Sec. 2.1, strict feasibility implies that from the *dual* formulation [BV04] of the primal problem, it is possible to define a set of operators $\{F_{a|x}\}_{ax}$, which are such that the linear functional $\hat{w}$ (2.14) acting on $\sigma_{a|x}$ provides a strictly positive value only if the assemblage $\sigma_{a|x}$ demonstrates steering. Thus, $\hat{w}$ constitutes a witness for bipartite entanglement with one party holding untrusted devices. Furthermore, since the primal problem is strictly feasible, *strong duality* holds, and the dual and primal solutions coincide [BV04] giving $\hat{w}\left(\sigma^{B}_{a|x}\right) = r^*$.

Figure 3.1.: **Tripartite semi-DI scenarios.** *Left:* If only Alice holds an untrusted device, Bob and Charlie observe a bipartite state $\sigma^{BC}_{a|x}$. *Right:* With two parties holding untrusted devices, Charlie receives a state $\sigma^{C}_{ab|xy}$ conditioned on the statistics observed both by Alice and Bob.

3.2.2. Tripartite case

We now move on to the tripartite case, for which we wish to certify the presence of entanglement in the whole state ρ distributed to Alice, Bob and Charlie. In analogy with (2.1), ρ is said to be *fully separable* if it can be written as a convex combination of product states:

$$\rho = \sum_{\lambda} p_\lambda \ \rho^{A}_{\lambda} \otimes \rho^{B}_{\lambda} \otimes \rho^{C}_{\lambda}. \tag{3.1}$$

If the previous decomposition cannot be found, ρ is *tripartite entangled*. Notice however that a state can be separable across a bipartition without being fully separable. For instance, it could be that ρ presents entanglement among Bob and Charlie, but is separable with respect to Alice (*e.g.* $\rho = \rho^{A} \otimes |\phi^+\rangle\langle\phi^+|$, where $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + \langle 11|)$ denotes the maximally entangled state of two qubits for Bob and Charlie). In this case the state is said to be separable across the bipartition A:BC. In particular, a state which contains entanglement across all three bipartitions A:BC, B:CA and C:AB is said to be *genuinely multipartite entangled* (GME) [HHHH09].

In what follows we present the construction of witnesses of tripartite entanglement, but note that the construction of witnesses for the certification of GME follows the same reasoning and the details can be found in Ref. [MSA+17].

One untrusted device We treat first the case in which only Alice uses an untrusted device, while Bob and Charlie's devices remain trusted. In this case, Bob and Charlie are provided with the assemblage:

$$\sigma^{BC}_{a|x} = \mathrm{Tr}_{A}\left[\left(M_{a|x} \otimes \mathbb{1}^{B} \otimes \mathbb{1}^{C}\right) \ \rho\right], \tag{3.2}$$

which, after using (3.1), takes the form:

$$\sigma^{BC}_{a|x} = \sum_{\lambda} p(a|x\lambda) \ \rho^{B}_{\lambda} \otimes \rho^{C}_{\lambda}. \tag{3.3}$$

A decomposition of $\sigma^{\mathrm{BC}}_{a|x}$ of the form (3.3) can readily be seen to be similar to the one in (2.4), with the only difference that now the bipartite states of Bob and Charlie conditioned on a and x are separable. This last requirement (separability) cannot, in general, be translated to a finite number of linear matrix inequalities and positive constraints as before, because the set of separable states has a complicated structure. However, separability can be relaxed to *positivity under partial transposition* [HHHH09], which is a valid SDP constraint and equivalent to separability whenever the product of the dimensions of B and C satisfies $d_B d_C \leq 6$. Therefore, we define the *relaxed* set:

$$\Sigma^{\mathrm{BC}}_{\mathrm{A:B:C}} = \left\{ \sigma^{\mathrm{BC}}_{a|x} \mid \sigma^{\mathrm{BC}}_{a|x} = \sum_{\mu} D_{\mu}(a|x)\sigma^{\mathrm{BC}}_{\mu}, \sigma^{\mathrm{BC}}_{\mu} \geq 0,\ \left(\sigma^{\mathrm{BC}}_{\mu}\right)^{T_{\mathrm{B}}} \geq 0 \right\} \tag{3.4}$$

where T_{B} denotes the partial transposition operation with respect to system B. With the help of the maximally mixed assemblage for Bob and Charlie, namely $\mathsf{I}^{\mathrm{BC}}_{a|x} = \frac{1}{o_A}\mathrm{Tr}_{\mathrm{A}}\left[\frac{\mathbb{1}_{\mathrm{ABC}}}{d_A d_B d_C}\right]$, we obtain the corresponding SDP test for tripartite entanglement with one party holding untrusted devices:

$$\begin{aligned} \min \quad & r \\ \text{s.t.} \quad & (1-r)\sigma^{\mathrm{BC}}_{a|x} + r\mathsf{I}^{\mathrm{BC}}_{a|x} \ \in \ \Sigma^{\mathrm{BC}}_{\mathrm{A:B:C}}. \end{aligned} \tag{3.5}$$

Here, again, duality theory allows one to retrieve operators $\{F_{a|x}\}_{ax}$ defining a new witness $\hat{w}$ with the exact same structure and such that $\hat{w}\left(\sigma^{\mathrm{BC}}_{a|x}\right) > 0$ guarantees that ρ is tripartite entangled.

Two untrusted devices. In the case of two parties, say Alice and Bob, holding untrusted devices, Charlie observes the assemblage:

$$\sigma^{\mathrm{C}}_{ab|xy} = \mathrm{Tr}_{\mathrm{AB}}\left[\left(M_{a|x} \otimes M_{b|y} \otimes \mathbb{1}^{\mathrm{C}}\right)\ \rho\right], \tag{3.6}$$

which, after replacing ρ with its separable form (3.1), gives:

$$\sigma^{\mathrm{C}}_{ab|xy} = \sum_{\lambda} p(ab|xy\lambda)\ \rho^{\mathrm{C}}_{\lambda}. \tag{3.7}$$

Since $p(ab|xy\lambda)$ arises from local measurements on a separable state, it can be written as a convex combination of products of deterministic strategies for Alice and Bob [BCP+14]. Thus, the relevant set of unnormalized assemblages for tripartite entanglement with two parties using untrusted measurements is:

$$\Sigma^{\mathrm{C}}_{\mathrm{A:B:C}} = \left\{ \sigma^{\mathrm{C}}_{ab|xy} \ | \sigma^{\mathrm{C}}_{ab|xy} = \sum_{\mu\nu} D_{\mu}(a|x)D_{\nu}(b|y)\sigma^{\mathrm{C}}_{\mu\nu},\ \sigma^{\mathrm{C}}_{\mu\nu} \geq 0 \right\} \tag{3.8}$$

and since membership in $\Sigma^{C}_{A:B:C}$ involves valid SDP constraints, we obtain the corresponding SDP test:

$$\begin{aligned} \min \quad & r \\ \text{s.t.} \quad & (1-r)\sigma^{C}_{ab|xy} + r\mathsf{I}^{C}_{ab|xy} \;\in\; \Sigma^{C}_{A:B:C}, \end{aligned} \tag{3.9}$$

where $\mathsf{I}^{C}_{ab|xy} = \frac{1}{o_A o_B}\mathrm{Tr}_{AB}\left[\frac{\mathbb{1}_{ABC}}{d_A d_B d_C}\right]$ is the maximally mixed assemblage for C. The set of dual variables $\{F_{ab|xy}\}_{abxy}$ of program (3.9) define the witness:

$$\hat{w} : \; \pi_{ab|xy} \;\mapsto\; \sum_{abxy} \mathrm{Tr}\left[F_{ab|xy}\; \pi_{ab|xy}\right], \tag{3.10}$$

which is strictly positive only if $\pi^{C}_{ab|xy}$ demonstrates steering, and $\hat{w}(\sigma^{C}_{ab|xy}) = r^*$.

3.2.3. Multipartite steering of the W state

Here we provide numerical values for the three-qubit W state $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$ and discuss the fact that each party can check for all kinds of entanglement without trusting the devices of the others. The measurements performed by all trusted boxes are Pauli observables, namely, $\hat{X}$, $\hat{Y}$ and $\hat{Z}$. Our theoretical findings regarding the witness values r are summarized in Table 3.1.

Since the W state is symmetric, all reductions are equivalent regardless of the party that is discarded. Specifically, $\rho_{\mathrm{red}} = 2/3\,|\psi^+\rangle\langle\psi^+| + 1/3\,|00\rangle\langle 00|$, where $|\psi^+\rangle$ denotes the two-qubit maximally entangled state $|\psi^+\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$. The reduced state turns out to be steerable with a theoretical violation of $r^* = 0.11$. This value is relatively small because of the detrimental contribution of the

	Theory	**Experiment**
Ent. in reductions	0.1112	0.07 ± 0.01
Ent. *(1 untrusted)*	0.7297	0.77 ± 0.01
Ent. *(2 untrusted)*	0.5355	0.500 ± 0.008
GME *(1 untrusted)*	0.4581	0.41 ± 0.01
GME *(2 untrusted)*	0.3244	0.32 ± 0.01

Table 3.1.: **Witness values r^* from the three qubit W state**. A strictly positive value certifies the presence of: entanglement in the reduced state (first row), entanglement in the full tripartite state (second and third rows), genuine multipartite entanglement (fourth and fifth rows).

separable state $|00\rangle$. Such violation not only guarantees the presence of entanglement in the reduced state, but it also certifies the presence of entanglement across any bipartition of the tripartite network, regardless of whether the third party (the discarded one) is using a trusted device or not.

For the tripartite W state, we observe the presence of entanglement and GME both in the "one untrusted" scenario and in the "two untrusted" scenario as well (see lines 2-5 of Table 3.1). Note that the violations for the "one untrusted" scenario are always better than for the "two untrusted" scenario, because in the former case there is more useful information available (about the state) than in the latter case. The values for tripartite entanglement are also always better than the values obtained for GME, as the presence of the latter implies the presence of the former, but the converse is not true in general.

3.3. Experimental implementation

To demonstrate the practical utility of the theoretical results presented in the previous Sections, we produced a three-qubit W state using photon pairs produced by Spontaneous Parametric Down Conversion (SPDC).

3.3.1. Setup

For concreteness in Fig. 3.2 we show the experimental setup. Two 1mm thick type-I non-linear BBO crystals with optical axes oriented perpendicularly were pumped with a 325nm continuous-wave He-Cd laser, producing degenerate photon pairs centered around 650nm. Using an additional half-wave plate in the path of photon 1, the crossed-crystal arrangement produces two polarization entangled photons in the target state [KWW$^+$99]:

$$|\psi\rangle = \cos\theta\,|VH\rangle_{12} + e^{i\varphi}\sin\theta\,|HV\rangle_{12}\,. \tag{3.11}$$

Qubits B and C were encoded in the polarization of the photons 1 and 2, respectively. Qubit A was encoded in the path of photon 2. Initially, qubit A is in the state $|0\rangle_A$. To produce the W state, we entangle the path and polarization degrees of freedom (DOF) of photon 2 using a polarization-dependent Mach-Zehnder interferometer composed of two beam displacers (BDs) and several half-wave plates (HWPs), as described in more detail in Refs. [FAVH$^+$12, AVHD$^+$14]. We label the input and output paths such that when the polarization state is $|H\rangle_C$, the output state is $|0H\rangle_{AC}$. For input vertical polarization, the interferometer implements the

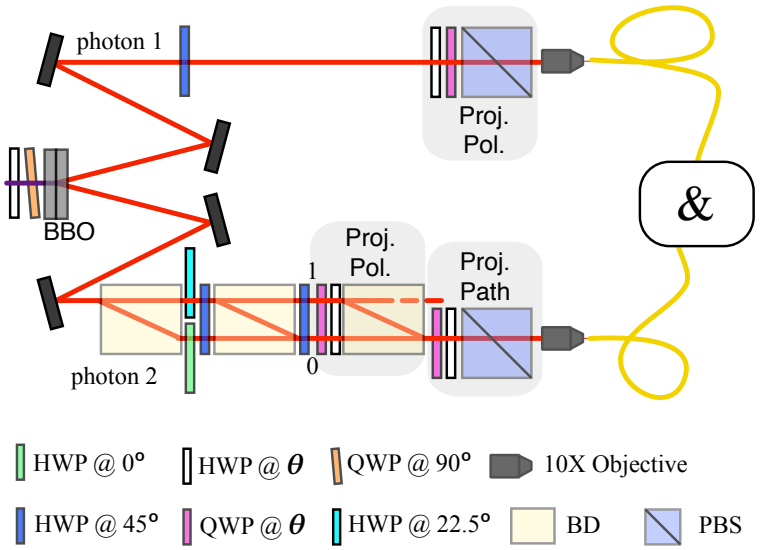

Figure 3.2.: **Experimental setup.** Polarization-entangled photons are produced using SPDC. A third qubit is encoded in the path degree of freedom of photon 2. An interferometer consisting of beam displacers is used to produce a three-qubit W state. Projective measurements on the polarization (Proj. Pol.) and Path (Proj. Path) measurements are performed using wave plates and polarizers.

transformation

$$|0V\rangle_{AC} \longrightarrow \frac{1}{\sqrt{2}}|0V\rangle_{AC} + \frac{1}{\sqrt{2}}|1H\rangle_{AC}\,. \tag{3.12}$$

By controlling the polarization of the pump laser [KWW+99], the initial polarization entangled state was prepared with $\cos\theta = 1/\sqrt{3}$ and $\varphi = 0$. Renaming the polarization state $|H\rangle \to |0\rangle$ and $|V\rangle \to |1\rangle$, our setup produces a three-qubit state that is ideally a W state [FAVH+12].

A set of 216 joint projective measurements in the $\hat{X}$, $\hat{Y}$ and $\hat{Z}$ Pauli basis was performed on all three qubits, which allowed us to evaluate the SDP tests developed above. To perform projective measurements on qubit B (polarization of photon 1), the usual system consisting of a quarter-wave plate (QWP), HWP and a polarizing beam splitter (PBS) is used. For projective measurements on qubit C, a QWP, HWP and BD are used. This measurement system works in much the same way as that of qubit B, however, after the projection on a given polarization state, the BD maps the state of the path DOF at its input into the polarization DOF at its output. In this fashion, the state describing the path DOF, which is now encoded in the polarization DOF, can be measured using the same arrangement as in photon 1. The photons were filtered with 3nm FWHM

bandwidth filters centered at 650nm (not shown in the figure), coupled into single-mode optical fibers using 10× microscope objectives and registered with single photon detectors and coincidence electronics (the "&" box in Fig. 3.2).

The methods described were designed to detect entanglement and certify randomness from an observed *physical* assemblage σ^{phys}. However, due to the unavoidable problem of finite statistics in any experiment, the assemblage that is experimentally observed σ^{exp} does not satisfy the non-signalling property although non-signalling conditions are within the statistical error. To overcome this problem we took the following steps. First, we construct a physical assemblage that approximates the experimental data. This step is done with a least-squares optimization, an SDP program that minimizes the distance from the experimental assemblage to the set of physical assemblages bounded by the non-signalling constraints. The second step consists of using the constructed physical assemblage to obtain the desired witness $\hat{w}^{\text{phys}}$, following the SDP techniques for entanglement detection. The last step is to apply the derived witness, which is simply a linear functional, to the experimental assemblage to show the presence of entanglement in the network.

3.3.2. Results

Our experimental results are summarised in Table 3.1. The error bars were calculated by performing Monte Carlo simulation (494 rounds) assuming Poissonian coincidence counting statistics of our measurement results. Experimentally, the reduced state is not entirely symmetric because of imperfections in the optical setup, such as temporal and spatial mode mismatch in the interferometer. Thus, we analyzed all reductions and found that the highest violation of 0.07 ± 0.01 is obtained when discarding Bob, corresponding to the polarization of photon 1.

As far as the experimental certification of tripartite entanglement and GME are concerned, the corresponding observed witness values are shown in lines 2-3 and 4-5 of Table 3.1, respectively. One obtains a strictly positive value for these two types of tripartite entanglement, both in the “one untrusted” and in the “two untrusted” scenarios. The experimental witness values are close to the theoretical ones, although these do not always fall within the error margins obtained. This is expected since the experimental state is not perfectly pure (see [MSA$^+$17]). The case where the measured value agrees with the theory within the error interval corresponds to the situation where the correlations between two internal degrees of freedom of the same photon (path and polarization) are the most relevant. In this special case the purity of the reduced state can be very high experimentally. Even with these small discrepancies between theory and experiment, we successfully certify the presence of entanglement and GME in the considered semi-device

independent networks. For completeness the reader may find the numerical values for all steering inequalities described in this work at the Git online repository: github.com/mattarcon2tes/Steering.

3.4. Discussion

In this Chapter we showed that it is possible to certify all types of entanglement from a three-qubit W state in the semi-DI framework, both in theory and in practice. Such semi-DI entanglement certification was achieved in all tripartite steering scenarios, and without the need to consider different measurements among different scenarios. We studied in detail the case of a tripartite configuration, even though the method is valid for larger networks. Our experimental results, obtained with an optical setup yield good qualitative agreement with the theory, and verify a strong dependence of the witnessed entanglement on the degree of purity of the initial state. We notice that it is still an open question whether the reduced state of the W state can violate any Bell inequality [SZDM15, BPB$^+$15], although here we showed that it does present steering. The results derived promote the W state as a key candidate for the implementation of semi-device independent protocols.

4. A measure of nonlocality without anomalies

In the previous two Chapters we explained and demonstrated how practical witnesses —inequalities— of steering and nonlocality can be constructed from analyzing the geometry of the space in which these quantum resources lie in. Such inequalities will be the main ingredient for the development and implementation of practical semi-DI and DI protocols in the next Chapters. However, we have also learned that these inequalities cannot be directly considered as a proper, read fundamental or universal, measure, since they induce different orderings and certify more steering or nonlocality of a given resource than others (recall Sec. 2.3).

In this Chapter we leave for a moment the practical perspective to dig into the more fundamental problem of properly measuring nonlocality. What is an appropriate measure of nonlocality? Perhaps one which acts directly at the level of the quantum states; could it be one which is monotone with the the degree of the entanglement of the underlying state? Indeed, it is crucial to understand the subtle relation that exists among entanglement, nonlocality, since some entangled states might be more valuable than others for specific DI and semi-DI quantum information tasks. In this context, we introduce a quantifier for nonlocality which does not present *anomalies of nonlocality*: cases for which maximal entanglement does not imply maximal nonlocality. With our measure we show that no anomaly ever occurs when restricting to qubits in a broad range of situations.

4.1. Motivation

Understanding the relation between entanglement and nonlocality has been a focus of attention for the work of many. Werner revealed the subtlety of the question by providing an explicit construction of a family of mixed entangled states that do not violate any Bell inequality when subjected to projective measurements [Wer89]. Werner's result was later extended to general measurements, not necessarily projective, by Barrett [Bar02]. For pure states, the situation seemed to clarify since Gisin recognized that all pure entangled states of any dimension display nonlocality when applying appropriate measurements on them [Gis91].

4. A measure of nonlocality without anomalies

When going to quantitative aspects, the relation between entanglement and nonlocality is not fully understood not even for bipartite pure states. Early work by Tsirelson demonstrated that the maximal quantum violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality [CHSH69], the simplest Bell inequality, can only be achieved when measuring a two-qubit maximally entangled state [Cir80]. It was then natural to expect maximal entanglement to be indispensable to retrieve the maximal quantum violation of Bell inequalities. However, subsequent examples showed that the maximal quantum violation of certain Bell inequalities crucially requires partial entanglement [ADGL02], even when considering states of arbitrary Hilbert space dimension [LVB11, VW11]. Furthermore, the phenomenon of obtaining more nonlocality from less pure-state entanglement happened to occur not only for the amount of violation of a given Bell inequality, but also for other measures of nonlocality, such as the robustness of nonlocality to noise [ADGL02], losses [Ebe93], statistical strength of Bell tests [AGG05] and the simulation of quantum correlations with nonlocal resources [BGS05]. The inequivalence, from a quantitative point of view, between pure-state entanglement and nonlocality was dubbed *anomaly* in [MS07] and this is the terminology we adopt here.

It is desirable to understand if such an anomaly is related to a fundamental aspect of quantum nonlocality, or instead, if it is possible to define an operational notion of nonlocality for which maximally entangled states correspond to maximal nonlocality. Interestingly, the authors of [FP15] recently reported that the anomaly originally observed in [ADGL02] for the Collins-Gisin-Linden-Massar-Popescu (CGLMP) inequality [CGL$^+$02] for three-outcome measurements disappears when considering a novel, yet intuitive, measure of nonlocality. For a given quantum state $|\psi\rangle$, this measure is defined with respect to a specific Bell inequality, CGLMP in the case of [FP15], and corresponds to the probability to violate the inequality when random projective measurements are performed on the state $|\psi\rangle$. The authors of [FP15] numerically showed that the probability to obtain a violation of the CGLMP inequality for three outcomes when pairs of random measurements are performed on each part of a bipartite two-qutrit pure state is always maximized by the maximally entangled state. It is worth noting that this result can be seen as an extension to higher dimensions, namely qutrits, of the work of Liang *et al.* [LHBR10], which introduced the same measure of nonlocality based on random sampling of observables to estimate the nonlocality of Greenberger-Horne-Zeilinger (GHZ) states of many qubits with respect to the Mermin-Ardehali-Belinski-Klyshko (MABK) inequalities [Mer90, RS91, Ard92, BK93] and even with respect to the family of Bell inequalities introduced in [WW01, idZB02].

The measure of nonlocality considered by Refs. [FP15, LHBR10] aims to be an alternative to the use of Bell inequalities, but at the same time forces one to consider some pre-established Bell inequality. Furthermore, it only assessed

systems of low dimension and only a few examples of Bell inequalities were considered: the CHSH, the CGLMP and the MABK inequalities. Motivated by these two issues, we dispense with the choice of a particular inequality and directly consider the space of behaviors, which local polytopes inhabit, considering as an indicator of nonclassicality the probability of generating nonlocality from randomly sampled observables. Our quantifier of nonlocality relaxes the need for a specific Bell inequality (it covers all possible Bell inequalities for a given scenario at the same time) and is therefore a natural generalization of the work of Refs. [FP15, LHBR10].

Equipped with this measure, we prove that no anomaly of nonlocality ever occurs when considering any number of projective measurements per side for any even number N of qubits, for all scenario based on full-correlator inequalities (defined later on). We then explore the limits of this result and show that our proof cannot be extended to qutrits, nor to inequalities involving marginal terms. Finally, we briefly discuss whether our measure can be adapted to steering.

4.2. Nonlocality measure

We first consider the bipartite nonlocality scenario[1] that has already been formally introduced in Sec. 2.1. Specifically, the scenario is defined by the set of four natural numbers $[m_A, m_B, o_A, o_B]$ corresponding to the number of measurements and outcomes of Alice and Bob. The Bell test is fully described by the behavior $\vec{p} = \{p(ab|xy)\}$ whose elements are given by Born's rule (2.6), $p(ab|xy) = \mathrm{Tr}\left[M_{a|x} \otimes M_{b|y}\ \rho\right]$. Within the set $\mathcal{Q}$ of such quantum correlations (2.7), the set of local correlations $\mathcal{L}$ is formed by those admitting an LHV model (2.8). Recall that a nonlocal behavior $\vec{p} \notin \mathcal{L}$ is a manifestation of entanglement in the state ρ, but the converse statement is in general not true.

As detailed in Chap. 2, the nonlocality of a given behavior $\vec{p}$ is witnessed through the violation of a Bell inequality $\mathbf{g}$ if the quantity $\mathbf{g} \cdot \mathbf{p} := \sum_{abxy} g_{abxy} p(ab|xy)$ (2.15) is strictly larger than a fixed real number g_{loc} known as the local bound of the inequality [BCP+14]. $\{g_{abxy}\}$ are real coefficients defining the inequality $\mathbf{g}$ in question.

Bell operator. In turn, one can also witness such a Bell inequality violation by working with operators directly at the level of the shared state ρ. Given the

[1] Note however that in this Section we do not assume device-independence, in the sense that the measurements and the state can actually be retrieved, and are not assumed to be prepared in a malicious way by Eve.

measurements performed by Alice and Bob, one can construct the *Bell operator* [BCP+14]:

$$\hat{B}_{\mathbf{g}} = \sum_{abxy} g_{abxy} M_{a|x} \otimes M_{b|y}. \tag{4.1}$$

With the Bell operator one can now define $\hat{g}(\rho) := \mathrm{Tr}\left[\rho \hat{B}_{\mathbf{g}}\right]$ and from Born's rule $\hat{g}(\rho) = \mathbf{g}\cdot\mathbf{p}$ holds. The Bell operator formalism therefore enables the possibility to understand how distinct properties of ρ —such as its degree of entanglement— may affect the observed Bell violation $\hat{g}(\rho)$.

Anomaly of nonlocality. For concreteness let's take an example and consider that Alice and Bob share a pure state of two qubits $|\psi_\theta\rangle = \cos(\theta)|00\rangle + \sin(\theta)|11\rangle$ parametrized by $\theta \in [0; \frac{\pi}{4}]$. In this case it is always possible to find measurements $\{M_{a|x}\}$ and $\{M_{b|y}\}$ producing a nonlocal behavior $\vec{p} \notin \mathcal{L}$ from $|\psi_\theta\rangle$ as long as $\theta > 0$ [Gis91]. But which among all these states $|\psi_\theta\rangle$ yields more nonlocality? The question is troublesome as the answer typically depends on the scenario and on the Bell inequality considered. In the case of two dichotomic measurements per side, the state which maximally violates the CHSH inequality upon optimization of the measurements is the maximally entangled state obtained for $\theta = \frac{\pi}{4}$ and denoted $|\phi^+\rangle$. Actually, there exists a monotonous relation between entanglement and nonlocality in this case [WPGF09].

Intuitively, such monotonous relation between entanglement and nonlocality is expected to hold for inequalities in broader scenarios involving states of higher dimension. In [ADGL02], however, it was found that the CGLMP inequality [CGL+02] with $o_A = o_B = 3$ outcomes and with a two-qutrit state of the form $|\Psi_3^\gamma\rangle = \frac{1}{\sqrt{2+\gamma^2}}(|00\rangle + \gamma|11\rangle + |22\rangle)$ with $\gamma \simeq 0.79$ achieves a higher violation than with the two-qutrit maximally entangled state $|\Phi_3^+\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$. Furthermore, this anomaly of obtaining more nonlocality from less entanglement happens to occur for states of arbitrary dimension, and for several other measures of nonlocality as well [Ebe93, AGG05, BGS05].

Nonlocality from random measurements. To fix the entanglement anomaly detected in [ADGL02] for the CGLMP inequality, Ref. [FP15] considered a different measure of nonlocality, to be understood as the probability that correlations generated with randomly chosen measurements on ρ violate the inequality by any extent. A state ρ_1 is, in this sense, more nonlocal than the state ρ_2 if uniform randomly drawn measurements have a higher probability of generating correlations violating the inequality when performed on ρ_1 than on ρ_2.

Interestingly, it was found that such a measure of nonlocality does not reveal any anomaly for the CGLMP inequality [FP15]. The probability of finding a violation

for this particular Bell inequality when Alice and Bob perform one out of two measurements picked randomly, is always the highest for the maximally entangled state $|\Phi_3^+\rangle$. This in fact constitutes the first measure of nonlocality for which the CGLMP anomaly does not occur.

As said, this measure is to be understood as the probability for the generated correlations to violate a particular inequality $\mathbf{g}$ with randomly drawn measurements. But witnessing nonlocality in correlations with only one Bell inequality is limiting as correlations can often be nonlocal without violating a given inequality. For this reason, we consider a measure for which the nonlocality of ρ is witnessed by *all possible* Bell inequalities for a given scenario.

Consider the volume $\mathcal{V}(\rho)$ of the set of measurements which lead to nonlocal correlations when performed on the state ρ. This defines the probability of the state to generate a nonlocal behaviour from uniformly random sampled measurements:

$$P(\rho) = \frac{1}{N} \int_{\mathcal{V}(\rho)} \mathrm{d}^n s, \tag{4.2}$$

where the integration is taken uniformly over the space of measurement operators, and with N a normalization factor equal to the volume of the entire space. Here $P(\rho)$ does not depend on any fixed inequality $\mathbf{g}$, making (4.2) a natural and appealing measure of nonlocality of the state ρ. In particular, by taking the sampling of the measurements uniformly according to the Haar measure, our quantifier $P(\rho)$ is invariant under local unitaries applied on the state ρ, which was not considered by [FP15]. To show local unitary invariance of our measure, notice that $P(\rho)$ can be written as:

$$P(\rho) = \int \mathrm{d}U_{x=0} \ldots \mathrm{d}U_{y=m_B-1} f^{\mathrm{NL}}(\mathbf{p}), \tag{4.3}$$

with $f^{\mathrm{NL}}(\mathbf{p})$ being an indicator function such that $f^{\mathrm{NL}}(\mathbf{p}) = 1$ if the behavior $\mathbf{p}$ generated by ρ and by the sampled measurements is nonlocal. Conversely, $f^{\mathrm{NL}}(\mathbf{p}) = 0$ if $\mathbf{p} \in \mathcal{L}$. The sampled measurements are projectors whose elements are obtained from the action of unitaries randomly sampled acording to Haar's measure, that is, $M_{a|x} = U_x |a\rangle\langle a| U_x^\dagger$ and $M_{b|y} = U_y |b\rangle\langle b| U_y^\dagger$ for all x, y and some computational basis $\{|a\rangle\}_a$ and $\{|b\rangle\}_b$. Consider now that V_A and V_B are fixed unitaries acting locally on ρ at Alice and Bob sites, respectively. Then,

$$P(V_A \otimes V_B \rho V_A^\dagger \otimes V_B^\dagger) = \int \mathrm{d}U_{x=0} \ldots \mathrm{d}U_{y=m_B-1} f^{\mathrm{NL}}(\mathbf{q}), \tag{4.4}$$

where $\mathbf{q}$ is now the behavior obtained from the measurements with elements $M_{a|x} = V_A U_x |a\rangle\langle a| U_x^\dagger V_A^\dagger$ and $M_{b|y} = V_B U_y |b\rangle\langle b| U_y^\dagger V_B^\dagger$. Then, by simply applying the variable changes $\{U_x \leftarrow V_A U_x\}_x$ and $\{U_y \leftarrow V_B U_y\}_y$, and using the fact

that Haar's measure satisfies unitary invariance as a probability measure, namely, $\mathrm{d}U_x = \mathrm{d}V_A U_x$ and $\mathrm{d}U_y = \mathrm{d}V_B U_y$ for all x, y, it follows that $P(V_A \otimes V_B \rho V_A^\dagger \otimes V_B^\dagger) = P(\rho)$ holds for any local unitaries V_A and V_B.

In general, evaluating explicitly the integral in (4.2) is hard because of a lack of a precise characterization of the set $\mathcal{V}(\rho)$. We approach the problem alternatively and directly analyze inclusion relations of sets $\mathcal{V}(\rho)$ of different states. Crucially, we show that in many situations the set $\mathcal{V}(|\psi_\theta\rangle)$ obtained from any non-maximally entangled state is included in the set $\mathcal{V}(|\phi_+\rangle)$ derived from the maximally entangled one. This will naturally imply that $P(|\phi_+\rangle) \geq P(|\psi_\theta\rangle)$ and thus that no anomaly appears in these situations. Furthermore, in more complex situations, the operational character of our measure allows us to numerically estimate $P(\rho)$ via Monte Carlo simulations.

4.3. Less anomalies for nonlocality

Our main result concerns *full-correlator* Bell inequalities. These inequalities are defined as those in which only two-body correlators appear, and hence can be written as $g^{\langle\cdot,\cdot\rangle} = \sum_{x,y} g_{x,y}\langle A_x B_y\rangle$, where $\langle A_x B_y\rangle$ denotes the expectation value of observables A_x and B_y. We show that when restricting to full-correlator inequalities, maximal two-qubit entanglement and maximal nonlocality are always in correspondence for our measure (4.2). This is achieved by proving the inclusion relation $\mathcal{V}(|\psi_\theta\rangle) \subset \mathcal{V}(|\phi^+\rangle)$ for full-correlator inequalities. To do so, we prove that measurements which yield nonlocality when performed on $|\psi_\theta\rangle$ from a full-correlator inequality will always yield nonlocality if performed on $|\psi_{\theta'}\rangle$ for any $\theta' \geq \theta$. The result holds for any number m_A and m_B of projective measurements.

Theorem. For any full-correlator Bell inequality $g^{\langle\cdot,\cdot\rangle}$ with local bound g_{loc},

$$g^{\langle\cdot,\cdot\rangle}(|\psi_\theta\rangle) > g_{\mathrm{loc}} \quad \Rightarrow \quad g^{\langle\cdot,\cdot\rangle}(|\psi_{\theta'}\rangle) > g^{\langle\cdot,\cdot\rangle}(|\psi_\theta\rangle), \;\; \forall\; \theta' > \theta. \tag{4.5}$$

In words, if the full-correlator Bell inequality $g^{\langle\cdot,\cdot\rangle}$ is violated by correlations generated by the measurements $\{M_{a|x}\}$ and $\{M_{b|y}\}$ acting on a partially entangled state $|\psi_\theta\rangle$, then any state $|\psi_{\theta'}\rangle$ with $\theta' > \theta$ will provide a higher violation of $g^{\langle\cdot,\cdot\rangle}$ from the same measurements.

Proof. Suppose that:

$$b_\theta \equiv \mathrm{Tr}\left[|\psi_\theta\rangle\langle\psi_\theta|\hat{B}_{g^{\langle\cdot,\cdot\rangle}}\right] > g_{\mathrm{loc}}, \tag{4.6}$$

where $\hat{B}_{g^{\langle\cdot,\cdot\rangle}}$ is the Bell operator associated with the inequality $g^{\langle\cdot,\cdot\rangle}$, as explained in Sec. 4.2. Observe that $|\psi_\theta\rangle$ can always be written as:

$$|\psi_\theta\rangle = \left(\frac{\cos\theta + \sin\theta}{\sqrt{2}}\mathbb{1} + \frac{\cos\theta - \sin\theta}{\sqrt{2}}\sigma_z\right) \otimes \mathbb{1} \; |\phi^+\rangle. \tag{4.7}$$

Since the inequality $g^{\langle\cdot,\cdot\rangle}$ is full-correlator it does not involve marginal terms and thus the decomposition of the Bell operator $\hat{B}_{g^{\langle\cdot,\cdot\rangle}}$ in the Pauli basis does not contain terms proportional to $\mathbb{1}\otimes\mathbb{1}$, $\mathbb{1}\otimes\sigma_i$ and $\sigma_i\otimes\mathbb{1}$, for $i = x, y, z$. Using this fact and expression (4.7), the left-hand side of inequality (4.6) is re-written as:

$$b_\theta = \frac{b_+ + b_-}{2} + \frac{\sin 2\theta}{2}(b_+ - b_-) > g_{\text{loc}}, \tag{4.8}$$

where $b_\pm \equiv \langle\phi^\pm| \hat{B}_{g^{\langle\cdot,\cdot\rangle}} |\phi^\pm\rangle$ denotes the expectation value of $\hat{B}_{g^{\langle\cdot,\cdot\rangle}}$ on the maximally entangled state $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$.

$\frac{b_+ + b_-}{2}$ is in fact the expectation value of $\hat{B}_{g^{\langle\cdot,\cdot\rangle}}$ on the separable state $|00\rangle$ and is thus smaller or equal to g_{loc}. Since $\sin 2\theta$ is positive for $\theta \in [0, \frac{\pi}{4}]$, (4.8) implies that $b_+ > b_-$. Hence the violation b_θ given by (4.8) is monotonously increasing with θ (with $\sin 2\theta$ to be precise), achieving the maximum value for the maximally entangled state at $\theta = \pi/4$. This means that, for any full-correlator inequality there exists a (strictly) monotonous relation between two-qubit entanglement and nonlocality, and $b_{\theta'} > b_\theta$ holds for any $\theta' > \theta$, which completes the proof.

In particular, the theorem shows that for full-correlator Bell inequalities, the set of measurements leading to nonlocality on $|\psi_\theta\rangle$ is included in the corresponding set for the maximally entangled state $|\phi^+\rangle$. Moreover, it is possible to show that the inclusion of sets is strict and $\mathcal{V}_{\langle\cdot,\cdot\rangle}(|\psi_\theta\rangle) \subset \mathcal{V}_{\langle\cdot,\cdot\rangle}(|\phi^+\rangle)$, where $\mathcal{V}_{\langle\cdot,\cdot\rangle}(|\psi_\theta\rangle)$ ($\mathcal{V}_{\langle\cdot,\cdot\rangle}(|\phi^+\rangle)$) denotes the set of measurements leading to nonlocality on $|\psi_\theta\rangle$ (on $|\phi^+\rangle$) provided that only full-correlator inequalities are considered. Consequently, and in the spirit of definition (4.2), it follows that:

$$P_{\langle\cdot,\cdot\rangle}(|\psi_\theta\rangle) < P_{\langle\cdot,\cdot\rangle}(|\phi^+\rangle), \tag{4.9}$$

where $P_{\langle\cdot,\cdot\rangle}(|\psi_\theta\rangle)$ and $P_{\langle\cdot,\cdot\rangle}(|\phi^+\rangle)$ are defined in the same fashion as in (4.2), but assuming that nonlocal correlations may only be witnessed from the class of full-correlator inequalities. Crucially and in sound contrast with previous works [LVB11, FP15, dRGP$^+$17], our result is valid for any number of quantum measurements. It is also worth noting that in most bipartite scenarios facet inequalities — those delimiting the local set $\mathcal{L}$ — are not of the CHSH type [BCP$^+$14], meaning that our result hence applies to a broad class of inequalities in any scenario.

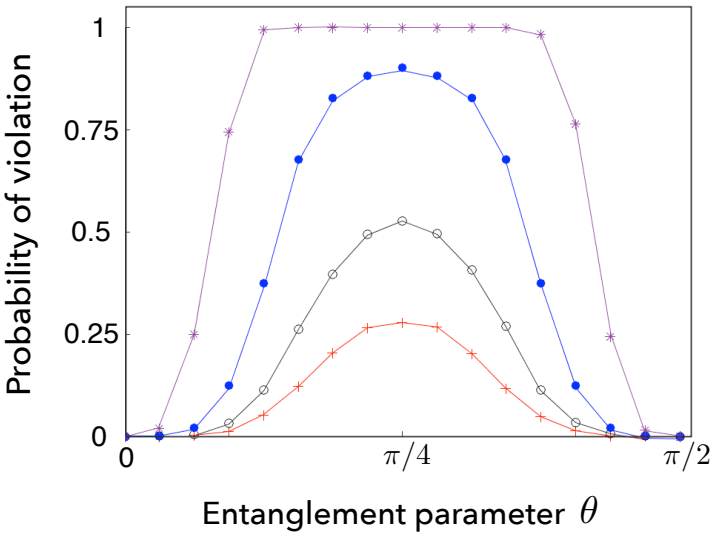

Figure 4.1.: **Probability of violation for qubits.** The probability is obtained from random measurements and is plotted as a function of entanglement parameter θ. For clarity of the image the range of θ has been extended to $\frac{\pi}{2}$ due to symmetry of the state $|\psi_\theta\rangle$. Measurement scenarios: $(+)$ – [2,2,2,2], $(\circ)$ – [2,3,2,2], $(\bullet)$ – [3,4,2,2], $(*)$ – [8,8,2,2].

4.4. Marginal terms and higher dimensions

Can our theorem be extended to inequalities with marginal terms related to single-body correlators, or to systems of larger dimension than $\mathbb{C}^2 \otimes \mathbb{C}^2$? A numerical search supplied a counter-example of measurements producing nolocality on $|\psi_\theta\rangle$ for $\theta = \frac{3\pi}{16}$ but not on $|\phi^+\rangle$ in the $[3, 4, 2, 2]$ scenario. We verified that the Bell inequalitiy which is violated by the partially entangled state contains indeed marginal terms (see [LCMA]). This counterexample closes the possibility to generalize the theorem onto single-body correlator Bell inequalities. Therefore, the sets $\mathcal{V}(|\psi_\theta\rangle)$ and $\mathcal{V}(|\phi_+\rangle)$ are not contained one into the other and we cannot order $P(|\psi_\theta\rangle)$ and $P(|\phi^+\rangle)$ based on inclusion relations. Still, in Fig. 4.1 we provide numerical evidence for a wide range of scenarios which indicate that the probability of generating nonlocality from random measurements is always the largest for the maximally entangled state, and conjecture that the relation $P(|\psi_\theta\rangle) < P(|\phi^+\rangle)$ holds in general. This observation coincides with the numeric results of Ref. [LHBR10], which more recently were confirmed by Ref. [dRGP$^+$17].

We also considered two-qutrit states in the Hilbert space $\mathbb{C}^3 o \times \mathbb{C}^3$. Here, the notion of correlators is not uniquely defined, but one can generalize the definition

of correlators by using the roots of unity (see Ref. [SAT+16] for instance). A numerical optimization revealed that $|\Psi_3^\gamma\rangle$ with $\gamma \simeq 0.79$ violates a full-correlator inequality in the [2,2,3,3] scenario with projective measurements, while for the same settings the canonical maximally entangled state $|\Phi_3^+\rangle$ generates a local behavior. Not surprisingly, the inequality in question is of the CGLMP form (see [LCMA]).

In spite of the fact that our main result cannot be generalized to the qutrit case, an extensive numerical search of the [2,2,3,3], [3,3,3,3] and [4,4,3,3] scenarios with projective measurements suggests that the probability (4.2) is always the largest for $|\Phi_3^+\rangle$, as shown in Table 4.1. Thus, we conjecture that the state having the highest probability of generating a nonlocal behavior is the maximally entangled qutrit state $|\Phi_3^+\rangle$, and hence no anomaly should ever occur for our measure in this case.

γ	Probability for scenario:		
	[2,2,3,3]	[3,3,3,3]	[4,4,3,3]
0.25	0.0549	0.3021	0.6529
0.5	0.1033	0.5191	0.8913
0.6	0.1345	0.6131	0.9351
0.7	0.1649	0.6785	0.9577
0.79	0.1851	0.7117	0.9673
0.9	0.1977	0.7327	0.9729
1.0	0.2030	0.7382	0.9743

Table 4.1.: **Probability of violation for qutrits.** Random measurements were sampled uniformly according to Haar's measure, and applied to the parametrized qutrit state $|\Psi_3^\gamma\rangle$. The maximally entangled state ($\gamma = 1$ is the one achieving the largest probability of violation.

4.5. Multipartite case

It is also relevant to ask if our theorem (4.5) may generalize to the multipartite case, namely, if it could hold in a situation of N parties sharing N qubits. This situation was partially addressed by Liang *et al.* who numerically showed the probability that GHZ states $\frac{1}{\sqrt{2}}(|0...0\rangle + |1...1\rangle)$ violate the MABK inequalities from

random measurements rapidly increases with the number N of qubits. We successfully managed to prove that our theorem does hold for the case where N is even, showing that the GHZ state is the one with the highest probability to yield nonlocality among the family entangled states of the form $\cos\theta\,|0...0\rangle + \sin\theta\,|1...1\rangle$, when considering full-correlator inequalities and regardless of the number of measurements considered.

More precisely, if $|\psi_\theta^N\rangle = \cos\theta\,|0...0\rangle + \sin\theta\,|1...1\rangle$ denotes the partially entangled state of N qubits above mentioned and b_θ^N denotes the violation achieved of a full-correlator inequality from $|\psi_\theta^N\rangle$, then the following implication always holds: if $\theta \geq \theta'$ then $b_\theta^N > b_{\theta'}^N$. In other words, there is monotonicity of the Bell violation with respect to entanglement for any full-correlator inequality for this familly of states. Furthermore, this also implies monotonicity of the probability of violation, namely $P_{\langle\cdot\cdot\rangle}(|\psi_\theta^N\rangle) < P_{\langle\cdot\cdot\rangle}(|\psi_{\theta'}^N\rangle)$. For simplicity we refer the reader to Ref. [LCMA] for details about this generalization.

4.6. Anomalies in the steering case

We naturally adapt our measure and raise the question about entanglement anomalies in the steering framework: does the maximally entangled state have the largest probability of demonstrating steering from randomly drawn measurements? We show that measurements performed by Alice on a partially entangled state $|\Psi_d\rangle$ of any dimension generate an assemblage violating a steering inequality if and only if the same measurements on the maximally entangled $|\Phi_d^+\rangle$ state also do so. Such an observation is made possible through results that were already known by the quantum information community [QVB14, UMG14].

Theorem. Let $\{\sigma_{a|x}^\nu\}$ be the assemblage retrieved when Alice performs any arbitrary number of general measurements $\{M_{a|x}\}$ on $|\Psi_d\rangle$, a partially entangled state of any finite dimension. Let $\sigma_{a|x}^+$ be the assemblage retrieved when the same measurements $\{M_{a|x}\}$ are performed on the maximally entangled state of the same dimension. Then:

$$\sigma_{a|x}^\nu \text{ is not LHS} \;\Leftrightarrow\; \sigma_{a|x}^+ \text{ is not LHS}\,. \tag{4.10}$$

The proof of this implication comes directly from the equivalence between steering and non-joint-measurability [QVB14]. Randomly sampled measurements will be non-jointly-measurable with unit probability, in which case it is always possible to find a steering inequality for which any pure entangled state demonstrates steering [QVB14]. More precisely, it is always possible to write an LHS model

if the measurements of Alice are jointly measurable, regardless of the degree of entanglement of the shared state.

It follows that the volume of the set of measurements $\mathcal{V}^{(d)}_{\text{steer}}(|\Psi_d\rangle)$ leading to steering of the non-maximally entangled state $|\Psi_d\rangle$ is equal to the volume of the set of measurements $\mathcal{V}^{(d)}_{\text{steer}}(|\Phi^+_d\rangle)$ which lead to steering of the maximally entangled one. In particular, our measure would trivially imply that $P_{\text{steer}}(|\Psi_d\rangle) = P_{\text{steer}}(|\Phi^+_d\rangle) = 1$. This observation holds for any number of measurements and any dimension d. Thus, our measure does not provide any insight to discuss anomalies of nonlocality —or any other property of the quantum states— in the framework of steering, or at least not when restricting to pure states.

4.7. Discussion

In this Chapter we proposed a natural and operational measure of nonlocality which acts directly at the level of the quantum states and which simultanously encompases all Bell inequalities. With this measure we showed that no anomalies of nonlocality occur for two-qubit states for scenarios based on full-correlator inequalities. We showed that this result generalises to the multipartite case for an even number of parties. We also provided numerical evidence suggesting that our measure does not reveal anomalies in scenarios with systems of higher dimension or in scenarios with inequalities involving marginal terms. In particular, our results confirmed the numerical findings of Refs. [LHBR10, dRGP$^+$17]. In particular, Ref. [dRGP$^+$17] presented recently an exhaustive numerical search for systems of up to 5 qubits and qutrits, onto which up to ≈ 10 random projective measurements uniformly sampled according to the Haar measure were locally applied. Among several interesting numerical results, Ref. [dRGP$^+$17] found evidence suggesting that with our measure of nonlocality no anomaly appears for two-qubit and two-qutrit systems.

Our main result, presented in detail in Sec. 4.3, enables interesting operational implications beyond the fundamental study of entanglement and nonlocality. In a situation where one wants to check if given measurements are useful to violate a full-correlator inequality with a two-qubit state, thanks to our observation it is sufficient to check if a violation is retrieved from the maximally entangled state only. In the same manner, our theorem guarantees that considering the maximally entangled state is the best choice to succeed in a two-qubit nonlocality test lacking control over the measurements performed, as such a maximally entangled state would be the one with the highest probability to reveal nonlocality.

Our measure was then attempted to be adapted to the steering framework in Sec. 4.5, but in this case the equivalence between steering and non-joint-

measurability implied that our measure trivially yields a unit value for the probability to demonstrate steering from randomly sampled measurements for any pure entangled state of any dimension.

Finally, note that a downside of our measure is that it does not seem to have the potential to enable DI and semi-DI tasks, because it acts directly at the level of the states and therefore assumes a certain knowledge of them and of the measurements that are being implemented. For this reason in the next Chapters we come back to the standard use of inequalities to develop and implement protocols for genuine random number generation and device-independent quantum key distribution.

5. Certified random number generation

After having reviewed the basic concepts for genuine randomness certification in Sec. 2.4, we implement the first proof-of-principle experiment demonstrating one-sided DI random number generation in Sec. 5.1. Then, in Sec. 5.2 we show how genuine randomness can be further increased in experiments by tailoring the measurements and avoiding post-processing of the observed data. Finally, with a more refined setup, we manage in Sec. 5.3 to implement an extremal POVM with high fidelity, which allows to experimentally certify more than one bit of randomness from one entangled bit, both under semi-DI and under fully DI conditions.

5.1. Experimental one-sided DI randomness certification

In this Section we implement the methods for one-sided DI randomness certification (2.20) to the photonic three-qubit W state whose generation was explained already in Sec. 3.3. Since the methods can only be applied on a bipartite scenario we first analyze the reduced state ρ_{red}. Then, we shall consider bipartitions of the W state, namely, that two black boxes are held by a single party.

5.1.1. From reductions of the W state

The reduced state of the three-qubit W state $|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$ is obtained, after tracing-out *e.g.* the third party, to be $\rho_{\text{red}} = 2/3\,|\psi^+\rangle\langle\psi^+| + 1/3\,|00\rangle\langle 00|$, where $|\psi^+\rangle$ denotes the two-qubit maximally entangled state $|\psi^+\rangle = 1/\sqrt{2}(|01\rangle + |10\rangle)$. In Chap. 3 we showed that ρ_{red} is in fact steerable when applying the three Pauli observables on the untrusted box, with a theoretical violation —using (2.13)— of $r = 0.11$. We furthermore achieved an experimental violation of $r = 0.07 \pm 0.01$ (see Table 3.1).

It is therefore intuitive to expect that ρ_{red} should yield some genuine semi-DI randomness from one of the Pauli observables that is applied on the black box. Interestingly, no one-sided DI randomness could be extracted from ρ_{red}.

Indeed, after deriving the corresponding assemblage σ from ρ_{red} and from the Pauli observables, we found that $G_\sigma(x^*) = 1$ for any of the three possible measurement choices $x^* = \hat{X}, \hat{Y}, \hat{Z}$.

The fact that no one-sided DI randomness could be extracted from the reduced state of the three-qubit W state is unfortunate but interesting. This is analogous to a similar phenomenon, known as *bound randomness* [ACP+16], which arises in the fully DI scenario where the two parties hold untrusted devices. More precisely, in the fully DI scenario, bound randomness arises in nonlocal correlations for which the eavesdropper, Eve, can find out a posteriori the result of any implemented measurement. Thus, the fact that any reduction of the W state is steerable but does not allow for one-sided randomness certification, may tentatively be refered to as *one-sided bound randomness*: a form of steerable correlations for which an eavesdropper can predict the result of any of the measurements performed on the untrusted side.

Experimentally, we checked that the experimental data of each of the the reduced states does not reveal any amount of one-sided randomness, as predicted by the theory. Due to the unavoidable problem of finite statistics, we had to derive the steering inequality for randomness (from the dual of (2.20)) from the closest non-signalling assemblage σ^{phys} to the one observed in the experiment, σ. Then we applied the inequality to σ. In particular, this three-step method will also be applied in the following Subsection.

5.1.2. From bipartitions of the W state

In our experimental implementation of the photonic W state presented in Fig. 3.2, a physical bipartition of the state stems between the two photons produced. In this sense, it is natural to consider the photon encoding both polarization and path qubits as a single party, and analyze the amount of randomness of the outcomes $s = (a, b)$ retrieved when untrusted measurements are performed on such physical part of the system. Thus, the scenario presented in Fig. 5.1 turns out to be relevant and well suited to analyze our experimental data.

When two of the boxes are seen as a single untrusted measurement $m = (x, y)$ performed on some unknown quantum state, while the other qubit, C, remains trusted, we manage to certify $\log_2(3) \approx 1.58$ random bits from the outcome $s = 00, 01, 10, 11$ of the measurement m^* corresponding to the observables $\hat{X}$ and $\hat{Z}$ acting on the two-qubit subspace reduction of the W state.

Experimentally, we managed to certify 0.26 ± 0.04 bits from the above mentioned bipartition of the photonic W state. This value falls far from the theoretical value of $-\log_2(2/3) \approx 1.58$ bits. This discrepancy is due to the fact that the amount of randomness is extremely sensitive to the visibility v of the pure W

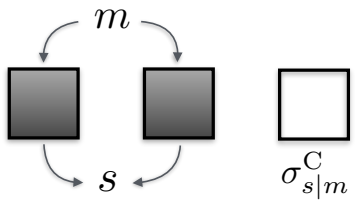

Figure 5.1.: **One-sided DI randomness from bipartitions.** Alice and Bob are thought as a single party holding two untrusted boxes, performing at each round a measurement m and obtaining some result s. This scenario allows us to analyze the amount of randomness of the result s when $\sigma^{C}_{r|m}$ is observed by Charlie.

state with respect to white noise. For instance, we observe that for $v = 0.994$ the number of one-sided DI random bits certified is already less than unity.

5.2. Optimization over experimental conditions

The experimental certification of 0.26 ± 0.04 semi-DI random bits from a bipartition of the three-qubit W state detailed in the previous section is a promising result to pursue the development of randomness certification with uncharacterized devices. However, the fact that this number is small (only 16%) with respect to the theoretically achievable amount of $-\log_2(2/3) \approx 1.58$ bits, draws considerable attention. Is there room for improvement of experimental conditions to increase this amount? From the technological perspective, it is of paramount relevance to quantitatively increase the efficiency —the number of random bits certified per use— of quantum random number generators. From the fundamental perspective it is desirable to explore the upper limits of genuine quantum randomness generation and in this way continue probing the limits of quantum theory. In this Section we first derive in Sec. 5.2.1 a three-step method which requires little experimental effort to increase by a notably large amount the randomness that can be certified from Bell experiments. (For simplicity we narrow our focus to the nonlocality framework, but the methods developed here are straightforwardly applied in future Sections to the steering framework). To show the performance of the method, we then apply it in Sec. 5.2.2 to a realistic model of optical Bell experiments, where certify up to four times more randomness than previous methods.

5.2.1. Method

In Section 2.4 we discussed how to retrieve the maximal amount of randomness available for Alice and Bob from an observed behavior $\mathbf{p}$, that is, the randomness optimized over all possible Bell inequalities. Still, there are several degrees of freedom in $\mathbf{p}$ that can be further optimized to provide even more randomness. More precisely, tailoring these degrees of freedom always leads to different behaviours, which in turn yields different –and hopefully higher– amounts of randomness.

Keeping as much data as possible. In particular, the number of outcomes o_A and o_B can be adjusted without much experimental effort. All loophole-free Bell experiments so far [HBD+15, SMSC+15, GVW+15] have relied violation of the CHSH inequality. This assumes the local observation of two outcomes per party. However, in addition to the two good outcomes, loss and imperfections lead to events where no detector clicks, resulting in a third outcome per party; this means that a local binning process was applied in all these experiments to reduce the size of the original behavior to two outcomes.

It is intuitive to expect that more randomness can be certified when binning strategies are avoided; any binning strategy represents a loss of potentially useful information. Still, it could be the case that the amount of certifiable randomness would not get diminished for some particular binning. Our results show that this is not the case in general. In fact, In Ref. [MSB+15] we explicitly showed how any binning strategy applied to CHSH correlations with inefficient detectors will systematically decrease the amount of certifiable randomness. Hence, to certify optimal amounts of randomness, Alice and Bob must ensure that the number of outcomes o_A and o_B is kept as high as possible.

Taking experimental parameters into account. The observed quantum behavior $\mathbf{p}$ possesses physical degrees of freedom that can be adjusted in the experimental setup to produce higher amounts of randomness. The solution of (2.21) can be minimized over all the possible realistic values that such parameters (which we label $\mathcal{P}$) can take. In this way, the optimal amount of randomness that can be certified to the order is now the solution of:

$$\begin{cases} G(x^*) \;=\; \min\limits_{\mathcal{P}} \;\; G_{\mathbf{p}}(x^*) \\ \\ \text{s.t.} \;\; G_{\mathbf{p}}(x^*, y^*) \text{ solves the SDP of eq. (4.4).} \end{cases} \tag{5.1}$$

In particular, notice that this program could optimize $G_{\mathbf{p}}(x)$ over the number of measurements m_A and m_B, which may be seen as implicit quantities in $\mathcal{P}$. In practice, program (5.1) is difficult to solve because the dependence of $\mathbf{p}$ in terms

of the physical parameters $\mathcal{P}$ is (highly) nonlinear. Still, a numerical nonlinear optimization can be carried with different algorithms, providing possibly sub-optimal, though still relevant, parameters. As mentioned, an analogous program to (5.1) is also realizable in the steering framework for $G_\sigma(x^*)$. In summary, our three-step method for optimal randomness generation is presented in Box 4.

Box 4. General directions for optimal DI randomness certification.

(i) Estimate the most general behavior $\mathbf{p}$, without any binning.

(ii) Construct $G_{\mathbf{p}}$, the device-independent guessing probability optimized over all possible Bell inequalities. See (2.21).

(iii) Optimize $G_{\mathbf{p}}$ over the parameters $\mathcal{P}$ that can be adjusted in the experimental setup. See (5.1).

5.2.2. Focus on optical Bell experiments

The methods presented above are general and can be adjusted to any bipartite Bell experiment. We focus and describe in the following the architecture of optical implementations based on polarisation measurements of entangled photons distributed from a spontaneous parametric down-conversion (SPDC) source (see Fig. 5.2). The source is characterized by three adjustable quantities: two squeezing parameters g_1 and g_2 and a total number of modes N onto which the photons may be distributed. Each mode locally splits into two orthogonal polarisations. In terms of bosonic creation operators, the unnormalized state produced by S is given by [CVSB$^+$15]:

$$\prod_{k=1}^{N} \exp\left[\tanh(g_1) a_k^\dagger b_{k\perp}^\dagger - \tanh(g_2) a_{k\perp}^\dagger b_k^\dagger\right] |0\rangle\,, \tag{5.2}$$

were $|0\rangle$ is the vacuum state associated to the $4N$ bosonic operators $a_1^\dagger, \ldots, a_{N\perp}^\dagger$, $b_1^\dagger, \ldots, b_{N\perp}^\dagger$, and the a-modes (b-modes) are distributed to Alice (Bob).

All the different types of losses including detectors inefficiencies are modeled, without loss of generality, by two beam-splitters (not shown in Fig. 5.2) placed at any point between the users and the source. The transmittance η of these beam-splitters is the overall detection efficiency of the experiment.

The measurements are performed with polarizing beam-splitters (PBS) and $\frac{\lambda}{2}$ half-wave plates (HWP) and $\frac{\lambda}{4}$ quarter-wave plates (QWP) which allow splitting

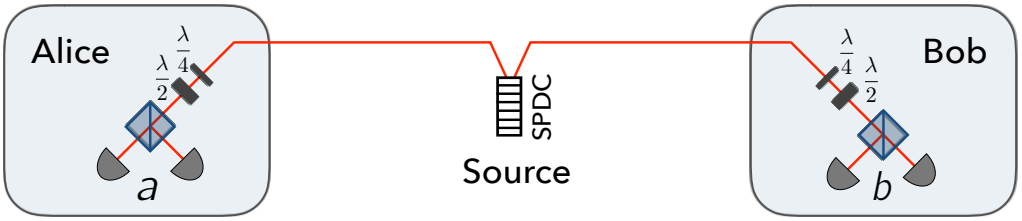

Figure 5.2.: Experimental setup for optical Bell experiments based on SPDC and polarization measurements. See main text and App. A for details.

the orthogonal modes along arbitrary directions [CMA+13, GMR+13, CVSB+15]. Each measurement u is fully characterized by two angles (θ_u, ϕ_u) defining a projection in the Bloch sphere. Each of the parties holds two detectors, which do not resolve photon number (half-circles in Fig. 5.2). Hence, for each detector only the outcomes "0=No click" and "1=Click" can be distinguished, and the maximal number of local outcomes (without binning) is $o_A = o_B = 4$.

5.2.3. Results

In this Subsection we apply the three step method presented in Sec. 5.2.1 to the optical setup whose modeling was described in Sec. 5.2.2.

Global randomness. To take full profit of the genuine randomness from the Bell experiment we consider the task of global randomness certification. This is strictly equivalent to the local case already described in (2.21), with the only difference that now we are interested in bounding the predictability of the two black boxes. In this case, Eve is simultaneously trying to guess the output of Alice and Bob when they chose measurements $x*$ and $y*$ respectively, and program (2.21) is transformed to:

$$\begin{aligned} G_{\mathbf{p}}(x^*, y^*) \;=\; & \max_{\{\mathbf{p}^e\}} \; \sum_e p\,(e, (a, b) = e | x^*, y^*) \\ & \text{s.t.} \quad \sum_e \mathbf{p}^e = \mathbf{p} \\ & \mathbf{p}^e \in \widetilde{\mathcal{Q}} \quad \forall e \end{aligned} \tag{5.3}$$

The difference between (5.3) and (2.21) is that now Eve requires $o_A o_B$ strategies $\{\mathbf{p}^e\}_e$, since she is guessing the output of the two parties. The objective function has also been adjusted accordingly, but the program itself remains the same.

Optimal randomness with $m_A = m_B = 2$ measurements per side. Optimal global randomness is retrieved from (5.1) upon optimization of all adjustable parameters, which include the number of measurements in the experiment. Optimizing G over m_A and m_B is of particular relevance for the setup that we consider as distinct rotation directions of the incoming modes can be achieved by adjusting the HWP and QWP, *i.e.* without the need of further experimental resources. Still, to illustrate the performance of our methods we consider first the simplest case $m_A = m_B = 2$.

We find that whenever the parties are restricted to $o_{\text{bin}} = 2$ outcomes, more global randomness is certified when no specific Bell inequality is considered. This was to be expected a and the line of research of [NSPS14, BSS14] (see dashed and dotted curves in Fig. 5.3). However, we improve considerably this expected result by suppressing the binning of the outcomes and letting $o = 4$, as we explained before (solid curve in Fig. 5.3). For $\eta = 1$ our methods certify 0.74 bits of global randomness per source use, four times more than the 0.19 bits that are certified from the CHSH inequality (we provide the Bell inequality that certifies this improvement in [MSB$^+$15]).

The numerical values of the optimal parameters $\mathcal{P}$ are given in Fig. 5.4 for several values of η. Intuitively, the ratio $t = \tanh(g_1)/\tanh(g_2)$ quantifies the degree of entanglement of the source, as (5.2) shows. For $\eta = 1$ optimal randomness is obtained from a "maximally entangled" state, *i.e.* $t = 100\%$, but as η decreases t also decreases. This was to be expected for the lower values of η, where nonlocality can only be certified with non-maximally entangled states [Ebe93]. Interestingly, for $\eta \approx 1$ the optimal measurements are not similar to the ones that intuitively maximize the violation of the CHSH inequality on two maximally entangled qubits (*e.g.* they are not mutually unbiased); see [MSB$^+$15] for the exact expressions. That is, the optimal measurements for optimal randomness certification are not the same as those maximizing the CHSH violation. The number of modes attains the maximal value that we allow ($N = 100$) whenever η is greater than $2\sqrt{2}-2$. For η smaller than this value, the single mode case $N = 1$ is sufficient to obtain maximal randomness; this fact was noticed in [CVSB$^+$15] for the maximization of the CHSH inequality violation. Finally, we have found that the improvement obtained when increasing the number of modes beyond ≈ 25 is very small.

Optimal randomness with more than two measurements. Our next goal is to see whether deploying more measurements yields an improvement in the number of random bits. In the previous subsection we considered the case $m_A = m_B = 2$; however, by adjusting the HWP and QWP located in front of their PBS, Alice and Bob can measure their incoming subsystem along any arbitrary polarisation

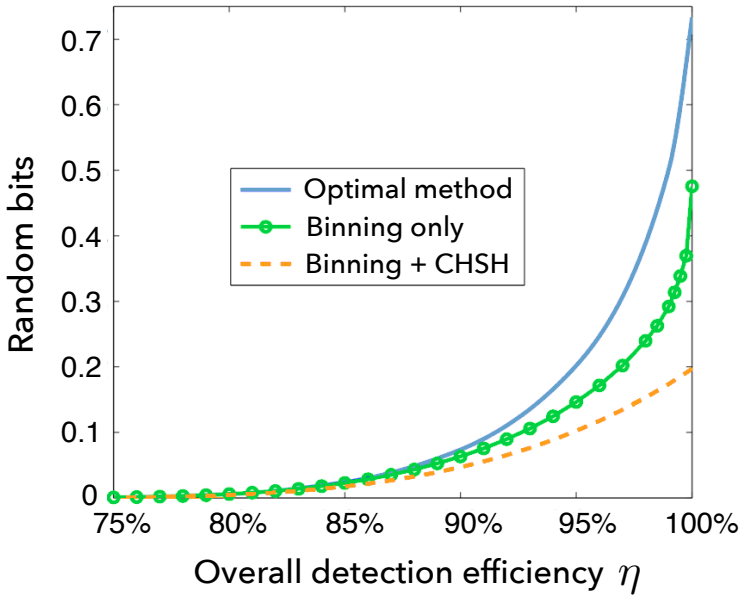

Figure 5.3.: Global randomness for the case $m_A = m_B = 2$. For the three curves, the parameters $\mathcal{P}$ are optimized at each point. The solid curves are the min-entropy of the solution of program (5.1) for $o_A = o_B = 4$ (optimal) and for $o_A = o_B = 2$ (binning).

direction of the Bloch sphere. These adjustments can thus be obtained with relatively low experimental cost, the main drawback being a non-negligible increase in the amount of statistical data (the size of $\mathbf{p}$ increases with $m_A m_B$).

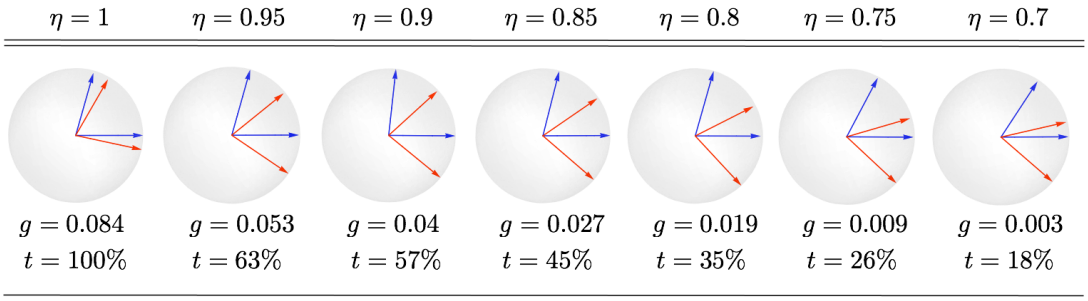

Figure 5.4.: Color online. Optimal parameters $\mathcal{P}$ for different values of η. t is the ratio between $\tanh(g_1)$ and $\tanh(g_2)$, while $g = \max(g_1, g_2)$. N always reaches 100. Blue (Red): optimal measurements for Alice (Bob) in the Bloch sphere representation.

Our results in Table 5.1 show that more measurements certify more randomness, even in scenarios for which a binning strategy had to be considered and $\mathcal{P}$ could not be fully optimized due to computational limitations. The time required to solve (5.1) becomes large as the number of measurements increases, since the total number of SDP variables describing the behaviours $\mathbf{p}^e$ in (5.3) increases as $(m_A m_B)^2$. The increase is less dramatic when *local* randomness is certified (equation (2.21)) *e.g.* from Alice's perspective, as there are only o_A (instead of $o_A o_B$) SDP matrices for each choice of $\mathcal{P}$.

SCENARIO	(2, 2)	(3, 2)	(3, 3)	(4, 3)	(4, 4)	(5, 5)
Total SDP variables	1348	3340	8392	15748	29620	$\sim 10^5$
Local random bits	0.454	0.459	0.519*	0.523*	0.557*	N/A

Table 5.1.: Local randomness certified for different scenarios for $\eta = 1$. The scenario specifies the couple (m_A, m_B). The * symbol is used when full optimization was not possible, and instead: *(i)* the optimization was only carried over the number of modes, with $g_1 = g_2 = 0.1$; *(ii)* the measurements were inspired from the chained inequality [BC90] and *(iii)* we considered 3 outcomes per party by locally binning the "no click-no click" and the "click-click" outcomes.

In particular, with four measurements per party we certify 0.557 local random bits. This is 3 times more than the amount that is certified from the CHSH inequality (≈ 0.17 bits) under the same considerations.

Experiments with only one detector per side The setup depicted in Fig. 5.2 has been hitherto central in our analysis as it captures the general architecture for Bell experiments with entangled photons. Unfortunately, state-of-the-art superconducting detectors, *i.e.* those which achieve detection efficiencies above 70% and thus enable a true Bell violation without post-selection, represent an extremely high experimental cost nowadays.

This situation can be alleviated (the cost can be reduced by half) by realizing that a Bell test can still be carried on with the use of only one detector on each arm of the experiment [CMA+13, GMR+13]. Given the techniques that we have shown so far, it is interesting to see how the optimal amount of randomness is affected. For a fixed overall detection efficiency η, how does the optimal amount of randomness that can be certified in an experiment with only one detector compare to the optimal amount of randomness that can be certified with two detectors?

The statistics of an experiment with only one detector are straightforwardly obtained from the statistics of an experiment with two detectors. As discussed in Sec. 5.2.2, the possible local outcomes of an experiment with two detectors are 00, 01, 10 and 11 where the first (second) number labels the outcome of the first (second) detector"0=No click" and "1=Click". Then, applying the local binning $\mathcal{B}_{1\text{Det}} = \{00 \to 0', \ 01 \to 0', \ 10 \to 1', 11 \to 1'\}$ on Alice and Bob's sides yields the statistics of the experiment without the second detector.

We observe that for $\eta \leq 0.8$ no disadvantage occurs if the second detector is removed: the optimal amount of local and global randomness than can be certified in both cases is $\sim 6 \times 10^{-4}$ bits. On the other hand, as η becomes close to 1 removing a detector negatively affects the optimal amount of randomness: for $\eta = 1$ the optimal amount of local (global) random bits certified with two detectors is ≈ 0.45 (≈ 0.73) bits, while with only one detector the optimal amount is ≈ 0.31 (≈ 0.34) bits.

5.2.4. Conclusion

Summarizing, in this section we have explicitly shown the benefits of optimizing randomness in a Bell experiment over the adjustable parameters in an experiment and over all possible inequalities, and the negative consequences that occur when information is lost through a binning of the resulting outcomes. We carefully analysed and characterized optical setups based on SPDC and certified up to four times more randomness when all of the physical parameters were optimized. To put it in a nutshell, here are the important facts to be aware of in order to retrieve optimal amounts of randomness from an optical Bell implementation based on SPDC *(and their experimental cost)*:

1. Keep the whole statistics and avoid binning the outcomes. *(no cost).*

2. Use as many polarisation measurements as possible. *(small cost).*

3. Use many modes to distribute the entangled photons. *(high cost in principle, but keep in mind that more than* ≈ 25 *modes will provide little improvement).*

4. For $\eta \approx 1$, the optimal measurements for randomness extraction are not the ones that maximize the violation of the CHSH inequality. *(no cost).*

5. For $\eta \leq 0.8$ it is enough to use a single mode to distribute entanglement and use a single detector per side. *(no cost).*

5.3. Experimentally certifying more than one random bit from one entangled bit

In the previous Section we focused our attention on optimizing the amount of randomness with little improvements of experimental conditions and a better processing of the data generated in a given Bell setup; namely, by keeping the entire statistics, adjusting the physical parameters and optimizing the guessing probability over all possible inequalities. As mentioned, the methods described for nonlocality straightforwardly apply for the steering framework.

A more fundamental question is to ask for the maximal amount of randomness that a given quantum state allows for. At the level of the quantum states, entanglement is the key resource to produce nonclassical correlations and in particular the two-qubit maximally entangled state, $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is considered as the fundamental entanglement unit, known also as an *entangled bit,*, or *e-bit*. If the two parties locally perform 2-outcome projective measurements on such an e-bit, at most 1 bit of local randomness can be certified from Alice's device (this situation corresponds to the case where the eavesdropper makes a fully random guess on the outcome a, as explained in Sec. 5.2). In fact, Ref. [AMP12] showed that this limit can always be achieved using 2 projective measurements per side, and even with arbitrary small amounts of entanglement.

Still, there exist non-projective measurements which allow for more outcomes, the so-called Positive Operator-Valued Masure (POVM) measurements, encountered already in Chap. 4. POVM measurements correspond to the most general formulation of a measurement in the theory of quantum physics. Can the use of POVM measurements yield more than one bit of local randomness from one entangled bit? If so, what is the maximal amount that such general measurements, can achieve? And most importantly, would such a quantitative theoretical improvement be substantial in a realistic situation, that is, within an experiment?

5.3.1. Background

In this Section we recall theoretical background to retrieve the maximum amount of genuine local randomness extractable from one entangled bit with the use of extremal POVM measurements, and briefly explain how this limit can actually be obtained with quantum correlations. Next, we show how such a POVM can be realized by an orthogonal (projective) measurement in a Hilbert space of larger dimension, by attaching an ancillary system to $|\phi^+\rangle$.

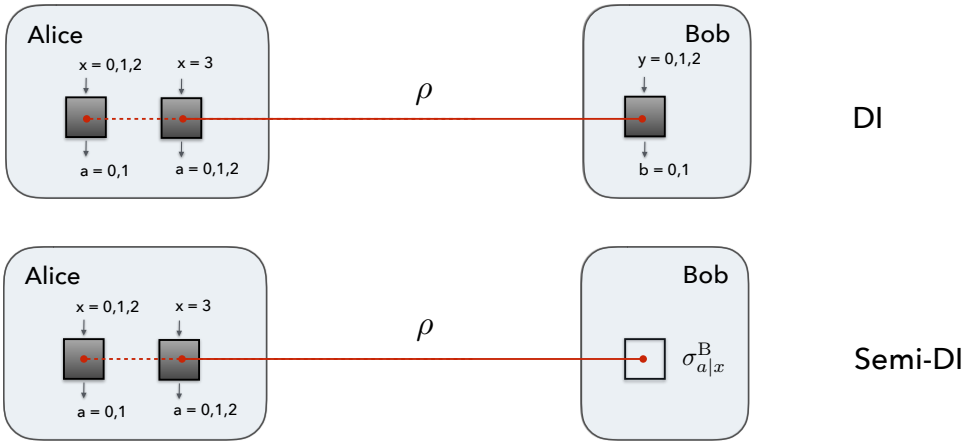

Figure 5.5.: **Scenarios for DI and semi-DI certification of more than one bit of randomness from one e-bit.** At each round Alice randomly chooses her measurement among a 3-outcome POVM and three 2-outcome projective measurements. In the DI scenario Bob chooses among three projective measurements, while in the semi-DI approach he applies tomographic measurements (*e.g.* the Pauli observables) to reconstruct his share of the state.

2 bits of local randomness. We start by stating a rather straightforward observation: no more than $2\log(d)$ bits of local randomness can be certified by measuring an entangled state of dimension $d \times d$. This follows from the fact that a POVM acting on space of dimension d can always be decomposed as a convex sum of POVMs of at most d^2 outputs [DPP05]. In the case of qubits, no more than 2 bits of local randomness can be certified, i.e. twice as much than using projective measurements [AMP12]. In Ref. [APVW16] two examples of qubit correlations saturating this bound were obtained, thus providing examples of optimal local randomness certification from one e-bit. The examples were obtained by providing Alice with projective measurements and a 4-outcome extremal POVM x^* with elements $\{M_{a|x^*}\}_a$ such that $\mathrm{Tr}\left[M_{a|x^*}\right] = \frac{1}{2}$ and $M_{a|x^*} = \frac{1}{2}|\psi_a\rangle\langle\psi_a|$ for all $a = 0, 1, 2, 3$. In particular the POVM x^* gives $P(a|x^*) = \frac{1}{4}$ for all a. The idea is to provide Bob with three tomographically complete measurements, the Pauli observables σ_x, σ_y and σ_Z, which simultaneously guarantee the presence of the e-bit and the extremality of the POVM through *self-testing* properties [MY98].

Scenario. Unfortunately, both examples of Ref. [APVW16] are quite sensitive to noise, as a fraction of (white) noise of the order of 1% makes the obtained randomness smaller than one bit. In particular, the first construction, which re-

quires 6 projective measurements for Alice, does not provide any advantage in terms of noise tolerance with respect to the second construction, which only requires 3 projective measurements on each side. A numerical search, based on the methods from Sec. 5.2 revealed that no improvement in terms of noise tolerance is obtained by having more than 3 measurements per side. In fact, in the task of certifying more than one bit of randomness the numerical optimization also revealed that roughly the same noise robustness to certify more than one random bit is achieved when considering an extremal POVM of three outcomes (instead of four), which reduces the complexity and cost of the experiment (see Table 5.2 and Fig. 5.8). For the reasons mentioned, we consider the scenario depicted in Fig. 5.5, which consists of one 3-outcome POVM for Alice labeled $x = x^* = 3$, and three projective measurements for each of the parties, labeled $x = 0, 1, 2$ and $y = 0, 1, 2$.

Neumark's theorem. To implement the POVM measurement x^* in her share of the e-bit, Alice needs to operate in a Hilbert space of larger dimension. Crucially, Neumark's theorem guarantees that any POVM can always be realized by extending the Hilbert space to a larger space, and performing orthogonal measurement in the larger space [NC00]. Concretely, suppose that Alice attaches an ancillary qubit C to her qubit A, then she applies some unitary U on the system AC and finally she performs a projective measurement of the coupled system AC in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. We label $\Pi^{\mathsf{AC}}_{a|x^*}$ the four projectors associated to this measurement. In this case, the joint statistics of the test, observed by Alice and Bob and given by Born's rule, read:

$$p(ab|x^*y) = \mathrm{Tr}\left[U \otimes \mathbb{1}_{\mathsf{B}} \left(|\gamma\rangle\langle\gamma| \otimes |\phi^+\rangle\langle\phi^+|\right) U^\dagger \otimes \mathbb{1}_{\mathsf{B}} \ \left(\Pi^{\mathsf{AC}}_{a|x^*} \otimes M_{b|y}\right)\right], \quad (5.4)$$

where $|\gamma\rangle$ denotes the initial state of the ancilla C. Using the fact that the trace operator is cyclic, we have:

$$p(ab|x^*y) = \mathrm{Tr}\left[\left(U^\dagger \Pi^{\mathsf{AC}}_{a|x^*} U \ |\gamma\rangle\langle\gamma| \otimes \mathbb{1}_{\mathsf{A}}\right) \otimes M_{b|y} \left(\mathbb{1}_{\mathsf{C}} \otimes |\phi^+\rangle\langle\phi^+|\right)\right]. \quad (5.5)$$

By taking first the partial trace over C, one finally arrives to:

$$p(ab|x^*y) = \mathrm{Tr}\left[\left\{\mathrm{Tr}_{\mathsf{C}}\left[U^\dagger \ \Pi^{\mathsf{AC}}_{a|x} \ U \ |\gamma\rangle\langle\gamma| \otimes \mathbb{1}_{\mathsf{A}}\right]\right\} \ \otimes M_{b|y} \ |\phi^+\rangle\langle\phi^+|\right], \quad (5.6)$$

and the term in brackets in (5.6) can be identified as the elements $M_{a|x^*}$ of a generalized, 4-outcome, measurement acting on Alice's qubit:

$$M_{a|x^*} := \mathrm{Tr}_{\mathsf{C}}\left[U^\dagger \ \Pi^{\mathsf{AC}}_{a|x^*} \ U \ |\gamma\rangle\langle\gamma| \otimes \mathbb{1}_{\mathsf{A}}\right]. \quad (5.7)$$

Note that a formula equivalent to (5.6) is obtained when Bob is trusted in the steering approach, producing the assemblage $\sigma_{a|x^*} = \mathrm{Tr}_{\mathsf{A}}\left[M_{a|x^*} \otimes \ \mathbb{1}_{\mathsf{B}} \ |\phi^+\rangle\langle\phi^+|\right]$ with $M_{a|x^*}$ given by (5.7).

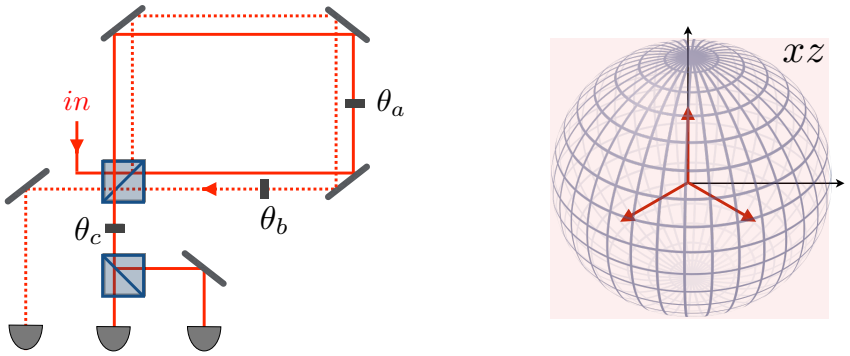

Figure 5.6.: **Implementation of extremal 3-outcome POVM measurement with double-path interferometer.** A PBS initially splits polarizations H and V into a clockwise and a counter-clockwise path inside the interferometer. By adjusting the rotation angles of the HWPs according to $\theta_a = 0$, $\theta_b = 2\sin^{-1}\left(\sqrt{\frac{2}{3}}\right)$ and $\theta_c = \frac{\pi}{2}$ the 3-outcome extremal POVM depicted in the right is obtained. The elements of this POVM are proportional to rank-one porjectors in the $(xz)-$plane.

5.3.2. Optical Setup

Alice's POVM measurement is implemented by using the available propagation modes of Alice's down-converted photon, when it is sent through a polarization-based double-path Sagnac interferometer (see Fig. 5.6). The propagation modes of a photon within this interferometer are not co-propagating and depend on its polarization state. This allows for conditional polarization transformations to be implemented with half-wave plates (HWPs) paramterized by rotation angles θ_a and θ_b placed inside the interferometer. These two propagation modes are then superposed again at the PBS. At one of the output ports of the interferometer an extra HWP with rotation angle θ_c and a polarizing beam-splitter (PBS) are set. From (5.7) and according to the HWP and PBS transformations (made explicit in App. A), the POVM elements are found to be:

$$
\begin{aligned}
M_{0|x^*} &= \begin{pmatrix} \cos^2\left(\frac{\theta_a}{2}\right)\cos^2\left(\frac{\theta_c}{2}\right) & -\frac{1}{2}\cos\left(\frac{\theta_a}{2}\right)\cos\left(\frac{\theta_b}{2}\right)\sin(\theta_c) \\ -\frac{1}{2}\cos\left(\frac{\theta_a}{2}\right)\cos\left(\frac{\theta_b}{2}\right)\sin(\theta_c) & \cos^2\left(\frac{\theta_b}{2}\right)\sin^2\left(\frac{\theta_c}{2}\right) \end{pmatrix} \\
M_{1|x^*} &= \begin{pmatrix} \cos^2\left(\frac{\theta_a}{2}\right)\sin^2\left(\frac{\theta_c}{2}\right) & \frac{1}{2}\cos\left(\frac{\theta_a}{2}\right)\cos\left(\frac{\theta_b}{2}\right)\sin(\theta_c) \\ \frac{1}{2}\cos\left(\frac{\theta_a}{2}\right)\cos\left(\frac{\theta_b}{2}\right)\sin(\theta_c) & \cos^2\left(\frac{\theta_b}{2}\right)\cos^2\left(\frac{\theta_c}{2}\right) \end{pmatrix} \\
M_{1|x^*} &= \begin{pmatrix} \sin^2\left(\frac{\theta_a}{2}\right) & 0 \\ 0 & \sin^2\left(\frac{\theta_b}{2}\right) \end{pmatrix}
\end{aligned}
\tag{5.8}
$$

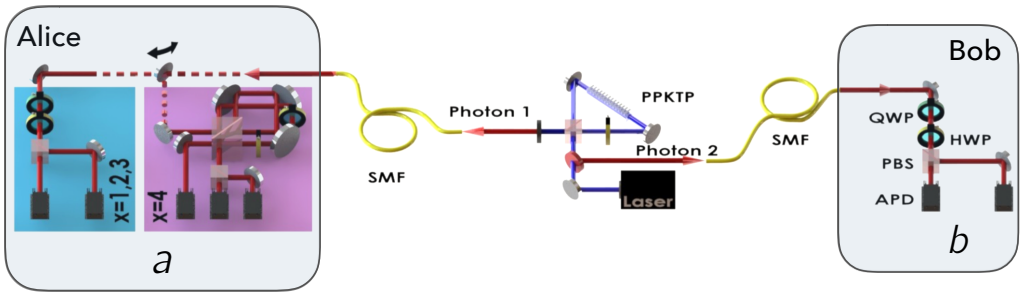

Figure 5.7.: **Experimental setup.** A type-II PPKTP crystal is pumped by a continuous wave 405 nm laser to generate 810 nm polarization-entangled photons. The non-linear crystal is placed inside an intrinsically phase-stable Sagnac interferometer, which is composed of two laser mirrors, a HWP, and a polarizing PBS cube. The clockwise and counter-clockwise propagating modes of the generated pair of photons overlap inside the interferometer resulting in the photonic state given by (5.2). High-quality narrow bandpass (FWHM of 0.5 nm) filters centered at 810 nm are used to ensure phase-matching conditions. We use a high-resolution coincidence field programmable gate array electronics to implement 500 ps coincidence windows, thus drastically reducing the accidental coincidence count probability to less than 10^{-5} . The measurements $x, y = 0, 1, 2$ are implemented in each laboratory using high-quality polarizing optical components. Alice's measurement $x = 0$ is a three-outcome POVM which is implemented using the double-path interferometer.

In particular, when taking the values for the rotation angles of the HWPs $\theta_a = 0$, $\theta_b = 2\sin^{-1}\left(\sqrt{\frac{2}{3}}\right)$ and $\theta_c = \frac{\pi}{2}$ (See App. A also) the elements in (5.8) become:

$$M_{0|x^*} = \begin{pmatrix} \frac{1}{2} & \frac{-1}{2\sqrt{3}} \\ \frac{-1}{2\sqrt{3}} & \frac{1}{6} \end{pmatrix}, \quad M_{1|x^*} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2\sqrt{3}} \\ \frac{1}{2\sqrt{3}} & \frac{1}{6} \end{pmatrix}, \quad M_{2|x^*} = \begin{pmatrix} 0 & 0 \\ 0 & \frac{2}{3} \end{pmatrix}. \tag{5.9}$$

It can be checked that with this choice $\mathrm{Tr}\left[M_{a|x^*}\right] = \frac{2}{3}$ for all a, and furthermore each element is proportional to a rank-one projector in the xz-plane, pointing to the vertices of an equilateral triangle in the Bloch sphere (see Fig. 5.6).

In our implementation, which is based on the scenario from Fig. 5.5, we produce pairs of photons entangled in polarization degrees of freedom. The quality of our implementation allows to observe a two-photon visibility of 99.7 ± 0.2 extracted from row coincidences detection, that is, without extra manipulation of the observed signal for the calculation of $P(ab|xy)$. The details of our experimental

methods are explained in the captions of Fig. 5.7.The binary projective measurements corresponding to $x, y = 0, 1, 2$ are implemented by using a set composed of a quarter wave-plate (QWP), a HWP, a PBS, and high- efficiency polarizing films placed in front of each detector (not shown in Fig. 5.7). Alice's measurement labeled by x = 0 is the POVM measurement with three outcomes implemented according to Fig. 5.6, as discussed in the previous paragraphs. The down-converted photons are registered in coincidence using Perkin-Elmer single-photon avalanche detectors with an overall detection efficiency of 15%.

5.3.3. Results

	3-outcome POVM		4-outcome POVM	
	White	Dephasing	White	Dephasing
Device-independent	99.2	98.4	99.3	98.3
Steering (Semi-DI)	98.7	93.3	98.4	93.3

Table 5.2.: **Theoretical results.** Critical weights v^* (%) to certify more than one bit of randomness from the state initial state $v\,|\phi^+\rangle\langle\phi^+| + (1 - v)\rho_{\text{noise}}$, for two types of noise: white noise, which draws the state to a maximally mixed state $\rho_{\text{noise}} = \mathbb{1}/4$, and dephasing noise, which is less destructive, and for which $\rho_{\text{noise}} = (\sigma_z \otimes \mathbb{1}_B)\,|\phi^+\rangle\langle\phi^+|\,(\sigma_z \otimes \mathbb{1}_B)^\dagger$.

For the 3-outcome POVM case, in the device-independent approach, we consider that A can perform a measurement among the 3-outcome POVM parametrized by $(\theta, \phi, \theta_a, \theta_b, \theta_c)$ and three PMs parametrized by angles $(\theta_i^A, \phi_i^A)_{i=1,2,3}$, while Bob can perform 3 PMs parametrized by $(\theta_j^B, \phi_j^B)_{j=1,2,3}$. In the steering approach A's side is unchanged but now Bob performs tomography on his system, which can be achieved by measuring Pauli observables σ_x, σ_y and σ_z, for example.

The 4-outcome POVM is parametrized by $(\theta, \phi, \theta_a, \theta_b, \theta_c, \theta_d, \phi_d)$, and A can still choose among this POVM and 3 PMs. In the device-independent approach, Bob can perform now 4 PMs parametrized by $(\theta_j^B, \phi_j^B)_{i=1,2,3,4}$, while in the steering approach he keeps performing tomography on his system.

Following the methods of the previous Section for optimal randomness certification, we numerically searched for the optimal parameters $\vec{\lambda}^*$ that allow the lowest value of the critical weight v^*. The values of v^* obtained for the device-independent approach and for the steering approach are exposed in Table 5.2, for the two different noise models considered. In particular, little improvement on

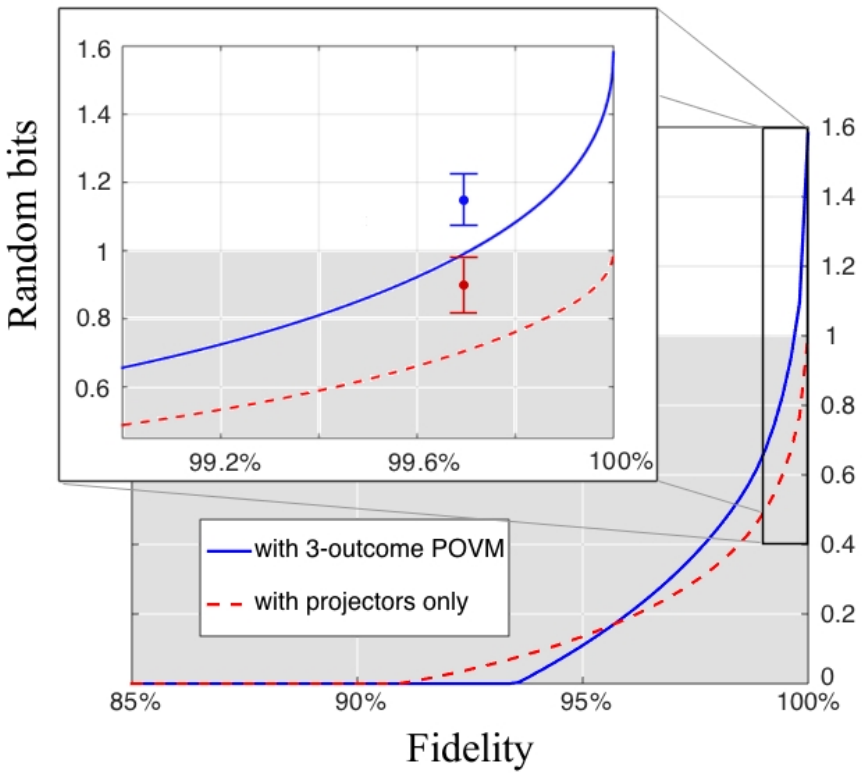

Figure 5.8.: **Experimental results in the DI framework.** The experimental fidelity of the state is $\approx 99.7\%$. The theoretical curves were obtained assuming the white noise model, which is a worse case assessment producing completely uncorrelated results and thus systematically lies below the experimental points.

was found by considering more than 3 projective measurements per side, and by employing a 4-outcome measurement rather than 3-outcome one.

In the semi-DI case, the measurements of Alice which provided the lowest values for v^* where the Pauli observables. In the full DI case, the best measurements found are those which maximize the violation of the chained inequality in the XZ plane: defining the operator $R(\theta) = \frac{1}{2}(\mathbb{1} + \cos\theta\hat{\sigma}_z + \sin\theta\hat{\sigma}_x)$, the Bloch vectors associated with the first outcome $x = 0$ are $M_{0|1} = R(\frac{\pi}{6})$, $M_{0|2} = R(\frac{\pi}{2})$ and $M_{0|3} = R(\frac{5\pi}{6})$ for Alice, and $M_{0|1} = R(0)$, $M_{0|2} = R(\frac{\pi}{3})$ and $M_{0|3} = R(\frac{2\pi}{3})$ for Bob. For the 3-outcome POVM the best parameters found are those yielding the extremal POVM detailed in Fig. 5.6. For the 4-outcome POVM, the optimal parameters found correspond to the extremal POVM used by Ref. [APVW16] and whose Bloch vectors point to the vertices of a tetrahedron.

The experiment was thus performed with the parameters above mentioned for the 3-outcome POVM, yielding a collection of observed experimental frequencies $f(ab|xy)$. Retrieving the optimal amount of randomness from these observed experimental frequencies $f(ab|xy)$ is not straightforward because the behavior obtained upon normalizing these frequencies does not satisfy the nonsignaling conditions defined in Sec. 2.2 due to the finite statistics regime of any implementation. This same problem was encountered when analysing the amount of one-sided randomness form the experimental data in Sec. 5.1.

To circumvent the signaling problem in the DI case we used the *Collins-Gisin parametrization* to construct a nonsignalling behavior $\mathbf{p}$. The Collins-Gisin parametrization discards all the statistics about the last outcome of each measurement (indeed, such statistics are implicit in the normalization condition when the behavior satisfies nonsignaling) enforcing in this manner the nonsignaling constraints. In the semi-DI case, we used a least-squares optimization to find the closest nonsignaling assemblage to the experimental data, just as in Sec. 5.1. From the nonsignaling behavior and the nonsignaling assemblage we obtained the desired inequalities, which come from the dual formulation of programs (2.21) and (2.20), as explained in Sec. 2.4.

In the full DI approach our methods finally managed to certify 1.18 ± 0.08 bits of genuine randomness. As a matter of comparison we also calculated the randomness we can obtain from our setup using only projective measurements to be 0.929 ± 0.085. In Fig. 5.8 we compare our experimental data with a simulation of the protocol assuming a pure maximally entangled state under the influence of the a depolarizing channel. In the semi-DI approach Bob's measurement devices can be trusted to be perfectly calibrated. In this case, we were able to certify 1.27 ± 0.14 bits of randomness, which is considerably more than the amount retrieved in the DI case.

5.3.4. Conclusion

While our results demonstrate the possibility of achieving high-quality DI-RNG with current technologies, we hope that it is just the starting point for a new generation of DI-RNG. There is still room for several improvements both in the theoretical and experimental side. In particular, more robust strategies are welcome, and overcoming natural limitations as low detection efficiencies would be desirable, since in this proof-of-principle experiment we assumed fair-sampling and discarded all round with inconclusive results. Following the line of research of Ref. [BKG+17] If could also be appealing to perform a statistical analysis of our experiment beyond the i.i.d. case.

5.4. Discussion

In this Chapter we have presented the first proof-of-principle experiment demonstrating one-sided DI random number generation. We found that the number of random bits certified (0.26 random bits) in this experiment was very distant from the theoretic value (1.58 random bits), which motivated us to introduce methods to increase genuine randomness in experiments by tailoring the measurements and avoiding post-processing of the observed data. The performance of these methods was first theoretically applied to bipartite optical Bell experiments, increasing the number of random bits certified by up to four times. Second, the methods were experimentally used in an ultra-high visibility setup, where we managed to implement an extremal POVM with high fidelity, which allowed us to experimentally certify more than one bit of randomness from one entangled bit, both under semi-DI and under fully DI conditions.

We became aware of another Bell-type randomness generation setup based on SPDC, which considers path entanglement and displacement measurements [VSB$^+$15]. For this setup a CHSH optimization —as in [CVSB$^+$15]— was derived; it could be interesting to apply our methods to derive the optimal amount of randomness that this recent experimental setup based on SPDC allows for.

It is also worth noting that new genuine random number generation techniques have recently been exposed to deal with the problem of finite statistics that was encountered along the experiments of this Chapter. In particular, Ref. [NSBSP16] has introduced protocols secure against classical side information, that rely on the estimation of an arbitrary number of Bell expressions or even directly on the experimental frequencies of measurement outcomes. Ref [BKG$^+$17] introduced and experimentally demonstrated a new protocol secure against nonsignalling eavesdroppers which performs well in experimental regimes characterized by low violation of Bell inequalities. Finally, Ref. [LaYZB$^+$17] recently introduced estimates in the i.i.d. regime converging to the underlying quantum distribution faster than the relative frequencies of the experiment. We note however that although these References might improve the randomness rate, the approach that we have considered —based on the min-entropy of the guessing probability— has the crucial advantage of being directly linked to the secret key which is achievable when considering the DIQKD task; this will in fact be the matter of the following Chapter.

6. Loss: the main issue for DIQKD

In this Chapter we present techniques for realistic DIQKD, a task which, in contrast with the certification of genuine randomness, is still experimentally awaited. Indeed, DIQKD is experimentally more challenging than the randomness certification task because the devices are far from each other and transmission loss increases exponentially over channels, which rapidly opens the detection loophole. In Sec. 6.1 we review plausible solutions, based on heralded preparation, to the problem of closing the detection loophole at long distances. Then in Sec. 6.2 we explain how loss also negatively affects the information reconciliation step of the protocol, which is an issue that has remained mostly unaddressed so far. We show how this issue can be alleviated by evaluating the optimal amount of randomness from the post-processed data of conclusive rounds, which turns out to be a direct application of the methods exposed by Ref. [TdlTB+16] in the context of genuine random number generation.

6.1. Detection loophole in the context of DIQKD

Loopholes in the context of DIQKD. Recall the DIQKD scenario presented in Fig. 2.3. Since Alice and Bob are each located in a secure place and control the information going in and out of their locations, the value of the inputs x and y and of the outputs a and b does not leak out unwillingly of Alice's and Bob's secure place. Thus, DIQKD is not affected by locality loopholes [BCP+14]. In fact, the locality loophole only becomes an issue if one cannot guarantee that the information on the choice of input is not transmitted from one device to the other. But if the devices can leak unwanted information to break the protocol, why shouldn't they simply broadcast, for instance to the eavesdropper, the outputs used to construct the secret key? In our view, making a distinction between inputs and outputs is rather arbitrary and artificial in this context[1]. Among several other loopholes affecting Bell experiments [Lar14], DIQKD is principally difficult experimentally because of the detection loophole, which sets a critical overall detection efficiency η for the observation of conclusive outcomes in the experiment. Roughly speak-

[1] This of course does not mean that the locality loophole is not relevant in other contexts in which Bell inequalities are tested.

ing η is the product of the efficiencies of all the physical processes (transmission, coupling, detection, ...) occurring between the source and the users. In particular, if the overall efficiency of the test is below a critical η, security can no longer be guaranteed (see for instance Ref. [GLLL$^+$11a]).

The detection loophole has been successfully closed first in Bell experiments based on light-matter interaction [RKM$^+$01, ABW$^+$09, HKO$^+$12] and then in purely optical-based ones [CMA$^+$13, GMR$^+$13]. More recently, three experiments managed to successfully produce a loophole-free Bell test [HBD$^+$15, GVW$^+$15, SMSC$^+$15].

As seen in the previous Chapter, these loophole-free Bell experiments directly enable device-independent random number generation, which relies on the same security assumptions than DIQKD for the two boxes used in the protocol, but with the difference that the two boxes might be arbitrarily close to each other in the randomness certification case. Thus and contrary to DIQKD, experimental setups for genuine randomness certification do not need to deal with the problem of long distances, as was confirmed in Chap. 5.

Indeed, in spite of the technological advances recently made to achieve higher detecion efficiencies in Bell experiments, DIQKD remains experimentally difficult at long distances due to the exponential decrease of transmission efficiency in the channel separating the two parties. In fact, in the standard DIQKD protocol (see Fig. 2.3), with polarization entangled pairs of photons used as information carriers and with current optic fibre technology, the detection loophole is already opened for a distance of the order of $\approx 4\ km$ [GLLL$^+$11b].

Partial solutions. It is worth noting that partial solutions -namely, semi-device independent approaches- to the problem of DIQKD have been developed in the recent years. One first relaxation to this problem is that of Measurement-Device-Independent Quantum Key Distribution (MDIQKD) [LCQ12], in which the two parties willing to share a secret key prepare specific quantum states that are sent to a measurement station in between them. The state preparation is device-dependent, as the protocol relies on the preparation of specific quantum states for each round, but the measurement process in the middle remains, indeed, device-independent. Very recently, MDIQKD has been experimentally demonstrated at high rates with continuous variable systems [POS$^+$15, YCY$^+$16]. Another possibility for relaxing DIQKD consists of assuming that one of the two parties trusts his measurement apparatus while the other party remains untrusted. This relaxation is often known as One-Sided-DIQKD [TR11, BCW$^+$12] and is formally based on steering correlations [WJD07, SNC14]. Finally, one last semi-device-independent approach worth to mention consists on assuming that the dimension of the states prepared in the protocol is always bounded. Recently, security

proofs have been derived under such "bounded dimension" assumption for different prepare-and-measure QKD protocols [PB11, WP15]. These three relaxations discussed here are certainly easier to implement than DIQKD and provide higher key rates. However, the price to pay at the level of security seems to be high, since the corresponding setups remain vulnerable to hacking attacks on the internal working of some of the devices used, unless one has a tomographic control of *everything that happens* at the trusted sites, which seems rather unrealistic, as explained already.

Intuitively speaking, a general solution to the detection loophole problem consists on having *some way* to guarantee that the photons arrive to Alice and Bob before they decide which measurement they will perform. This requires an auxiliary measurement, which announces to the users that their system has arrived without destroying its carried information. It is crucial that the auxiliary measurement remains independent of the choice of settings that Alice and Bob make, since otherwise Eve could tailor an attack announcing the arrival of the systems depending on the choice of x and y. In this case, the nonlocality of the correlations could be faked with classical resources [GLLL$^+$11b]. In the following we present two types of solutions which use such auxiliary measurement to avoid the detection loophole; in the first solution the auxiliary measurement is directly held by the parties, while in the second one it is made by a third party.

Local heralding. The first solution to overcome the problem of channel loss in DIQKD was realized by Gisin, Pironio and Sangouard [GPS10]. The scheme is based on the heralded noiseless qubit amplification [RL09], which given a state with a vacuum and single-photon component $\alpha|0\rangle + \beta|1\rangle$, it amplifies with some non-zero probability the single-photon component $\alpha|0\rangle + G\beta|1\rangle$, up to normalisation, with $G > 1$. The success probability is smaller for higher values of the gain factor G. Then idea of [GPS10] is to use the heralded amplification as an approximation to a quantum non-demolition (QND) measurement at Bob's site to herald to him the arrival of his photon, without destroying its carried information (see top Fig. 6.1). In this way, the source can now be placed next to Alice (to avoid loss on her side of the channel), and Bob only measures his system whenever the amplification measurement succeeds.

The source in Ref. [GPS10] is assumed to produce pairs of polarization entangled photons (5.2). To perform the noise-less amplification, at each round Bob inserts two single photons with orthogonal polarizations on a beam-splitter of transmittance $T \approx 1$. The reflected modes are jointly measured with his input mode via a Bell state measurement (this defines the amplification measurement). Whenever two clicks are observed in two of the detectors corresponding to orthogonal polarizations at the Bell state measurement, the transmitted mode (output

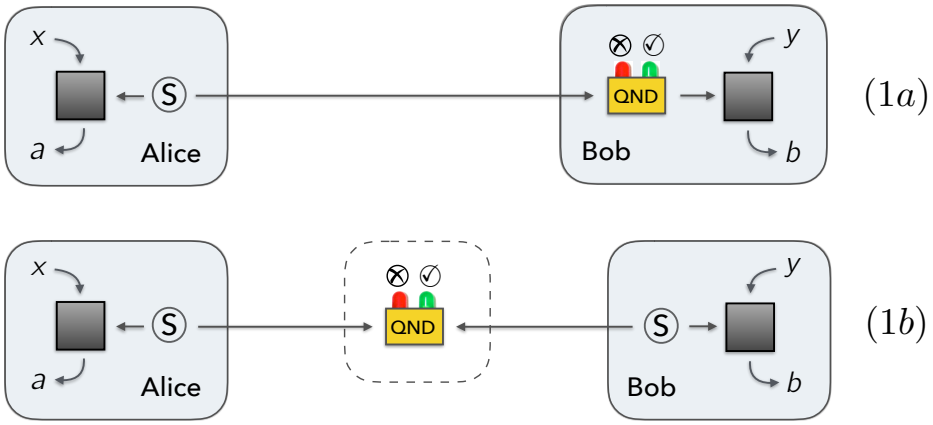

Figure 6.1.: **Solutions to implement DIQKD.** In DIQKD, Alice and Bob are in secure locations (black squares) from which they control information leaks. They receive from a source S a quantum state possibly prepared by Eve, onto which they perform randomly sampled measurements labelled x and y, producing outcomes a and b. The devices are treated as black-boxes since the only assumption made is that they produce a behavior $\mathbf{p} = \{p(ab|xy)\}$ compatible with the laws of quantum physics. To prevent channel loss from opening the detection loophole in practical situations, an additional signal is required to herald the successful arrival of the state. *(Top, 1a)*: This heralding signal may be the outcome of a QND measurement locally performed by one of the parties. *(Bottom, 1b)* Alternatively, the measurement can be performed by a third party, which later publicly announces which rounds were heralded.

mode) is projected to the original input state (see the top of Fig. 7.4 for a refined version of the heralded qubit amplification scheme). Heralded qubit amplification has been observed in a proof-of-principle experiment recently, first with polarization entangled pairs of photons in the visible regime [KXRP13], and subsequently in the telecom regime with time-bin entangled pairs of photons [BPM+16], although without closing the detection loophole. This represents an important achievement for the future of DIQKD. Especially, since these setups are entirely optical, they potentially allow for high repetition rates ($\approx 10^8$ *Hz* [GPS10]). A similar proposal by Curty and Moroder managed to slightly enhance the rates and decrease the critical efficiencies of the qubit amplifier [CM11]. Such proposal is based on standard quantum relays for entanglement swapping with linear optics, but for the previously mentionned reasons, it also represents a great challenge. Another proposal, by Pitkanen et al. [PMW+11] slightly modified the scheme of

Gisin *et al.* to discard several false-positive events at the heralding measurement, achieving a larger robustness to losses. This proposal will be presented with detail in the next Chapter.

A different alternative to implement DIQKD with a QND measurement following the architecture of top of Fig. 6.1 was proposed in [MBA13] with light-matter interaction systems, see also [BYHR13]. In these schemes, the entanglement between photon pairs is transferred to solid state (spin) qubits mediated by cavity QED interactions. As this transfer is achieved in a heralded way, the spin is only measured when the transfer succeeds. The main advantage of such light-matter interaction schemes is that the spin state can subsequently be measured with near unit efficiency, the drawback being the fact that such spin read-out measurements take in general long times, which considerably limit the attainable repetition rates. Also, inefficient frequency conversion processes might be needed in order to successfully transfer the photonic state of the incoming system into the cavity. Note that very recently, such heralding mapping of a photonic qubit into an atomic state within a cavity has been experimentally achieved with a $\approx 90\%$ fidelity [KRRR15]. The DIQKD scheme based on spin-coupled cavities of Ref. [MBA13] will be thoroughly analysed in the following Chapter.

Post-selection with a third party. A different approach for overcoming channel loss in Bell experiments was proposed by Bell himself [Bel87]. The key idea is to record an additional signal to indicate whether the required state was successfully shared between Alice and Bob. This idea has been developed in entanglement swapping protocols [PBWZ98] and is to some extent the basis for quantum repeater technologies [BDCZ98, MKL$^+$14]. For concreteness, and without loss of generality, such additional signal can be seen as the outcome c of an untrusted measurement performed by a third party, Charlie, located somewhere between Alice and Bob (see bottom of Fig. 6.1). Crucially, the outcome c has to be independent of the choices of measurements and outcomes made by Alice and Bob. In a standard Bell experiment, this can be guaranteed through space-like separation. In DIQKD, this independence is guaranteed by default as Alice and Bob have full control of all the information about a, b, x and y that exits their secure locations.

Hence, by conditioning the validity of rounds on the outcome c, failed distribution events (those for which Alice and Bob's particles sent to Charlie got lost in the channel) can be safely excluded at the end of the protocol. In other terms, because of the independence of c from x, y, a and b, the scheme depicted at the bottom of Fig. 6.1 can be simply seen as a heralded preparation from Charlie to Alice and Bob, with the remarkable advantage that no channel loss occurs between the sources S and the main users.

This idea has been implemented in the recent years in several light-matter inter-

action systems, successfully closing the detection loophole [PAM+10, HKO+12], and even attaining a loophole-free realisation [HBD+15]. Initially, matter-photon entanglement is created at each site. Subsequently, photons are sent to Charlie who performs a joint measurement that swaps the entanglement to the matter spins. Alice and Bob then read-out their spins with near unit efficiency. Finally, using classical communication, only rounds for which Charlie's measurement succeeded are kept. As mentioned earlier, the principal inconvenient of working with matter systems is the slow times required to perform the read-out (tipically few μs). Naturally, this strongly limits the number of secret bits that can be certified per time unit. Thus, an interesting alternative would be to analyze the architecture for DIQKD of the bottom of Fig. 6.1 within all-optical implementations, which potentially allow for much higher repetition rates. We will report on this matter in the following Chapter.

Conclusion. There exist two distinct architectures to overcome the difficult problem of channel loss in the frame of DIQKD physical implementations. The main drawback of the first method (local heralding) with respect to the second one (post-selection with a third party) is the necessity for an ancilla to perform the QND measurement. It is difficult to say if the future development of quantum memories will soon be sufficient to consider seriously the use of such ancillary systems, but for the time being, the second solution seems easier to achieve. In fact, as we mentioned earlier, only the second solution has successfully closed the detection loophole, and in several occasions [PAM+10, HKO+12], recently together with the locality loophole [HBD+15].

It is also worth noting a general trade-off occurring in both solutions, between high detection efficiency and high repetition rate. The use of matter systems (spins) allows for high detection efficiencies, but the repetition rate is strongly limited by the long times required to prepare and read-out the spins. On the other hand, entirely optical systems benefit from high repetition rates as measurements are generally fast and no re-initialization of the system is required at each round, but the detection process in such optical systems is difficult due to coupling losses and inefficiency of photo-detectors. Near future development of either photo-detectors or faster fluorescent methods for matter systems could lean the balance in favor of either purely optical systems or matter-based ones.

6.2. Information reconciliation with losses

In the previous section we showed how the detection loophole issue in the context of long-distance Bell experiments can be circumvented by means of an auxiliary

measurement. Unfortunately, a loophole-free Bell test is not sufficient to distill a positive number of secret key bits, because the information reconciliation term, the conditional entropy $H(A|B)$, must be included in (2.22). In this Section we first show how loss negatively affects $H(A|B)$. Indeed, Bob cannot correlate his result to Alice's if he did not obtain a conclusive result. Then we introduce a post-processing method —which does not open the detection loophole— to alleviate this issue. The idea is to decrease the value of $H(A|B)$ by looking only at those conclusive events, while maintaining some randomness in the output of Alice.

Conditional entropy in the presence of loss. From a general perspective, whenever Alice and Bob share correlations $\mathbf{p}$ which satisfy $G_{\mathbf{p}}(x^*) < 1$, they can certify a number $-\log_2 G_{\mathbf{p}}(x^*)$ of private random bits in the outcome a observed by Alice from her measurement x^*, as explained in Sec. 2.5. However, this does not imply that a positive key can be distilled, as the information reconciliation term, the conditional entropy $H(A|B)$, must be included in (2.22). Recall that $H(x^*|y^*)$ is the number of bits per round that have to be published from the data of measurements x^* and y^* in order to reconcile the two bit strings.

Furthermore, when considering lossy setups, one must also account for the destructive impact of loss on $H(A|B)$. However, all proposals aiming towards a physical implementation of DIQKD that we could find in the literature, with the exception of [PMW+11] do not take into account the fact that loss negatively affects the term $H(x^*|y^*)$. In fact, all these references [GPS10, CM11, MBA13, MSBB+13, STS15] apply a variation of the Devetak-Winter (DW) formula [DW05] in the context of DIQKD security against collective attacks [ABG+07]. (To some extent, the DW formula is equivalent to eq. (2.22)). This variation of the DW formula accounts indeed for loss effects on the min-entropy part of the secret key, but it assumes that $H(x^*|y^*)$ is estimated from the post-selected rounds for which a conclusive event was recorded both for A and B (see [GPS10] for the derivation). In our view, there is no justifiable reason for such a post-selection.

Let us analyze the situation carefully. For instance, consider the following simple strategy that A and B may perform in presence of loss. They decide always to output the value 0 whenever no photodetection click was recorded. Here we are assuming that the auxiliary QND measurement has succeeded and hence Alice and Bob have successfully received their share of the state. Thus, loss in this context refers to local detection efficiency parameterized by η_d. Naively, restricting to conclusive outcomes, $H(A|B) = 0$. Although this remains true if loss occur at both sites, $H(A|B)$ crucially does not vanish if loss occurs only at one of the sites.

Suppose that Alice and Bob retrieve 2 conclusive outcomes $0, 1$ and one inconclusive (lossy) outcome ϕ. In the case of local loss parametrized by η_d, the joint probability distribution of outcomes a and b conditioned on the choice of

measurements x^* and y^* is given by:

$$P(ab|x^*y^*) = \begin{array}{c|ccc} & b=0 & b=1 & b=\phi \\ \hline a=0 & \eta_d^2 P(00) & \eta_d^2 P(01) & \frac{\eta_d(1-\eta_d)}{2} \\ a=1 & \eta_d^2 P(10) & \eta_d^2 P(11) & \frac{\eta_d(1-\eta_d)}{2} \\ a=\phi & \frac{\eta_d(1-\eta_d)}{2} & \frac{\eta_d(1-\eta_d)}{2} & (1-\eta_d)^2 \end{array}, \tag{6.1}$$

where we have dropped the x^*y^* conditioning inside the table for the terms $P(00)$, $P(01)$, $P(10)$ and $P(11)$. The corresponding conditional entropy is given by:

$$H(x^*|y^*) = -\sum_{ab} P(ab|x^*y^*) \log_2 \frac{P(ab|x^*y^*)}{P(b|y^*)}. \tag{6.2}$$

Using the data from (6.1) in (6.2) and assuming that the outcomes 0 and 1 locally occur with the same probability, one arrives to:

$$H(x^*|y^*) = \eta_d^2 H_{\mathcal{K}}(x^*|y^*) + \eta_d(1-\eta_d) + h(\eta_d) \tag{6.3}$$

where $h(x) = -x\log_2(x) + (1-x)\log 2(1-x)$ is the binary entropy and $H_{\mathcal{K}}(x^*|y^*)$ is the conditional entropy computed from the probability distribution of conclusive events. Since $H_{\mathcal{K}}(x^*|y^*) \geq 0$, one obtains a lower-bound on $H(x^*|y^*)$ by a function which increases with loss:

$$H(x^*|y^*) \;\geq\; \eta_d(1-\eta_d) + h(\eta_d), \tag{6.4}$$

with equality in the case where perfect correlations are observed by A and B in the subset of conclusive outcomes $\mathcal{K} = \{(a,b)|a \neq \phi \;\&\; b \neq \phi\}$. $h(x) = -x\log_2(x) + (1-x)\log 2(1-x)$ is the binary entropy and η_d denotes the local detection efficiency of each party.

Hence, one cannot achieve $H(A|B) = 0$ for any $\eta_d < 1$. One can show that, even if Alice and Bob observe the maximal violation $2\sqrt{2}$ of the CHSH inequality [CHSH69] from their subset of conculsive events, the Devetak-Winter formula requires local efficiencies larger than $\eta_d \geq 92.9\%$ to yield a positive secret key (This figure is significantly higher than the 82.8% threshold originally set by [GPS10])!

Guessing probability with data post-processing. Motivated by such unaddressed issue, here we introduce a method to safely discard inconclusive events for information reconciliation purposes in the context of DIQKD. The method is inspired on a recent result for certifying randomness from post-processed data

[TdlTB+16]. In particular, we show how, in some situations, this method allows to maintain a positive secret key for lower efficiency values that cannot be reached with (2.22). Intuitively, the price one has to pay when discarding data is a cut-back in the total key rate, since more rounds are rejected as efficiency diminishes. Surprisingly, we show that this intuition is incorrect and observe cases in which the post-processing method leads to an increase in the secret key rate.

Let $\mathcal{K} = \mathcal{K}_\mathcal{A} \times \mathcal{K}_\mathcal{B}$ be a product subset of $\mathcal{O}_\mathcal{A} \times \mathcal{O}_\mathcal{B}$. We are interested in keeping only those rounds for which the outcomes (a, b) belong to $\mathcal{K}$. For instance, $\mathcal{K}_\mathcal{A}$ ($\mathcal{K}_\mathcal{B}$) could be the subset of conclusive outcomes of A (B), but keep in mind that the reasoning we present is general and actually works for any choice of subsets $\mathcal{K}_\mathcal{A}$ and $\mathcal{K}_\mathcal{B}$.

In contrast with the standard DIQKD protocol presented in Sec. 2.5, here we consider that once the measurement outcomes are registered, the classical information about whether or not $(a, b) \in \mathcal{K}$ becomes public knowledge. From a practical point of view, such information can be made public at the end of the protocol, with Alice and Bob announcing whether or not $(a, b) \in \mathcal{K}$ for each round, but without revealing the actual values of a and b. In this way, if $(a, b) \in \mathcal{K}$, Alice and Bob keep the round in question, while otherwise they discard it.

From the security point of view, the information about whether or not $(a, b) \in \mathcal{K}$ could have been initially preset by Eve. We define the observed probability for Alice and Bob to obtain a result from the set $\mathcal{K}$:

$$p_{\mathsf{AB}}(K) = \sum_{(a,b)\in\mathcal{K}} p(a, b|x^*, y^*) \tag{6.5}$$

where we have simplified the notation by dropping x^* and y^*, which are assumed to be fixed. After Alice and Bob's measurements x^* and y^* are applied on $\mathrm{Tr}_\mathsf{E}\rho_{\mathsf{ABE}}$, the classical-classical-quantum (ccq) state is given by:

$$\rho_{\mathsf{ABE}}^{x^*y^*\mathcal{K}} = \sum_{a,b} p_{\mathsf{AB}}(a, b|x^*, y^*, \mathcal{K}) \left|a, b\right\rangle \left\langle a, b\right| \otimes \rho_\mathsf{E}^{abx^*y^*\mathcal{K}} \tag{6.6}$$

where $\rho_\mathsf{E}^{abx^*y^*\mathcal{K}}$ denotes the quantum state of Eve conditioned on a, b, x^*, y^* and on the classical information $\mathcal{K}$. Let $\{M_{e|z}\}$ be the ensemble of POVM elements characterizing the measurement z that Eve performs on $\rho_\mathsf{E}^{abx^*y^*\mathcal{K}}$. Then, according to Born's rule, it follows that $p_\mathsf{E}(e|a, b, x^*, y^*, \mathcal{K}, z) = \mathrm{Tr}\left(\rho_\mathsf{E}^{abx^*y^*\mathcal{K}} M_{e|z}\right)$. The device-independent guessing probability is defined as the probability for Eve to correctly guess the outcome a maximized over all possible measurements z and over all possible quantum realizations for the behavior $\mathbf{p}$ with elements $P_{\mathsf{AB}}(a, b|x, y)$:

$$G_\mathbf{p}(x^*, y^*|K) = \max \sum_{a,b} p_{\mathsf{AB}}(a, b|\mathcal{K}) p_\mathsf{E}(e = a|a, b, \mathcal{K}) \tag{6.7}$$

where we dropped the dependence on x^*, y^* and z^* which are fixed settings in all this discussion. Using Bayes rule: $p_{\mathsf{E}}(e|a,b,\mathcal{K}) = \frac{p_{\mathsf{E}}(e|\mathcal{K})p_{\mathsf{AB}}(a,b|\mathcal{K},e)}{p_{\mathsf{AB}}(a,b|\mathcal{K})}$, (6.7) transforms to:

$$G_{\mathbf{p}}(x^*,y^*|K) = \max \sum_{e,b} p_{\mathsf{E}}(e|\mathcal{K})p_{\mathsf{AB}}(a=e,b|\mathcal{K},e). \tag{6.8}$$

With $p_{\mathsf{E}}(e|\mathcal{K}) = \frac{p_{\mathsf{E}}(e)p_{\mathsf{AB}}(K|e)}{p_{\mathsf{AB}}(K)}$ and $p_{\mathsf{AB}}(a=e,b|\mathsf{K},e) = \frac{p_{\mathsf{AB}}(a=e,b,K|e)}{p_{\mathsf{AB}}(K|e)}$, (6.8) becomes:

$$G_{\mathbf{p}}(x^*,y^*|K) = \max \frac{1}{p_{\mathsf{AB}}(K)} \sum_{e,b} p_{\mathsf{E}}(e)p_{\mathsf{AB}}(a=e,b,K|e), \tag{6.9}$$

Notice now that $p_{\mathsf{AB}}(a=e,b,K|e) = p_{\mathsf{AB}}(a=e,b|e)$ if $(a,b)\in\mathcal{K}$ and vanishes otherwise. With this, we finally obtain (6.10), as wanted:

$$G_{\mathbf{p}}(x^*,y^*|K) = \max \frac{1}{p_{\mathsf{AB}}(K)} \sum_{(e,b)\in\mathcal{K}} p_{\mathsf{E}}(e)p_{\mathsf{AB}}(a=e,b|e). \tag{6.10}$$

Thus, under the assumption of i.i.d. runs, the local guessing probability $G_{\mathsf{A}}^{\mathbf{p}}(x^*,y^*|K)$ of Alice's outcome conditioned on the observation of $\mathbf{p}$ and on the occurrence of K, is given by the solution of the following SDP:

$$\begin{aligned} G_{\mathbf{p}}(x^*,y^*|K) \;=\; & \max_{\{\mathbf{p}^e\}} \frac{1}{p_{\mathsf{AB}}(K)} \sum_{(e,b)\in\mathcal{K}} p(e,a=e,b) \\ & \text{s.t. } \sum_e \mathbf{p}^e = \mathbf{p} \text{ and } \mathbf{p}^e \in \widetilde{Q},\ \forall\ e\in\mathcal{K}_{\mathcal{A}}. \end{aligned} \tag{6.11}$$

Notice that, in contrast with (2.21), here E only requires as many behaviors $\mathbf{p}^e$ as elements in $\mathcal{K}_{\mathcal{A}}$. In fact, E is only interested in learning the outcome of the kept rounds (which she can know beforehand as the occurence of K is controlled by herself), as the remaining rounds will be discarded. Notice also that $p_{\mathsf{AB}}(K)$ is a quantity *observed* by A and B and hence does not play a role in the maximization of (6.11). Thus $p_{\mathsf{AB}}(K)$ can safely be placed outside from the maximization, which guarantees linearity of the objective function in (6.11). Notice also that this new local guessing probability with data post-processing involves both of the measurements of A and B, namely x^* and y^*, which was not the case in (2.21) and (B.5), nor in the work of ref. [TdlTB$^+$16]. Still, if $\mathcal{K}_{\mathcal{A}} = \mathcal{O}_{\mathcal{A}}$ and $\mathcal{K}_{\mathcal{B}} = \mathcal{O}_{\mathcal{B}}$ no post post-processing takes place, and one retrieves (2.21) from (6.11), as expected [2]. Finally, note that, in spite of the data post-processing, E is still required to reproduce the entire statistics $\mathbf{p}$ (and not only the kept part); crucially, this ensures that the detection loophole is never open, as pointed-out in [TdlTB$^+$16].

[2] The dependence on the measurement choice y vanishes because of non-signalling constraints.

DIQKD with data post-processing. Just as in Sec. 2.5, in order to consider a DIQKD protocol one must possess a linear functional $\mathbf{g}$ such that $\mathbf{g} \cdot \mathbf{p} = G_{\mathbf{p}}(x^*, y^*|K)$. $\mathbf{g}$ is optimal and is retrieved from the dual formulation of (6.11).

From this, as long as $G_{\mathbf{p}}(x^*, y^*|K) < 1$, Alice and Bob may reconcile their bit strings (which now contain conclusive results only) with standard error correction. The number of bits that has to be published is $N_K H_{\mathcal{K}}(x^*|y^*)$, where $N_K = p_{\text{AB}}(K)N$ is the number of rounds kept by Alice and Bob, and $H_{\mathcal{K}}(A|B)$ is the conditional entropy computed from the post-selected probability distribution of kept events. The number of bits with data post-processing certified per N_K rounds is thus given by:

$$r_{\text{pp}} = -\log_2 G_{\mathbf{p}}(x^*, y^*|K) - H_{\mathcal{K}}(x^*|y^*), \tag{6.12}$$

where the subindex "pp" indicates that post-processing took place. Critically, and in sound contrast with the standard secret key r (2.22), one may in principle choose $\mathcal{K}$ to contain perfectly correlated outcomes, so that the conditional entropy $H_{\mathcal{K}}(x^*|y^*)$ now vanishes for any value of η_d.

The expected drawback of the secret key with post processing r_{pp} (6.12) is a cutback in the total key rate, since any round with inconclusive event(s) is systematically rejected. However, this intuition is incorrect; namely, below we will observe, in the next Chapter, realistic situations for which the post-processing method can actually increase the total key rate.

6.3. Discussion

DIQKD is fundamentally hard due to the fact that channel loss rapidly opens the detection loophole when considering a standard bipartite architecture. In this Chapter we presented two architectures based on heralded preparation, which circumvent the problem of closing the detection loophole at long distances. While the first architecture requires an auxiliary system —which in practice might need be initialized at each round— the second architecture requires a third party. It is difficult to forecast which of these two solutions would be more advantageous in the future development of DIQKD technologies, but the second one is the only one of the two that has managed to close the detection (and the locality, actually) loophole, and unlike the first architecture it is naturally suited for quantum repeater extensions.

We explained how loss negatively affects the information reconciliation step of the protocol, which is an issue inherent to all QKD protocols. We showed how this issue can be alleviated by evaluating the optimal amount of randomness from the post-processed data of conclusive rounds. In the next Chapter we shall see

that, surprisingly, when considering concrete setups this method not only increases the loss tolerance but it even allows to certify more secret bits per round. We note that the only reference that we could find in the literature to be aware of this issue is Ref. [PMW+11], who addressed the question whether the key rate could be improved by using knowledge of the positions within the data string that, for example, have been assigned random values due to inconclusive results. Ref. [PMW+11] demonstrated a generic way of making use of the knowledge, without the need to revisit the full security proof. It would be interesting to carfeully analyse the similarities and edges of our technique (based on the work of Ref. [TdlTB+16]) with theirs.

7. Implementations for DIQKD

In this Chapter we apply the techniques of the previous Chapter to propose experimental implementations for DIQKD. In particular we consider and compare the two solutions for DIQKD (see Fig. 6.1) under similar experimental conditions. After formally defining in Sec. 7.1 the total key rate, which is the figure of merit used to quantify the performance of DIQKD protocols, we present a hybrid implementation based on light-matter interaction in Sec. 7.2. In contrast, in Sec. 7.3 we introduce two purely optical setups. In Sec. 7.4 we give discuss the advantages and limitations of these proposals and present an outlook for the future of DIQKD.

7.1. Achievable rate of DI secret key bits

In Sec. 2.5 we reviewed the protocols of Refs. [ABG+07, MPA11, PMLA13] for DIQKD. We saw that the work of Pironio *et al.* [PMLA13] achieves DIQKD security under the realistic assumption that the memory of the eavsdropper is limited in time, which is more than reasonable given the state-of-the-art of quantum technologies. The security proof yields in this case an expression (2.22) for the number of secret key bits certified per round, r, in terms of the guessing probability and the conditional entropy. Furthermore, the recent work of Friedman *et al.* [AFRV16] has shown that the same bound (2.22) can actually be promoted to be secure against generalised quantum eavesdroppers.

With (2.22) in mind, it is not difficult to see that if the experiment consists of a large number of rounds occurring at a repetition rate f_{rep}, and that each round is only accounted in the case that the auxiliary heralding measurement C succeeded (produced the outcome c, as explained in the previous Chapter), then the key rate of bits certified per second is given by:

$$K \;=\; f_{\text{rep}}\; p(c)\; r \tag{7.1}$$

with r being the secret key bits per round given by (2.22). In the case of using the post-processing (pp) method introduced in Sec. 6.2, the number of secret bits certified per kept round is given by (6.12). Indeed, among the rounds for which c succeeded, only the rounds with outcomes (a, b) belonging to the set $\mathcal{K}$

of conclusive-conclusive events are kept, and the key rate reads:

$$K_{\text{pp}} \;=\; f_{\text{rep}}\; p(c)\; p_{\text{AB}}(K)\; r_{\text{pp}} \tag{7.2}$$

whith $p_{\text{AB}}(K)$ given by (6.5). It is important to notice two trade-offs that will occur when using either (7.1) or (7.2) when we will consider specific DIQKD implementations in the next Sections:

Trade-off between r_{rep} and r. The first trade-off that is observed in (7.1) and (7.2) is the one recalled among purely optical systems and hybrid ones. Indeed, we have mentioned that hybrid proposals based on light-matter interaction will achieve high detection efficiency, and consequently a high value for the secret bits per round, r. However, these hybrid systems shall be limited by the slow times required to read-out and re-initialize the matter systems, which in turn results in not-too-high repetition rates f_{rep} (typically around 100 MHz). On the other hand, a purely optical implementation won't achieve such high local detection efficiencies when measuring the photon's polarization, which will diminish the values of r and r_{pp}, but it will achieve higher repetition rates (of the order of 10 GHz [GPS10]).

Trade-off between $p(c)$ and r. The second trade-off that occurs is between the probability to have a heralding round $p(c)$ and the number of bits certified per round, r (or r_{pp}). More precisely, there might exist physical parameters $\mathcal{P}$ which maximize r, but which won't necessary maximize $p(c)$, and vice-versa. In particular, when considering SPDC sources, a high value for the squeezing parameter in (B.1) will produce photons with high probability which in turn might increase $p(c)$, but such a high value favors the production of multiple —unwanted— pairs of photons, which in turn decreases the value of r. Thus, it will be crucial to optimize K and K_{pp} over the adjustable parameters $\mathcal{P}$, instead of optimizing r and $p(c)$ separately.

7.2. DIQKD with spin-coupled cavities

We first propose a hybrid DIQKD scheme based on interaction between light and spin-coupled cavities. An important advantage of spin-cavity systems is that the spin state can be measured with near unit efficiency, as no single-photon detection is required. At the same time, remote cavities can be entangled by mapping the entanglement from a pair of photons onto the spins in a heralded manner. The heralded arrival eliminates photon loss, and as the measurements settings for the spin measurement are only decided after successful heralding, the photon measurement constitutes a pre-selection that does not open any loopholes.

Together, these facts lead to improvements of the attainable key rate and the attainable distance. We first describe the protocol and then compute the key rates that can be achieved, taking into account realistic imperfections such as limited spin-photon coupling, spin decoherence, and optical detection efficiency.

Scheme with coupled cavities. The architecture of our scheme is shown in Fig. 7.1. We will consider both symmetric and asymmetric variants of the setup in which, respectively, both parties have cavities and a source of entangled photons is placed between them, or only Bob holds a cavity and the source is held by Alice who measures her photon directly. The schemes are based on local heralding and thus follow the architecture presented at the top of Fig. 6.1. The symmetric scheme closely resembles the Bell test setup of [BYHR13]. We note that while there heralding outcomes are communicated between the parties before the Bell test measurements, no such communication is necessary in the present scheme. That is, Alice does not need to learn Bob's heralding outcome before performing her measurement, and vice versa.

Spin-photon interface. For the spin-photon interface, we consider the setup proposed in [YHR13] which works in the low Q-factor regime. It is a single-sided spin-cavity system characterized by four constants: κ, the outcoupling rate via the front mirror, κ_s, the decay rate of light into other loss modes, g, the spin to cavity field coupling rate, and γ, the linewidth of the dipole transition. When $g^2 = \frac{\gamma(\kappa+\kappa_s)}{4}$ (resonance scattering [APG99]), any input photons resonant to the dipole-cavity system are scattered into loss modes, due to destructive interference between the input light and light scattered from the dipole. Thus, the presence of the spin strongly modifies the reflectivity of the cavity. The reflectivities for an empty cavity ($g = 0$), and for a cavity resonantly coupled to the spin, for a field at zero detuning, are given by [HYO+08]

$$r_e = \left|\frac{1-\kappa/\kappa_s}{1+\kappa/\kappa_s}\right| \qquad r_f = \frac{1}{1+\kappa/\kappa_s}. \tag{7.3}$$

Similar expressions apply to other systems, such as atoms, and NV-centers [BYHR13]. Whether an incident photon will couple or not to the cavity spin (i.e. see the cavity as empty or full) depends on the spin state and the photon polarization. The reflection coefficients for the joint circular polarization and spin states are r_f for $|R,\uparrow\rangle, |L,\downarrow\rangle$, and r_e for $|R,\downarrow\rangle, |L,\uparrow\rangle$. Clearly, when the outcoupling κ is small relative to the loss rate κ_s, all states transform the same, and there is no interaction between photons and spin. The ideal limit for our purposes is $\kappa \gg \kappa_s$ in which case $r_e \approx 1$ and $r_f \approx 0$.

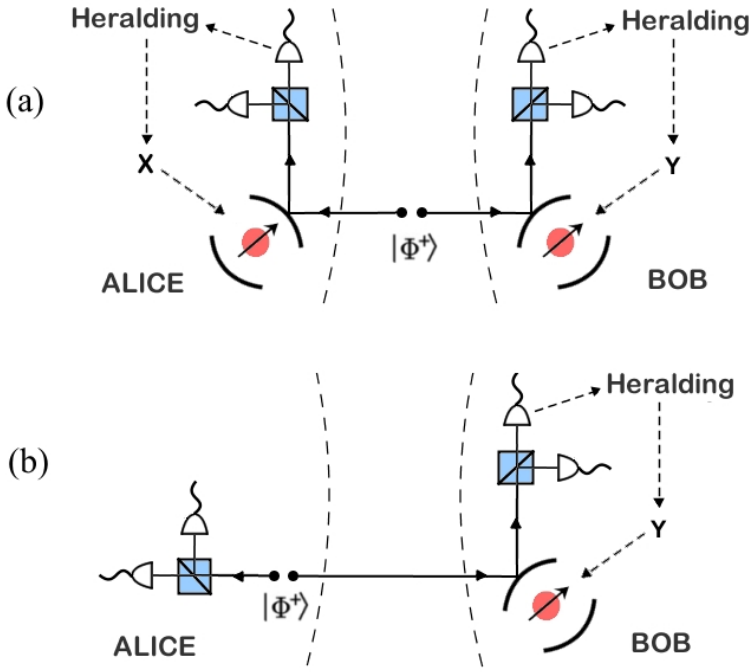

Figure 7.1.: **(a)** Symmetric protocol. A source emits entangled photon pairs. Each party holds a spin in a cavity, initialised in $(|\uparrow\rangle + |\downarrow\rangle)/\sqrt{2}$. One photon interacts with each cavity and, if reflected, is measured in the $|H\rangle$, $|V\rangle$ basis. When such a heralding detection occurs on both sides, the photonic entanglement is mapped onto the spins. Upon heralding, Alice chooses a basis and reads out her spin (similarly for Bob). The spin measurement data is used for the Bell test and key generation. **(b)** Asymmetric protocol. Bob proceeds as above, but Alice has no cavity. Instead, she directly measures the polarisation of the photon she receives. The source is located at Alice's side to minimise channel losses preceding her measurement.

Ideal protocol. To see how the spin-photon interaction is used in the protocol, consider the interaction of one (asymmetric protocol) or two (symmetric) spins initialized in the state $(|\uparrow\rangle + |\downarrow\rangle)/\sqrt{2}$ with a Bell state of light $|\Phi^+\rangle = (|RR\rangle + |LL\rangle)/\sqrt{2}$. Conditioning on reflection of the photon(s), the photon-spin states then become

$$|\psi^A\rangle = \frac{1}{2}\begin{cases} |H\rangle \otimes [r_e\,|\Psi^+\rangle + r_f\,|\Phi^+\rangle] \\ + \\ i\,|V\rangle \otimes [r_e\,|\Psi^-\rangle + r_f\,|\Phi^-\rangle] \end{cases}, \tag{7.4}$$

and

$$|\psi^S\rangle = \frac{1}{4}\begin{cases} |HH\rangle \otimes [(r_e^2 + r_f^2)\,|\Phi^+\rangle + 2r_e r_f\,|\Psi^+\rangle] \\ + \\ i\,|HV\rangle \otimes (r_e^2 - r_f^2)\,|\Phi^-\rangle \\ + \\ i\,|VH\rangle \otimes (r_e^2 - r_f^2)\,|\Phi^-\rangle \\ - \\ |VV\rangle \otimes [(r_e^2 + r_f^2)\,|\Phi^+\rangle + 2r_e r_f\,|\Psi^+\rangle]\,. \end{cases} \tag{7.5}$$

$|\Psi^\pm\rangle$, $|\Phi^\pm\rangle$ denote the four Bell states. One sees that, for $\kappa \gg \kappa_s$ (i.e. $r_e \approx 1$ and $r_f \approx 0$), a measurement of the reflected photon(s) in the $|H\rangle$, $|V\rangle$ basis leaves the remaining state (of photon-spin or spin-spin for $|\psi^A\rangle$, $|\psi^S\rangle$ respectively) maximally entangled. For finite values of κ/κ_s entanglement persists but is not maximal. The photonic measurement serves as a herald which primes the system for a subsequent Bell test. In the case of ideal detectors and no loss, the probabilities for each heralding outcome are $p_H = p_V = (r_e^2 + r_f^2)/4$ for the asymmetric and $p_{HH} = p_{VV} = [(r_e^2 + r_f^2)^2 + 4r_e^2 r_f^2]/16$, $p_{HV} = p_{VH} = (r_e^2 - r_f^2)^2/16$ for the symmetric protocol. The probabilities for successful heralding are thus $p^A_{her} = p_H + p_V = (r_e^2 + r_f^2)^2/2$ and $p^S_{her} = p_{HH} + p_{HV} + p_{VH} + p_{VV} = (p^A_{her})^2$.

Note that the shared state after heralding depends on the measurement outcome. Thus a natural way for Alice and Bob to proceed is to communicate their heralding results to each other and adapt the measurements of the Bell test to the state they have. However, this requires a time L/c where L is the distance between the parties and c is the signal speed. During this time the state will decohere, thus above some critical distance Bell inequality violation is no longer possible, and key distribution fails. To circumvent this problem, Alice and Bob can adapt the following communication-free strategy: whenever a party observes a "V" herald, a π phase-shift is applied to the spin. For the asymmetric protocol, the states after heralding are (n_A, n_S are normalization constants) [1]

$$|\varphi^A_{+/-}\rangle = \left[|\Psi^+\rangle \pm \frac{r_f}{r_e}\,|\Phi^+\rangle\right]/n_A \quad \text{H/V}, \tag{7.6}$$

[1] Note that it would be possible to make $|\varphi^A_{+/-}\rangle$ identical. However, the choice made here simplifies the computation of the key rate, see [MBA13].

and for the symmetric protocol

$$\begin{aligned} |\varphi_0^S\rangle &= |\Phi^+\rangle && \text{HV,HV,} \\ |\varphi_{+/-}^S\rangle &= \left[|\Phi^+\rangle \pm \frac{2r_e r_f}{r_e^2 + r_f^2} |\Psi^+\rangle\right] / n_S && \text{HH/VV.} \end{aligned} \tag{7.7}$$

The states for different heralding outcomes are not identical, however if κ/κ_s is not too small, they are close, and the Bell test can proceed by ignoring the herald and considering their mixture, with $|\varphi_{\pm}^A\rangle$ weighted by p_H and p_V, and $|\varphi_{0,\pm}^S\rangle$ weighted by $(p_{HV} + p_{VH})$, p_{HH}, and p_{VV} respectively. Which strategy to adopt is a matter of whether a higher key rate is extracted with communication, having more decoherence but optimal measurements, or without, having less decoherence but suboptimal measurements. We find that for the parameter ranges relevant here, the communication-free strategy is always better. (See Ref. [MBA13] for more details).

Experimental imperfections. The most important imperfection affecting the protocol is spin decoherence. To model it, we assume independent noise on separate spins (as they are far apart) and adopt a worst-case model of depolarizing noise with timescale τ. Each spin is subject to a channel [NC00]

$$\xi(\rho) = \sum_{i=0}^{3} \gamma_i \, \sigma_i \, \rho \, \sigma_i, \tag{7.8}$$

where σ_0 is the identity, σ_i the Pauli matrices, $\gamma_0 = (1 + 3\exp(-t/\tau))/4$, and $\gamma_i = (1 - \exp(-t/\tau))/4$ for $i = 1, 2, 3$. Here t is the time during which the spins decohere, which can be taken to be the time between heralding and the end of the spin measurement. For a communication-free strategy, this time is governed by the readout time Δt, while otherwise communication must be taken into account $t = \Delta t + L/c$ [2].

In addition to spin decoherence, we must account for coupling and transmission losses, inefficient photodetectors, and imperfections in the source. Transmission loss leads to a survival probability of each photon of $\eta_t^S = e^{-L/2L_{att}}$ (symmetric) or $\eta_t^A = e^{-L/L_{att}}$ (asymmetric protocol), where L_{att} is the attenuation length of the channel. The heralding detectors have efficiency η_{her}. The protocol is also affected by imperfections in the Bell test measurements. The spin readout

[2] Although the phase-shift operator σ_z does not commute with the Kraus operators of the noise, the order of noise and phase shifts is nevertheless arbitrary, because $\sigma_z^2 = \sigma_0$ and $\sigma_z \sigma_i = -\sigma_i \sigma_z$ for $i \neq z$, which implies e.g. for a phase shift on Alice's side $(\sigma_z \otimes \sigma_0)(\sigma_i \otimes \sigma_j)\rho(\sigma_i \otimes \sigma_j)(\sigma_z \otimes \sigma_0) = (\sigma_i \otimes \sigma_j)(\sigma_z \otimes \sigma_0)\rho(\sigma_z \otimes \sigma_0)(\sigma_i \otimes \sigma_j)$ for any i, j. We always take phase shifts to be applied before noise.

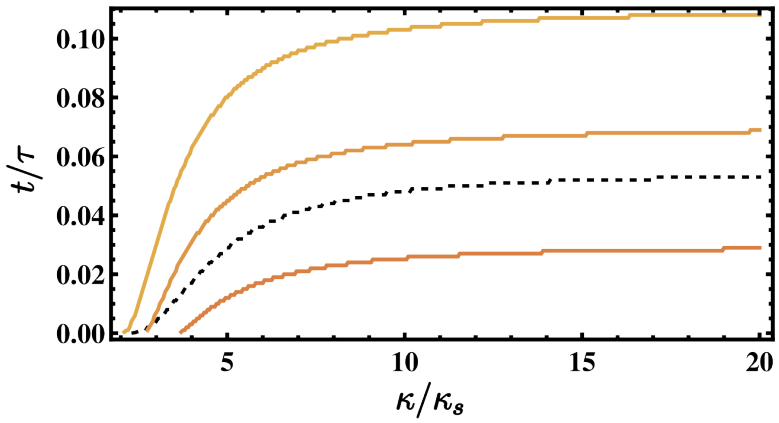

Figure 7.2.: A positive key rate can be obtained in the region under the curves for the symmetric (dotted) and the asymmetric protocol with $\eta_d = 1.0$, 0.9, and 0.8 (solid, top to bottom). Note that beyond $\kappa/\kappa_s \sim 10$ increasing κ/κ_s further does not improve the range for t/τ significantly.

efficiency can be very high, and so this is not a problem in the symmetric protocol, but in the asymmetric protocol, the efficiency η_d of Alice's optical measurement must be considered. Coupling inefficiencies can be absorbed in η_{her} and η_d. For the source, experimentally accessible techniques, such as spontaneous parametric down-conversion, do not generate ideal Bell states, but rather states like

$$|\text{vac}\rangle + \sqrt{p}\,|\Phi^+\rangle + O(p), \tag{7.9}$$

where p is the probability of generating a photon pair. This equation is indeed equivalent to (B.1). To avoid errors introduced by multi-photon contributions, p must be kept small. In our calculations, we include the leading order of multiphoton terms and optimize p to maximize the key rate K.

Results. As explained in Sec. 7.1, the figure of merit for DIQKD protocols is the key rate, i.e. how many bits of secret key can be generated per unit time. The achievable key rate depends on the level of security considered. Here we apply the bounds of Refs. [MPA11, HR09, PMLA13]. These bounds are valid for memoryless devices [MPA11, HR09] or, more realistically, in the bounded quantum storage (BQS) model, where the eavesdropper is assumed to have limited quantum memory [PMLA13]. For this model, existing security proofs are robust to noise and allow for protocols based on any Bell inequality [PMLA13], and since current quantum memories have short coherence times, the BQS assumption is very reasonable. Security has been proven without the BQS assumption, but unfortunately the proofs give zero [BCK12, RUV12b, RUV12a] or very little [VV14]

robustness to noise. We will consider a protocol based on the Clauser-Horne-Shimony-Holt (CHSH) Bell inequality, and for comparison with Ref. [GPS10], we also compute the key rate achievable for a protocol secure against collective attacks. This corresponds to a slightly lower level of security, and thus allows higher key rates.

For a detailed explanation of how to compute the key rate in the presence of the imperfections described above, see [MBA13]. Intuitively, the key rate is determined by the difference between Alice's and Bob's mutual information and the maximal information that an eavesdropper Eve can extract at each round. As long as the key rate is positive, Eve cannot extract complete information about the data shared by Alice and Bob, and secrecy is guaranteed. Following [MPA11, PMLA13] and the supplementary material of [GPS10], the key rate can be expressed in terms of the observed CHSH violation S, the quantum bit-error rate (the probability that Alice's and Bob's outcome are not correlated) Q, and the ratio μ of measurement events with indefinite (no click) to those with definite (click) outcomes. We have $\mu^S = 0$ and $\mu^A \approx (1-\eta_d)/\eta_d$ for small p (with weak dependence on L/L_{att}, η_{her}, κ/κ_s, and p). The violation S can be computed following [HHHH09] and Q in a similar manner.

For a fair comparison, we consider the methods of [GPS10] for the key rate computation. Fig. 7.2 shows the parameter regions that allow a positive key rate. For sufficiently large detection efficiency η_d, the asymmetric protocol tolerates more spin decoherence, which can be understood intuitively since only one spin, rather than two, decoheres. What parameter values in these regions are realistic? In [YHR13] a detailed analysis, inspired by the quantum dot pillar microcavity experiment of [Ra04], showed that lowering the number of DBR mirror pairs relative to a strong coupling regime, resonance scattering is achievable with $g = 80\mu eV$, $\gamma = 10\mu eV$, $\kappa_s = 180\mu eV$ and $\kappa = 2.38meV$, which yields $\kappa/\kappa_s \approx 13$. Ref. [BYHR13] estimates values of $\kappa/\kappa_s \approx 6$, 0.3, and 0.4 for strongly coupled atoms [RNH$^+$12], NV-centers [PCW06], and quantum dots [YOH$^+$11] respectively, and 2 for NV-centers in low-Q photonic crystal cavities [RMKH$^+$12]. For the spin coherence vs. readout time, Ref. [BYHR13] estimates that t/τ could go as low as 10^{-4} for atoms and NV-centers, 10^{-3} for low-Q cavities and 10^{-1} for quantum dots. Entangled source repetition rates f_{rep} may go as high as 10GHz [ZXT$^+$07, GPS10], however for interaction with dipoles in cavities, the source bandwidth is limited by the narrow cavity linewidth, and the rate is reduced. Ref. [BYHR13] estimates source repetition rates of 0.1MHz for atoms and NV-centers and many MHz for quantum dots. Note that for quantum dots, it can be challenging to achieve degeneracy of the two polarisation modes in the cavity, such that they are both resonant with a single transition in the dot. However the required tuning has been demonstrated in micropillar cavities [G$^+$11].

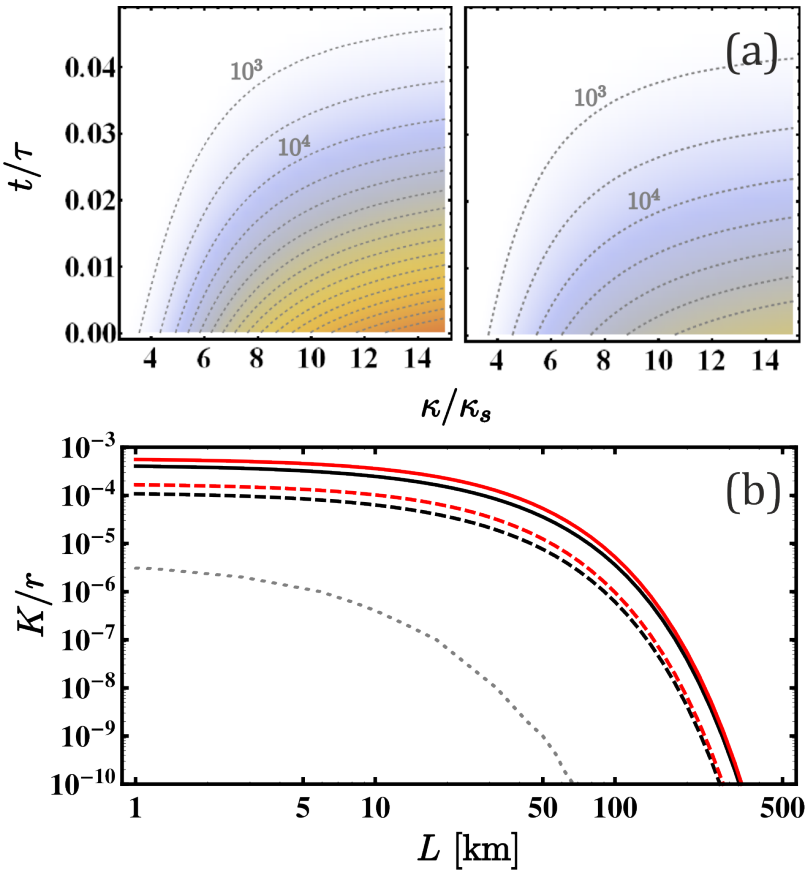

Figure 7.3.: **(a)** Secret key rate of the symmetric (left) and asymmetric (right) protocols at $L = 10$km with $f_{\text{rep}} = 100$MHz (contours separated by 5×10^3 bits/s). **(b)** Secret key rate in units of the repetition rate in the collective attacks (solid) and BQS (dashed) scenarios. The symmetric and asymmetric protocol rates are shown in each case (upper red and lower black curves), and $\kappa/\kappa_s = 6$, $t/\tau = 0.01$. The rate of Ref. [GPS10] is also shown (gray dotted). For all plots $\eta_{her} = \eta_d = 0.855$ and $L_{att} = 22$km.

Fig. 7.3 shows the key rates of the symmetric and asymmetric protocols. For comparison with the optical DIQKD-protocol [GPS10], we take $\eta_{her} = \eta_d = 0.9 \cdot 0.95$ as this corresponds to the joint coupling and detection efficiency used there. Fig. 7.3(a) shows the performance for varying decoherence and cavity coupling, assuming $f_{\text{rep}} = 100\text{Mhz}$. The symmetric protocol performs better than the asymmetric one in this case. However, for larger η_d, as the asymmetric protocol tolerates larger t/τ (see Fig. 7.2), it must outperform the symmetric for sufficiently large decoherence. In Fig. 7.3(b) we take $\kappa/\kappa_s = 6$ and $t/\tau = 0.01$ and plot the key rate measured in units of f_{rep} for our protocols as well as [GPS10]. The present protocol delivers a significant improvement in terms of key bits per use of the source, for security against collective attacks as in [GPS10] and even considering the stronger BQS model. For example at 75km we gain about five orders of magnitude. As mentioned, f_{rep} is more limited in the present scheme than for the purely optical scheme, because of the need to match the cavity linewidth. However, with five orders of magnitude improvement in efficiency of the source use, even for significantly lower repetition rates, considerable improvements can still be expected. We note that the distance over which a practically relevant key rate can be attained is also significantly improved, see Fig. 7.3(b).

Conclusion. Our scheme for device-independent quantum key distribution based on interaction between light and spins in cavities is found to be robust to spin decoherence as well as optical losses. Current state-of-the-art systems reach promising numbers, making the scheme a good candidate for experimental implementation of DI-QKD. We remark that a scheme for heralded mapping of photonic entanglement onto atoms in free space was also been proposed for a Bell test and can be readily adapted to DI-QKD along the same lines as the scheme presented here [SBM$^+$13]. We also note that the loophole-free Bell experiment of Ref. [HBD$^+$15] relied on our symmetric architecture. It would be interesting to compare the key rates achievable with these schemes to the present ones.

7.3. DIQKD with optical setups

In this Thesis we consider all potential systems to implement DIQKD. For this reason we focus in this Section on photonic schemes, which allow the use of telecom bandwidth and pre-existing fibre-optic infrastructures. We recall the reader that in the previous Chapter we sketched to types (*i*) and (*ii*) of architectures to implement DIQKD (recall Fig. 6.1). We present a modified version of a scheme of Pitkanen *et al.* [PMW$^+$11], the best known scheme of type (*i*), based upon

heralded qubit amplification [GPS10]. For type (*ii*), we present a scheme utilising a QND measurement by a third party, inspired by the entanglement distribution scheme of Lasota *et al.* [LRBT14]. We further consider the use of single-photon sources, the fabrication of which has lately grown immensely, with nearly on-demand single-photon sources with purity and indistinguishability above 99% already available [DHD+16, SGDS+16, LBH+16, SMM+17]. Combining these two key ingredients, we show that the outlook for experimental DIQKD as a viable future technology is significantly improved, tolerating much high transmission loss with a higher key generation rate.

Noiseless heralded-state-preparation Spontaneous parametric down-conversion (SPDC) sources produce photonic entanglement in two spatial modes and have been the workhorse of DIQKD proposals so far. In the proposal of Gisin *et al.* [GPS10] the SPDC source is held by Alice to avoid channel loss on her side, while Bob performs heralded qubit amplification [KXRP13] to obtain the desired signal c and confirm the arrival of his photonic system without revealing its carried information. Heralded qubit amplification has been demonstrated in the visible [KXRP13] and telecom [BPM+16] regimes, and more recently with path-entangled qubits [MVV+16], although never without the presence of the detection loophole. See the top of Fig. 7.4 for a refined version of the qubit amplification scheme.

Other authors [CM11, MSBB+13, STS15] subsequently introduced refined schemes requiring Alice and Bob to each hold an SPDC source; these schemes are based on entanglement-swapping relays to perform the heralding operation. As mentioned already, the entanglement swapping configuration is naturally suited for quantum repeater technologies, and has been experimentally demonstrated with pulsed SPDC sources [PBWZ98] and lately in the continuous variable regime [HBG+07].

In all these SPDC-based proposals, however, the heralding signal —which formally corresponds to one of the outcomes c of an auxiliary measurement C — dramatically reduces the purity and fidelity of the prepared state $\rho_{\mathsf{AB}|c}$. This is a consequence of false-positive events in c, stemming from combinations of vacuum SPDC productions with other multi-photon states. In fact, the contribution of false-positive events is inevitably large due to the highly inefficient character (nonlinearity) of the SPDC process. More precisely, the contribution of the target maximally entangled state $|\psi_{ab}\rangle$ that Alice and Bob wish to share upon success of C occurs at the same order as other unwanted states. If the initial unnormalised state prepared is $|0\rangle\langle 0| + p\,|\psi_{ab}\rangle\langle\psi_{ab}| + \ldots$, then after transmission and heralding (with heralding parameter $T \approx 1$), the unnormalised state is

$$\rho_{\mathsf{AB}|c} = (1-T)\,|0\rangle\langle 0| + T(1-T)p\eta_t\,|\psi_{ab}\rangle\langle\psi_{ab}| + \ldots \tag{7.10}$$

where additional terms of order p or higher are not written explicitly. For any fixed T, since $\eta_t \to 0$ exponentially with distance, the heralded state approaches vacuum, and is rapidly unable produce nonlocal statistics strong enough for DIQKD. As such, SPDC-based proposals are out of experimental reach.

To eliminate false-positives and maintain the fidelity of $\rho_{AB|c}$, we propose a way to suppress unwanted vacuum contributions by means of an architecture which does not rely on inefficient photonic entanglement production. Our scheme is based on single-photon sources, a new generation of quantum technology whose development has been boosted lately, achieving near-to-perfect fidelity and inidistinguishability values [DHD+16, SGDS+16, LBH+16, SMM+17]. Nevertheless, single photon sources are an expensive resource relative to SPDC sources, and hence it is desirable to consider schemes with fixed numbers of single-photon sources, used in conjunction with SPDC.

To maintain generality and a degree of comparison with the SPDC paradigm [3], we model each single-photon source with a quantum state containing an infinite tail of high-order contributions, and whose unnormalized expression in the photon-number basis is (see App. A) $\sigma = \sum_{n=1}^{\infty} p^{n-1}$, where p parametrizes the probability to produce high-order terms [4]. This source model does not assume any particular underlying physical process, and thus provides broad insight on how imperfect single-photon sources could perform in real DIQKD experiments, regardless of specific implementation details.

DIQKD optical schemes The first scheme requires Bob to produce two single photons with orthogonal polarizations H and V, while Alice has an SPDC source which produces a pair of maximally entangled photons with probability p. It is inspired by the qubit amplifier scheme of Pitkanen *et al.* [PMW+11] and is explained in Fig. 7.4 (a). The photons produced by Bob enter a beam-splitter (BS) of transmittivity T. The reflected polarization components are combined with a half-wave-plate (HWP) and then the resulting spatial mode is jointly analysed with the mode sent by Alice with a QND, a partial Bell-state measurement (BSM) denoted C. C triggers the heralding signal whenever the desired outcome c —two detector clicks corresponding to orthogonal polarizations— is observed.

Provided that $T \approx 1$ the desired event c will only arise when exactly one photon was reflected, meaning that the photon of Alice has arrived. Furthermore, this scheme is immune to false positive contributions which could occur in the case where the two photons are reflected; this instance is in fact the main limitation

[3] In particular our model can simulate an SPDC source for which one of the modes is used as trigger.

[4] In the same manner, the quantum state of an SPDC source is parametrized by a parameter which we also label p

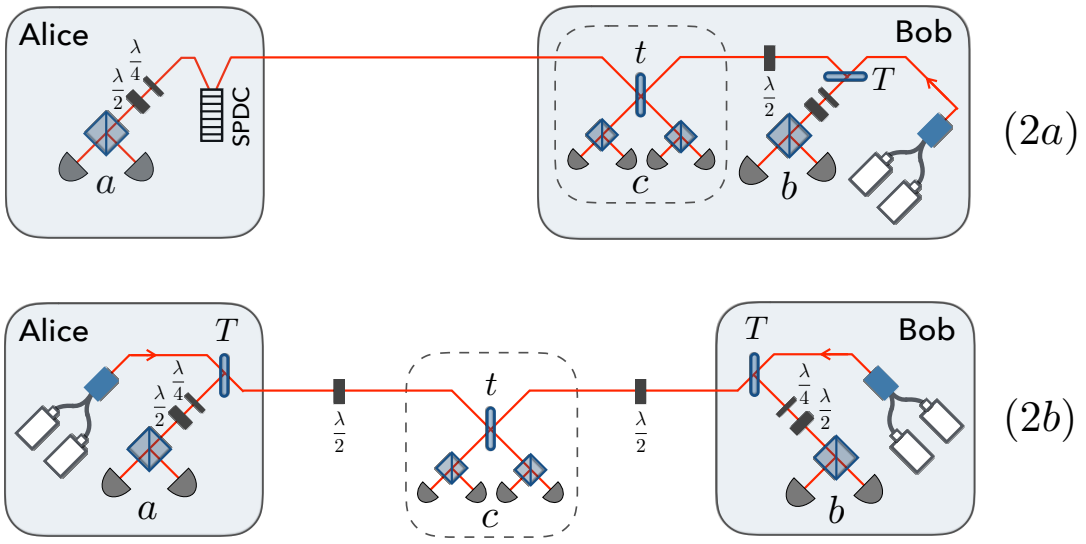

Figure 7.4.: **DIQKD schemes.** *(Top, 2a): Refined qubit amplifier scheme.* The SPDC source is kept close to Alice to avoid loss on her side of the channel. Bob inserts two single photons encoded in orthogonal polarizations H and V into a BS of transmittance T. The reflected mode is jointly analyzed with the system sent by Alice by a partial BSM: a partial BS of transmittance t, polarizing-BS (splitted squares) and binary on/off —non-photon number resolving— photodetectors (half-circles). This scheme follows the DIQKD approach presented at the top of Fig. 6.1. *(Bottom, 2b): Single-photon sources scheme.* Alice and Bob couple two single photons encoded in orthogonal polarizations into a BS of transmittance T. A HWP ($\frac{\lambda}{2}$) combines the transmitted polarization components, which are analayzed with a partial BSM. This scheme follows the approach presented at the bottom of Fig. 6.1. In both schemes, the output modes are measured by the users with a polarization analyser: a sequence of a quarter-wave plate ($\frac{\lambda}{4}$), a HWP, a polarizing BS and two binary detectors.

of the original proposal of Ref. [GPS10]. In this manner, the reflected photons are "prepared" by C with orthogonal polarizations, although the information about their concrete direction is "erased" by the partial BSM. Thus, the partial BSM prepares a polarization-entangled two-qubit state whose degree of entanglement depends on the transmittance t. In fact, the unnormalized state shared by Alice and Bob conditioned on c is:

$$\rho^{(i)}_{\mathsf{AB}|c} = \frac{p\ \eta_t T(1-T)}{2} |\psi^-_{ab}\rangle\langle\psi^-_{ab}| + \mathcal{O}(p^2) \tag{7.11}$$

where $|\psi^t_{ab}\rangle := |\psi^-_{ab}\rangle + t\,|\phi^-_{ab}\rangle$ is a coherent superposition of Bell states given, in second quantization, by $|\psi^-_{ab}\rangle = \frac{1}{\sqrt{2}}(a^\dagger_H b^\dagger_V - a^\dagger_V b^\dagger_H)\,|0\rangle$ and $|\phi^-_{ab}\rangle = \frac{1}{\sqrt{2}}(a^\dagger_H b^\dagger_H - a^\dagger_V b^\dagger_V)\,|0\rangle$. As mentioned, here p parametrizes the probability to produce a single pair in the SPDC process.

The second scheme requires Alice and Bob both to produce two single photons with orthogonal polarizations H and V, and is inspired by the entanglement distribution scheme of Lasota *et al.*[LRBT14]. Its detailed working is explained in Fig. 7.4 (b). The initial state is $\rho_{\mathrm{AB}} = \sigma^A_H \otimes \sigma^A_V \otimes \sigma^B_H \otimes \sigma^B_V$. The photons produced enter a BS of transmittivity T as illustrated in Fig. 7.4. The transmitted polarization components are combined with a HWP and then the spatial modes are analyzed again with a partial BSM denoted C.

Provided that T is kept small, the desired event c only arises when exactly one photon was transmitted by each party, meaning that the other photon was reflected. In this manner, the reflected photons are "prepared" by C with orthogonal polarizations, although the information about their concrete direction is "erased" by the partial BSM. Thus, the partial BSM prepares a polarization-entangled two-qubit state whose degree of entanglement depends on the transmittance t. In fact, the unnormalized state shared by Alice and Bob conditioned on c is:

$$\rho^{(ii)}_{\mathrm{AB}|c} = \frac{\eta_t T^2(1-T)^2}{2}\,|\psi^t_{ab}\rangle\langle\psi^t_{ab}| + \mathcal{O}(p), \tag{7.12}$$

Crucially, unlike in (7.10), in the above two schemes there are no vacuum terms after heralding. As such, the states in (7.11) and (7.12) to first order are pure and proportional to the transmission efficiency η_t. This guarantees that after normalisation, the states are independent η_t (to first order). Furthermore, the state $|\psi^t_{ab}\rangle = |\psi^-_{ab}\rangle + t\,|\phi^-_{ab}\rangle$ is maximally entangled at $t = 0$, but becomes product for $t = 1$. Hence, by adjusting the transmittivity t of the central BS we are able to prepare any pure two-qubit partially entangled state in a heralded manner. The high purity of $\rho^{(ii)}_{\mathrm{AB}|c}$ constitutes our main achievement: in fact, $|\psi^t_{ab}\rangle$ tolerates up to one third of loss [Ebe93] in the limit $t \to 1$ for which loophole-free nonlocality has already been experimentally certified [GVW$^+$15, SMSC$^+$15]. These substantial improvements allow us to achieve secret key rates as high and efficiency thresholds as low as never observed before within the experimental DIQKD framework.

Results In Table 7.1 we present a comparison of our single-photon sources-based scheme against that of Pitkanen *et al.* [PMW$^+$11], which is the state-of-the-art scheme for DIQKD based on SPDC. The two schemes are depicted in Fig. 7.4. To assess performance, by means of SDP techniques, we avoid truncation of the infinite tail of high-order terms in the SPDC state and in the single-photon sources state, as explained in App. B. We also use the post-processing method developed

DIQKD Scheme:	**New Qubit Amplifier**	**Single Photons**
Noise robustness (nonloc.)	**31.2%**	**35.7%**
Loss robustness (nonloc.)	**25.7%**	**30.8%**
Loss robustness (diqkd)	**8.9%**	**9.7%**
Secret key bits	**0.82**	**0.95**

Table 7.1.: **Performance of DIQKD schemes.** The local loss robustness for DIQKD is always lower than the one needed to certify nonlocality since the former constitutes a more demanding task than the latter. The number of secret bits are shown for the lossless case and under the assumption that the heralding signal occured.

in Sec. 6.2 to deal with the negative impact that loss has on the information reconciliation part of the protocol.

The single-photon sources-based scheme outperforms the qubit amplifer scheme for all the figures of merit considered. This can be readily understood by taking a look at the perturbative prepared state $\rho_{AB|c}$ (7.12), which does not contain spurious contributions at the order at which the scheme ideally works. This allows Alice and Bob to share an almost pure partially entangled state, tolerating 35.7% of maximally mixed noise in the lossless case. The nonlocality robustness to loss is very close to the ultimate bound [Ebe93] (33.3%), which is assymptotically reached by pure two-qubit partially entangled states. Outstandingly, in the lossless case the scheme manages to certify 0.95 secret bits, very close to the limit allowed by the quantum formalism for polarization (projective) measurements [AMP12].

Interestingly, the post-processing method for DIQKD allows to increase the loss tolerance from 5.7% (not presented in Table 3.1) to 9.7% for the single photons scheme. A similar increasing is also observed for the amplifier-based scheme. The intuition for such an increasing is the following: since almost no vacuum productions occur at the level of the sources in the single-photons scheme, any inconclusive event mostly stems from a loss process. This knowledge guarantees that no information is lost when inconclusive outcomes are discarded, which constitutes the main ingredient of the post-processing technique.

To compute the key rate in Fig. 7.5 we allow for 5% of local loss for Alice and Bob. We take a channel attenuation length of $L_{\text{att}} = 22$ km^{-1}, and an efficiency for the detectors used in the QND measurement (including both coupling and detection efficiency) of 85%. Upon optimization, we find that the parameters $T = 0.004$ and $t = 0.698$ ($T = 0.025$ and $t = 0.708$ respectively) yield the highest DIQKD rates for the single-photon scheme (with post-processing). Inter-

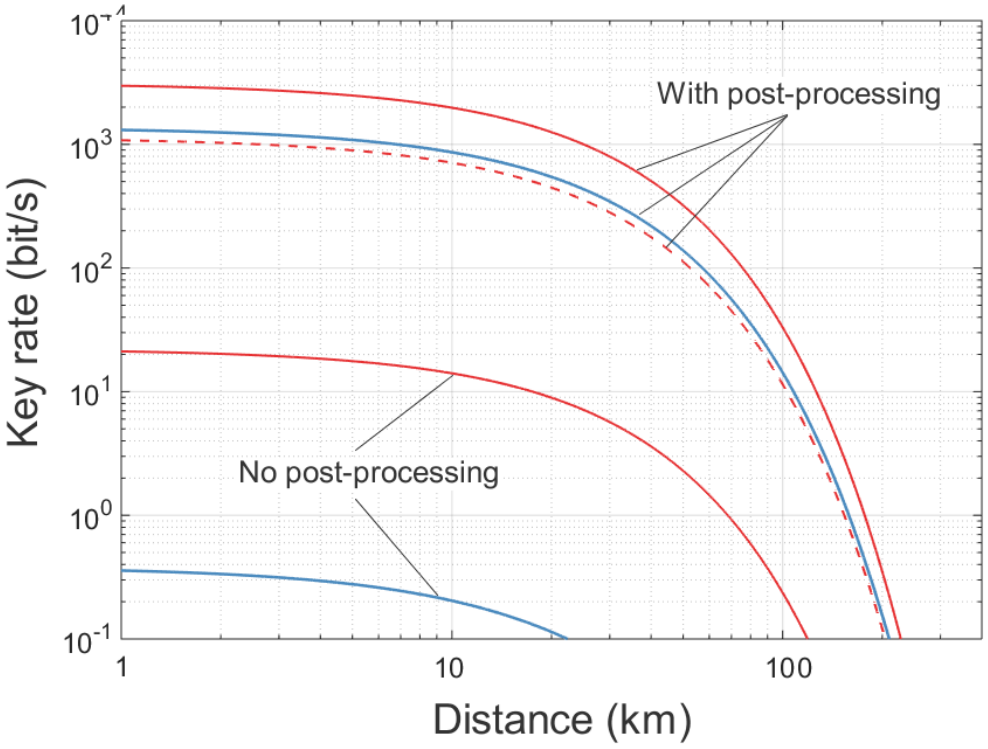

Figure 7.5.: **Key rates with 5% of local loss.** The curves in red (blue) show the key rates (in bits per second) attained by the central-heralding (side-heralding) scheme. For the bottom curves the secret key is extracted optimising the protocol within the standard DIQKD setting, while the upper curves also include the post-processing technique that then yields a considerable increase of the corresponding key rates. Each key rate is adequately optimised over all adjustable physical parameters, yet in the case of the single-photon sources impurity parameter the lowest possible value is always favoured. Hence, we set $p = 10^{-4}$ while computing all the solid curves while we choose $p = 10^{-2}$ in case of the dashed curve to more adequately refer to current experimental implementations. In the latter case, only the CH scheme with post-processing employed provides a positive and and a high key-rate. In all cases we consider the repetition rate of photon production to be 100 MHz

estingly, the post-processing method outperforms the standard DIQKD approach. In particular, for a distance $L = 50$ km, with $p = 10^{-4}$ we certify 320.8 secret bits per second with post-processing and 2.3 secret bits per second with the standard approach.

How imperfect the single-photon sources can be? Contrary to SPDC processes, optimizing the value of the parameter p describing single-photon sources imperfections always leads the lowest allowed value. (With an SPDC source, the value of $p = 0$ gives $p(c) = 0$ and hence the rate is zero). So far, our scheme outperforms the amplifier scheme, but the improvement is not so large. However, if we now look for more realistic values, e.g. $p = 10^{-2}$ (currently experimentally reachable) for which higher order terms contribute more, our scheme turns to be the only one to provide a positive key rate. In fact, for $p = 10^{-2}$ we still manage to certify 112.4 bits per second over $L = 50$ km. We can see that our single-photons scheme is robust to high values of p. Such values are in fact encouraging as they can be used to tolarate lower photonic quality to increase extraction efficiency [DHD+16].

Conclusion. In summary, we have presented two photonic DIQKD schemes based on the use of single-photon sources, for which vaccum does not constitute the leading term in the heralded state. This is a highly significant improvement with respect to previous optical proposals, for which no key can be generated after a few kilometers. Our two proposals respectively follow the two known possible solutions presented in the previous Chapter to avoid channel loss from opening the detection loophole. We found that the scheme relying on single-photons outperforms the qubit amplifier proposal, and furthermore is robust to impurity in terms of high-order contributions at the level of the sources. We applied the post-processing technique to avoid loss affecting the information reconciliation part of the protocol, and this turned to be beneficial both to increase the loss robustness and the key-generation rate of the two schemes. We believe that our results will foster new research ideas for the experimental implmentation of DIQKD.

7.4. Discussion

In this Chapter we have proposed and analysed physical implementations for DIQKD, based on heralding solutions to avoid opening the detection loophole at long distances. The first implementation that we presented in Sec. 7.2 is hybrid as it based on light-matter interaction, while the two proposals presented in Sec. 7.3 are purely optical and rely on the use of single-photon sources. While the hybrid proposal benefits from high local detection effiencies when reading-out the matter systems, the optical proposals allow for higher repetition rates since the photons are measured directly and no re-initialization of any system is required at each round. This trade-off was exposed at the beginning of this Chapter, and it was illustrated with the concrete proposals studied then.

To make a comparison let us take a concrete example. For a distance $L = 50$

km, on the one hand the hybrid proposal certifies $\approx 10^{-5}$ bits per second in units of repetition rate (see Fig. 7.3), both with the symmetric and asymmetric version. On the other hand, for the same distance the scheme based on single-photons with 5% of local loss certifies up to 10^{-6} bits per second, also in units of repetition rate Fig. 7.5. It is worth to consider the two following key points: *1)* We originally set the repetition rate to be $f_{\text{rep}} = 100\ MHz$ for both the hybrid and the purely optical proposals, but we believe that this number is less realistic for the hybrid scheme, which necessitates additional time to re-initialize and read-out the spins. *2)* We considered 5% of local loss for the optical schemes, which is promising given the progress of optical Bell experiments, but this number remains today out of experimental reach (current experiments may achieve around 25% of loss [GVW$^+$15]). We therefore conjecture that near future development of either photo-detectors or faster fluorescent methods for matter systems could lean the balance in favor of either purely optical systems or matter-based ones to implement DIQKD.

Moreover, we applied the techniques for DIQKD developed in the previous Chapter to the two optical schemes that were presented in Sec. 7.3. On the one hand, the technique to deal with high-order contributions from light sources turned to be efficient and not over-pessimistic, in the sense that for the values of the parameter p considered, the estimate of the constructed behavior was found to be already very close to the real one. On the other hand we also applied the post-processing technique for DIQKD and we found considerable improvements, as the robustness to losses, the number of secret key bits and the total key rate were enhanced when using this technique. We expect that these two techniques could be applied and foster research in other DIQKD setups and to other experimental proposals not necessarily related to DIQKD.

8. Conclusions and outlook

In This Thesis we worked on the development of quantum information theory towards the experimental implementation of protocols based on the minimalist, user-friendly, black-box paradigm. Our work tackled fundamental problems as the one of finding an adequate measure of nonlocality or probing the ultimate limits of certifying randomness with quantum resources. At the same time, we managed to propose realistic solutions to develop protocols for entanglement detection, randomness certification and quantum key distribution within the black-box paradigm. In some cases, we even achieved the ultimate objective of turning the theory into reality by going to the laboratory and successfully demonstrate the usefulness of such protocols in proof-of-principle experiments. In this last Chapter we shall recall all these results achieved, and we shall as well overview new directions for future work that this Thesis has opened.

Entanglement with uncharacterised devices We developed and implemented semi-definite programming (SDP) techniques to experimentally certify the presence of all kinds of entanglement on a three-qubit photonic W state in the steering scenario. The experimental W state revealed both genuine multipartite entanglement (GME) and entanglement in all of its reduced states, being therefore a flexible resource for quantum networks. We showed that all types of entanglement of the W state can in fact be certified in all tripartite steering scenarios in a scheme where each party applies the same set of measurements. In this way, each party can certify all types of entanglement without the need to rely on any characterisation of the measurement devices used by the others. It is still an open question whether the reduced state of the W state can violate any Bell inequality, although in this Thesis we managed to show —both in theory and in practice— that it does present steering. It would be highly desirable to assess this question in the near future, and also to adapt our techniques to other states and to larger networks. In particular, in the past two years new techniques based on few body correlators have emerged to probe the nonlocality of many particles.

We proposed a natural and operational measure of nonlocality which acts directly at the level of the quantum states and which simultaneously encompasses all Bell inequalities. With this measure we showed that no anomalies of nonlocality occur for two-qubit states for scenarios based on full-correlator inequalities. We

showed that this result generalises to the multipartite case for an even number of parties. We also provided numerical evidence suggesting that our measure does not reveal anomalies in scenarios with systems of higher dimension or in scenarios with inequalities involving marginal terms. Our results confirmed the numerical findings of other references working along the same direction, and it would be highly desirable to explore the possibility of have an analytic proof of our findings for any type of inequality, any dimension and any number of parties. Our results enabled interesting operational implications beyond the fundamental study of entanglement and nonlocality. In the same manner as some authors have developed an operational framework for entanglement and nonlocality, such an operational framework is still awaited to analyse measures of nonlocality which act directly at the level of the quantum state, like ours. We believe that proving local unitary invariance of our measure was a first step towards that direction. Our measure was then attempted to be adapted to the steering framework, but in this case the equivalence between steering and non-joint-measurability implied that our measure trivially yields a unit value for the probability to demonstrate steering from randomly sampled measurements for any pure entangled state of any dimension. It remains an open question for the future to study the existence of anomalies between entanglement and steering, or even between steering and nonlocality. It remains also an open question to assess mixed states with our measure.

Genuine random number generation In this Thesis have presented the first proof-of-principle experiment demonstrating one-sided DI random number generation. This was achieved by analysing the bipartitions of the W state. We found that the number of random bits certified (0.26 random bits) in this experiment was very distant from the theoretic value (1.58 random bits), which motivated us to introduce methods to increase genuine randomness in experiments by tailoring the measurements and avoiding post-processing of the observed data. The performance of these methods was first theoretically applied to bipartite optical Bell experiments, increasing the number of random bits certified by up to four times. Second, the methods were experimentally used in an ultra-high visibility setup, where we managed to implement an extremal POVM with high fidelity, which allowed us to experimentally certify more than one bit of randomness from one entangled bit. From the fundamental perspective, this probed the ultimate limits for randomness certification using quantum resources. From the practical perspective our scheme offers an advantage over standard Bell experiments based on projective measurements of up to 30% in the number of bits certified. Upon optimization of the physical parameters and of all possible Bell inequalities, our optical experiment based on polarization-entangled photons certifies 1.17 ± 0.08 full DI random bits. We further increased this number by assuming that the other

qubit in the experiment was trusted; in this case, we certify 1.27 ± 0.15 semi-DI random bits.

It would be interesting to apply our machinery to optimize the number of random bits and to deal with experimental problems, such as the presence of signalling in finite statistics, to the other Bell-type randomness generation setup based on SPDC, which considers path entanglement and displacement measurements. It would also be desirable to compare the performance of our methods to the newer genuine random number generation techniques that have recently been exposed to deal with the problem of finite statistics. In particular, protocols secure against classical side information that rely on the estimation of an arbitrary number of Bell expressions or even directly on the experimental frequencies of measurement outcomes have been introduced recently. Also, this year new protocol secure against nonsignalling eavesdroppers which performs well in experimental regimes characterized by low violation of Bell inequalities has been introduced and experimentally demonstrated. Finally, other estimates in the i.i.d. regime converging to the underlying quantum distribution faster than the relative frequencies of the experiment have also been presented lately.

Given that the random number generation task with uncharacterized devices is perhaps the device-independent quantum technology with highest chances to directly impact our society soon, it would be very interesting to explore the current industrial aspect of quantum random number generation: namely, to understand the needs of the market as well as the current limitations encountered. This could help to spot opportunities for which device and semi-device independent random number generation could bring a competitive edge to the market.

Device-independent quantum key distribution Unlike DI and semi-DI random number generation, DIQKD is still experimentally awaited because of the cumbersome problem of closing the detection loophole at long distances and achieving a high fidelity on the distributed state. We presented two architectures based on heralded preparation, which circumvent the problem of closing the detection loophole at long distances. While the first architecture requires an auxiliary system —which in practice might need be initialized at each round— the second architecture requires a third party. It is difficult to forecast which of these two solutions would be more advantageous in the future development of DIQKD technologies, but the second one is the only one that has managed to close the detection (and the locality, actually) loophole, and unlike the first architecture it is naturally suited for quantum repeater extensions.

We proposed physical implementations (one hybrid and two purely optical) for DIQKD, based on the developed heralding architectures to avoid opening the detection loophole at long distances. While the hybrid proposal benefited from high

local detection efficiencies when reading-out the matter systems, the optical proposals allowed for higher repetition rates since the photons are measured directly and no re-initialization of any system is required at each round. A comparison revealed that the performance of the schemes was comparable, and we conjecture that near future development of either photonic sources and photo-detectors or faster fluorescent methods for measuring matter systems could lean the balance in favor of either purely optical systems or matter-based ones to implement DIQKD.

As implementations remain awaited, experimental modelling is necessary though not easy due to the difficulty to consider all potential mismatches and imperfections into account. We presented an SDP method to efficiently and safely discard imperfections not accounted for in the modeling of an experiment, by granting this lack of knowledge into power to the eavesdropper to her own benefit. The method was applied to the optical DIQKD proposals developed in this Thesis in order to deal with high-order contributions from light sources. The method turned to be efficient and not over-pessimistic, in the sense that for the experimental values considered, the estimate of the constructed behavior was found to be already very close to the real one. Since the method is general, we believe that it could have interesting applications to the modelling of other experiments in the context of DI and semi-DI quantum information.

We revealed how loss negatively affects the information reconciliation step of any QKD protocol. We showed how this issue can be alleviated by evaluating the optimal amount of randomness from the post-processed data of conclusive rounds, which was a direct application of methods recently developed by other authors. This post-processing technique for DIQKD found considerable improvements when applied to the optical setups: the robustness to losses, the number of secret key bits and the total key rate were in fact enhanced when using this technique. It would be highly desirable to write a formal security proof for this method. It would also be useful to apply this technique to other potential setups in the future, and also to compare it with the only reference that we could find in the literature to be aware of this issue, which demonstrated a generic way of making use of the knowledge of the positions within the data string that have been assigned random values due to inconclusive results.

Appendices

A. Quantum optics components

In this section we present realistic modeling of experimental components required to implement DIQKD with linear quantum optics circuits, photons and photon-number non-resolving detectors. In Sec. A.1 we model SPDC sources and single-photon sources. In Sec. A.2 we present linear quantum optics transformations. These transformations are the building blocks of quantum circuits enabling interference between distinct output modes from the sources. In Sec. A.3 we model photodetection. Finally, in Sec. A.4 we analyze loss effects.

A.1. Sources

SPDC sources. The first sources that we consider are SPDC based. Ideally, they produce polarization entangled pairs of photons in two distinct spatial modes, and have been the workhorse of DIQKD proposals so far [GPS10, CM11, MSBB$^+$13, STS15]. Concretely, the unnormalized state produced per laser pulse by such an SPDC source in two output spatial modes a and b may be written as [KB00, CVSB$^+$15]:

$$\sum_{n=0}^{\infty} \frac{n+1}{2^n} p^n \left|\Psi_n\right\rangle\!\left\langle\Psi_n\right| = \left|0\right\rangle\!\left\langle 0\right| + p \left|\Psi_1\right\rangle\!\left\langle\Psi_1\right| + \ldots, \tag{A.1}$$

where $\left|\Psi_n\right\rangle = \frac{1}{n!\sqrt{n+1}} \left(a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger\right)^n \left|0\right\rangle$ denotes the state of n down-converted photon pairs and p is the probability to produce a single pair in the process. Here $a_H^\dagger$, $a_V^\dagger$, $b_H^\dagger$ and $b_V^\dagger$ are bosonic creation operators for which H and V denote orthogonal polarization directions, while $\left|0\right\rangle$ denotes the vacuum state of all modes.

Experimentally, the parameter p is kept small (below 10^{-2}) and it may be adjusted with squeezing techniques [GVW$^+$15, SMSC$^+$15]. Large values of p increase the production rate of maximally entangled states of two photons $\left|\Psi_1\right\rangle$, which correspond to the target production of the SPDC process. But large values of p also increase the relative contribution of spurious, higher-order, terms $\left|\Psi_{n>1}\right\rangle$, which constitute one of the main limitations for scalable photonic quantum communication, e.g. with quantum repeater technologies [MKL$^+$14].

Typically, in order to take the contribution of high-order terms into account, one truncates the SPDC state (B.1) up to a (small) total number of photon

pairs [GPS10, CM11, MSBB+13]. However, this approximation may not always be naively pursued within the DI approach to quantum protocols. Therefore, in order to provide a solution to this issue, we develop in Chap. 6 a technique that gives Eve full power to control high-order contributions which then do not have to be taken into account without opening loopholes.

Single-photon sources. The second type of sources that we consider ideally produce on-demand single photons in some desired output spatial mode and polarized along some adjustable direction. Such single photon sources have just been demonstrated with quantum dot micropillar systems achieving nearly perfect fidelity and inidistinguishability [DHD+16, SGDS+16, LBH+16]. We model each single-photon source with a quantum state containing high-order imperfections, and whose unnormalized expression in the Fock basis is:

$$\sum_{n=1}^{\infty} \bar{p}^{n-1} |n\rangle\langle n| = |1\rangle\langle 1| + \bar{p} |2\rangle\langle 2| + \dots \tag{A.2}$$

Note that, contrary to the SPDC state presented in (B.1), here the quantum state produced does not contain vacuum contributions. $\bar{p}$ is an experimental parameter quantifying high-order imperfections, but the model is kept general in the sense that no underlying physical process is assumed. Instead, the model provides a general perspective and insight on how imperfect single-photon sources should be expected to perform in real DIQKD experiments, regardless of the specific physical process used in the implementation.

Just as for the SPDC source modeling, instead of simply truncating expression (A.2) up to a maximal number of photons, we often employ the technique discussed in Chap. 6 that does not compromise the DI approach, as all higher-order contributions are assumed to be manipulated by Eve to her own benefit.

A.2. Linear quantum optics

The photonic state produced by a certain collection of sources described in the previous paragraph, undergoes a unitary evolution which allows to transform each output mode individually (e.g. rotate their polarization), but it also enables coherent interference between two (or more) output modes stemming from different sources. Physically, such unitary evolution can be implemented with optic-fiber-based linear circuit technology, built from concatenations of optical components such as: partial beam-splitters (BS), of given transmittivity which we parameterise as $\cos(\lambda/2)$; polarizing beam-splitters (PBS), which are assumed to always transmit (reflect) horizontally (vertically) polarized light; and arrangements of wave-plates (WP), which generally yield the following transformation for a given

pair of orthogonal polarization modes a_H and a_V and a given pair of real parameters (θ_a, ϕ_a):

$$\begin{cases} a_H^\dagger \longrightarrow \cos\left(\frac{\theta_a}{2}\right) a_H^\dagger + e^{i\phi_a} \sin\left(\frac{\theta_a}{2}\right) a_V^\dagger \\ a_V^\dagger \longrightarrow -e^{-i\phi_a} \sin\left(\frac{\theta_a}{2}\right) a_H^\dagger + \cos\left(\frac{\theta_a}{2}\right) a_V^\dagger. \end{cases} \tag{A.3}$$

A.3. Photodetection

Photodetectors are placed at the output modes of linear quantum optics circuit. These photodetectors are assumed to be non-photon number resolving. In other words, they produce each time one out of only two possible outcomes ("bucket" detectors): "click" and "no-click". They are assumed to be 100% efficient. (We will model photodetection inefficiency and other types of loss in the next section). Hence, the quantum measurement process at each output mode of the linear circuit is modeled with a 2-outcome projective measurement with elements $M_{\text{no-click}} = |0\rangle\langle 0|$ (projection into the vaccum state) and $M_{\text{click}} = \mathbb{1} - |0\rangle\langle 0|$.

A.4. Overall loss and efficiencies

Transmission loss. Transmission loss in the circuit is presumed to increase exponentially as a function of distance for each mode. This is modeled with a "lossy" BS of transmittivity $\eta_t = \exp(-L/L_{\text{att}})$ (the reflected mode is traced-out), where L denotes the spatial length of the given mode and L_{att} denotes the attenuation length of the optic fiber. Note that the exact location of the BS within a given mode is irrelevant, as such lossy BS commutes with linear unitary operations.

Photodetection inefficiencies. Photodetection efficiency is defined as the probability for a photodetector device to produce the conclusive "click" outcome, given the presence of *exactly* one photon at the input port of such a measurement device. Photodetection efficiency is denoted η_d and modeled with a lossy BS of transmittivity η_d placed before each detector. (Here, again, the exact location of the BS is redundant).

Coupling loss. In a similar fashion, coupling losses may be modeled with a lossy BS as well. But placing two lossy BS in a given mode amounts to placing only one lossy BS whose transmittivity is given by the product of the former two. Thus, it is legitimate to regard coupling loss implicitly accounted for in the parameter η_d, which encompasses all modes, since photodectors are placed in all of the circuit output modes. More generally, η_d accounts for both photodetection, coupling inefficiency and any other possible circuit loss (except transmission loss), and we will simply call η_d the local detection efficiency.

B. Assessment of uncharacterized imperfections

Realistic modelling of a quantum experiment is a delicate task since imperfections not accounted for in the model may lead to overestimations about the performance of the protocol, which in some cases can be completely misleading. The situation is even more dramatic in the DI framework, where such uncharacterized imperfections could be exploited by an eavesdropper. For this reason, in this Section we introduce a method which allows to assess imperfections which are known to be existent but which —for simplicity or for computational reasons— are not accounted for in the model. Concretely, it is assumed that any uncharacterised effect can be exploited by Eve to hack the protocol. The method can assess in principle any uncharacterized imperfection, but as a concrete example, we analyse the problem of dealing with the infinite tail of contributions of the quantum state produced by SPDC sources (5.2). Indeed, all DIQKD proposals so far rely on the use of several SPDC sources to produce photonic entanglement or single photons [GPS10, CM11, MSBB$^+$13, MBA13, PMW$^+$11]. Since no coherence between different number of photons components are observed, the unnormalized single mode SPDC state (5.2) can be written as a convex mixture:

$$\sum_{n=0}^{\infty} \frac{n+1}{2^n} p^n \left|\Psi_n\right\rangle\!\left\langle\Psi_n\right| = \left|0\right\rangle\!\left\langle 0\right| + p \left|\Psi_1\right\rangle\!\left\langle\Psi_1\right| + \ldots, \tag{B.1}$$

where $\left|\Psi_n\right\rangle = \frac{1}{n!\sqrt{n+1}} \left(a_H^\dagger b_V^\dagger - a_V^\dagger b_H^\dagger\right)^n \left|0\right\rangle$ denotes the state of n down-converted photon pairs and p is the probability to produce a single pair in the process. $a_H^\dagger$, $a_V^\dagger$, $b_H^\dagger$ and $b_V^\dagger$ are bosonic creation operators for which H and V denote orthogonal polarization directions, while $\left|0\right\rangle$ denotes the vacuum state of all modes. The parameter $p = 2\,\tanh(g)^2$ parametrizes the probability for high-order contributions. Typically, in the model one truncates the global state produced by all sources up to a certain order n, keeping only the terms of order $\mathcal{O}(p^n)$.

Nevertheless, this perturbative approximation may yield misleading conclusions about the nonlocal character of the observed correlations and compromise DIQKD security for a given setup. In fact, one has to guarantee that contributions not considered in the truncation will not contradict the conclusions about the nonlocal

character of the behavior in question. To avoid this problem, our method based on SDP techniques will allow to assume that all high-order contributions ($> n$) that are not taken into account are fully controlled by E to her benefit. This may seem too conservative, but the method turns to be efficient and not overpessimistic as the contribution of high-order terms becomes irrelevant for sufficiently low values of p, as illustrated in the next Chapter.

The key idea is to conceive higher-order contributions as producing an unknown and uncharacterized quantum behavior $\mathbf{p}_Q$ prepared by Eve for Alice and Bob. If $\mathbf{p}_n^{\text{est}}$ denotes the estimation of the behavior of A and B constructed in the model to the order n, then the first step of the method is to write the observed behavior $\mathbf{p}$ as a convex decomposition: $\mathbf{p} = (1 - \epsilon_n)\mathbf{p}_n^{\text{est}} + \epsilon_n \mathbf{p}_Q$.

Indeed, at the quantum level, the total state produced by a given collection of sources producing a perturbative state such as (B.1) may be written as a convex mixture $p(t)\rho_t + p(\bar{t})\rho_{\bar{t}}$, where ρ_t is the truncated state according to the estimation made at some order n. $\rho_{\bar{t}}$ is thus the remaining "tail" of high-order contributions, and $p(\bar{t}) = 1 - p(t)$. Moving to the level of probability distributions, linearity of Born's rule with respect to ρ implies that the elements of the observed behavior $\mathbf{p}$ conditioned on the outcome c of the QND measurement (see previous Section) may be decomposed in a similar fashion: $P(a, b|c) = p(t|c)P(a, b|c, t) + (1 - p(t|c))P(a, b|c, \bar{t})$. The probabilities $P(a, b|c, t)$ are nothing but the elements of the estimated behavior $\mathbf{p}_n^{\text{est}}$ to the order n. Using Bayes rule, it is possible to re-write $p(t|c)$ as:

$$p(t|c) = \frac{p(c|t)p(t)}{p(c)}. \tag{B.2}$$

The numerator in (B.2) is known, since in particular $p(c|t)$ is merely the estimated probability of c assuming the truncation at the level of the sources. The denominator is unknown as it corresponds to the probability of c without assuming any truncation. However, it is possible to set an upper bound on $p(c)$ (which in turn will correspond to a lower bound on $p(t|c)$):

$$p(c) = \sum_{\vec{k}=\vec{0}}^{\infty} p(\vec{k})p(c|\vec{k}) \leq \sum_{\vec{k}=\vec{0}}^{\vec{K}_n} p(\vec{k})p(c|\vec{k}) + \sum_{\vec{k}>\vec{K}_n}^{\infty} p(\vec{k}) := p_{\vec{K}_n}(c), \tag{B.3}$$

where the vector of variables $\vec{k} = (k_1, k_2, ..., k_s)$ describes the possible number of photons produced by each of the s sources. Concretely $p(\vec{k})$ gives the distribution of each of the possible combinations of photons (or pairs of photons) produced by the sources. $\vec{K}_n$ is the maximum number of photons that each source can produce and depends on the chosen order n, as expected. Using the bound (B.3) in (B.2),

one gets $p(t|c) \geq \frac{p(c|t)p(t)}{p_{\vec{K}_n}(c)}$, which in turn yields the desired bound:

$$\epsilon_n = 1 - \frac{p(c|t)p(t)}{p_{\vec{K}_n}(c)}. \tag{B.4}$$

ϵ_n is thus a fixed real number which goes to zero as the order n increases andn the limit $n \to \infty$, $\mathbf{p}_n^{\text{est}}$ becomes a better estimate of $\mathbf{p}$.

With this, the second step is now to define, in an analogous way to (2.21), the device-independent guessing probability to the order n as:

$$\begin{aligned} G_{\mathbf{p}^{(n)}}(x^*) \quad = \quad & \max_{\{\mathbf{p}^e\}} \sum_e p(e, a = e|x^*) \\ & \text{s.t.} \sum_e \mathbf{p}^e = (1-\epsilon_n)\mathbf{p}_n^{\text{est}} + \epsilon_n \mathbf{p}_Q, \\ & \mathbf{p}_Q \in Q \text{ and } \mathbf{p}^e \in \widetilde{Q}, \ \forall \ e \in \mathcal{O}_{\mathcal{A}}. \end{aligned} \tag{B.5}$$

Here Q ($\widetilde{Q}$) denotes the set of (un)normalized quantum behaviors. In fact, expression (B.5) is similar to (2.21), the only difference being that now Eve is *not* obliged to reproduce the input behavior of the program with her collection of unnormalized behaviors $\{\mathbf{p}^e|e \in \mathcal{O}_{\mathcal{A}}\}$. Instead, she possesses a supplementary quantum behavior $\mathbf{p}_Q$ that she can tailor to reproduce the statistics of the input $\mathbf{p}_n^{\text{est}}$ and guess the outcome of Alice's box in the best possible way, for a given fixed value ϵ_n.

We stress the fact that the methods presented here are quite general as they can be applied to any other uncharacterized imperfection parametrized by ϵ, such that its action arises as convex decomposition of the form $\mathbf{p} = (1-\epsilon)\mathbf{p}^{\text{est}} + \epsilon\mathbf{p}_Q$. For instance this occurs when one convexly adds an unknown noise at the level of the quantum state.

As we can see in Chap. 7, the method performs well when modelling experiments based on quantum optics circuits. We note that recently ref. [STS15] introduced a method based on Gaussian operations which allows to take into account the contribution of all SPDC terms from (B.1), without any truncation or approximation, for an entanglement swapping based setup.

Bibliography

[ABG+07] Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007.

[ABW+09] Markus Ansmann, Radoslaw C. Bialczak, H. Wang, Max Hofheinz, Erik Lucero, M. Neeley, A. D. O'Connell, D. Sank, M. Weides, J. Wenner, A. N. Cleland, and John M. Martinis. Violation of bell's inequality in josephson phase qubits. *Nature*, 461, September 2009.

[ACP+16] Antonio Acin, Daniel Cavalcanti, Elsa Passaro, Stefano Pironio, and Paul Skrzypczyk. Necessary detection efficiencies for secure quantum key distribution and bound randomness. *Phys. Rev. A*, 93:012319, Jan 2016.

[ADGL02] A. Acín, T. Durt, N. Gisin, and J. I. Latorre. Quantum nonlocality in two three-level systems. *Phys. Rev. A*, 65:052325, May 2002.

[AFRV16] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. *arXiv e-print [quant-ph]*, page 1607.01797, 2016.

[AGG05] Antonio Acín, Richard Gill, and Nicolas Gisin. Optimal bell tests do not require maximally entangled states. *Phys. Rev. Lett.*, 95:210402, Nov 2005.

[AMP12] Antonio Acin, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Phys. Rev. Lett.*, 108:100402, Mar 2012.

[APG99] Lucio Claudio Andreani, Giovanna Panzarini, and Jean-Michel Gérard. Strong-coupling regime for quantum boxes in pillar microcavities: Theory. *Phys. Rev. B*, 60:13276–13279, Nov 1999.

[APVW16] Antonio Acín, Stefano Pironio, Tamás Vértesi, and Peter Wittek. Optimal randomness certification from one entangled bit. *Phys. Rev. A*, 93:040102, Apr 2016.

[Ard92] M. Ardehali. Bell inequalities with a magnitude of violation that grows exponentially with the number of particles. *Phys. Rev. A*, 46:5375–5378, Nov 1992.

[AVHD+14] G. H. Aguilar, A. Valdés-Hernández, L. Davidovich, S. P. Walborn, and P. H. Souto Ribeiro. Experimental entanglement redistribution under decoherence channels. *Phys. Rev. Lett.*, 113:240501, Dec 2014.

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

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

[BBS+13] Julio T. Barreiro, Jean-Daniel Bancal, Philipp Schindler, Daniel Nigg, Markus Hennrich, Thomas Monz, Nicolas Gisin, and Rainer Blatt. Demonstration of genuine multipartite entanglement with device-independent witnesses. *Nat Phys*, 9:559–562, 09 2013.

[BC90] S. L. Braunstein and C. M. Caves. Writting out better bell inequalities. *Ann. Phys.*, 202:22, 1990.

[BCK12] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Unconditionally secure device-independent quantum key distribution with only two devices. *Phys. Rev. A*, 86:062326, Dec 2012.

[BCP+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86:419–478, Apr 2014.

[BCW+12] Cyril Branciard, Eric G. Cavalcanti, Stephen P. Walborn, Valerio Scarani, and Howard M. Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A*, 85:010301, Jan 2012.

[BDCZ98] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, Dec 1998.

[Bel64] John Bell. On the einstein podolsky rosen paradox. *Physics*, 1:195–200, 1964.

[Bel87] John Stewart Bell. *Speakable and unspeakable in quantum mechanics*. Collected papers on quantum philosophy. Cambridge Univ. Press, Cambridge, 1987.

[BGLP11] Jean-Daniel Bancal, Nicolas Gisin, Yeong-Cherng Liang, and Stefano Pironio. Device-independent witnesses of genuine multipartite entanglement. *Phys. Rev. Lett.*, 106:250404, Jun 2011.

[BGS05] Nicolas Brunner, Nicolas Gisin, and Valerio Scarani. Entanglement and non-locality are different resources. *New Journal of Physics*, 7(1):88, 2005.

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, Jun 2005.

[BK93] A V Belinski and D N Klyshko. Interference of light and bell's theorem. *Physics-Uspekhi*, 36(8):653, 1993.

[BKG+17] Peter Bierhorst, Emanuel Knill, Scott Glancy, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, and Lynden K. Shalm. Experimentally generated random numbers certified by the impossibility of superluminal signaling. *arXiv e-print [quant-ph]*, page 1702.05178, 2017.

[BPB+15] Tomer Jack Barnea, Gilles Pütz, Jonatan Bohr Brask, Nicolas Brunner, Nicolas Gisin, and Yeong-Cherng Liang. Nonlocality of w and dicke states subject to losses. *Phys. Rev. A*, 91:032108, Mar 2015.

[BPM+16] Natalia Bruno, Vittorio Pini, Anthony Martin, Varun B. Verma, Sae Woo Nam, Richard Mirin, Adriana Lita, Francesco Marsili, Boris Korzh, Félix Bussières, Nicolas Sangouard, Hugo Zbinden, Nicolas Gisin, and Rob Thew. Heralded amplification of photonic qubits. *Opt. Express*, 24(1):125–133, Jan 2016.

[BSS14] Jean-Daniel Bancal, Lana Sheridan, and Valerio Scarani. More randomness from the same data. *New Journal of Physics*, 16(3):033011, 2014.

[BT03] D. Bacon and B. F. Toner. Bell inequalities with auxiliary communication. *Phys. Rev. Lett.*, 90:157904, Apr 2003.

[BV04] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, New York, NY, USA, 2004.

[BYHR13] Nicolas Brunner, Andrew B Young, Chengyong Hu, and John G Rarity. Proposal for a loophole-free bell test based on spin–photon interactions in cavities. *New Journal of Physics*, 15(10):105006, 2013.

[CBB15] Rafael Chaves, Jonatan Bohr Brask, and Nicolas Brunner. Device-independent tests of entropy. *Phys. Rev. Lett.*, 115:110501, Sep 2015.

[CGL+02] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. Bell inequalities for arbitrarily high-dimensional systems. *Phys. Rev. Lett.*, 88:040404, Jan 2002.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

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

[CM11] Marcos Curty and Tobias Moroder. Heralded-qubit amplifiers for practical device-independent quantum key distribution. *Phys. Rev. A*, 84:010304, Jul 2011.

[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. *Phys. Rev. Lett.*, 111:130406, Sep 2013.

[Col07] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. *PhD Thesis, University of Cambridge*, 2007.

[CS16] D. Cavalcanti and P. Skrzypczyk. Quantitative relations between measurement incompatibility, quantum steering, and nonlocality. *Phys. Rev. A*, 93:052112, May 2016.

[CS17] D Cavalcanti and P Skrzypczyk. Quantum steering: a review with focus on semidefinite programming. *Reports on Progress in Physics*, 80(2):024001, 2017.

[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. *Nat Commun*, 6, 08 2015.

[CVSB+15] V. Caprara Vivoli, P. Sekatski, J.-D. Bancal, C. C. W. Lim, B. G. Christensen, A. Martin, R. T. Thew, H. Zbinden, N. Gisin, and N. Sangouard. Challenging preconceptions about bell tests with photon pairs. *Phys. Rev. A*, 91:012107, Jan 2015.

[DdlTA14] Chirag Dhara, Gonzalo de la Torre, and Antonio Acin. Can observed randomness be certified to be fully intrinsic? *Phys. Rev. Lett.*, 112:100402, Mar 2014.

[DHD+16] Xing Ding, Yu He, Z.-C. Duan, Niels Gregersen, M.-C. Chen, S. Unsleber, S. Maier, Christian Schneider, Martin Kamp, Sven Höfling, Chao-Yang Lu, and Jian-Wei Pan. On-demand single photons with high extraction efficiency and near-unity indistinguishability from a resonantly driven quantum dot in a micropillar. *Phys. Rev. Lett.*, 116:020401, Jan 2016.

[dlTHD+15] Gonzalo de la Torre, Matty J. Hoban, Chirag Dhara, Giuseppe Prettico, and Antonio Acín. Maximally nonlocal theories cannot be maximally random. *Phys. Rev. Lett.*, 114:160502, Apr 2015.

[DPP05] Giacomo Mauro D'Ariano, Paoloplacido Lo Presti, and Paolo Perinotti. Classical randomness in quantum measurements. *Journal of Physics A: Mathematical and General*, 38(26):5979, 2005.

[dRGP+17] Anna de Rosier, Jacek Gruca, Fernando Parisio, Tamas Vertesi, and Wieslaw Laskowski. Multipartite nonlocality and random measurements. *arXiv e-print [quant-ph]*, page 1704.0034, 2017.

[dV14] Julio I de Vicente. On nonlocality as a resource theory and nonlocality measures. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424017, 2014.

[DW05] Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Soci-*

ety of London A: Mathematical, Physical and Engineering Sciences, 461(2053):207–235, 2005.

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

[Eke91] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

[EPR92] Avshalom C. Elitzur, Sandu Popescu, and Daniel Rohrlich. Quantum nonlocality for each pair in an ensemble. *Physics Letters A*, 162(1):25 – 28, 1992.

[FAVH+12] O. Jiménez Farías, G. H. Aguilar, A. Valdés-Hernández, P. H. Souto Ribeiro, L. Davidovich, and S. P. Walborn. Observation of the emergence of multipartite entanglement between a bipartite system and its environment. *Phys. Rev. Lett.*, 109:150403, Oct 2012.

[Fin82] Arthur Fine. Hidden variables, joint probability, and the bell inequalities. *Phys. Rev. Lett.*, 48:291–295, Feb 1982.

[FP15] E. A. Fonseca and Fernando Parisio. Measure of nonlocality which is maximal for maximally entangled qutrits. *Phys. Rev. A*, 92:030101, Sep 2015.

[G+11] Jan Gudat et al. Permanent tuning of quantum dot transitions to degenerate microcavity resonances. *Applied Physics Letters*, 98(12):121111, 2011.

[GA15] Rodrigo Gallego and Leandro Aolita. Resource theory of steering. *Phys. Rev. X*, 5:041008, Oct 2015.

[GBHA10] Rodrigo Gallego, Nicolas Brunner, Christopher Hadley, and Antonio Acín. Device-independent tests of classical and quantum dimensions. *Phys. Rev. Lett.*, 105:230501, Nov 2010.

[Gis91] N. Gisin. Bell's inequality holds for all non-product states. *Physics Letters A*, 154(5):201 – 202, 1991.

[GLLL+11a] Ilja Gerhardt, Qin Liu, Antia Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat Commun*, 2, March 2011.

[GLLL+11b] Ilja Gerhardt, Qin Liu, Antia Lamas-Linares, Johannes Skaar, Valerio Scarani, Vadim Makarov, and Christian Kurtsiefer. Experimentally faking the violation of bell's inequalities. *Phys. Rev. Lett.*, 107:170404, Oct 2011.

[GMDLT+13] Rodrigo Gallego, Lluis Masanes, Gonzalo De La Torre, Chirag Dhara, Leandro Aolita, and Antonio Acín. Full randomness from arbitrarily deterministic events. *Nature Communications*, 4:2654 EP –, 10 2013.

[GMR+13] Marissa Giustina, Alexandra Mech, Sven Ramelow, Bernhard Wittmann, Johannes Kofler, Jorn Beyer, Adriana Lita, Brice Calkins, Thomas Gerrits, Sae Woo Nam, Rupert Ursin, and Anton Zeilinger. Bell violation using entangled photons without the fair-sampling assumption. *Nature*, 497:227 – 230, Sep 2013.

[GPS10] Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier. *Phys. Rev. Lett.*, 105:070501, Aug 2010.

[GT09] Otfried Guhne and Gheza Toth. Entanglement detection. *Physics Reports*, 474:1 – 75, 2009.

[GVW+15] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015.

[GWAN12] Rodrigo Gallego, Lars Erik Würflinger, Antonio Acín, and Miguel Navascués. Operational framework for nonlocality. *Phys. Rev. Lett.*, 109:070401, Aug 2012.

[HBD+15] B. Hensen, H. Bernien, A. E. Dreau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526:682–686, 10 2015.

[HBG+07] Matthaus Halder, Alexios Beveratos, Nicolas Gisin, Valerio Scarani, Christoph Simon, and Hugo Zbinden. Entangling independent photons by time measurement. *Nature*, 3, October 2007.

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Rev. Mod. Phys.*, 81:865–942, Jun 2009.

[HKO+12] Julian Hofmann, Michael Krug, Norbert Ortegel, Lea Gérard, Markus Weber, Wenjamin Rosenfeld, and Harald Weinfurter. Heralded entanglement between widely separated atoms. *Science*, 337(6090):72–75, 2012.

[HMP00] Richard J. Hughes, George L. Morgan, and C. Glen Peterson. Quantum key distribution over a 48 km optical fibre network. *Journal of Modern Optics*, 47(2-3):533–547, 2000.

[HR09] Esther Hänggi and Renato Renner. Device-independent quantum key distribution with commuting measurements. *arXiv e-print [quant-ph]*, page 1009.1833, 2009.

[HYO+08] C. Y. Hu, A. Young, J. L. O'Brien, W. J. Munro, and J. G. Rarity. Giant optical faraday rotation induced by a single-electron spin in a quantum dot: Applications to entangling remote spins via a single photon. *Phys. Rev. B*, 78:085307, Aug 2008.

[idZB02] Marek Żukowski and Časlav Brukner. Bell's theorem for general n-qubit states. *Phys. Rev. Lett.*, 88:210401, May 2002.

[KB00] Pieter Kok and Samuel L. Braunstein. Postselected versus nonpostselected quantum teleportation using parametric down-conversion. *Phys. Rev. A*, 61:042304, Mar 2000.

[KLH+15] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew,

and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat Photon*, 9(3):163–168, 03 2015.

[KRRR15] Norbert Kalb, Andreas Reiserer, Stephan Ritter, and Gerhard Rempe. Heralded storage of a photonic quantum bit in a single atom. *Phys. Rev. Lett.*, 114:220501, Jun 2015.

[KRS09] R. Koenig, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Th.*, 55(9), 2009.

[KWW+99] Paul G. Kwiat, Edo Waks, Andrew G. White, Ian Appelbaum, and Phillipe H. Eberhard. Ultrabright source of polarization-entangled photons. *Phys. Rev. A.*, 60:R773, 1999.

[KXRP13] S. Kocsis, G. Y. Xiang, T. C. Ralph, and G. J. Pryde. Heralded noiseless amplification of a photon polarization qubit. *Nat Phys*, 9:23–28, 01 2013.

[Lap14] Pierre Simon Laplace. *A philosophical essay on probabilities*. 1814.

[Lar14] Jan Larsson. Loopholes in bell inequality tests of local realism. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424003, 2014.

[LaYZB+17] Pei-Sheng Lin, Denis Rosset amd Yanbao Zhang, Jean-Daniel Bancal, , and Yeong-Cherng Liang. Taming finite statistics for device-independent quantum information. *arXiv e-print [quant-ph]*, page 1705.09245, 2017.

[LBH+16] J. C. Loredo, M. A. Broome, P. Hilaire, O. Gazzano, I. Sagnes, A. Lemaitre, M. P. Almeida, P. Senellart, and A. G. White. Boson-sampling with single-photon fock states from a bright solid-state source. *arXiv e-print [quant-ph]*, page 1603.00054, 2016.

[LCMA] Victoria Lipinska, Florian Curchod, Alejandro Máttar, and Antonio Acin. *Unpublished*.

[LCQ12] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[LHBR10] Yeong-Cherng Liang, Nicholas Harrigan, Stephen D. Bartlett, and Terry Rudolph. Nonclassical correlations from randomly chosen local measurements. *Phys. Rev. Lett.*, 104:050401, Feb 2010.

[LRBT14] Mikołaj Lasota, Czesław Radzewicz, Konrad Banaszek, and Rob Thew. Linear optics schemes for entanglement distribution with realistic single-photon sources. *Phys. Rev. A*, 90:033836, Sep 2014.

[LS98] Maciej Lewenstein and Anna Sanpera. Separability and entanglement of composite quantum systems. *Phys. Rev. Lett.*, 80:2261–2264, Mar 1998.

[LVB11] Yeong-Cherng Liang, Tamás Vértesi, and Nicolas Brunner. Semi-device-independent bounds on entanglement. *Phys. Rev. A*, 83:022108, Feb 2011.

[LWW+10] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat Photon*, 4:686–689, Oct 210.

[MBA13] Alejandro Máttar, Jonatan Bohr Brask, and Antonio Acín. Device-independent quantum key distribution with spin-coupled cavities. *Phys. Rev. A*, 88:062319, Dec 2013.

[Mer90] N. David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65:1838–1840, Oct 1990.

[MKL+14] Sreraman Muralidharan, Jungsang Kim, Norbert Lütkenhaus, Mikhail Lukin, and Liang Jiang. Ultrafast and fault-tolerant quantum communication across long distances. *arXiv e-print [quant-ph]*, page 1310.529, 2014.

[MPA11] Lluis Masanes, Stefano Pironio, and Antonio Acin. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat Commun*, 2:238–, March 2011.

[MS07] André Allan Méthot and Valerio Scarani. An anomaly of non-locality. *Quantum Info. Comput.*, 7(1):157–170, January 2007.

[MS16] Carl A. Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM*, 63(4):33:1–33:63, October 2016.

[MSA+17] Alejandro Máttar, Paul Skrzypczyk, Gabriel Aguilar, Ranieri Nery, Paulo Souto Ribeiro, Stephen Walborn, and Daniel Cavalcanti. Experimental multipartite entanglement and randomness certification

of the w state in the quantum steering scenario. *Quantum Science and Technology*, 2017.

[MSB+15] Alejandro Máttar, Paul Skrzypczyk, Jonatan Bohr Brask, Daniel Cavalcanti, and Antonio Acín. Optimal randomness generation from optical bell experiments. *New Journal of Physics*, 17(2):022003, 2015.

[MSBB+13] Evan Meyer-Scott, Marek Bula, Karol Bartkiewicz, Antonín Černoch, Jan Soubusta, Thomas Jennewein, and Karel Lemr. Entanglement-based linear-optical qubit amplifier. *Phys. Rev. A*, 88:012327, Jul 2013.

[MVV+16] F. Monteiro, E. Verbanis, V. Caprara Vivoli, A. Martin, N. Gisin, H. Zbinden, and R. T. Thew. Heralded amplification of path entangled quantum states. *arXiv e-print [quant-ph]*, page 1612.01802, 2016.

[MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th IEEE Conference on Foundations of Computer Science*, 1998.

[NC00] M. Nielsen and I. C. Chuang. *Quantum Computation and Quantum Information*. 2000.

[NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acin. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, Jan 2007.

[NSBSP16] Olmo Nieto-Silleras, Cédric Bamps, Jonathan Silman, and Stefano Pironio. Device-independent randomness generation from several bell estimators. *arXiv e-print [quant-ph]*, page 1611.00352, 2016.

[NSPS14] O. Nieto-Silleras, S. Pironio, and J. Silman. Using complete measurement statistics for optimal device-independent randomness evaluation. *New J. Phys.*, 16, Jan 2014.

[NV16] Sandor Nagy and Tamas Vertesi. Epr steering inequalities with communication assistance. *Scientific Reports*, 6:21634 EP –, 02 2016.

[PAM+10] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. FHayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by bells theorem. *Nature*, 464, April 2010.

[PB11] Marcin Pawłowski and Nicolas Brunner. Semi-device-independent security of one-way quantum key distribution. *Phys. Rev. A*, 84:010302, Jul 2011.

[PBWZ98] Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger. Experimental entanglement swapping: Entangling photons that never interacted. *Phys. Rev. Lett.*, 80:3891–3894, May 1998.

[PCSA15] Elsa Passaro, Daniel Cavalcanti, Paul Skrzypczyk, and Antonio Acin. Optimal randomness certification in the quantum steering and prepare-and-measure scenarios. *New Journal of Physics*, 17(11):113010, 2015.

[PCW06] Young-Shin Park, Andrew K. Cook, and Hailin Wang. Cavity qed with diamond nanocrystals and silica microspheres. *Nano Letters*, 6(9):2075–2079, 2006.

[Pea70] Philip M. Pearle. Hidden-variable example based upon data rejection. *Phys. Rev. D*, 2:1418–1425, Oct 1970.

[PMLA13] S. Pironio, Ll. Masanes, A. Leverrier, and A. Acin. Security of device-independent quantum key distribution in the bounded-quantum-storage model. *Phys. Rev. X*, 3:031007, Aug 2013.

[PMW+11] David Pitkanen, Xiongfeng Ma, Ricardo Wickert, Peter van Loock, and Norbert Lutkenhaus. Efficient heralding of photonic qubits with applications to device-independent quantum key distribution. *Phys. Rev. A*, 84:022325, Aug 2011.

[POS+15] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen. High-rate measurement-device-independent quantum cryptography. *Nat Photon*, 9:397–402, Jun 2015.

[QVB14] Marco Túlio Quintino, Tamás Vértesi, and Nicolas Brunner. Joint measurability, einstein-podolsky-rosen steering, and bell nonlocality. *Phys. Rev. Lett.*, 113:160402, Oct 2014.

[QVC+15] Marco Túlio Quintino, Tamás Vértesi, Daniel Cavalcanti, Remigiusz Augusiak, Maciej Demianowicz, Antonio Acín, and Nicolas Brunner. Inequivalence of entanglement, steering, and bell non-

locality for general measurements. *Phys. Rev. A*, 92:032107, Sep 2015.

[Ra04] J. P. Reithmaier and al. Strong coupling in a single quantum dot-semiconductor microcavity system. *Nature*, 432:197–200, 2004.

[RFSB+12] Denis Rosset, Raphael Ferretti-Schöbitz, Jean-Daniel Bancal, Nicolas Gisin, and Yeong-Cherng Liang. Imperfect measurement settings: Implications for quantum state tomography and entanglement witnesses. *Phys. Rev. A*, 86:062325, Dec 2012.

[RKM+01] M. A. Rowe, D. Kielpinski, V. Meyer, W. M.. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a bell's inequality with efficient detection. *Nature*, 409, February 2001.

[RL09] T. C. Ralph and A. P. Lund. Proceedings of 9th international conference on quantum measurement and computing. pages 155 (e–print arXiv:0809.0326). AIP, New York, 2009.

[RMKH+12] Janine Riedrich-Moller, Laura Kipfstuhl, Christian Hepp, Elke Neu, Christoph Pauly, Frank Mucklich, Armin Baur, Michael Wandt, Sandra Wolff, Martin Fischer, Stefan Gsell, Matthias Schreck, and Christoph Becher. One- and two-dimensional photonic crystal microcavities in single crystal diamond. *Nat Nano*, 7(1):69–74, 2012.

[RNH+12] Stephan Ritter, Christian Nolleke, Carolin Hahn, Andreas Reiserer, Andreas Neuzner, Manuel Uphoff, Martin Mucke, Eden Figueroa, Joerg Bochmann, and Gerhard Rempe. An elementary quantum network of single atoms in optical cavities. *Nature*, 484(7393):195–200, 2012.

[RS91] S. M. Roy and Virendra Singh. Tests of signal locality and einstein-bell locality for multiparticle systems. *Phys. Rev. Lett.*, 67:2761–2764, Nov 1991.

[RUV12a] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems via rigidity of chsh games. *arXiv e-print [quant-ph]*, page 1209.0449, 2012.

[RUV12b] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of chsh games. *arXiv e-print [quant-ph]*, page 1209.0448, 2012.

[San92] Emilio Santos. Critical analysis of the empirical tests of local hidden-variable theories. *Phys. Rev. A*, 46:3646–3656, Oct 1992.

[SAT+16] Alexia Salavrakos, Remigiusz Augusiak, Jordi Tura, Peter Wittek, Antonio Acin, and Stefano Pironio. Bell inequalities for maximally entangled states. *arXiv e-print [quant-ph]*, page 1607.0457, 2016.

[SBC+15] Ana Belén Sainz, Nicolas Brunner, Daniel Cavalcanti, Paul Skrzypczyk, and Tamás Vértesi. Postquantum steering. *Phys. Rev. Lett.*, 115:190403, Nov 2015.

[SBM+13] Nicolas Sangouard, Jean-Daniel Bancal, Philipp Müller, Joyee Ghosh, and Jürgen Eschner. Heralded mapping of photonic entanglement into single atoms in free space: proposal for a loophole-free bell test. *New Journal of Physics*, 15(8):085004, 2013.

[Sch35] E. Schrödinger. Die gegenwärtige situation in der quantenmechanik. *Naturwissenschaften*, 23:807–844, 1935.

[SGDS+16] N. Somaschi, V. Giesz, L. De Santis, J. C. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Anton, J. Demory, C. Gomez, I. Sagnes, N. D. Lanzillotti-Kimura, A. Lemaitre, A. Auffeves, A. G. White, L. Lanco, and P. Senellart. Near-optimal single-photon sources in the solid state. *Nat Photon*, advance online publication, March 2016.

[SK14] Valerio Scarani and Christian Kurtsiefer. The black paper of quantum cryptography: Real implementation problems. *Theoretical Computer Science*, 560, Part 1:27 – 32, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of {BB84}.

[SMM+17] Justin B. Spring, Paolo L. Mennea, Benjamin J. Metcalf, Peter C. Humphreys, James C. Gates, Helen L. Rogers, Christoph Söller, Brian J. Smith, W. Steven Kolthammer, Peter G. R. Smith, and Ian A. Walmsley. Chip-based array of near-identical, pure, heralded single-photon sources. *Optica*, 4(1):90–96, Jan 2017.

[SMSC+15] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E. Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan L. Migdall,

Yanbao Zhang, Daniel R. Kumor, William H. Farr, Francesco Marsili, Matthew D. Shaw, Jeffrey A. Stern, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Thomas Jennewein, Morgan W. Mitchell, Paul G. Kwiat, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam. Strong loophole-free test of local realism*. *Phys. Rev. Lett.*, 115:250402, Dec 2015.

[SMWF+07] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G. Rarity, Anton Zeilinger, and Harald Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98:010504, Jan 2007.

[SNC14] Paul Skrzypczyk, Miguel Navascués, and Daniel Cavalcanti. Quantifying einstein-podolsky-rosen steering. *Phys. Rev. Lett.*, 112:180404, May 2014.

[STS15] Kaushik P. Seshadreesan, Masahiro Takeoka, and Masahide Sasaki. Towards practical device-independent quantum key distribution with spontaneous parametric downconversion sources, on-off photodetectors and entanglement swapping. *arXiv e-print [quant-ph]*, page 1512.06876, 2015.

[SZDM15] Adel Sohbi, Isabelle Zaquine, Eleni Diamanti, and Damian Markham. Decoherence effects on the nonlocality of symmetric states. *Phys. Rev. A*, 91:022101, Feb 2015.

[TdlTB+16] Le Phuc Thinh, Gonzalo de la Torre, Jean-Daniel Bancal, Stefano Pironio, and Valerio Scarani. Randomness in post-selected events. *New Journal of Physics*, 18(3):035007, 2016.

[TR11] Marco Tomamichel and Renato Renner. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.*, 106:110506, Mar 2011.

[UMG14] Roope Uola, Tobias Moroder, and Otfried Gühne. Joint measurability of generalized measurements implies classicality. *Phys. Rev. Lett.*, 113:160403, Oct 2014.

[VSB+15] V Caprara Vivoli, P Sekatski, J-D Bancal, C C W Lim, A Martin, R T Thew, H Zbinden, N Gisin, and N Sangouard. Comparing different approaches for generating random numbers device-independently using a photon pair source. *New Journal of Physics*, 17(2):023023, 2015.

[VV14] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014.

[VW11] Thomas Vidick and Stephanie Wehner. More nonlocality with less entanglement. *Phys. Rev. A*, 83:052310, May 2011.

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

[WJD07] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, entanglement, nonlocality, and the einstein-podolsky-rosen paradox. *Phys. Rev. Lett.*, 98:140402, Apr 2007.

[WP15] Erik Woodhead and Stefano Pironio. Secrecy in prepare-and-measure clauser-horne-shimony-holt tests with a qubit bound. *Phys. Rev. Lett.*, 115:150501, Oct 2015.

[WPGF09] Michael M. Wolf, David Perez-Garcia, and Carlos Fernandez. Measurements incompatible in quantum theory cannot be measured jointly in any other no-signaling theory. *Phys. Rev. Lett.*, 103:230402, Dec 2009.

[WW01] R. F. Werner and M. M. Wolf. All-multipartite bell-correlation inequalities for two dichotomic observables per site. *Phys. Rev. A*, 64:032112, Aug 2001.

[YCY+16] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.*, 117:190501, Nov 2016.

[YHR13] A. B. Young, C. Y. Hu, and J. G. Rarity. Generating entanglement with low-q-factor microcavities. *Phys. Rev. A*, 87:012332, Jan 2013.

[YOH+11] A. B. Young, R. Oulton, C. Y. Hu, A. C. T. Thijssen, C. Schneider, S. Reitzenstein, M. Kamp, S. Höfling, L. Worschech, A. Forchel, and J. G. Rarity. Quantum-dot-induced phase shift in a pillar microcavity. *Phys. Rev. A*, 84:011803, Jul 2011.

[ZFQ+08] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78:042333, Oct 2008.

[ZQM+06] Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, and Li Qian. Experimental quantum key distribution with decoy states. *Phys. Rev. Lett.*, 96:070502, Feb 2006.

[ZXT+07] Qiang Zhang, Xiuping Xie, Hiroki Takesue, Sae Woo Nam, Carsten Langrock, M. M. Fejer, and Yoshihisa Yamamoto. Correlated photon-pair generation in reverse-proton-exchange ppln waveguides with integrated mode demultiplexer at 10 ghz clock. *Opt. Express*, 15(16):10288–10293, Aug 2007.