UNIVERSIDAD DE CONCEPCIÓN
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DOCTORADO EN CIENCIAS FÍSICAS

Device Independent Certification in Quantum Information

Certificación Dispositivo Independiente en Información Cuántica

Profesor Guía: Dr. Gustavo Moreira Lima
Departamento de Física
Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Tesis para optar al grado de Doctor en Ciencias Físicas de la Universidad de Concepción

JOHANNA LORENA FIGUEROA BARRA
CONCEPCIÓN - CHILE
2016

Comisión Examinadora : Dr. Gustavo Moreira Lima

Dr. Guilherme Xavier Barreto

Dr. Aldo Delgado Hidalgo

dedicado a mis matriarcas, Oriettita y Valy

Contents

List of Figures

List of Tables

Agradecimientos (Acknowledgments)

Primero que todo agradecer al gran grupo humano con el que tuve el agrado de trabajar durante todo el desarrollo de mi doctorado. A mi tutor el Dr. Gustavo Lima, quién me ha guiado, apoyado y dado todas las herramientas necesarias para convertirme en una investigadora integral, su visión de como debe hacerse ciencia y su entusiasmo por fomentar la cooperación internacional me ha motivado enormemente. A mis queridos compañeros de laboratorio, Gustavo, Esteban y Pablo, con los cuales siempre he podido discutir ideas y que me han dado su apoyo siempre que lo he necesitado.

Durante el último período de mi doctorado tuve la suerte de poder realizar una pasantía con el grupo del Dr. Marcin Pawłowski en el National Quantum Information Centre en Gdańsk, Polonia, a quien también quiero agradecer por su gran disposición para colaborar y discutir nuevas ideas. Esta pasantía además me dió una visión mucho más amplia de como funciona el mundo de la investigación en otras partes del mundo, lo cual es muy importante para el desarrollo de un investigador.

Mis más grandes agradecimientos a mi gran familia, a mi abuelita Orietta y mi madre Valeria, quienes siempre tienen las mejores palabras y gestos de apoyo en momentos de flaqueza. A mi compañero de aventuras, Diego, por apoyarme y darme la libertad de desarrollarme como investigadora, con todos los sacrificios que ello conlleva. A mis amigos de siempre, Marcos y Macarena, que nunca fallan y que siempre quieren aprender algo más de la *universifísica*. A mis amigos de la ciencia, Alejandra, Pablo, Nataly y Gabriel, con los cuales nos acompañamos en cada aventura científica y en otras no tan científicas también.

También quisiera agradecer a todos los investigadores que conforman el Centro de Óptica y Fotónica, por el apoyo brindado para poder desarrollar exitosamente este doctorado, tanto en la discusión de ideas como en el apoyo financiero para mi participación en congresos. A los integrantes de mi comisión, los Dr. Aldo Delgado y Dr. Guilherme Xavier, por interesarse en mi trabajo.

Mi doctorado fue financiado por la Beca de Doctorado Nacional de la Comisión Nacional de Investigación Científica y Tecnológica (CONICYT); y por el Centro de Óptica y Fotónica (CEFOP) e Iniciativa Científica Milenio (ICM) quienes me brindaron apoyo financiero para asistencia a congresos.

Abstract

This thesis is completely devoted to the problem of testing the dimension of Hilbert spaces. Protocols that aim to put lower bounds on the Hilbert space dimension of an unknown system are named *dimension witnesses*. But, is the dimension of a quantum system an experimentally measurable quantity? The answer is yes!, dimension witnesses are the tools that allow us to turn the Hilbert space dimension, which is a very abstract concept, into an experimentally measurable property. Dimension witnesses are generally linear functions of probabilities, therefore, by using them we are able to find the minimal dimension d necessary to reproduce a given set of probabilities.

Why dimension witnesses are important? Because the dimensionality of physical systems is a key resource for quantum information processing since it is a form to quantify the power of quantum correlations, therefore, being able to (i) certify that a source produces systems of at least certain dimensions, and (ii) distinguish between quantum systems from classical systems of the same dimension, is of practical importance in many quantum information protocols.

The first dimension witness that we study on this thesis is the one presented by Gallego *et al.* in [Phys. Rev. Lett. **105**, 230501 (2010)]. Their dimension witness was designed under the "prepare-and-measure" scenario described by two black boxes, one being the state preparator and the other the measurement device, then the experiment is described by the probability distribution $P(b|x, y)$, corresponding to the probability of obtaining the outcome b when the measurement box performs a measurement y over the state ρ_x prepared by the state preparation box. Therefore, any statement about the minimal dimension of the system ρ_x is giving from the observed data, which means that this test is *device independent*.

We were motivated to study the dimension witness of Gallego *et al.* because it fulfils points (i) and (ii) for systems of any dimension, in a device independent way. For that reason, we perform the test that allowed us to experimentally witness in a device independent manner the generation of six-dimensional quantum systems, which, to our knowledge, was the highest dimension experimentally certified at that time. This work will be fully described in Chapter 2.

However, the device independent dimension witness described above is not adequate

to test high-dimensional systems due to the amount of parameters involved in the test, increases as $2d^2$. Thus, it is necessary to find new tools that allow us to certify the dimension of the systems produced by our sources, that be feasible for high-dimensional systems, where by feasible we mean that for example it requires a tractable amount of measurements or the difference between the classical and quantum bound is big enough to be observed in an experiment.

As a result of a collaboration with the group of Dr. Marcin Pawłowski we started to work with a communication task called *quantum random access codes*, which is the quantum version of the task random access codes. These tasks were developed under the following scenario: one user, Alice, encodes her n bits message into a m bits system or a m qubits systems, for the classical and quantum version respectively, with $m < n$, and sends it to another user, Bob, who performs a measurement in order to access and recover, with the highest probability p, the value of one of the n bits of Alice's message. Nevertheless, these tasks are not restricted to two dimensional systems, but the generalization for any dimension is not straightforward, so an exhaustive research is needed for any particular dimension different than two. The importance of quantum random access codes is that it shows lots of potential as a tool to solve the problem of lack of dimension witnesses for high-dimensional systems, however, the experimental implementation of d-dimensional quantum random access codes would need d detectors, which is not feasible for high-dimensions.

To overcome this problem, we worked in a modified version of quantum random access codes where the output is binary instead of d-dimensional. With this modified version we propose a dimension witness for physical systems of dimension eight that also works as a *quantumness indicator*, which means that it is capable to discriminate between classical and quantum eight-dimensional systems. The most important property of our modified version of quantum random access codes is that in its experimental implementation only need the averages probabilities. This other work will be discussed in its entirety in Chapter 3.

Resumen

Esta tesis esta totalmente dedicada al problema de certificar las dimensiones de los espacios de Hilbert. Los protocolos que apuntan a establecer límites inferiores para las dimensiones de los espacios de Hilbert de sistemas desconocidos son llamados *testigos de dimensión*. Pero, Â¿es la dimensión de un sistema cuántico desconocido una cantidad medible experimentalmente? La respuesta es sí!, los testigos de dimensión son las herramientas que nos permiten convertir un concepto tan abstracto como lo es la dimensión del espacio de Hilbert en una propiedad medible experimentalmente. Debido a que los testigos de dimensión son generalmente funciones lineales de probabilidades, al hacer uso de ellos somo capaces de encontrar la mínima dimensión d necesaria para reproducir un dado conjunto de probabilidades.

Â¿Por qué som importantes los testigos de dimensión? Pues porque la dimensionalidad de los sistemas físicos es un recurso clave para el procesamiento de inforamción cuántica, ya que es una forma de cuantificar el poder de las correlaciones cuánticas, de esta forma, ser capaces de (i) certificar que una fuente produce sistemas de al menos cierta dimensión, y (ii) distinguir entre sistema clásicos y sistemas cuánticos de la misma dimensión, es de suma importancia para varios protocolos de información cuántica.

El primer testigo de dimensión que estudiamos en esta tesis fue aquel presentado por Gallego *et al.* en [Phys. Rev. Lett. **105**, 230501 (2010)]. Este fue diseñado bajo el escenario de "preparación-y-medición", el cual está descrito por dos cajas negras, una representando la preparación de estados y la otra al dispositivo de medición, de esta forma el experimento es descrito por la distribución de probabilidad $P(b|x, y)$, la cual corresponde a la probabilidad de obtener el resultado b cuando el dispositivo de medición realiza la medida y sobre el estado ρ_x preparado por el dispositivo de prepapración de estados. Luego, cualquier afirmación sobre la mínima dimensión del sistema ρ_x es hecha a partir de la data observada, lo que significa que este análisis es *dispositivo independiente*.

La motivación para estudiar el testigo de dimensión de Gallego *et al.* fue que cumplía con los puntos (i) y (ii), mencionados anteriormente, para sistemas de cualquier dimensión, en una forma dispositivo independiente. Este estudio nos llevó a realizar un test que nos permitió certificar experimentalmente de una forma dispositivo in-

dependiente la generación de sistemas cuánticos seis-dimensionales, la cual a nuestro conocimiento, era la más alta dimensión certificada esperimentalmente hasta el momento. Este trabajo será descrito durante todo el Capítulo 2.

Sin embargo, el testigo de dimensión dispositivo independiente descrito anteriormente no es adecuado para certificar sistemas de altas dimensiones debido a que la cantidad de parámetros involucrados en la certificación incrementa con la dimensión de la forma $2d^2$. Por lo tanto, es necesario encontrar nuevas herramientas que nos permitan certificar la dimensión de los sistemas producidos por nuestras fuentes, que sean realizables para sistemas de altas dimensiones, donde por realizables nos referimos a que por ejemplo requieran una cantidad razonable de mediciones o que la diferencia entre los límites clásicos y cuánticos sea lo suficientemente grande como para ser observada experimentalmente.

Como resultado de la colaboración con el grupo del Dr. Marcin Pawłowski, comenzamos a trabajar con una tarea de comunicación llamada *quantum random access codes*, la cual es la versión cuántica de la tarea random access codes. Estas tareas fueron desarrolladas en el siguiente escenario: un usuario, Alice, codifica su mensaje de n bits en un sistema de m bits o m qubits, para la versión clásica y cuántica respectivamente, con $m < n$, y se lo envía a otro usuario, Bob, quien realiza una medida para poder decodificar, con la mayor probabilidad posible p, el valor de uno de los n bits del mensaje de Alice. Cabe mencionar que estas tareas no están restringidas a sistemas bidimensionales, pero su generalización para cualquier dimensión no es directa, por lo que un estudio exhaustivo es necesario para cualquier dimensión en particular diferente a dos. La importancia de los quantum random access codes es que muestra un gran potencial como herramienta para resolver el problema de la falta de testigos de dimensión para sistemas de altas dimensiones, no obstante, la implementación experimental de un quantum random access code d-dimensional requeriría d detectores, lo cual no es realizable para altas dimensiones.

Para superar este problema, trabajamos en una verisón modificada de quantum random access codes donde las salidas son binarios en vez de d-dimensionales. Con esta versión modificada propusimos un testigo de dimensión para sistemas físicos de dimensión ocho, el cual además también funcionaba como un *indicador de cuanticidad*, es decir, que era capaz de discriminar entre sistemas clásicos y cuánticos de dimensión ocho. La propiedad más importante de nuestra versión modificada de quantum random access codes es que en su implementación experimental sólo necesita promedios de probabilidades. Este segundo trabajo será abordado en su totalidad durante el Capítulo 3.

1 Introduction

Traditionally, theoretical models are built upon assumptions of the system under study, such as its dimensions or its degrees of freedom. This leads to requirements when proving experimentally the theoretical predictions, such as a complete description of the devices involved. However, about ten years ago it was noticed that with the statistics obtained by Bell tests it was possible to characterize the quantum systems involved in the test, without any "a priori" knowledge of, for example, the dimensions of the systems, the degrees of freedom that are measured, or the level of entanglement between the systems. Based on this fact of Bell tests, a reformulation of quantum theory without a previous description of quantum systems has been recently proposed under the name of device-independent (DI) [1]. The DI approach is very appealing from an experimental perspective, because, to have a full knowledge of the devices is very demanding, so, even when the tests features untrusted devices and there are no assumptions about the nature of the systems under study, statements can be made based on measurements data only. The first protocol that took advantage of the DI approach was quantum key distribution (QKD) [2, 3], where it was established that a secure distribution of the key is possible in a DI scenario if the quantum correlations between the measurements of the parties involved are nonlocal, which they proved by means of Bell inequalities violations [4].

An important problem which can be addressed in a device independent manner is the one of providing a lower bound on the dimension of unknown physical systems. Dimensionality of physical systems is a key resource for quantum information processing because it is a form to quantify the power of quantum correlations. For this reason, being able to (i) certify that a source produces systems of at least certain dimensions, and (ii) distinguish between quantum systems from classical systems of the same dimension, is of practical importance in many quantum information protocols.

Responding to the need of tools to provide lower bounds for the dimensions of physical systems, the concept of dimension witness (DW) was introduced [5], giving experimental access to the dimension of Hilbert spaces for the the first time. This work motivates further dimension witnesses, some based on Bell-type inequalities [6, 7, 8], where lower bounds on the dimension of locally measured entangled states are provided, others related to quantum random access codes [9], and recently in [10] they make use

of noncontextuality inequalities to bound the dimension of single systems by performing sequential measurements on them. However, these dimension witnesses were defined to test systems of certain dimensions or in complex scenarios, but the work presented in [11] filled the gap by introducing a family of device independent dimension witnesses able to test systems of arbitrary dimensions. Nonetheless, the DI DW family proposed in [11] do not offer a feasible scenario to certify quantum systems of high-dimension of the order $d \geq 2^5$, where by feasible we mean that for example it requires a tractable amount of measurements or the difference between the classical and quantum bound is big enough to be observed in an experiment.

But why high-dimension systems? Nowadays is has been noticed that in order to satisfied the requirements of our digital networked society, we need to be able to manipulate quantum systems of high dimensions. Therefore, with no doubt, the lack of both, theoretical tools and experimental methods that allow the certification of quantum systems of dimensions $d \geq 2^5$, is a relevant problem.

A communication task called quantum random access codes (QRACs) shows lots of potential as a tool to solve the problem of lack of dimension witnesses for high-dimensional systems. In general QRAC stands for "encoding a long message into fewer qubits with the ability to recover (decode) any one of the initial bits (with some probability of success)". The idea behind QRACs first appeared in a paper by S. Wiesner [12] and was called *conjugate coding*. Later, these codes were re-discovered by Ambainis *et al.* in [13, 14] and studied in the context of quantum finite automata. Over the years, QRACs were shown to be useful for various other applications: locally decodable codes [15], network coding [16], reduction of communication complexity [17], semi-device independent random number expansion [18], semi-device independent key distribution [19], and also as device independent dimension witness, as we will show in Chapter 3.

Here I will introduce the basic knowledge about the device independent approach, the dimension witness protocol and the communication task quantum random access codes, needed for the understanding of this thesis.

1.1 Device Independent Reformulation of Quantum Theory

A reformulation of quantum theory without a previous description of quantum systems has been formally presented under the name of device-independent in [3]. This reformulation was based on the fact that the evaluation of a Bell test does not rely on the knowledge of the degrees of freedom that are measured, this means that any "a priori" knowledge of the systems like its Hilbert space dimension, how is the system encoded, in which bases the systems are going to be measured, etc, are completely dispensed with at the moment of analyzing Bell tests [1].

Since the introduction of the device independent reformulation of quantum theory, many quantum information protocols originally implemented with trusted devices have been successfully translated to it. Moreover, device independent scenarios were conceived in the context of quantum key distribution(QKD), when Mayers and Yao in [20] propose the concept of "self-checking source" which requires the manufacturer of the photon source to provide certain tests designed such that, if passed, the source is guaranteed to be adequate for the security of the quantum key distribution protocol.

Nevertheless, it wasn't until 2004 that the concept of device independent started to take form, when again Mayers and Yao presented the work *"Self testing quantum apparatus"* [21]. In this work they consider the problem of testing a quantum system without trusting the measuring apparatus that are used in the test, and in particular, they didn't assume any a priori information about the dimension of the measured systems or the rank of the measurement operators. In both works, by *"self testing" or "self-checking"* they refers to the fact that some statistics predicted by quantum theory determine the state and the measurement as uniquely as possible, therefore a "self testing" corresponds to a device independent characterization of the state and measurement.

The concept *device independent scenarios* was first mentioned in the work *"From Bell's Theorem to Secure Quantum Key distribution"* [2], where it was shown that, differently from standard quantum key distribution protocols, the security proof was no longer based on the assumption that legitime partners know how their correlation was established, instead, in this more general scenario where the devices were untrusted, any security proof of QKD should make use of quantum nonlocality. While this work contemplated only individual attacks, the generalization for collective attacks was done in [3], which allow us to apply the QKD protocol in situations where the quantum apparatuses are noisy, or where uncontrolled side channels are present, and even in the situation where the apparatuses are completely untrusted and provided by the eavesdropper herself.

Because to have a full knowledge of the devices is very demanding, many device independent quantum key distribution (DIQKD) protocols have been presented in the literature since the idea was formally introduced in [3]. To name a few, in [22] they made a proposal for implementing DIQKD that provides a realistic solution to overcome the problem of channel losses in Bell tests; in [23] it was shown that with DIQKD it is possible to achieve key rates comparable to those of standard schemes; a protocol that requires Alice and Bob to have only one device each was introduced in [24]; in [25] a realistic DIQKD implementation based on the interaction between light and spins stored in cavities was described; a simple DIQKD protocol that do not require the parties to share any reference frame was proposed in [26]; and recently in [27] it was shown that the honest parties do not need to have a initial random seed as a resource, in order to perform secure DIQKD.

Another protocol benefited from the device independent reformulation was quantum tomography. As we said before, "self testing" corresponds to a device independent characterization of the state and measurement, which means that it is a black-box tomography, where even when the experimenter controller is no longer under perfect control of the measurement devices, is able to characterize the produced state based only on the observed statistics. At the time this was first presented in [21], was mostly applied in the ideal situation, however, later on various works have demonstrated self-testing robust to external noise [28, 29, 30, 31, 32], although very small, but in [33] a resolution of this issue is given, allowing the self-testing of quantum states and measurement devices in realistic experimental situations.

Finally, to mention one more protocol which has been taken advantage from the device independent approach, we are going to briefly discuss multipartite entanglement witnesses. Usual entanglement witnesses assume that the dimension of the Hilbert space is known, however, this assumption may be affecting the conclusions about the

entanglement present in the system. Even when this assumption is justified, we can't be sure that in order to reproduce the measured data entanglement between n systems is needed instead of m entangled systems, with $m < n$. These remarks motivate the introduction of device independent entanglement witnesses (DIEW), witnesses that are able to guarantee genuine n-partite entanglement without relying on assumptions about the relevant Hilbert space dimension or the measurements performed [34, 35, 36, 37, 38, 39].

Besides the ones that I mentioned above there are many more protocols redefined by the device independent approach, however, the is a particular one that enormously caught my attention, which was formally introduce by the name of *dimension witness* because undertake the problem of providing a lower bound on the dimension of unknown physical systems. As a result of the big interest that this protocol generated in me, this thesis will be devoted to it.

To finish this section I would like to make an observation. For many of the works cited earlier entanglement was a key resource, which has a negative effect on the complexity of the devices. This led to the introduction of *semi-device independent scenarios*, where the devices are still uncharacterized but only assumed to produce quantum systems of a given dimension, which can be seen as a good compromise between the device independent scenario and experimental feasibility. Some works that make use of the semi-device independent scenario are: [40] to bound entanglement, [19] for QKD, and [18] for randomness expansion.

1.2 Dimension Witnesses

The dimension of a system was always intrinsic to the theoretical model, but this changes when the following question was proposed: "is it possible to assess the Hilbert space dimension from experimental data without an *a priori* model?"

This question was answered positively by Brunner *et al.* in [5]. They introduced the concept of *dimension witness* for the first time in the context of Bell inequalities with devices seen as black boxes, which means, in a device independent scenario. The scenario is the following: a source prepare a state ρ in $\mathbb{C}^d \otimes \mathbb{C}^d$ which is sent to two parties, Alice and Bob, and each of them perform a local measurement, M_a^x and M_b^y respectively, acting on $\mathbb{C}^d$, producing the probabilities $P(ab|xy)$. In their work, a d-dimensional witness was defined as a linear function of the probabilities $P(ab|xy)$ described by a vector $\vec{w}$ of real coefficients w_{abxy}, given by the following expression

$$\vec{w} \cdot \vec{p} \equiv \sum_{a,b,x,y} w_{abxy} P(ab|xy) \leq w_d, \tag{1.1}$$

such that if $\vec{w} \cdot \vec{p} > w_d$ we can assure that quantum systems of at least dimension $d+1$ are needed in order to reproduce the given set of probabilities $P(ab|xy)$.

With no doubt this work paved the way for further dimension witnesses, but the one that stand out, in my opinion, is the work presented in [11], because making use of the most simple scenario they were able to introduced a family of device independent dimension witnesses (DIDW) capable to test systems of arbitrary dimensions. This family of DIDW was named I_N and it was designed under a "prepare-and-measure"

scenario. The scenario is the following: the state preparation device has a set of N buttons, so by pressing the button $x \in \{1, ..., N\}$ we are defining which one of the states ρ_x is going to be sent to the measurement device, which received the state and by pressing the button $y \in \{1, ..., m\}$, select one of its $m = N-1$ measurements to perform over the state ρ_x, obtaining as a result the outcome $b \in \{1, ..., k\}$. The probabilities $P(b|x, y)$ of obtaining the outcome b by performing the measurement y over the state ρ_x are the ones that describe the experiment, which means that any statement about the dimension of the physical system is given by the output data, therefore, this protocol is recognize as device independent. Furthermore, I_N works as a *quantumness indicator*, which means that it is capable to distinguish between classical and quantum states of the same dimension, in this particular case, dimension $d = N - 1$.

As I said before, this problem caught my interest deeply, specially this work, and for that reason it will be thoroughly discuss in Chapter 2.

The knowledge of the dimension of the systems under study is a powerful ability and at this moment it is extremely needed, for that reason it is of utterly important to find theoretical tools and experimental methods that allow the certification of quantum systems in a feasible way, where by feasible we mean that for example it requires a tractable amount of measurements or the difference between the classical and quantum bound is big enough to be observed in an experiment. In the context of quantum information processing this problem needs to be solved for instance:

- to investigate quantum contextuality [41, 42], considering that depending of the non-contextual inequality systems of dimension $d \geq 3$ are required,
- to assure security on quantum communications, where the error rate allowed for unconditional security increases with the dimension of the systems [43, 44]. Also, there are certain protocols that demand the knowledge of the dimension in order to be able to certify secure communication [19],
- to characterize quantum states, where the choice of the method to be used depends on the dimension of the considered system [45],
- to simplify quantum logic, because in order to shorten processing times, high dimensional systems are needed [46], so we have to be able to certify them.

As you can see, this is not a trivial problem, and because of that we decided to devote this thesis to it.

1.3 Quantum Random Access Codes

The tremendous information processing capabilities of quantum mechanical systems may be attributed to the fact that the state of a n qubit system is given by a unit vector in a 2^n dimensional complex vector space. Nevertheless, with the discovery of a fundamental result in quantum information theory, Holevo's theorem [47], which states that no more than n classical bits of information can be transmitted by transferring n quantum bits from one party to another, it was thought that the exponentially many degrees of freedom latent in the description of a quantum system must necessarily stay hidden or inaccessible.

However, in general quantum measurements do not commute, which implies that by performing a quantum measurement over a system, this one is disturbed and thereby some or all the information that would have been revealed by another possible measurement is destroyed. This fact about quantum measurements was the starting point for the communication task called quantum random access codes (QRACs).

The idea behind QRACs first appeared in a paper by S. Wiesner [12] and was called *conjugate coding*, where he defined a *conjugate code* as "any communication scheme in which the physical systems used as signals are placed in states corresponding to elements of several conjugate basis of the Hilbert space describing the individual systems. In the case where the sequence of signals has more than one element the above definition does not require the vectors describing entire transmissions to be elements of conjugate base sets." In his work he refers to mutually unbiased bases (MUBs) as conjugate basis, where MUBs are sets of basis in which each pair of orthonormal bases in the set, lets say $\{e_i\}_{i=1}^d$ and $\{f_j\}_{j=1}^d$ in an d dimension Hilbert space $\mathcal{C}^d$, satisfy the following expression: $|\langle e_i|f_j\rangle|^2 = \frac{1}{d}\ \forall i,j \in \{1,...,d\}$.

QRACs were re-discovered in by Ambainis *et al.* in [13, 14], where they consider the possibility of encoding n classical bits into much fewer m quantum bits so that an arbitrary bit from the original n bits can be recovered with a good probability p. They formally defined a quantum random access encoding as an encoding map from $\{0,1\}^n$ to $\mathcal{C}^2$ together with a sequence of m possible measurements, where if the ith measurement applied to the encoding $a = a_1...a_n$, the outcome is a_i with probability at least p; and characterized by $n \xrightarrow{p} m$.

In their works Ambainis *et al.* shown that there exists $2 \xrightarrow{0.85} 1$ QRAC and mention that Chuang proved that $3 \xrightarrow{0.79} 1$ QRAC also exist. In 2009, a protocol similar to QRACs was presented in [48] under the name *parity-oblivious multiplexing*, which has the additional cryptographic constrain that Alice is not allowed to transmit any information about the parity of the input string, where the first experimental demonstration of $2 \to 1$ and $3 \to 1$ QRACs is discussed.

On the other hand, Hayashi *et al.* in [16] shown that it is impossible to construct $4 \xrightarrow{p} 1$ QRAC with $p > \frac{1}{2}$, in a general scenario where Alice and Bob are allowed to use randomized strategies but only having access to local coins. Nevertheless, it is possible to consider an even more general scenario, in which both parties share a common coin. This means that Alice and Bob are allowed to cooperate by using some shared source of randomness to agree on which strategy to use. Such source was named *shared randomness* and it was proposed in [49], where they proved that in this new scenario $n \xrightarrow{p} 1$ QRACs with $p > \frac{1}{2}$ can be constructed for all $n \geq 1$.

It is important to note that generalization of QRACs can be made, being the most interesting for this thesis, the case when d-level systems are used. This generalization is first discussed in [50], where they construct $(d+1) \to 1^d$ QRACs for dimensions $d = 2, 3, 4, 5, 7, 8$, with $(d+1) \to 1^d$ meaning that a string of $(d+1)$ elements of dimension d was encoded in a single quantum systems of dimension d. Another generalization was made recently by Tavakoli *et al.* in [51], in this case for both, RACs and QRACs in a scenario Where Alice has a string $x = x_1, ..., x_n$, with $x_i \in \{1, ..., d\}$, which she encodes into a classical or quantum d-dimensional systems, depending of if she is considering RACs or QRACs respectively, which is sent to Bob who should be able to recover the

x_j of his interest with an average probability of $p_{n,d}$. This scenario is described by the abbreviation $n^{(d)} \overset{p_{n,d}}{\to} 1$. They conjectured that the optimal classical strategy is for Alice to use majority encoding and Bob does identity decoding, which was later proven positively in [52]. With that assumption Tavakoli *et al.* found analytical bounds for the average success probability for RACs in the cases $n = 2, 3$ for any dimension. They also constructed two families of QRACs of the form $2^d \to 1$ and $3^{(d)} \to 1$, and found an analytical expression for its average success probability for any dimension, showing in both cases $n = 2, 3$ that high-dimensional QRACs enable significantly larger advantages over the corresponding RACs than what can be achieved with QRACs using systems of dimension $d = 2$.

Finally, I would like to mention the great potential that QRACs shows as a tool to solve the problem of lack of dimension witnesses for high-dimensional systems. This was first noticed in [9], where they tackle the problem of find lower bound on the dimension of a quantum system given measured data based in the construction of QRACs. They relate both problems in the following way: "Suppose we were given states $\rho_1, ..., \rho_l$ and measurements $M_1, ..., M_m$ that give us the desired probabilities $p(a|M_j, \rho_x)$, which represents the probability to obtain the output a when the measurement M_j is performed over the state rho_x. For simplicity, assume for now that $l = 2^m$ and $a \in \{0, 1\}$. Then the states $\rho_1, ..., \rho_l$ form a generalized QRAC, where each state represents an encoding of a m-bit string x and we think of M_j as the measurement that we can apply to extract bit x_j with probability $p(a|M_j, \rho_x)$." As a result, they obtain a simple lower bound that places a fundamental limit on how large the dimension of the state has to be to implement certain measurement strategies. To our knowledge, little attention has been directed to this connection, but recently, we worked in a modified version of QRACs, where the output b is binary. With this modified version of QRACs we propose a dimension witness for physical systems of dimension eight that also works as a quantumness indicator, which means that it is capable to discriminate between classical and quantum 8-dimensional systems. This work will be extensively discuss in Chapter 3.

2

Device Independent Dimension Witness

In this chapter I will introduce the concepts of Device Independent Dimension Witness and describe their development around the recent years. There was in particular one work that proposed a protocol very appealing for experimental implementation, which was tested for dimensions two and three. Motivated by these tests, we wanted to study if such certification will be experimentally feasible for high dimensional quantum systems, and we answered this question positively by presenting an experimental certification of six-dimensional quantum systems, which will be fully described at the end of this chapter.

2.1 Development of Dimension Witnesses

It all begin with the question *"is the dimension of a quantum system an experimentally measurable quantity?"* made by Brunner *et al.* [5]. This question arise from the necessity of characterize Hilbert space dimension for quantum information science, where dimensionality is a key resource. In [5], the concept of **dimension witness** was introduced and its figure of merit corresponds to a linear function of the probabilities obtained after the system under study was measured. The upper bound of this function is reach when systems of dimension d are used, so by means of dimension witnesses (DW) we are able to answer the question: *"what is the minimal dimension d needed to reproduce the given set of probabilities?"*.

Brunner *et al.* introduced the concept of dimension witness in the context of Bell inequalities in a black box scenario, where a source prepare a state ρ in $\mathbb{C}^d \otimes \mathbb{C}^d$ which is sent to two parties, Alice and Bob, and each of them perform a local measurement, M_a^x and M_b^y respectively, acting on $\mathbb{C}^d$, producing the probabilities $P(ab|xy)$. Then, they establish that a d-dimensional witness will be given by

$$\vec{w} \cdot \vec{p} \equiv \sum_{a,b,x,y} w_{abxy} P(ab|xy) \leq w_d, \tag{2.1}$$

such that if $\vec{w} \cdot \vec{p} > w_d$ we can assure that quantum systems of at least dimension $d+1$ are needed in order to reproduce the given set of probabilities $P(ab|xy)$. This work motivates further dimension witnesses based on Bell-type inequalities [6, 7, 8],

where lower bounds on the dimension of locally measured entangled states are provided. However, the use of nonlocal correlations as a dimension witness can be interpreted as a test of the amount of levels that the user is able to entangled, because if the user is unable to produce an entangled state, it will be imposible to certify the dimension of the local system [10].

Simultaneously, there were other approaches to tackle the problem of estblish a lower bound on the dimension of a system, in a single particle scenario [9, 53], but the first work that undertake this problem directly without adapting other techniques and, more important, introduced a generalized device independent dimension witness (DI DW) for arbitrary dimension systems, was the one presented by Gallego *et al.* [11].

In [11] they proposed a DI DW in a simple scenario called "prepare and measure", where two black boxes are considered, one for the state preparation and the other to measure the state. In order to certify the preparation of d-dimensional systems, $N = d + 1$ states labeled by x and $m = N - 1$ binary measurements labeled by y are needed, so the DI DW is described by the expectation values $E_{xy} = P(b = +1|x, y) - P(b = -1|x, y)$ obtained when measurements y are performed over the prepared states x giving as outputs $b \in \{+1, -1\}$, and has the form

$$\vec{W} \cdot \vec{E} = \sum_{x,y} w_{xy} E_{xy} \leq Q_d. \tag{2.2}$$

A DI DW for $d = 2$, able to discriminate between bits and qubits, is introduced with the name I_3, which is then generalized for classical and quantum systems of any dimension and presented as a family of dimension witnesses by the name of I_N.

The DI DW family I_N was experimentally tested in [54, 55] for systems of dimension $d = 2$ and $d = 3$, where the bounds for the respective dimension witnesses are given by

$$I_3 \overset{bit}{\leq} 3 \overset{qubit}{\leq} 1 + 2\sqrt{2} \overset{trit,qutrit}{\leq} 5, \tag{2.3}$$

$$I_4 \overset{bit}{\leq} 5 \overset{qubit}{\leq} 6 \overset{trit}{\leq} 7 \overset{qutrit}{\leq} 7.97 \overset{quart,ququart}{\leq} 9. \tag{2.4}$$

In both experiments, they prepared classical and quantum states of dimensions two, three and four, and in particular, they prepared the set of states that reaches the maximum value for that DI DW in the respective dimension, in order to clearly observe the difference between classical and quantum systems of the same dimension. Later, in [56] we made a experimental certification of six-dimensional quantum systems encoded in the orbital angular momentum of single photons using the DI DW I_7. To accomplish this certification, first it was necessary to calculate numerically the quantum bounds of I_7, because only the classical limits of I_N have analytical expressions. We were able to certify the generation of six-dimensional quantum systems and to demonstrate that classical systems cannot be used to simulate the results obtained for I_7 with quantum systems of dimension $d = 6$. However, within this work we realized that the DI DW family I_N is not a good candidate to certify the generation of high-dimensional systems, because the amount of variables involved in the numerical calculation of the quantum bounds and necessary to control in the experimental implementation increase as $2d^2$, which is almost unmanageable if we consider for example $d > 2^5$.

The performance of the DI DW family I_N was also analyzed in the presence of loss in [57], where critical values for the detection efficiency were provided in order to

(i) successfully lower bound the dimension of the systems and (ii) discriminate between classical and quantum nature of the system. The expressions for each of them are giving by:

$$1 - \frac{2-\sqrt{2}}{d} \geq \quad \eta_{dim} \quad , \tag{2.5}$$

$$\frac{d-1}{d} \geq \quad \eta_{qc} \quad \geq \frac{d-1}{d-2+\sqrt{2}}, \tag{2.6}$$

where Eq. (2.5) corresponds to case (i) and Eq. (2.6) to case (ii). Nevertheless, in both cases η asymptotically goes to 1 really fast as d increases, so we can see that the problem to lower bound the dimension of a high-dimensional quantum systems cannot be solved by the DI DW family I_N.

Later on, Brunner *et al.* [58] also pointed out the strong link between the problems of dimension witnesses and quantum state discrimination. The distinguishability of quantum states is an important issue in the dimension witness problem in the prepare and measure scenario, because if we consider that the dimension d is greater or equal to the number of states that the user is able to prepare, N, then it will be possible for the measuring device to perfectly distinguish the state that was prepared, which implies that the statistics $P(b|x,y)$ can be simulated and no statement about the dimension of the system can be made. On the other hand, if the dimension d is lower than the amount of available preparations N, then it is not possible to prepare perfectly distinguishable states and it will be impossible to reproduce the statistics $P(b|x,y)$, which allow us to make statements about the dimension in a device independent way. Therefore, based on this, they used the notion of trace distance to propose a dimension witness that can discriminate between classical and quantum states of the same dimension for any $d < N$, which is an improvement in comparison with the one proposed in [11], however it needs $N/2$ times more measurements.

Another improvement is pointed out in the work of Gühne *et al.* in [10], where they showed how the bounds of noncontextuality inequalities can be used to lower bound the dimension of quantum systems. They focus on sequential measurements on a single system and derive bounds for important noncontextuality inequalities considering different scenarios. What it is important to emphasize from this work is that by using contextuality as a resource for bounding the dimension of quantum systems it is possible to derive state independent dimension witnesses.

Recently, another approaches has been taken to propose dimension witnesses. In [59] they assume full independency between the preparation and the measurement device, which leads to a nonconvex problem, different from the other approaches where shared randomness is allowed between the devices, making the problem convex. Then, nonlinear dimension witnesses based on the determinant of a matrix are constructed in a scenario where $2k$ preparations labeled by $x \in \{0, ..., 2k-1\}$ and k binary measurements labeled by $y \in \{0, ..., k-1\}$ with outcomes $b \in \{0, 1\}$ are needed. Taking the probabilities $p(b=0|x,y) = p(x,y)$, the following $k \times k$ matrix is constructed

$$\mathbf{W}_k(i,j) = p(2j,i) - p(2j+1,i), \tag{2.7}$$

with $0 \leq i, j \leq k-1$, and the d-dimensional witnesses corresponds to $W_k = |det(\mathbf{W}_k)|$, where for classical systems of dimension d $W_k = 0$ if $d \leq k$ and $W_k \geq 1$ if $d > k$, while

for quantum systems of dimension d $W_k = 0$ for $d \leq \sqrt{k}$ and $W_k > 0$ for $d > \sqrt{k}$. Therefore, they obtain dimension witnesses that allow to discriminate between classical and quantum systems of dimension d with a quadratic separation, while the number of preparations and measurements only grows linearly. On the other hand, in [60] they consider the framework of communication networks to construct classical and quantum dimension witnesses, however they only present dimension witnesses for systems of $d = 2$ and $d = 3$.

As you can see the problem of lower bound the dimension of a physical system is getting more and more attention due to its importance in numerous protocols of quantum information, so, the problem has been presented in various scenarios and adopting different techniques in order to achieve a method experimentally feasible and general to test systems of any dimension.

2.2 Device independent dimension witness I_N

As we mention above, Gallego *et al.* [11] were the first ones that developed a general formalism to address the problem of testing the dimension of arbitrary physical systems. The scenario considered goes under the name of "prepare and measure" because it involves a state preparation and a measurement device, and since both devices are treated as black boxes and no assumptions are made on them, any statement about the dimension of the physical system will be given by the output data, then this protocol is recognize as device independent.

The state preparation device has a set of N buttons, so by pressing the button $x \in \{1, ..., N\}$ we are defining which one of the states ρ_x is going to be sent to the next stage. The measurement device received the state and performs one of its $m = N - 1$ measurements on it, which is selected by pressing the button $y \in \{1, ..., m\}$, and obtains as a result the outcome $b \in \{1, ..., k\}$. The scenario just described is depicted in Figure 2.1.

The probabilities $P(b|x, y)$ of obtaining the outcome b by performing the measurement y over the state ρ_x are the ones that describe the experiment. Now the question is, what is the minimal dimension needed for the mediating particle in order to describe correctly the observed probabilities $P(b|x, y)$?

To answer the question above, the authors characterize the set of realizable experiments in the scenario where the problem is meaningful, and to do they restricted the analysis to a scenario where the devices share classical correlations. If first consider the case when $d \geq N$, then it is possible for the measurement device to have full access to x and y because the preparation choice x could be perfectly encode in the state ρ_x. On the other hand, if $d < N$ it is impossible to perfectly encode the preparation choice x because there is not enough distinguishable states, so the statistics $P(b|x, y)$ cannot be reproduced by the measurement device and relevant device independent statements can be made.

It is important to notice that, for simplicity, they used measurements with binary outcomes $b \in \{-1, +1\}$, and for that reason they prefer to work with expectation values $E_{xy} = P(b = +1|x, y) - P(b = -1|x, y)$. With all these considerations, they construct a device independent dimension witness family called I_N, which is given by the following

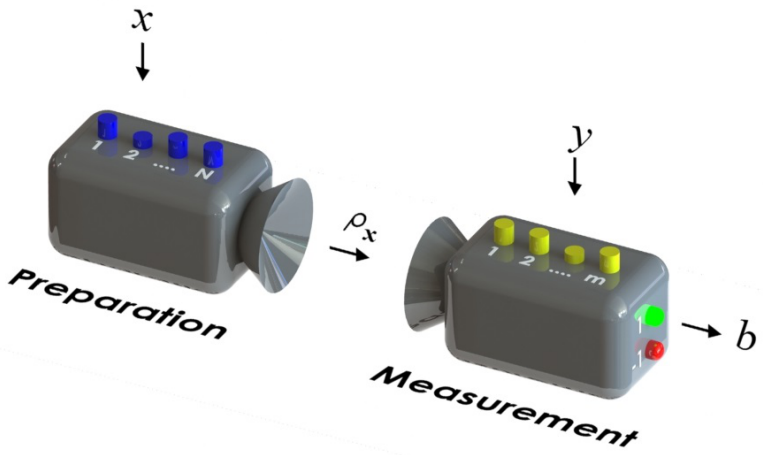

Figure 2.1: Prepare and measure scenario for the dimension witness I_N. The preparation device has a set of N buttons corresponding to the set of N states to be prepared. The measure device has a set of $m = N - 1$ buttons corresponding to the set of m measurements to be performed.

expression

$$I_N \equiv \sum_{j=1}^{N-1} E_{1j} + \sum_{i=2}^{N} \sum_{j=1}^{N+1-i} \alpha_{ij} E_{ij}, \tag{2.8}$$

$$\text{where} \quad \alpha_{ij} = \begin{cases} 1 & \text{if} \quad i+j \leq N \\ -1 & \text{otherwise.} \end{cases}$$

The authors were able to find analytical bounds for I_N when classical states of dimension $d \leq N$ are considered, so in those cases

$$I_N \leq L_d = \frac{N(N-3)}{2} + 2d - 1, \tag{2.9}$$

with $L_{d=N}$ being the algebraic bound. However, to obtain the quantum bounds of I_N numerical calculations are needed. In any case, they proved that the inequality $I_N < L_{d=N}$ corresponds to a quantum dimension witness for quantum systems of dimension $d = N - 1$. Also, they conjecture that $I_N \leq L_{d=N-1}$ is a tight classical dimension witness for any dimension, thus by violating the value $L_{d=N-1}$ and obeying the quantum dimension witness $I_N < L_{d=N}$ we can assure that we are assessing a quantum system of dimension $d = N - 1$.

This protocol is highly relevant, because it was the first one that allows us (i) to certify if the source is producing systems of at least dimension $d = N - 1$, and most important, (ii) to distinguish between quantum systems from classical systems of the same dimension, in this particular case, $d = N - 1$.

2.2.1 Robustness of I_N

In views of experimental implementations of the witness DI DW family I_N, Dall'Arno *et al.* [57] studied the robustness of this DI DW in the presence of loss. A scenario where classical correlations are shared between the preparation and measurement device,

and where the events are independent and identically distributed is considered. They specifically analyzed the case when the losses are concentrated in the measurement process, where the detection efficiency η is not ideal, which means that $\eta < 1$. It is assumed that all measurements posses the same detection efficiency, which is reasonable if it is considered that the same physical implementation is used for all the detectors involved, however, in a more general and precise model, any measurement could be described by a different detection efficiency.

For the study, they define the DI DW as

$$W(p) := \sum_{x,y,b} c_{x,y,b} P(b|x,y), \tag{2.10}$$

where $c_{x,y,b}$ are real coefficients. Then, considering the situation where $N = d + 1$, $m = d$ and $k = 3$, because each measurement with losses has one more outcome than in the ideal case, which corresponds to the no-click event, and by doing an optimization of the witnesses (2.10) with pure states, they demonstrated that the witnesses defined by the following coefficients

$$c_{x,y,b} = \begin{cases} -1 & \text{if } x + y \leq N, \quad \text{b} = +1, \\ +1 & \text{if } x + y = N + 1, \quad \text{b}=1, \\ 0 & \text{otherwise}, \end{cases} \tag{2.11}$$

are the most robust in a scenario with $\eta < 1$. This DI DW is denoted by I^*_{d+1} and it is directly related to I_N. Then making use of the known bounds of I_N, they provide lower and upper bounds for the witnesses I^*_{d+1}

$$d - 2 + \sqrt{2} \overset{d_q}{\leq} I^*_{d+1} \overset{max}{\leq} d, \tag{2.12}$$

where d_q means that the value on the left is the maximum with quantum systems of dimension d and max means that the value on the right is the maximum for the expression I^*_{d+1} attainable with systems of any dimension higher than d.

Now, having all the above in consideration, they are able to provide the lower threshold detection efficiency required to perform reliable dimension witnessing in nonideal scenarios.

1. **Threshold detection efficiency to set a lower bound on the dimension of a system.**
   In order to determine if it is necessary a $(d + 1)$-dimension system to reproduce certain data in a lossy scenario, the detection efficiency of the measurements are bounded by

$$\eta > \eta_{dim} := I^*_{d+1}/d, \tag{2.13}$$
$$\text{where} \qquad \eta_{dim} \geq 1 - \tfrac{2-\sqrt{2}}{d}.$$

2. **Threshold detection efficiency to discriminate between classical and quantum d-dimensional systems.**

To determine if a d-dimensional system is of classical or quantum nature, measurements with the following detection efficiency are needed

$$\eta > \eta_{qc} := (d-1)/I^*_{d+1}. \tag{2.14}$$

For better understanding of this bound, it is important to notice that the classical bound for I^*_{d+1} when classical d-dimensional systems are used is $(d-1)$. Then, from Eq. (2.12) it is possible to set the lower and upper bound of the detection efficiency η_{nc}, which are given by

$$\frac{d-1}{d} \leq \eta_{qc} \leq \frac{d-1}{d-2+\sqrt{2}}. \tag{2.15}$$

With these results they are able to characterize the threshold detection efficiencies of lossy scenarios necessaries to provide lower bounds on the dimension of a system and also discriminate if it is of classical or quantum nature. However, they notice that even when their main results have analytical proofs, they are based in the numerical evidence that the dimension witness I^*_{d+1} is the most robust for any d in the proposed lossy scenario.

Indeed, they leave open questions about generalizations of the problem of provide lower bounds on the dimension of systems. For example, in a scenario without correlations between the preparation and measuring device, where the problem is nonconvex; or the another generalizations where the prepararing and measuring devices share entanglement or share entangled particles.

2.2.2 First experimental implementations of I_N

The DI DW family I_N showed to be very appealing for experimental implementations, and for that reason, two different groups demonstrated simultaneously that their sources were able to prepare quantum systems of dimension $d = 2$ and $d = 3$.

The first work we will discuss is the one from Ahrens *et al.* [55], where they used the DI DW I_3 and I_4. First, they test the DW I_3 to certify classical and quantum systems of at least dimension $d = 2$, by using a set of $N = 3$ states and $m = 2$ measurements with binary outcomes. The expression for the DW I_3 and its corresponding classical and quantum bounds are given by

$$I_3 \equiv |E_{11} + E_{12} + E_{21} - E_{22} - E_{31}| \overset{bit}{\leq} 3 \overset{qubit}{\leq} 1 + 2\sqrt{2} \overset{trit,qutrit}{\leq} 5. \tag{2.16}$$

Secondly, they test the DI DW I_4 to certify classical and quantum systems of at least dimension $d = 3$, this time using a set of $N = 4$ states and $m = 3$ dichotomic measurements. This witness and its bounds are given by

$$\begin{aligned} I_4 \equiv \; & |E_{11} + E_{12} + E_{13} + E_{21} + E_{22} - E_{23} + E_{31} - E_{32} - E_{41}| \\ & \overset{bit}{\leq} 5 \overset{qubit}{\leq} 6 \overset{trit}{\leq} 7 \overset{qutrit}{\leq} 7.97 \overset{quart,ququart}{\leq} 9. \end{aligned} \tag{2.17}$$

Classical and algebraic bounds are obtained by using the corresponding value of d in Eq. (2.9), so for example, the algebraic bound of 5 for I_3 corresponds to consider $d = N = 3$

and the classical bound of 7 for trits in I_4 is obtained when $d = 3$. Quantum bounds are determined by numerical calculations. If we label by d_c the dimension of classical systems and by d_q the dimension of quantum systems, the bounds $\overset{d_c}{\leq}$ and $\overset{d_q}{\leq}$ means that, in order to achieve values higher than this bound, systems of dimension higher than d_c and d_q, respectively, are needed. Finally, it is important to notice that the algebraic bound do not discriminate between classical and quantum systems.

Before presenting the results, they emphasize the relevance of the user's degree of control over the device, in the sense that if the user doesn't have knowledge in which degree of freedom the measurements are performed, he could not be sure if by obtaining a value in between 5 and 6 for I_4 he is actually observing a qubit or noisy higher dimensional systems. On the other hand, if the user known at what dimension his measurements are confined, he is able to make statements based on the observed results. Consequently, in this scenario the measurement device must be trusted.

To perform the experiment, they used photons encoded in polarization and in two spatial modes, so it is possible to construct a base with four states. The overall work features two experiments involving I_3 to certify the generation of qubits and 3-dimensional systems, and four experiments involving I_4 to certify the generation of qubits, trits, qutrits and 4-dimensional systems. All the experiments considered the set of states and measurements that reach the witnesses boundaries in order to experimentally obtain the biggest differences between the values for classical and quantum systems. Their experimental results for all the tests are summarised in Table 2.1.

	exp. $d_q = 2$	exp. $d_c = 3$	exp. $d_q = 3$	exp. d = 4
I_3	3.7815 ± 0.0782	4.9303 ± 0.1032		—
I_4	5.9533 ± 0.1232	6.9608 ± 0.1443	7.6020 ± 0.1650	8.9089 ± 0.1845

Table 2.1: Experimental results for the tests of dimension witnesses I_3 and I_4 obtained by Ahrens *et al.* in [55]. It is possible to observe that in all the cases they almost reach the maximum value. For I_3 the experimental value obtained with $d_c = 3$ and $d_q = 3$ is the same because it corresponds to the algebraic bound so the nature of the 3-dimension system cannot be determined by this test. Moreover, for I_4 the last column experimental value is labeled by $d = 4$ for the same reason, because it could be either a quart or a ququart.

The second work corresponds to the one presented by Hendrych *et al.* [54], where they test the DI DW I_4, and by implementing a continuous transition from quantum to classical states, they were able to test all the bounds of I_4. To encode the states, they make use of the polarization and the orbital angular momentum of photons. The experimental results are presented in Table 2.2.

Only experimental values for the case of qubits, qutrits and quarts are presented because these are the sets of states prepared, then by a temporal transition, these states are turn into classical ones, which they shown that are not able to attain values higher than the classical bounds for its respective dimensions.

These two first experimental tests of the DI DW family I_N, certify the generation of classical and quantum systems of dimension two, three and four using the witnesses I_3 and I_4. However, its practicability in higher dimensions had not been proven. This

	exp. $d_q = 2$	exp. $d_q = 3$	exp. d = 4
I_4	5.66 ± 0.15	7.57 ± 0.13	8.57 ± 0.06

Table 2.2: Experimental results for the tests of dimension witness I_4 obtained by Hendrych *et al.* in [54]. It is possible to observe that both, qubits and qutrits, surpass the classical bound for its respective dimension. To test the algebraic bound they only consider quarts to demonstrate that physical systems of dimension higher than three are needed to reach this value.

motivated us to work on device independent certification of six-dimensional quantum systems encoded in the orbital angular momentum of single photons [56].

2.3 Device independent certification of six-dimensional quantum systems, I_7

At this point is been mention several times how important is the certification of the dimension of quantum systems in a device independent way for several quantum information protocols. In the previous section we describe the most appealing theoretical method at the moment to certify the dimension and nature of systems of any dimension d, the DI DW family I_N. This witness has only been used to experimentally certify quantum systems of dimension $d = 2$ and $d = 3$, therefore motivated for the lack of evidence for higher dimensions, which are demanded for realistic quantum information applications, we take the challenge to experimentally certify the generation of six-dimensional quantum systems.

To experimentally witness the generation of six-dimensional quantum systems, and show that our results cannot be simulated with six-dimensional classical systems, we use the simplest DI DW of the family I_N [11] capable to do that, namely I_7. The scenario for I_7 is the one depicted in Fig. 2.1, with $N = 7$, then for the preparation box we have a set of seven states, and for the measurement box a set of six measurements. With equation (2.8) it is possible to obtain the expression for I_7, given by

$$\begin{aligned} I_7 \equiv\ & |E_{11} + E_{12} + E_{13} + E_{14} + E_{15} + E_{16} \\ & + E_{21} + E_{22} + E_{23} + E_{24} + E_{25} - E_{26} \\ & + E_{31} + E_{32} + E_{33} + E_{34} - E_{35} \\ & + E_{41} + E_{42} + E_{43} - E_{44} \\ & + E_{51} + E_{52} - E_{54} \\ & + E_{61} - E_{62} \\ & - E_{71}|. \end{aligned} \tag{2.18}$$

Since there only exist analytical expressions for classical limits of I_N for systems of dimension $d \leq N-1$, we need to use numerical techniques to obtain the quantum limits of I_N. In order to do so, a general parametrization to define the d-dimensional states and measurements is needed. In the literature we found the generalization of spherical coordinates and we decided to use it to define the states and measurements in the most

general way. The elements of this parametrization are the followings:

$$\lambda_1 = \cos\phi_1, \tag{2.19a}$$

$$\lambda_j = \cos\phi_j \prod_{k=1}^{j-1} \text{sen}\phi_k, \tag{2.19b}$$

$$\lambda_{d-1} = \cos\phi_{d-1} \prod_{k=1}^{d-2} \text{sen}\phi_k, \tag{2.19c}$$

$$\lambda_d = \text{sen}\phi_{d-1} \prod_{k=1}^{d-2} \text{sen}\phi_k, \tag{2.19d}$$

with $j = 2, ..., d-2$, where the angles $\phi_j \in [0, \pi]$ and the angle $\phi_{d-1} \in [0, 2\pi)$, and we consider an unitary hypersphere, which means that its radio is $r = 1$. Having this, the quantum states to be prepared will be defined by $\rho_x = |\Phi_x\rangle\langle\Phi_x|$, where

$$|\Phi_x\rangle \equiv \sum_{i=0}^{d-1} \lambda_{i+1}^{(x)} |i\rangle. \tag{2.20}$$

The measurements to be made are given by $M_y^+ = |\Phi_y\rangle\langle\Phi_y|$, where the states $|\Phi_y\rangle$ are defined by the same sum showed in Eq. (2.20) but labeled by (y) instead of (x).

Now, having all the parameters needed to define the DI DW I_7, it is possible to estimate its bounds with the conjugated gradient method, where in order to reach the closest maximum point of I_7, the local gradient is calculated in a point of I_7 parameter space, which is defined by the angles ϕ_i in Eqs. (2.19). To map all the local maxima and decide which is the global one, we ran the conjugated gradient algorithm for a large uniform sample of points in the parameter space, corresponding approximately to 5×10^8 trials, for each dimension considered.

In Table 2.3, it is possible to observe the different bounds that I_7 achieve depending on the dimension that is tested. I_7 was designed to certify 6-dimensional systems, so we can assure that our system is at least of dimension 6 if the value of I_7 is greater than 24.8987. But, I_7 allows us to go further and distinguish between classical and quantum 6-dimensional systems, so if we obtain a value greater than 25 we can also assure that our 6-dimensional system is quantum. However, despite the fact that I_7 was designed to certify 6-dimensional systems, we can see from Table 2.3 that with I_7 is also possible to distinguish between classical and quantum systems of dimensions two and three.

For the experiment we used the set of states and measurements that allow us to reach the quantum bound of 26.1017, to be able to obtain experimentally a value greater than 25. The states and measurements that lead to this quantum bound are presented in Table 2.4. Notice that, with the parametrization of Eqs. (2.19), one needs to control $N(d-1)$ parameters related to the N states to be prepared, plus $(N-1)(d-1)$ parameters related to the $N-1$ required projections, which leads, in terms of d, to a total of $2d^2 - d - 1$ parameters.

d	I_{7c}	I_{7q}
2	17	17.3976
3	19	20.7085
4	21	23.2167
5	23	24.8987
6	25	26.1017

Table 2.3: (Source Ref. [56]) "Limits of I_7 for classical (I_{7c}) and quantum (I_{7q}) systems of dimension d".

x	$\phi_1^{(x)}$	$\phi_2^{(x)}$	$\phi_3^{(x)}$	$\phi_4^{(x)}$	$\phi_5^{(x)}$
1	4.8501	1.8679	5.1341	1.5056	4.4493
2	1.7085	-0.1307	2.9637	0.2325	1.0858
3	1.4347	1.3779	5.0763	4.8358	6.2086
4	4.5814	1.4557	0.6297	4.5888	-0.1338
5	4.8343	1.8268	4.9946	0.5796	1.6284
6	4.6016	1.3527	4.2510	0.5860	4.9691
7	π	2.2358	5.2280	2.8465	0.5110
y	$\phi_1^{(y)}$	$\phi_2^{(y)}$	$\phi_3^{(y)}$	$\phi_4^{(y)}$	$\phi_5^{(y)}$
1	0	6.0542	3.8912	1.8371	0.378
2	1.3491	1.3527	2.0322	2.5556	1.8275
3	1.7849	1.7926	1.3549	3.6187	1.6015
4	1.3718	1.5194	-0.5647	4.8676	3.2279
5	1.3932	1.4595	5.0187	4.8270	-0.1914
6	1.7268	6.4857	5.7731	1.2669	4.4619

Table 2.4: (Source Ref. [56]) "Orientations of the x states and y measurements that maximize I_7 while considering six-dimensional systems".

In the experiment, the prepared states are encoded in the orbital angular momentum (OAM) of single photons [61], because this degree of freedom allow the user to implement qudits of, in principle, arbitrary d using single photons. Here we choose the following OAM eigenstates subset as a logical basis: $\{|-3\rangle_O, |-2\rangle_O, |-1\rangle_O, |1\rangle_O, |2\rangle_O, |3\rangle_O\}$, where $|l\rangle_O$ identifies the state of a photon with $l\hbar$ of orbital angular momentum.

In Figure 2.2 the experimental setup is illustrated. At the generation stage, single photons in the fundamental TEM00 Gaussian state ($l = 0$) are prepared in the desired OAM superposition state, to obtain one of the seven $|\Phi_x\rangle$ states, by means of a spatial light modulator (SLM1). This device modulates the phase wave front according to computer generated holograms specifically calculated to maximize the state fidelity [62]. At the analysis stage, a second spatial light modulator (SLM2) is used in combination with a single mode fiber and a single photon detector to perform a projective measurement, selected from the set of six $|\Phi_y\rangle\langle\Phi_y|$ projectors, on the desired state. The overall setup

implements a DI DW, where by remembering the scenario depicted in Fig. 2.1, each button in the preparation stage corresponds to a different hologram to be displayed on SLM1 and each button on the measurement stage corresponds to a different hologram to be displayed on SLM2. Using this setup we were able to generate and project over all the states required to test I_7. The generation and measurement processes were completely automated and computer controlled.

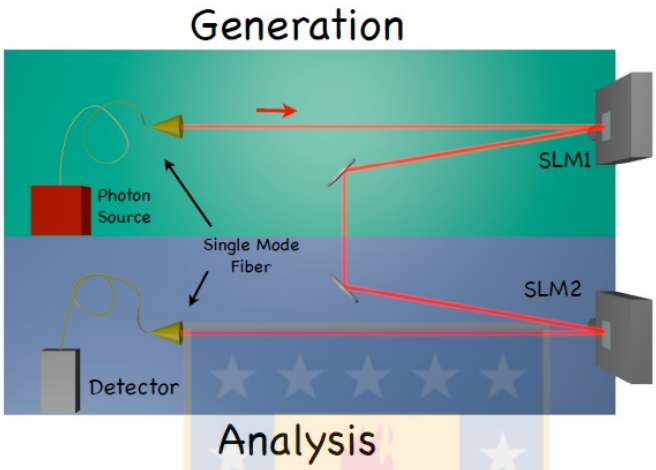

Figure 2.2: (Source Ref. [56]) "Experimental implementation for device independent dimension witnessing. The setup consist of two stages, labeled as "generation" and "analysis". In the generation stage, heralded single photons are produced by spontaneous parametric down-conversion in beta barium borate nonlinear crystal. The heralding photon is directly sent to a detector which acts as a trigger (not shown in figure), the signal photon is projected on the fundamental TEM00 Gaussian state ($l = 0$) by means of a single mode fiber (Photon Source). The orbital angular momentum (OAM) state of signal photons is then manipulated with the spatial light modulator SLM1 in order to prepare each one of the 7 states required. In the analysis stage, projective measurements are performed by means of the spatial light modulator SLM2 in combination with a single mode fiber and a singlephoton detector".

To check the quality of he experimental projectors, for each M_y^+ we measured the fidelity $F(M_y^+) = |\langle\Phi_y|\Phi_y\rangle|^2$, which corresponds to the probability of obtaining a photon count when a state is projected over itself. As a result we obtained an average fidelity of $F = (99.10 \pm 0.02)\%$, removing the contribution of the dark counts. Having done this, we measured all the probabilities needed for I_7, obtaining an experimental value of $I_7^Q = 25.95 \pm 0.02$, removing dark counts. The error was calculated considering a Poissonian statistics for photon counts. As you can see, the experimental value of I_7 is higher than 25, which certifies that our source is generating six-dimensional quantum systems. However, we need to show that classical states of dimension six produce smaller values for I_7, and in order to do that we prepared classical states defined as

$$\rho_x = \sum_{i=0}^{d-1} \lambda_{i+1}^2 |i\rangle\langle i|. \tag{2.21}$$

Considering that the classical bounds of I_7 are given by analytical expressions, we used again the conjugated gradient method to obtain the orientations that maximize I_7 when only six-dimensional classical states are studied. Like in the quantum case, in the classical case we measured fidelities for all the projectors involved in the dimension witness, and an average value of $F = (99.000 \pm 0.005)\%$ was reached, removing dark counts. Finally, the measured value for I_7 was $I_7^C = 24.825 \pm 0.004$, removing dark counts.

The experimental results are compared with the theoretical bounds in Figure 2.3. Specifically, Fig. 2.3 shows the experimental results obtained for the DI DW I_7 when classical and quantum systems of dimension $d = 6$ were generated. The results clearly show that the values obtained using six-dimensional quantum systems cannot be simulated with classical systems of the same dimension.

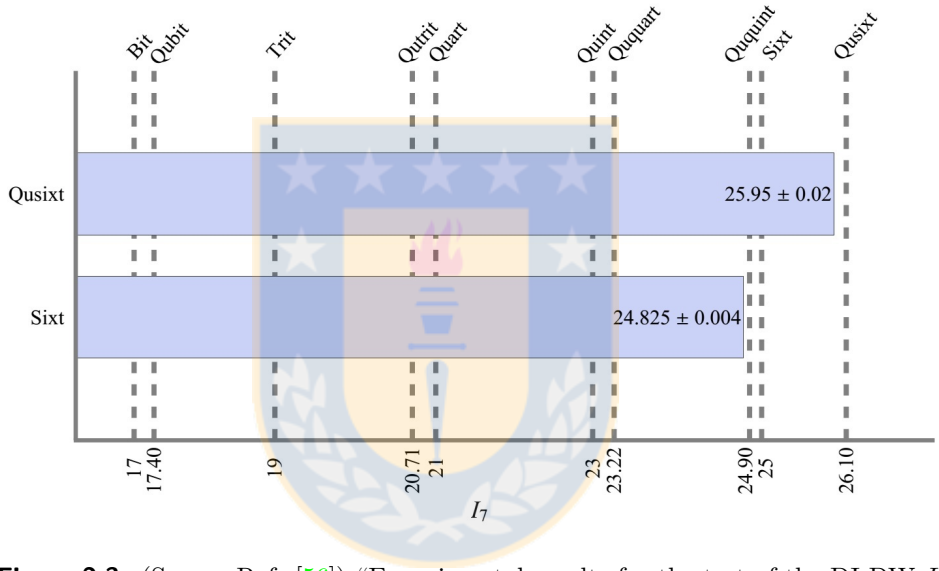

Figure 2.3: (Source Ref. [56]) "Experimental results for the test of the DI DW I_7 using quantum systems of dimension 6 (qusixt) and classical systems of dimension 6 (sixt)."

With this work we showed that the device independent certification of quantum systems of high-dimension, in particular, of high-dimensional photonic systems, was experimentally feasible. Moreover, these results demonstrate the feasibility of the device independent approach for realistic high-dimensional quantum information processing. Nevertheless, there is still the challenge to certify quantum systems of high-dimension of the order $d \geq 2^5$, where the DI DW family of I_N do not offer a feasible scenario for realistic implementations.

3

Quantum Random Access Codes as Dimension Witnesses

Higher dimensions are the future of quantum information, in the sense that dimensionality of physical systems is a form to quantify the power of quantum correlations. For this reason, being able to (i) certify that a source produces systems of at least certain dimensions, and (ii) distinguish between quantum systems from classical systems of the same dimension, is of practical importance because it has been proven that higher dimensions improve the performance of quantum information protocolos.

However, higher dimensions poses experimental and theoretical problems. For this reason, in order to solve these problems, a test with the following characteristics is needed: (i) allow us to certify quantum systems for any dimension, (ii) the amount of outputs of the test be less than the dimension, and (iii) explores the whole space of quantum states, by this we mean that we need to define the measurements in terms of full sets of MUBs. When we are considering high dimensions a full set of mutually unbiased bases (MUBs) involve an amount of settings that would be getting unmanageable as the dimension increase. Therefore, we need that this test, in practice, not use all the settings.

In this chapter we introduce such a test, based on quantum random access codes (QRACs), and report its experimental results.

3.1 Binary Quantum Random Access Codes

Quantum random access codes is a communication task that shows lots of potential as a tool to solve the problem of lack of dimension witnesses for high-dimensional systems. However, the general scenario of QRACs involve d outcomes, which makes its experimental implementation impossible for high-dimensional systems. What we do to overcome this problem, was to modify the scenario of QRACs adding a second input in the measurement device, which allow us to change the multi-outcome decoding strategy into a binary-outcome decoding strategy.

First of all we are going to describe the general scenario for QRACs and then we will describe the scenario for the modify binary version that we developed.

1. **Scenario for Standard Quantum Random Access Codes**.
   The preparation box (Alice) has inputs $a = a_1a_2...a_n$, where a corresponds to a string of n dits, represented by a_i with $i \in \{1, ..., n\}$, then a_i takes values between 1 and d. Notice that the amount of inputs depends on the dimension and the amount of dits on the message. The message a is encoded in a qudit state ρ_a, which is sent to a measurement box (Bob), where a measurement is performed in the base defined by the input $y \in \{1, ..., n\}$, and as a result the outcome $b \in \{1, ..., d\}$ is obtained. It is important to notice that the amount of bases needed is equal to the amount of dits on the string a, because in order to access to the ith dit it is necessary to perform a measurement in the ith base, and this could be understood as Bob trying to recover the value of the ith dit. This scenario is illustrated in Figure 3.1.

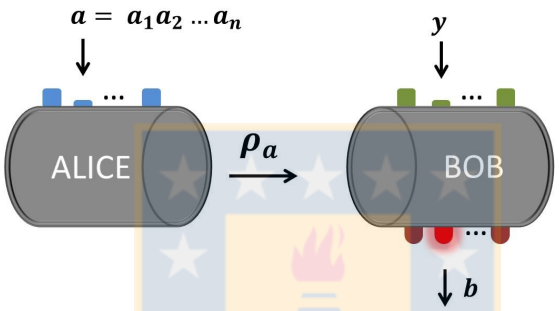

Figure 3.1: llustration of QRACs general scenario.

2. **Scenario for Binary Quantum Random Access Codes**.
   For the preparation box (Alice) the scenario is the same, the input a is encoded in a qudit state ρ_a which is sent to a measurement box (Bob). Now, the measurement box has two inputs, $y \in \{1, ..., n\}$, as in standard QRACs, defining the base in which the measurement will be perform and the new input $k \in \{1, ..., d\}$, which represents in what element of the base y is going to be projected the state sent by Alice. Then, Bob is no longer trying to recover the value of the dit y, instead, he is asking "is the value of the dit $a_y = k$?", so now the output b is binary and corresponds to the answers YES for the value 0 and NO for the value 1. The scenario for binary QRACs is depicted in Figure 3.2

It is important to mention that despite the fact that QRACs can be consider in a general scenario, where Alice and Bob use d-level systems to encode and decode the message, in the literature little attention has been directed to such generalization. To pave the way for this generalization, initial steps has been taken in [17, 50], and more recently in [51] a study of RACs and QRACs with high-level communication was presented, where they generalize, for any dimension, the family of $2^d \xrightarrow{p_d} 1$ RACs and QRACs, which corresponds to the case where $n = 2$ d-dimensional systems are encoded into $m = 1$ d-dimensional system. However, the family of $2^d \xrightarrow{p_d} 1$ RACs and QRACs are the only one for which its bounds are known for any dimension.

With our modified binary version of QRACs we propose a dimension witness for physical systems of dimension eight that also works as a quantumness indicator, which

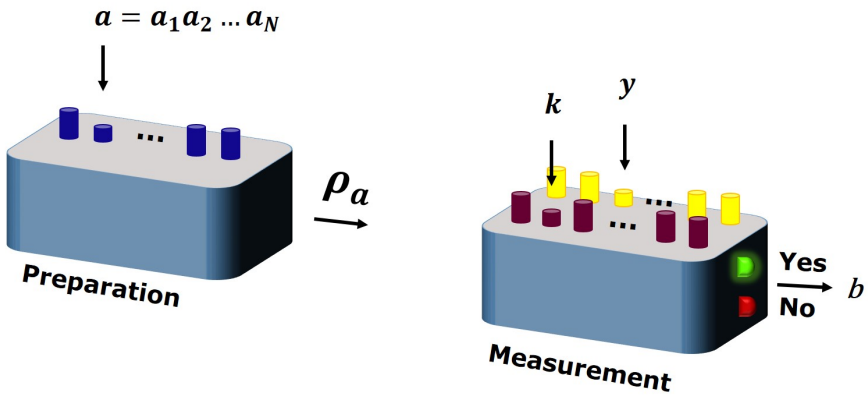

Figure 3.2: llustration of the scenario for binary QRACs.

means that it is capable to discriminate between classical and quantum 8-dimensional systems. Nevertheless, the generalization for any dimension is no straightforward and requires a comprehensive study to obtain the classical and quantum limits considering: the dimension, the amount of dits in which the message will be encoded, the variables distributions, among others.

Now I will introduce the game based in the binary QRAC that I described above.

3.1.1 Optimal Payoff Function

We are given the following task:

1. Alice receives n numbers $a_1, ..., a_n$ from 1 to d each, namely n dits.
2. Alice sends one of the n numbers corresponding to a d message to Bob.
3. Bob gets two inputs $y = 1, ...n$ and $k = 1, ..., d$.
4. Bob needs to answer the question: is $a_y = k$? and his answer is encoded in a variable G which is 0 when his guess is YES and 1 for NO.

Having the game settled, we are free to reward the parties with any number of points, specified by a payoff function $T(a_1, ..., a_n, y, k, G)$ but for simplicity we assume that this function does not depend on the values of numbers a with indexes different than y. Moreover, we were also going to assume that

$$T(a_y, y, k, 0) = -T(a_y, y, k, 1) \tag{3.1}$$

and that the absolute value of T takes only two values: T_{YES} when $a_y = k$ and T_{NO} when $a_y \neq k$.

The average payoff function, which is a linear combination of payoffs for all possible inputs, is going to be our final figure of merit, and for that reason, without loss of generality, we can normalize all the payoffs in any way we want, therefore, we choose

$T_{NO} = 1$. Summing up, our payoff function is

$$T(a_y, y, k, G) = \begin{cases} T_{YES} & \text{when } a_y = k \text{ and } G = 0 \\ -T_{YES} & \text{when } a_y = k \text{ and } G = 1 \\ 1 & \text{when } a_y \neq k \text{ and } G = 1 \\ -1 & \text{when } a_y \neq k \text{ and } G = 0 \end{cases} \tag{3.2}$$

Now we have to choose T_{YES} in such a way that the difference between the average payoff function for quantum and classical cases is the largest.

Without loss of generality we may assume that Bob behaves in the following way. He is divided in two parts, initial Bob, B_I, and final Bob, B_F. B_I gets the message from Alice and his input y and forwards d bits $b_1, ..., b_d$ to B_F. Each of these bits represents the answer that B_F should give for different questions, in other words, B_I generates in advance a string of d bits representing the answers for the questions "is $a_y = k$?". Then B_F receives the message from B_I and his input k, and returns b_k. To be more clear, consider the case when $n = 9$ and $d = 8$ illustrated in Figure 3.3. Alice receives then 9 numbers that can take values from 1 to 8, in the particular case of this example, she receives the string $a = a_1...a_9 = 123456781$. She sends one of this numbers to Bob, where B_I receives the message and the input $y = 4$, which means that Bob is interested in the value of a_4. Then B_I makes the following set of 8 questions in order to generate the answers b_i with $i = 1, ..., d$:

$$\text{is } a_4 = \begin{cases} 1? & \text{NO}, & \text{then } b_1 = 1 \\ 2? & \text{NO}, & \text{then } b_2 = 1 \\ 3? & \text{NO}, & \text{then } b_3 = 1 \\ 4? & \text{YES}, & \text{then } b_4 = 0 \\ 5? & \text{NO}, & \text{then } b_5 = 1 \\ 6? & \text{NO}, & \text{then } b_6 = 1 \\ 7? & \text{NO}, & \text{then } b_7 = 1 \\ 8? & \text{NO}, & \text{then } b_8 = 1 \end{cases} \tag{3.3}$$

B_I sends this string of bits to B_F, where the latter chooses which answer to look by means of the input k, therefore in this case B_F delivers the answer $b_5 = 1$. As we said before $G = 0$ corresponds to the answer YES and $G = 1$ for NO, so in this case the answer to the question "is $a_4 = 5$?" is NO.

Now we will show that if Alice and Bob use the optimal classical strategy to maximize the average payoff then for any message and input y only one of bits b should be equal to 0 and all the others to 1 (at least for some values of n and d).

Optimal strategy of B_I

Before receiving Alice's message Bob knows nothing about the string a, however, in each round of the protocol, after receiving the message that from now on we will call t, B_I can calculate the joint probability distribution of Alice's numbers $p(a_1, ..., a_n|t)$ and the marginal probabilities $p(a_i|t)$. But, because B_I also receives the input y, he is only interested in the probability $p(a_y|t)$, so now lets call $p_j = p(a_y = j|t)$. Depending on the payoff function, there is a critical value of p_{crit} such that, if by sending $b_j = 0$ $p_j > p_{crit}$ then the average payoff will be larger than sending $b_j = 1$.

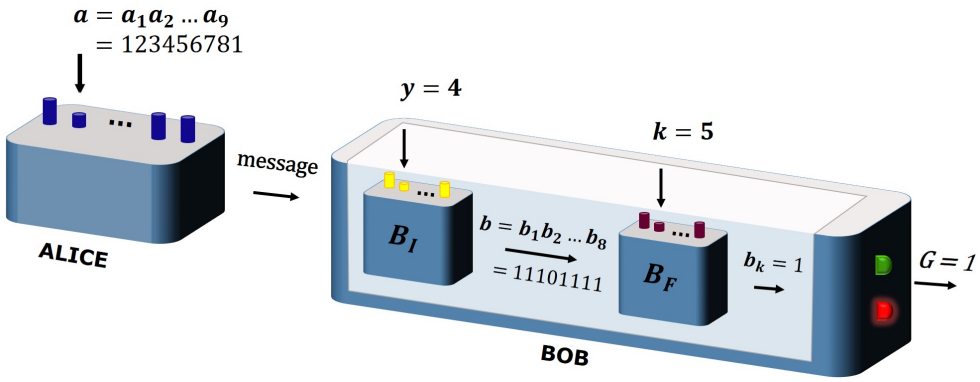

Figure 3.3: Illustration of how binary random access codes can be understand in order to maximize the average payoff using the optimal classical strategy, for the case when $n = 9$ and $d = 8$ is considered.

Sending $b_j = 0$ leads to answer $G = 0$ for $j = k$, which gives T_{YES} points with probability p_j and -1 points with probability $1 - p_j$. On the other hand, for the answer $b_j = 1$, which corresponds to $G = 1$, one gets $-T_{YES}$ points with probability p_j and 1 point with proability $1 - p_j$. We want to maximize the average payoff for the first case so in order to obtain p_{crit} we make

$$\begin{aligned} T_{YES}p_j - (1 - p_j) &\geq -T_{YES}p_j + (1 - p_j) \\ (T_{YES} + 1)p_j &\geq 1 \\ p_j &\geq \frac{1}{T_{YES} + 1} = p_{crit}. \end{aligned} \tag{3.4}$$

Then, the optimal strategy for B_I for a message t and input y, leads to an average payoff of

$$T(t, y) = \frac{1}{d} \sum_{j=1}^{d} |(T_{YES} + 1)p_j - 1|. \tag{3.5}$$

Now we need to optimize the probability distribution in order to obtain the biggest separation between the quantum and the classical case. Let m be the number of bits b that the optimal strategy sets to 0 for a given probability distribution. Without loss of generality we may assume that p_j are ordered in such a way that $p_j \geq p_{j+1}$. Then the average payoff becomes

$$\begin{aligned} T(y, t) &= \frac{1}{d} \left[\underbrace{\sum_{j=1}^{m} |(T_{YES} + 1)p_j - 1|}_{\text{average payoff for } b_j = 0} + \underbrace{\sum_{j=m+1}^{d} |1 - (T_{YES} + 1)p_j|}_{\text{average payoff for } b_j = 1} \right] \\ &= \frac{T_{YES} + 1}{d} \left[\sum_{j=1}^{m} - \sum_{j=m+1}^{d} \right] + \frac{d - 2m}{d}. \end{aligned} \tag{3.6}$$

Because in eq. (3.6) the average payoff only depends on the sums $\sum_{j=1}^{m} p_j$ and $\sum_{j=m+1}^{d} p_j$, and not the individual elements of the sums we can choose that all the elements in each sum are equal. If we denote by p the value of each one of p_j for $j = 1, ..., m$, then the normalization $\sum_j p_j = 1$ implies that the value of each p_j for $j = m+1, ..., d$ is given by $\frac{1-mp}{d-m}$. This allow us to express $T(y,t)$ as a function of m and p

$$\begin{aligned} T(y,t) &= \frac{T_{YES}+1}{d}[mp-(1-mp)] + \frac{d-2m}{d} \\ &= \frac{(T_{YES}+1)(2mp-1)+d-2m}{d}. \end{aligned} \tag{3.7}$$

Our aim is to find a value for p_{crit} such that the optimal value of m be $m = 1$. We use the formula (3.5) to calculate the value of the payoff for a few obvious classical strategies and the quantum strategy to find the range of values of p_{crit} in which the quantum strategy is better than the classical ones when we consider $n = 9$ and $d = 8$, and we obtained that $0.1376 \leq p_{crit} \leq 0.3372$. Because the distance between the quantum strategy and the classical ones decreases when p_{crit} increases, we will be looking for the minimal p_{crit} that implies the optimality of the strategies with $m = 1$. By doing a thorough analysis on the values of p_{crit} we find that the optimal $p_{crit} = 0.185$, which corresponds to $T_{YES} = 4.405$ as you can see from eq. (3.4).

3.1.2 Classical and Quantum Bounds

Now that we have the value for T_{YES} we are able to find the values for

- the **average success probability** p_{succ}, which in standard QRAC corresponds to the probability to successfully recover the dit send by Alice and in the binary QRAC corresponds to the probability of answer successfully the question "is $a_y = k$?", and
- the **average payoff** T_{ave},

for both, the classical and quantum case, when we consider $n = 9$ and $d = 8$.

Classical Bounds

From the previous section we can say that the optimal strategy for B_I is to forward to B_F exactly one number k for which he should give the outcome 0. This is nothing else but forwarding his best guess of the number a_y, and for obtaining the best guess of a_y Alice and B_I should employ the strategy of sending the majority dit, which is the optimal strategy for standard random access codes (RAC).

To calculate the average classical success probability for a n dit string we need to take into account all the possible input, which is nd^n. Now consider that in the n-dit string given to Alice the i-th dit, with $i \in \{1, ..., d\}$, appears x_i times, so the number of combinations for the differents x_i that may occur is the same as the number of solutions in positive integers of the eq. (3.8)

$$x_1 + x_2 + ... + x_d = n, \tag{3.8}$$

and the number of solutions is given by $\binom{n+d-1}{n}$. Then, in each given solution Alice will communicate $max\{x_1, ..., x_d\}$ to Bob, so the number of successes is given by $\frac{n!}{x_1!...x_d!} max\{x_1, ..., x_d\}$, with $\frac{n!}{x_1!...x_d!}$ corresponding to the number of possible combinations of a n-dit string for a given set of x_i and $max\{x_1, ..., x_d\}$ to the number of times where Bob will guess the correct dit. Having this, we can calculate the average classical success probability, which is given by

$$p^C_{succ} = \frac{1}{nd^n} \sum \frac{n!}{x_1!...x_d!} max\{x_1, ..., x_d\}, \tag{3.9}$$

where the summation is over all $\binom{n+d-1}{n}$ possible solutions of eq. (3.8), and for our particular case of $n = 9$ and $d = 8$ we obtain $p^C_{succ} = 0.3118$.

Quantum Bounds

In order to calculate the average quantum success probability we first need to find the optimal states for the $9^8 \to 1$ QRAC, and to do that we need to use the following family of mutual unbiased bases (MUBs) [63, 64]:

$$U^{(1)} = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & -i & -1 & i & -1 & i & 1 & -i \\ -i & 1 & i & -1 & i & -1 & -i & 1 \\ -i & 1 & -i & 1 & i & -1 & i & -1 \\ 1 & -i & 1 & -i & -1 & i & -1 & i \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ -i & 1 & i & -1 & -i & 1 & i & -1 \\ -i & 1 & -i & 1 & -i & 1 & -i & 1 \\ 1 & -i & 1 & -i & 1 & -i & 1 & -i \end{pmatrix},$$

$$U^{(2)} = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & -1 & -1 & 1 & -i & i & i & -i \\ 1 & 1 & -1 & -1 & -i & -i & i & i \\ -1 & 1 & -1 & 1 & i & -i & i & -i \\ 1 & 1 & 1 & 1 & -i & -i & -i & -i \\ -i & i & i & -i & 1 & -1 & -1 & 1 \\ -i & -i & i & i & 1 & 1 & -1 & -1 \\ i & -i & i & -i & -1 & 1 & -1 & 1 \\ -i & -i & -i & -i & 1 & 1 & 1 & 1 \end{pmatrix},$$

$$U^{(3)} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & i & 0 & -i & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ i & 0 & i & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & i & 0 & -i \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & i & 0 & i & 0 \end{pmatrix},$$

$$U^{(4)} = \frac{1}{2}\begin{pmatrix} 1 & -1 & 0 & 0 & -1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & -1 & -1 \\ 0 & 0 & -1 & 1 & 0 & 0 & -1 & -1 \\ 1 & 1 & 0 & 0 & -1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & -1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & -1 \end{pmatrix},$$

$$U^{(5)} = \frac{1}{\sqrt{8}}\begin{pmatrix} 1 & -i & -i & -1 & -1 & -i & i & -1 \\ -i & 1 & -1 & -i & -i & -1 & -1 & i \\ -i & -1 & 1 & -i & i & -1 & -1 & -i \\ -1 & -i & -i & 1 & -1 & i & -i & -1 \\ -i & 1 & -1 & -i & i & 1 & 1 & -i \\ 1 & -i & -i & -1 & 1 & i & -i & 1 \\ -1 & -i & -i & 1 & 1 & -i & i & 1 \\ -i & -1 & 1 & -i & -i & 1 & 1 & i \end{pmatrix},$$

$$U^{(6)} = \frac{1}{2}\begin{pmatrix} 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \\ 0 & i & 0 & -i & 0 & -i & 0 & i \\ 1 & 0 & 1 & 0 & -1 & 0 & -1 & 0 \\ 0 & i & 0 & i & 0 & -i & 0 & -i \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 \\ i & 0 & -i & 0 & i & 0 & -i & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ i & 0 & i & 0 & i & 0 & i & 0 \end{pmatrix},$$

$$U^{(7)} = \frac{1}{2}\begin{pmatrix} 1 & -i & 0 & 0 & -1 & i & 0 & 0 \\ -i & 1 & 0 & 0 & i & -1 & 0 & 0 \\ 0 & 0 & 1 & -i & 0 & 0 & -1 & i \\ 0 & 0 & -i & 1 & 0 & 0 & i & -1 \\ 0 & 0 & i & 1 & 0 & 0 & i & 1 \\ 0 & 0 & 1 & i & 0 & 0 & 1 & i \\ i & 1 & 0 & 0 & i & 1 & 0 & 0 \\ 1 & i & 0 & 0 & 1 & i & 0 & 0 \end{pmatrix},$$

$$U^{(8)} = \frac{1}{\sqrt{8}}\begin{pmatrix} 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -1 & -1 \end{pmatrix},$$

$$U^{(9)} = \frac{1}{2}\begin{pmatrix} 1 & 0 & -i & 0 & -1 & 0 & i & 0 \\ 0 & 1 & 0 & -i & 0 & -1 & 0 & i \\ -i & 0 & 1 & 0 & i & 0 & -1 & 0 \\ 0 & -i & 0 & 1 & 0 & i & 0 & -1 \\ -i & 0 & 1 & 0 & -i & 0 & 1 & 0 \\ 0 & -i & 0 & 1 & 0 & -i & 0 & 1 \\ 1 & 0 & -i & 0 & 1 & 0 & -i & 0 \\ 0 & 1 & 0 & -i & 0 & 1 & 0 & -i \end{pmatrix}.$$

Now to construct the optimal states we take the 9 MUBS $U^{(i)}$, with $i = 1, ..., 9$, where each column represents a basis vector for that MUB. We will identify the j-th vector of the i-th MUB by $|j\rangle_i$, for example, the first vector of the first MUB is given by $|1\rangle_1 = \frac{1}{\sqrt{8}}(1, -i, -i, 1, 1, -i, -i, 1)$, therefore we will have that the projector on this state is $P^i_j = |j\rangle_i\langle j|_i$.

When Alice gets the input $a = a_1...a_9$ with $n = 9$ dits, following the procedure described in [50], we define an operator

$$O(a_1, ..., a_9) = \sum_{i=1}^{9} P^i_{a_i}, \tag{3.10}$$

for which we need to find the eigensystem, this is, eigenvectors and eigenvalues. Then from the eigensystem, we have to pick the largest eigenvalue and its corresponding eigenvector, because this eigenvector corresponds to the optimal state $|\Phi_{a_1,...,a_9}\rangle$ for QRAC when Alice get the input $a = a_1...a_9$.

Thus, we have that the encoding of the $n = 9$ dits is made in one of the optimal 8-dimensional states $|\Phi_{a_1,...,a_9}\rangle$, this message goes to Bob, where the input $y \in \{1, ..., 9\}$ corresponds to select one of the 9 MUBs listed above and the input $k \in \{1, ..., 8\}$ select one of the basis vectors of the y-th MUB, in which the state $|\Phi_{a_1,...,a_9}\rangle$ is going to be projected. Having this, we are able to compute the average quantum success probability, obtaining $p^Q_{succ} = 0.3372$ [50].

Summing up, for $n = 9$ and $d = 8$ it seems that the largest separation between the classical and the quantum case is for $T_{YES} = 4.405$. For these parameters both classical and quantum bounds are obtained by first using the optimal strategy for a standard RAC and QRAC, respectively, and then simply checking if the value returned is equal to k. The success probabilities are $p^C_{succ} = 0.3118$ and $p^Q_{succ} = 0.3372$ for classical and quantum case respectively.

Having the values of the success probabilities, using eq. (3.2) we can calculate the average payoff for the classical and quantum strategies. From eq. (3.2) we see that there are two cases: $a_y = k$ and $a_y \neq k$, then we have that

1. when $a_y = k$ with probability p_{succ} we get the outcome $G = 0$ and $T_{YES} = 4.405$ points, and with probability $(1 - p_{succ})$ we get $G = 1$ and loose 1 point. On average we get

$$T_{a_y=k} = T_{YES}p_{succ} - (1 - p_{succ}) = \begin{cases} 0.6853 & \text{for the classical case} \\ 0.8226 & \text{for the quantum case} \end{cases} \tag{3.11}$$

2. when $a_y \neq k$ the probability to get the outcome $G = 0$ and loose $T_{YES} = 4.405$ points is very small and corresponds to $\frac{(1-p_{succ})}{7}$, on the other hand, with probability $1 - \frac{(1-p_{succ})}{7}$ we get 1 point. On average we get

$$T_{a_y\neq k} = -T_{YES}\frac{(1 - p_{succ})}{7} + 1 - \frac{(1 - p_{succ})}{7} = \begin{cases} 0.4687 & \text{for the classical case} \\ 0.4882 & \text{for the quantum case} \end{cases} \tag{3.12}$$

Since Alice's and Bob's inputs are independent we have that $a_y = k$ occurs with probability $\frac{1}{8}$ and $a_y \neq k$ with probability $\frac{7}{8}$, therefore the average payoff is given by $T^C_{ave} = 0.4957$ for the classical optimal strategy and by $T^Q_{ave} = 0.5300$ for the quantum optimal strategy.

3.2 Experimental Implementation of 8-dimensional Binary QRAC

Here, we will show that with the modification described above for QRACs, which simplifies its experimental realization, it is possible to experimentally observe the quantum advantage of the 8-dimensional Binary QRAC by considering only ("yes-and-no") dichotomic answers associated to the system detection at one of the outcomes of such measurements, at a time.

The importance of this experiment is that we only need the averages of the success probability and detection efficiency, instead to estimate them for any state. This fact implies that the experimental data analysis will be as simple as possible, because in order to estimate the average success probability and the average payoff function we only need the following data:

- $\mathbf{x_1}$ - number of experimental rounds where the settings are chosen such that $a_y = k$,
- $\mathbf{x_2}$ - number of experimental rounds where the settings are chosen such that $a_y \neq k$,
- $\mathbf{D_1}$ - number of times a particle is registered when $a_y = k$,
- $\mathbf{D_2}$ - number of times a particle is registered when $a_y \neq k$,
- η - overall detection efficiency.

Then, considering that each experimental round has an optical pulse of one photon, we have that the average success probability will be given by

$$p^{exp}_{succ} = \frac{D_1}{\eta x_1},$$

and the experimental average payoff can be calculated using eqs. (3.11) and (3.12), obtaining

$$T^{exp}_{ave} = \frac{1}{8}[T_{YES}(2p^{exp}_{succ} - 1) - 2(1 - p^{exp}_{succ}) + 7].$$

3.2.1 The Experiment

For the experimental realization of the 8-dimensional QRACs, we resort to the linear transverse momentum of single-photons to encode the required 8-dimensional quantum systems. Our experimental setup is depicted in Fig. 3.4. At the state preparation block the single-photon regime is achieved by heavily attenuating optical pulses, which are generated with an acousto-optical modulator (AOM) placed at the output of a

continuous-wave laser operating at 690nm. Well calibrated attenuators are used to set the average number of photons per pulse to $\mu = 0.6$, and in this case, the probability of having non-null pulses, this is, of having pulses containing at least one photon is $P(\mu = 0.6|n \geq 1) = 45\%$, where pulses containing only one photon are the vast majority of the non-null pulses generated and accounts to 73% of the experimental runs. The probability of high multi-photon events is negligible, therefore, our source can be seen as a good approximation to a non-deterministic single photon source, as commonly adopted in quantum key distribution [65].

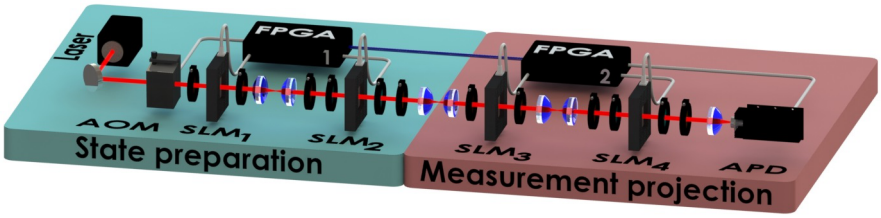

Figure 3.4: Experimental setup. We employ a prepare-and-measure scheme to generate and detect eight dimensional quantum states encoded on the linear tranverse momentum of single photons [42, 66, 67, 68, 69]. At the State Preparation block, the encoding is applied through two spatial light modulators (SLMs). The projections are likewise performed by two SLMs combined with a point-like single-photon detector (APD) fixed at the origin of the far-field plane.

Using spatial light modulators (SLM), SLM1 and SLM2, we generate $d = 8$ parallel transmissive slits, effectively creating 8-dimensional quantum states encoded in the propagation modes available for the single photon transmission. Each slit is 96 μm wide and they are equally separated by 128 μm. See Fig. 3.5 for a graphic description. After the SLM2, which is placed at the image plane of SLM1 through a set of lenses, the state of the transmitted photon is given by $|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{-l_d}^{l_d} \sqrt{t_l} e^{\phi_l} |l\rangle$, where $|l\rangle$ corresponds to the state of the photon transmitted by the lth slit, $l_d = \frac{d-1}{2}$, N is a normalization factor [63, 70, 71, 72], t_l represents the transmission and ϕ_l the phase associated to the lth slit, which are controlled by SLM1 and SLM2, respectively.

The amplitude and relative phase for each SLM needs to be characterize in order to obtain the modulation curves as a function of the grey level of the SLMs [73]. We found that the modulation functions are:

- for the SLM1, which controls the transmission, is given by

$$f(r) = 239.74 r^{0.446221} + 13.7239 r, \tag{3.13}$$

  where r corresponds to the amplitude of each component of the state $|\Psi\rangle$;

- for the SLM2, which controls the phase, is given by

$$\begin{aligned} f(\theta) \quad = \quad & 25107.7\theta^{0.6} - 52337.7\theta^{0.5} + 37014.4\theta^{0.3} + (3.72012 \times 10^{-11})\theta^{21} \\ & -0.000213162\theta^{11} + 0.00322919\theta^{9} - 1091.09\theta, \end{aligned} \tag{3.14}$$

  where θ corresponds to the phase of each component of the state $|\Psi\rangle$.

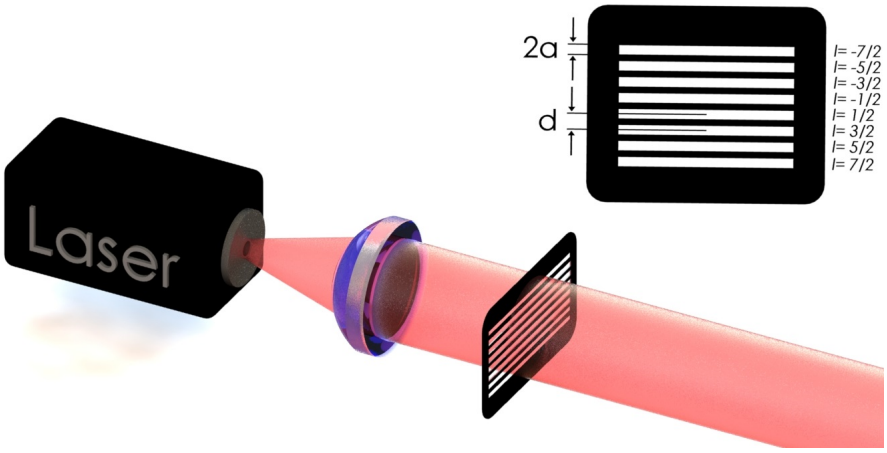

Figure 3.5: llustration of set-up to make use of the linear angular momentum of single-photons to encode 8-dimensional quantum systems. With a SLM, 8 slits are generated, defining 8 possible paths, where each slit is of the same width $2a = 96\mu$m and equally spaced $d = 128\mu$m.

Having this, the encoding of the 8-dimensional quantum states is complete at the state preparation block.

At the measurement block we use a similar scheme as in the state preparation block, but now with SLM3 and SLM4, and a pointlike avalanche single-photon detector (APD) to implement the desired measurements [42, 66, 67, 68, 69]. Analogously, the amplitude and phase of the state projectors are individually set by SLM3 and SLM4 respectively. By placing the pointlike APD at the far-field plane, and properly adjusting the SLM3 and SLM4 modulations, one can post-select for detection any outcome of an eight dimensional projective measurement [63]. As expected, the probability that a photon is detected is proportional to the overlap between the generated and post-selected states.

By means of two field-programmable gate arrays (FPGA) electronic modules we are able to automate and actively control both blocks of the setup. At the state preparation block, the state $|\Psi\rangle$ is randomly prepared into one of the 8^9 states of the set defined by our eight dimensional QRAC protocol. For this purpose, a quantum random number generator (QRNG - Quantis) is connected to FPGA1. The FPGA1 also controls the optical pulse production by the AOM, set at repetition rate of 30 Hz to synchronize with the refresh rate of the SLMs [66]. At the measurement block, a second QRNG is connected to FPGA2, providing an independent and random selection for the projection at each round.

The protocol is executed as follows:

1. In each round (as dictated by the synchronization pulse), FPGA1 reads from its QRNG a string of 27 random bits to generate the $y = 1, ..., 9$ 8-dimensional a_y dits that are univocally associated to one of the 8^9 states to be randomly generated; 27 bits are needed because the 8-dimensional dits are encoded in numbers form 0 to 7, therefore 3 bits are needed for each a_y dit.

2. Based on this string, following the procedure described earlier to find the optimal

state associated to the string we obtain the components of the state, then the FPGA1 calculates the amplitude and phase of each slit from SLM1 and SLM2 using eqs. (3.13) and (3.14), therefore encoding the desired state onto the single-photon generated in that experimental round.

3. Simultaneously, FPGA2 reads from its QRNG a 7-bit string to determine one of the 72 possible projections p_k^b to be implemented, where $b = 1, ..., 9$ denotes one of the nine measurement bases considered, and $k = 1, ..., 8$ denotes the selected projection within base b.

4. Similar to what is done in the state preparation block, FPGA2 also calculates the amplitude and the phase for each slit in SLM3 and SLM4 to implement the randomly chosen projection.

In this experiment, is necessary to dynamically generate all possible states, as it would be unfeasible to pre-record the modulation information of each of the 8^9 states on the FPGA1. Thus, note that for each experimental run, the detection block implements the required "yes-and-no" dichotomic tests checking whether the a_y generated dit was equal or not to k. That is, if the photon is detected let's say when $b = 3$ and $k = 4$, one can positively answer that the a_3 dit was equal to 4. If there is no detection, we can say that this was not the case. For this reason, in each round, FPGA2 also records whether or not a detection occurred in the APD. The overall detection efficiency is approximately $\eta = 20.000 \pm 0.002\%$. After several experimental runs one can then estimate the average success probability and its corresponding confidence region, while dealing with unavoidable experimental misalignment and detector's dark counts. To accumulate more events and minimize statistical uncertainties, the experiment automated worked over ≈ 100 hours, with the number of experimental runs, detections, and employed settings displayed in Table 3.1.

D_1	D_2	x_1	x_2
46303	273784	1.507.214	10.532.786

Table 3.1: Experimental results. D_1 number of times a particle was recorded when $a_{y=b} = k$; D_2 number of times a particle was recorded when $a_{y=b} \neq k$; x_1 number of experimental rounds where the settings are chosen such that $a_{y=b} = k$; x_2 number of experimental rounds where the settings are chosen such that $a_{y=b} \neq k$.

As explained before, in our method there is no need to record the statistics for all the states of the set of 8^9 states to estimate the success probability. Nevertheless, it is important to demonstrate that in our experiment we were indeed uniformly selecting such states to avoid biased results. This is done by monitoring the number of times that each state was selected. A random ensemble of 3000 states generated is plotted in Fig. 3.6(a). As one can see from the histogram, each state was selected only once, as expected. In Fig. 3.6(b) we also show the probability that each one of the 72 possible projections has been selected in our experimental run. Uniformity is guaranteed when all the probabilities are equally likely ($\frac{1}{72} \approx 0.01388$). Thus, from Figs. 3.6(a) and 3.6(b)

one can see that the probability distributions for the state generation and measurement projections can be well approximated by an uniform distribution.

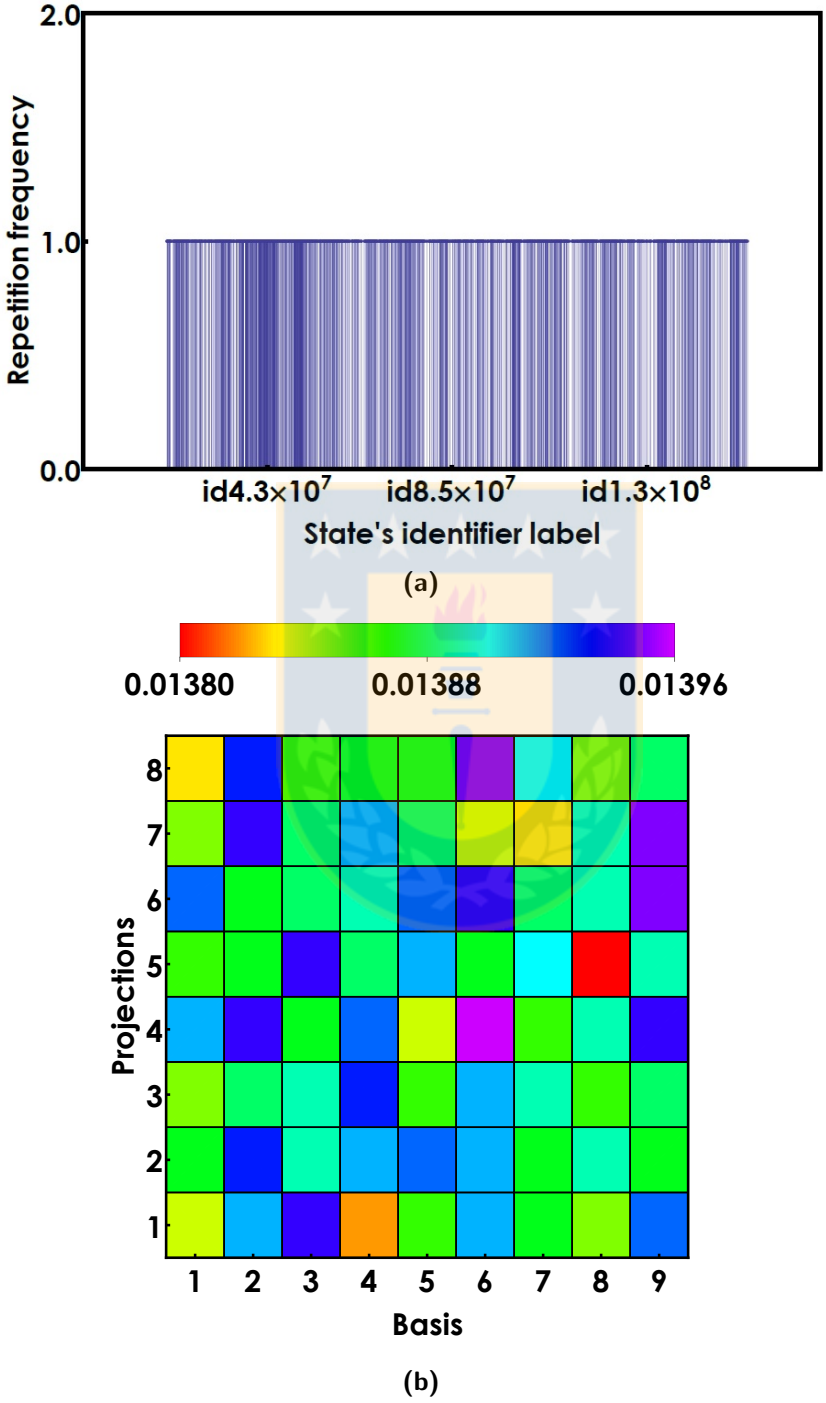

Figure 3.6: (a) State generation repetition frequency for a random ensemble of 3000 states generated in our experiment. To order the states, we consider the string $a = a_8, ..., a_0$ as one big number encoded in the octal numeral system. (b) The projection probability distribution observed in our experiment.

From the experimental results given in Table 3.1, one can calculate the observed average success probability p_{succ}, which is shown in Fig. 3.7(a). As explained in the beginning of this section, it is given by

$$p_{succ} = \frac{D_1}{\eta P(\mu = 0.6|n \geq 1)x_1},$$

where $P(\mu = 0.6 \geq 1)$ is the probability of having pulses containing at least one photon. As you can see, we clearly violate the classical bound by more than 23 standard deviations, therefore certifying the quantum nature of the 8-dimensional systems employed to transmit information. In Fig. 3.7(b) we also display the corresponding payoff function.

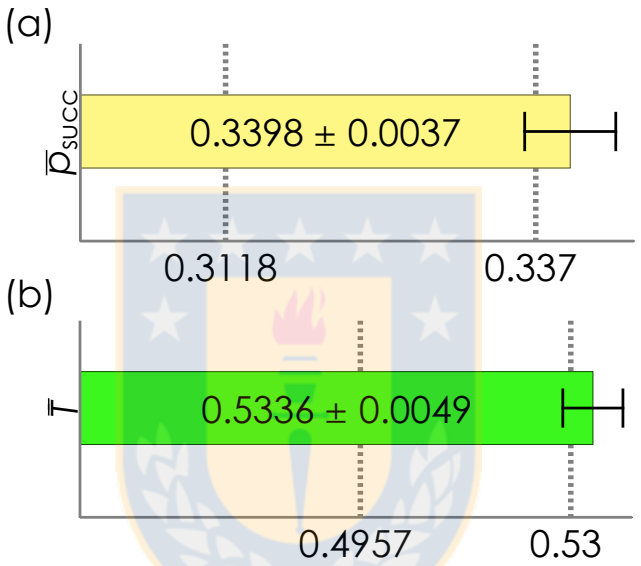

Figure 3.7: (a) Observed success probability and (b) the corresponding payoff function.

With this work we have shown that it is possible to simplify quantum random access codes in higher dimensions. By modifying the protocol into binary quantum random access codes we were able to proved that only with the averages of "yes-and-no" answers associated to the system detection at one of the outcomes was possible to observe the quantum advantage that QRACs provide when 8-dimensional quantum systems are used to encode the information. The fact that only the averages were necessary was the one that allow us to greatly simplify its experimental realization, because otherwise we would have needed to measure for a ridiculously huge amount of time in order to obtain the success probability of each measured state.

Besides, other important properties of this protocol are that it works both as a dimension witness and as a quantumness indicator for 8-dimensional systems, which means that if we are able to reach values for $p_{succ} \geq 0.3118$ we are witnessing 8-dimensional systems, moreover, if we observe values for $p_{succ} \geq 0.337$ we can assure that 8-dimensional quantum systems were used in the protocol.

Based on the promising results of the modified version of QRACs for 8-dimensional systems we make the hypothesis that it is possible to find dimension witnesses for

systems of high dimensions, that also work as quantumness indicators. Moreover, we presume that a generalization can be made, however, it requires a comprehensive study to obtain the classical and quantum limits considering the dimension, the amount of dits in which the message will be encoded, the variables distributions, among others.

Conclusions

Within this thesis we address the problem of certify the dimension of the systems produced by the sources, in particular we focus on the problem of high dimensions, which is our case were systems of dimension six and eight. We study the family of dimension witnesses I_N, and we proved that this family is not an adequate theoretic tool to experimentally certify systems of dimensions $d > 2^4$, due to the great amount of parameters which will be needed to be controlled in the laboratory. This fact about the device independent dimension witness I_N lead us to a search for an suitable protocol to certify the dimension of high-dimensional systems, where thanks to the collaboration with Dr. Pawłowski group, we realized about the great potential that the communication task of quantum random access codes has as dimension witness. Then, based on a modified version of the quantum random access codes, we were able to propose a dimension witness, which involves binary outputs and average probabilities, making the process of experimental certification of the dimension of an unknown systems as easy as possible.

Having said that, we can conclude that the objectives of this thesis were successfully achieved, because we were able to experimentally certify the quantum nature and the dimension of unknown systems of dimension six and eight, using two different protocols. It is important to mention that to our knowledge, to this date there is no documentation of dimension witnesses that certify dimensions higher than eight.

Conclusiones

En esta tesis discutimos el problema de certificar la dimensión de los sistemas producidos por una fuente, en particular nos enfocamos en el problema de dimensiones altas, que en nuestros casos de estudio fueron sistemas de dimensión seis y ocho. Estudiamos la familia de testigos de dimensión I_N, la cual mostramos no es una herramienta adecuada para certificar experimentalmente sistemas de dimensiones $d > 2^4$, debido a la gran cantidad de parámetros que sería necesario controlar en el laboratorio es inmanejable. Esto nos derivó a la búsqueda de un protocolo adecuado para la certificación de sistemas altas dimensiones, donde gracias a la colaboración con el grupo del Dr. Pawłowski, nos dimos cuenta del gran potencial que tiene la tarea de quantum random access code de funcionar como un testigo de dimensión. Fue así como logramos proponer un testigo de dimensión basado en una versión modificada de la tarea de quantum random access code, la cual involucra resultados binarios y promedios de probabilidades, haciendo la certificación experimental de la dimensión de un sistema cuántico desconocido lo más simple posible.

Por todo lo anterior, podemos concluir que los objetivos de esta tesis fueron logrados con éxito, ya que logramos certificar la naturaleza cuántica y la dimensión de sistemas tanto de dimensión seis como de dimensión ocho, utilizando diferentes protocolos. Es importante mencionar que a nuestro conocimiento, a la fecha no existe certificación de sistemas de dimensiones mayores utilizando testigos de dimensión.

Bibliography

[1] V. Scarani, Acta Physica Slovaca **62**, 347 (2012). 1, 1.1

[2] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006). 1, 1.1

[3] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007). 1, 1.1

[4] J. S. Bell, Physics **1**, 195 (1964). 1

[5] N. Brunner, S. Pironio, A. Acín, N. Gisin, A. A. Méthot, and V. Scarani, Phys. Rev. Lett. **100**, 210503 (2008). 1, 1.2, 2.1

[6] T. Vértesi and K. F. Pál, Phys Rev. A **79**, 042106 (2009). 1, 2.1

[7] T. Vértesi, S. Pironio, and N. Brunner, Phys. Rev. Lett. **104**, 060401 (2010). 1, 2.1

[8] M. Junge, C. Palazuelos, D. Pérez-García, I. Villanueva, and M. M. Wolf, Phys. Rev. Lett. **104**, 170405 (2010). 1, 2.1

[9] S. Wehner, M. Christandl, and A. C. Doherty, Phys. Rev. A **78**, 062112 (2008). 1, 1.3, 2.1

[10] O. Gühne, C. Budroni, A. Cabello, M. Kleinmann, and J.-Å. Larsson, Phys. Rev. A **89**, 062107 (2014). 1, 2.1, 2.1

[11] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. **105**, 230501 (2010). 1, 1.2, 2.1, 2.1, 2.2, 2.3

[12] S. Wiesner, SIGACT News **15**, 78 (1983). 1, 1.3

[13] A. Ambainis, A. Nayak, A. Ta-Shma, U. Vazirani, *Proceedings of the 31st Annual ACM Symposium on Theory of Computing (STOC'99)*, 1999 (ACM, New York, 1999), pp. 376-383. arXiv:quant-ph/9804043v2 1, 1.3

[14] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, J. ACM **49**, 496 (2002). 1, 1.3

[15] I. Kerenidis, Ph.D. thesis, University of California at Berkeley, 2004. 1

[16] M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, *Proceedings of 24th International Symposium on Theoretical Aspects of Computer Science (STACS 2007)*, Lecture Notes in Computer Science 4393, pp. 610-621, 2007. 1, 1.3

[17] E. F. Galvão, Ph.D. thesis, University of Oxford, 2002. 1, 3.1

[18] H. W. Li, Z. Q .Yin, Y. C. Wu, X. B. Zou, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, Phys. Rev. A **84**, 034301 (2011). 1, 1.1

[19] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011). 1, 1.1, 1.2

[20] D. Mayers and A. Yao, Proceedings of the 39th IEEE Conference on Foundations of Computer Science; 1998.quant-ph/9809039. 1.1

[21] D. Mayers and A. Yao, Quantum Inform. Comput. **4**, 273 (2004). 1.1

[22] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010). 1.1

[23] L. Masanes, S. Pironio, and A. Acín, Nat. Commun. **2**, 238 (2010). 1.1

[24] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. A **86**, 062326 (2012). 1.1

[25] A. Máttar, J. B. Brask, and A. Acín, Phys. Rev. A **88**, 062319 (2013). 1.1

[26] J. A. Slater, C. Branciard, N. Brunner, and W. Tittel, New J. Phys. **16**, 043002 (2014). 1.1

[27] E. A. Aguilar, R. Ramanathan, J. Kofler, and M. Pawłowski, Phys. Rev. A **94**, 022305 (2016). 1.1

[28] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, Phys. Rev. A **80**, 062327 (2009). 1.1

[29] M. McKague, T. H. Yang, and V. Scarani, J. Phys. A: Math. Theor. **45**, 455304 (2012). 1.1

[30] C. A. Miller and Y. Shi, arXiv:1207.1819. 1.1

[31] B. W. Reichardt, F. Unger, and U. Vazirani, Nature (London) **496**, 456 (2013). 1.1

[32] T. H. Yang and M. Navascúes, Phys. Rev. A **87**, 050102(R) (2013). 1.1

[33] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascúes, Phys. Rev. Lett. **113**, 040401 (2014). 1.1

[34] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, Phys. Rev. Lett. **106**, 250404 (2011). 1.1

[35] K. F. Pál and T. Vértesi, Phys. Rev. A **83**, 062123 (2011). 1.1

[36] J.-D. Bancal, C. Branciard, N. Brunner, N. Gisin, and Y.-C. Liang, J. Phys. A: Math. Theor. **45**, 125301 (2012). 1.1

[37] N. Brunner, J. Sharam, and T. Vértesi, Phys. Rev. Lett. **108**, 110501 (2012). 1.1

[38] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, Phys. Rev. Lett. **111**, 030501 (2013). 1.1

[39] J. T. Barreiro, J.-D. Bancal, P. Schindler, D. Nigg, M. Hennrich, T. Monz, N. Gisin, and R. Blatt, Nat. Phys. **9**, 559 (2013). 1.1

[40] Y.-C. Liang, T. Vértesi, and N. Brunner, Phys. Rev. A **83**, 022108 (2011). 1.1

[41] S. Kochen and E. P. Specker, J. Math. Mech. **17**, 59 (1967). 1.2

[42] M. Arias, G. Cañas, E. S. Gómez, **J. F. Barra**, G. B. Xavier, G. Lima, V. D'Ambrosio, F. Baccari, F. Sciarrino, and A. Cabello, Phys. Rev. A **92**, 032126 (2015). 1.2, 3.4, 3.2.1

[43] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002). 1.2

[44] M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. Cerf, J. Phys. A **35**, 10065-10076 (2002). 1.2

[45] W. K. Wooters and B. D. Fields, Ann. Phys. (N. Y.) **191**, 363 (1989). 1.2

[46] B. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White, Nat. Phys. **5**, 134 (2009). 1.2

[47] A.S. Kholevo, Problems of Information Transmission **9** (1973). 1.3

[48] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner, and G. J. Pryde, Phys. Rev. Lett. **102**, 010401 (2009). 1.3

[49] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, arXiv:0810.2937. 1.3

[50] A. Casaccino, E. F. Galvão, and S. Severini, Phys. Rev. A **78**, 022310 (2008). 1.3, 3.1, 3.1.2, 3.1.2

[51] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Phys. Rev. Lett. **114**, 170502 (2015). 1.3, 3.1

[52] A. Ambainis, D. Kravchenko, and A. Rai, arXiv:1510.03045. 1.3

[53] M. M. Wolf and D. Perez-García, Phys. Rev. Lett. **102**, 190504 (2009). 2.1

[54] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres, Nat. Phys. **8**, 588 (2012). 2.1, 2.2.2, 2.2

[55] J. Ahrens, P. Badziąg, A. Cabello, and M. Bourennane, Nat. Phys. **8**, 592 (2012). 2.1, 2.2.2, 2.1

[56] V. D'Ambrosio, F. Bisesto, F. Sciarrino, **J. F. Barra**, G. Lima, and A. Cabello, Phys. Rev. Lett. **112**, 140503 (2014). 2.1, 2.2.2, 2.3, 2.4, 2.2, 2.3

[57] M. Dall'Arno, E. Passaro, R. Gallego, and A. Acín, Phys Rev. A **86**, 042312 (2012). 2.1, 2.2.1

[58] N. Brunner, M. Navascués, and T. Vértesi, Phys. Rev. Lett. **110**, 150501 (2013). 2.1

[59] J. Bowles, M. T. Quintino, and N. Brunner, Phys. Rev. Lett. **112**, 140407 (2014). 2.1

[60] J. Bowles, N. Brunner, and M. Pawłowski, Phys. Rev. A **92**, 022351 (2015). 2.1

[61] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, and J. P. Woerdman, Phys. Rev. A **45**, 8185 (1992). 2.3

[62] V. D'Ambrosio, F. Cardano, E. Karimi, E. Nagali, E. Santamato, L. Marrucci, and F. Sciarrino, Sci. Rep. **3**, 2726 (2013). 2.3

[63] G. Lima, L. Neves, R. Guzmán, E. S. Gómez, W. A. T. Nogueira, A. Delgado, A. Vargas, and C. Saavedra, Opt. Express **19**, 3542 (2011). 3.1.2, 3.2.1, 3.2.1

[64] A. B. Klimov, C. Muñoz, A. Fernández, and C. Saavedra, Phys. Rev. A **77**, 060303(R) (2008). 3.1.2

[65] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002). 3.2.1

[66] S. Etcheverry, G. Cañas, E. S. Gómez, W. A. T. Nogueira, C. Saavedra, G. B. Xavier, and G. Lima, Sci. Rep. **3**, 2316 (2013). 3.4, 3.2.1

[67] G. Cañas, S. Etcheverry, E. S. Gómez, C. Saavedra, G. B. Xavier, G. Lima, and A. Cabello, Phys. Rev. A **90**, 012119 (2014). 3.4, 3.2.1

[68] G. Cañas, M. Arias, S. Etcheverry, E. S. Gómez, A. Cabello, G. B. Xavier, and G. Lima, Phys. Rev. Lett. **113**, 090404 (2014). 3.4, 3.2.1

[69] D. Goyeneche, G. Cañas, S. Etcheverry, E. S. Gómez, G. B. Xavier, G. Lima, and A. Delgado, Phys. Rev. Lett. **115**, 090401 (2015). 3.4, 3.2.1

[70] L. Neves, G. Lima, J. G. Aguirre Gómez, C. H. Monken, C. Saavedra, and S. Pádua, Phys. Rev. Lett. **94**, 100501 (2005). 3.2.1

[71] G. Lima, A. Vargas, L. Neves, R. Guzmán, and C. Saavedra, Opt. Express **17**, 10688 (2009). 3.2.1

[72] G. Lima, E. S. Gómez, A. Vargas, R. O. Vianna, and C. Saavedra, Phys. Rev. A **82**, 012302 (2010). 3.2.1

[73] I. Moreno, P. Veláquez, C. R. Fernandez-Pousa and M. M. Sanchez-López, J. Appl. Phys. **94**, 36973702 (2003). 3.2.1