Single Photon Sources and
Single Quantum System enabled Communication –

Muhammad Alley Hameedi

Single Photon Sources and Single Quantum System enabled Communication

Muhammad Alley Hameedi

Thesis for the degree of Doctor of Philosophy in Physics
Department of Physics
Stockholm University
Sweden.

ISBN (printed) 978-91-7649-708-1
ISBN (pdf) 978-91-7649-709-8

Printed in Sweden by US-AB, Stockholm 2017.
Distributor: Department of Physics, Stockholm University.

Cover illustration: Parallel quantum random access codes (QRACs) for test of non-classicality of two-level quantum systems.

Abstract

Quantum information is a highly interesting and fast emerging field that involves processing information encoded into quantum systems and their subsequent use in various information tasks. The use of quantum resources such as superposition and entanglement has been shown to enhance information processing capabilities beyond classical means in a number of communication, information and computation tasks.

In this thesis, we have used single photons to study the advantage of d-level quantum systems (qudits) for a communication task commonly known as random access codes (RACs). A successful experimental demonstration of four dimensional quantum random access codes (QRACs) is realized to demonstrate that the higher dimensional QRACs not only outperform the classical RACs but also provide an advantage over their quantum bit (qubit) counterparts. QRACs are also studied in regards to two specific applications: certification of true randomness and for testing the non-classicality of quantum systems. A method for increased certification of generated randomness is realized for the former and a successful experimental demonstration of a test of non-classicality with arbitrarily low detection efficiency is provided for the latter. This is followed by an implementation of a QRAC in a one-path communication network consisting of preparation, transformation and measurement devices. We have shown that the distributed QRAC provides optimal success probabilities for a number of tasks.

Moreover, a novel quantum protocol for the solution to the problem of dining cryptographers and anonymous veto voting is presented. This single photon transmission based protocol provides an efficient solution, which is experimentally demonstrated for a three-party description.

Lastly, Nitrogen-Vacancy (NV) center in diamond is studied as a potential resource for single photon emission and two methods to enhance the photon collection efficiency are successfully explored. Due to this enhancement, single photons from an NV center may also be used in similar single quantum system based communication experiments.

This thesis is dedicated to my beloved parents...

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my PhD supervisor, Professor Mohamed Bourennane, for not only providing me with an opportunity to do my PhD in his group but also for his continuous support, guidance and supervision throughout the course of my graduate studies. It has been a totally wonderful learning experience, one that I am extremely thankful for.

Over the course of my PhD studies, I have had the privilege to get to know, learn from and work with some wonderful people. When I joined the KIKO group Magnus Rådmark, Elias Amselem, Hatim Azzouz, Johan Ahrens, Kate Blanchfield, Muhammad Sadiq and Christian Kothe, PhD students at the time, were all very helpful and made me feel welcomed. I look back fondly at all our work and off work discussions and activities.

Hatim Azzouz, a good friend, deserves a special mention for not only showing me the way around in the nanophotonics lab and clean room but also for passing along the technical know how and expertise that has served me well during my research. I would like to sincerely thank Muhammad Sadiq, who always had the patience and time for the long and rather frequent but extremely useful discussions that we had about our experiments and quantum optics in general. I never hesitated asking you any questions and have learned a lot from you. I have also thoroughly enjoyed the hospitality and all the delicious meals during my frequent visits to your apartment.

Special mention has to go to Breno Marques here. You have been a part of most of my projects and I have always considered you as my second supervisor. Your ability to explain and teach things is absolutely fantastic and something that I have always deeply appreciated. Your sense of humour and outlook on life is just brilliant and I have some excellent memories from our mutual activities. It was great to have you and your lovely wife Ana in Stockholm and I wish you all the best for your academic career.

A very special acknowledgement to all my research collaborators; Armin Tavakoli, Debashis Saha, Piotr Mironowicz, Marcin Pawłowski

and Marcin Wieśniak. It has been great fun to work and interact with all of you and doing these experiments.

For the other present and past members of the group: Ashraf Abdelrazig, Hammad Anwer, Mohamed Nawareg, Christoph Dittel, Victor Österberg, David Andersson, Hannes Hübel, Isabelle Herbauts, Hoshang Heydari, Guillermo Andler, Ian Davidson, Massimiliano Smania, Gerard Higgins, Fabian Pokorny, Marco Avesani, Muhammad Saeed, Muhammad Waqas, Teddy, Jonathan Klasén, David Farrell, Alexander Moritz, Chi Zhang, Adrian Holzäpfel and Arash Zanali. I have thoroughly enjoyed your presence and fabulous company and all of you have left a deep impression that will be cherished. I would also like to thank Victoria Lipinska for her invaluable, wholehearted and unwavering support for the most part of the last two years of my PhD. I wish all of you the very best for your future.

I would also like to thank Professor Ingemar Bengtsson, my mentor during my PhD studies, for your encouragement and for taking the time out to proof-read my thesis. Your feedback has helped me to improve this thesis and I am thankful for that.

During my PhD, I had the fortune to visit Professor Jörg Wrachtrup's research group in the University of Stuttgart for about 8 months. I would like to thank Professor Wrachtrup for this amazing learning opportunity and for the group's generous hospitality during my stay. I would also like to thank Sen Yang, Amit Finkler and Anurag Kanase for all the useful discussions and their help in the fabrication of the SILs and nanopillars. This was a great opportunity to learn, one that I have thoroughly enjoyed. Special mention has to go to other members of the group as Roland Nagy, Johannes Greiner, Thomas Oeckinghaus, Nabeel Aslam, Mohammad Rezai, Thomas Häberle, Sebastian Zaiser, Matthias Pfender, Matthias Widmann, Matthias Niethammer, Durga Dasari, Seyed Ali Momenzadeh, Felipe Favaro de Oliveira and Nathan Chejanovsky for their wonderful company and all the fun activities.

Lastly, this can not end without me acknowledging the sincerest, most loving, never ending and absolute support of my parents and my siblings. This would not have been possible without all of you always being there for me.

Contents

List of accompanying papers

The following papers, referred to in the text by their Roman numerals, are included in this thesis.

PAPER I: **Quantum Random Access Codes Using Single d-Level Systems**, A. Tavakoli, A. Hameedi, B. Marques and M. Bourennane, *Phys. Rev. Lett.*, **114**, 170502 (2015). DOI: 10.1103/PhysRevLett.114.170502

PAPER II: **Increased certification of semi-device independent random numbers using many inputs and more post-processing**, P. Mironowicz, A. Tavakoli, A. Hameedi, B. Marques, M. Pawłowski and M. Bourennane, *New J. Phys.*, **18**, 065004 (2016). DOI: 10.1088/1367-2630/18/6/065004

PAPER III: **Experimental test of nonclassicality with arbitrary low detection efficiency**, A. Hameedi, B. Marques, P. Mironowicz, D. Saha, M. Pawłowski and M. Bourennane, submitted (2016).

PAPER IV: **Distributed Random Access code with Quantum resources**, A. Hameedi, D. Saha, P. Mironowicz, M. Pawłowski and M. Bourennane, submitted (2017).

PAPER V: **Experimental quantum solution to the Dining Cryptographers Problem**, A. Hameedi, B. Marques, M. Sadiq, M. Wieśniak and M. Bourennane, submitted (2017).

Related papers not included

PAPER I: **Quantum communication complexity using the quantum Zeno effect**, A. Tavakoli, H. Anwer, A. Hameedi and M. Bourennane, *Phys. Rev. A*, **92**, 012303 (2015). DOI: 10.1103/PhysRevA.92.012303

Author's contribution

My contribution, to the five articles included in this thesis, is detailed below.

Paper I: I actively participated in the discussions for designing the experimental setup. I built the experimental setup, performed all the experimental measurements and did the data analysis for the experiment. I was also involved in the writing of the manuscript.

Paper II: The experimental setup and results of experiment were used from paper I. I was involved in the writing of the experimental part of the manuscript.

Paper III: I actively participated in the discussions for designing the experimental setup. I built the experimental setup, performed all the experimental measurements and did the data analysis for the experiment. The paper was written by all co-authors.

Paper IV: I performed all the simulations for the expected experimental outcomes and designed the experimental setup for the experiment after fruitful discussions with my supervisor. Moreover, I built the complete experimental setup, performed all the experimental measurements and did the data analysis for the experiment. The experimental part of the manuscript was written by me.

Paper V: I actively participated in the discussions for designing the experimental setup. I built the experimental setup, performed all the experimental measurements and did the data analysis for the complete experiment. The paper was written by all co-authors where I coordinated the whole process.

Sammanfattning

Kvantinformation är tveklöst ett mycket intressant och snabbt växande område. Dess fråga är hur man behandlar information som har kodats i kvantfysikaliska system. Kvantmekaniska resurser som superposition och snärjelse har visats kunna förbättra informationsbehandlingsförmågan inom ett antal kommunikations- , informations- , och beräkningsuppgifter.

Fysikaliska system med dimensioner d, baserade på enstaka fotoner används ofta att utreda de icke-klassiska resursernas företräden över dess klassiska motsvarigheter i många kommunikationsuppgifter. Vi har undersökt det samma för en kommunikationsuppgift som kallas random access codes (RAC) och visas experimentellt att RACs som använder kvantsystem (QRACs) med hög dimension ($d = 4$) överträffar båda de klassiska varianterna och QRAC med mindre dimensioner d.v.s kvantbit (qubit). Vi har också prövat QRACs med sikte på särskilda tillämpningar som certifiering av slumptalsgenerator och icke-klassiskalitet hos kommunicerade system. Vi presenterar en övergripande metod för ökad certifiering av slumptalsgenerator för den förra och en framgångsrik experimentell realisering med godtycklig låga detektionseffektivitet för den senare. Detta följs av en QRAC implementering i form av ett enkelriktad kommunikationsnätverk med förberedelse, transformation och mätningsredskap. Vi har funnit flera olika kommunikationsuppgifter för dessa fördelade QRAC där dessa fungerar optimalt.

Vi gör också ett kvantprotokoll för att lösa problemet med kryptografernas middag, och hur de kan skydda sin identitet vid en omröstning. Vi presenterar en effektiv lösning baserad på enkelfoton kommunikation som visas experimentellt för en tre-parter uppställning.

Sist men inte minst undersöks Kväve-Vakans-Centrum (NV), ett färgcentrum i diamant. Syftet är att observera generering av enstaka fotoner vilket sedan visas experimentellt i olika diamant prover. Två metoder att förbättra foton insamling från NV centrum prövas också och med hjälp av den observerade förbättringen i foton-insamlingen kan NV center förmodligen användas i liknande kvantkommunikationsexperiment med enstaka fotoner.

Abbreviations

QI	Quantum Information
QIP	Quantum Information Processing
Qudit	Quantum d-level
Qubit	Quantum bit
Qutrit	Three-level quantum system
Ququart	Four-level quantum system
QKD	Quantum key distribution
SPS	Single Photon Source
HBT	Hanbury Brown and Twiss
SPDC	Spontaneous Parametric Down Conversion
BBO	Beta Barium Borate
BIBO	Bismuth triborate
HWPs	Half-wave plates
QWPs	Quarter-wave plates
BS	Beam splitters
PBS	Polarization beam splitters
SMF	Single mode fiber
MMF	Multimode fiber
RAC	Random Access Code
QRAC	Quantum Random Access Code
EARAC	Entanglement assisted random Access Code
MUB	Mutually unbiased basis
APD	Avalanche photodiode

GHZ	Greenberger-Horne-Zeilinger
DW	Dimensional Witness
DI	Device Independent
SDI	Semi-device Independent
RNG	Random Number Generation
DDH	Decision Diffie-Hellman
NV	Nitrogen-Vacancy
HPHT	High-pressure high-temperature
CVD	Chemical vapor deposition
ppm	parts per million
ppb	parts per billion
SiV	Silicon-Vacancy
NE8	Nickle related Vacancy
QDs	Quantum dots
ZPL	Zero phonon line
FWHM	Full width half maximum
QEM	Quantum enhanced metrology
TIR	Total internal reflection
SIL	Solid Immersion Lens
FIB	Focused ion beam
EBL	Electron beam lithography
SEM	Scanning electron microscopy
HSQ	Hydrogen Silsesquioxane
RIE	Reactive ion etching
ICP	Inductively coupled plasma
Cr	Chromium
ODMR	Optically detected magnetic resonance
NMR	Nuclear magnetic resonance
CM	Confocal microscope

CW	Continuous wave
NA	Numerical Aperture
PL	Photoluminescence
SPCM	Single photon counting module

List of Figures

List of Tables

Thesis outline

This thesis is an account of all the experimental work conducted during my PhD studies and is based on the work produced in the articles **I-V**. Articles I-III presented here have also been a part of my licentiate and major parts of chapters 1 to 3 are adapted from my licentiate thesis.

The aim here is to emphasize on the experimental studies conducted during my PhD but necessary theoretical introduction is provided where required. The thesis is formulated such that for every topic covered, first a theoretical introduction is provided which is followed by the experimental details. As the emphasis is placed on the conducted experiments, other relevant details can be found in the articles that are a part of this thesis.

Chapter 1 contains details on preliminary concepts in quantum information that are relevant to the contents of this thesis.

Chapter 2 lays the ground work for random access codes (RACs), classical and quantum (QRACs), followed by an experimental demonstration of a high-level ($d = 4$) QRAC. This work is based on article I.

Chapter 3 focuses on two applications of QRACs: Generation and certification of randomness and test of non-classicality of physical systems with arbitrarily low detection efficiency. This chapter is based on articles II and III.

Chapter 4 focuses on distributed tasks using single quantum systems. First an experimental demonstration of a distributed QRAC is provided and is relevant to article IV. This is followed by an experimental realization of a quantum solution for the dining cryptographer and anonymous veto problems and is based on article V.

Chapters 5 and 6 cover the theoretical introduction and experimental investigation of single photon emission from the Nitrogen-Vacancy (NV) center in diamond. The defect center is studied exclusively from the view point of a single photon emitting source and two different alternatives to enhance the emitted photon collection efficiency are experimentally investigated. For the photon collection enhancement, facilities in the 3rd Institute of Physics at the University of Stuttgart and Max Planck

Institute for Solid State Research (Stuttgart) were used for ion implantation and annealing along with the fabrication of solid immersion lenses (SILs) and nanopillars in diamond membranes. The ion implantation and annealing processes were carried out by Andrej Denisenko and Felipe Favaro De Oliveira. For nanofabrication, due to licence conditions, the samples were handled by Sen Yang (SIL), Anurag Kanase and Amit Finkler (nanopillars) but I was involved in every step and supervised the whole process.

1. Quantum Information

1.1 Introduction

The theory of quantum mechanics was introduced more than a century ago and its intriguing yet remarkable properties of superpositions and entanglement, referred to as the spooky action at large distance by Einstein, have been extensively investigated as quantum resources for information processing. Superposition implies the simultaneous existence of a system in two or more states and in the quantum mechanical context, this holds even for systems consisting of particles. On the other hand, entanglement refers to the case when two or more parts of a system are correlated in a way that is–in a sense that can be made precise–stronger than anything that can be explained by their interactions in the past (while classical correlations are always explained by past interactions). The understanding, realization and applicability of these properties later led to a newer theory called quantum information, which promises unique applications such as quantum computation, quantum metrology and secure quantum communication, among others.

The word information comes from the latin verb *informare*, meaning literally *to inform* or *to form an idea of something*. Information, either in the form of knowledge or data, plays a critical role in our every day lives where we depend greatly on the exchange of information between people or different parties. For this purpose, information of any kind needs to be encoded in different levels of a physical system. Other than the old school methods of exchange of information as word of mouth or through a piece of paper, information is usually communicated between different parties in the form of data commonly known as binary digits or bits. The term bits was first introduced by John W. Tukey, an American statistician, while working at Bell Labs, as an abbreviation for the word *binary digit*. Claude E. Shannon, renowned American mathematician and engineer, was the first one to publicly use the term bits in his well-known article, *A Mathematical Theory of Communication*, in 1948 [1]. This remarkable theory treated communication as a rigorously stated mathematical problem that laid the ground work and presented the foun-

dations of communication and information theory. Hence it comes as no surprise that Shannon is widely regarded as the father of information theory. His work has contributed invaluably to the achieved progress as it forms the basis of all communication and modern day computers, which has totally revolutionized our way of living.

A binary digit, from now on referred to as a bit, is encoded in a two level system where the two different states of the system are represented by binary numbers 0 and 1 and a bit can only have two possible values. Classical information is in these states of the bit. A typical example of this is the electrical potential difference in electronic circuits where low and high voltages are used as a representation of the two binary states. The encoding of classical information into bits is not just restricted to the above case and there can be a multitude of different schemes used for a plethora of different applications as various nucleotides in a DNA sequence or the use of pulsed laser light in an optical fiber or free space networks [2].

Quantum information, on the other hand, is a generalization of classical information in the quantum regime where the physical system used for encoding information obeys the laws of quantum mechanics. A quantum bit (qubit), the quantum analogue of the classical bit, is the most commonly known quantum system and along with entanglement is considered an essential resource in many quantum information processing applications (QIP). The use of quantum resources for encoding information has properties and advantages that extend well beyond the capabilities of the classical systems. From an application point of view, the use of such quantum resources can make it possible to realize the implementation of quantum computers, factorization of very large numbers, secure communication based on quantum key distribution (QKD) between distant parties [3–5] and quantum dense coding [6; 7] otherwise not possible in the classical scenario. In the succeeding section we will look at some of the properties of a qubit which is the most fundamental element in quantum information science.

1.1.1 Quantum states and the density operator

The state of any system is the property that makes it distinguishable from other systems. In classical terms, objects or systems can be differentiated from each other based upon their characteristics. Similarly, the concept of state exists in quantum mechanics as well where states of a quantum system are represented by normalized vectors $|\psi\rangle$ on the Hilbert space or in other words, are arbitrary normalized linear combi-

nations of a set of basis vectors defined in the Hilbert space. Quantum mechanics, despite its probabilistic nature, can still provide complete information about the state of a system in certain situations (after a measurement). Such states are generally known as *pure* states which are completely described by their state vectors. Eqs. 1.1 and 1.3 are examples of a pure state. However, *pure* states are not the only type of quantum states and in fact, in reality, we mostly deal with mixtures or ensembles of two or more pure states otherwise known as *mixed* states. The only information we have is the probability with which a system can be in a number of pure states. *Mixed* states cannot be described completely by state vectors in the Hilbert space as is the case for *pure* states and are generally represented by density operators.

A density operator ρ is a positive semi-definite Hermitian matrix with a unit trace that is used to mathematically represent a quantum state. In the case of a pure state with state vector ψ, the density operator is given as

$$\rho = |\psi\rangle\langle\psi| \tag{1.1}$$

For pure states, the density operator is also known as a *Projection* operator as it projects a given state into the 1D subspace of the vector $|\psi\rangle$. For mixed states, the density operator is a normalized sum of pure states and is given as

$$\rho = \sum_i p_i \rho_i = \sum_i p_i |\psi_i\rangle\langle\psi_i| \text{ where } \sum_i p_i = 1,\ p_i \geq 0\ \forall\ i. \tag{1.2}$$

Some of the important properties of density operators are that they are normalized, which implies that $Tr(\rho) = 1$. ρ is positive semi-definite and have real positive eigenvalues. In addition, for pure states $\rho^2 = \rho$ and $Tr\left(\rho^2\right) = 1$ but for mixed states $Tr\left(\rho^2\right) < 1$. Hence, the density operator is also an efficient tool to distinguish between pure and mixed states.

1.1.2 The quantum bit

Now that we have a basic understanding of quantum states and know how to mathematically represent them, we will consider a qubit, which is essentially the simplest system in quantum information. For a qubit, there are two vectors constituting the basis of the Hilbert space. For simplicity, consider that the two levels are represented by orthogonal state vectors $|0\rangle$ and $|1\rangle$ and are the classical states of the system (as

they can be well explained by both quantum and classical theories). However, unlike the classical bit that can either be a 0 or 1, a qubit can exist in a superposition of the two states $|0\rangle$ and $|1\rangle$ as the superposition principle implies that any linear combination of two states is also a state of the system where the superposition is in itself also a pure state. The superpositions result every time when the coefficients α and β are not equal to one in eq. 1.3. A qubit can then be viewed as the amount of information needed to store all possible states of a two dimensional quantum system. The standard and vector representation of the qubit in the superposition state is represented as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \text{ or } |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{1.3}$$

where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ are the basis states of the qubit.

The coefficients $\alpha, \beta \in \mathbb{C}$ are arbitrary complex numbers that satisfy the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. After normalization, we are left with phase freedom, i.e., any global phase factor can be disregarded ($|\psi\rangle$ and $e^{i\phi}|\psi\rangle$ are the same states for any given ϕ) and hence it is commonly represented as

$$|\psi(\theta,\phi)\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} \tag{1.4}$$

where $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$ and these ranges are precisely the ranges for spherical coordinates thereby enabling the graphical representation of the state of a qubit by points on the surface of a unit sphere, as shown below for $|\psi\rangle$ in Fig. 1.1. This is more commonly known as the Bloch sphere. On the Bloch sphere, any two orthogonal states are always directly opposite to each other such that

$$\langle\psi|\psi_\perp\rangle = 0 \tag{1.5}$$

This is due to the Bloch vector ($\mathbf{r}$) described below and the resulting state $|\psi\rangle_\perp$ orthogonal to $|\psi\rangle$ becomes

$$|\psi(\theta,\phi)\rangle_\perp = |\psi(\pi-\theta,\pi+\phi)\rangle = \sin\left(\frac{\theta}{2}\right)|0\rangle - e^{-i\phi}\cos\left(\frac{\theta}{2}\right)|1\rangle \tag{1.6}$$

The Bloch sphere is a geometric visualization of the complete set of two dimensional quantum states. Such a straightforward geometric representation exists only for two dimensional systems and is difficult to grasp for systems of higher dimensions.

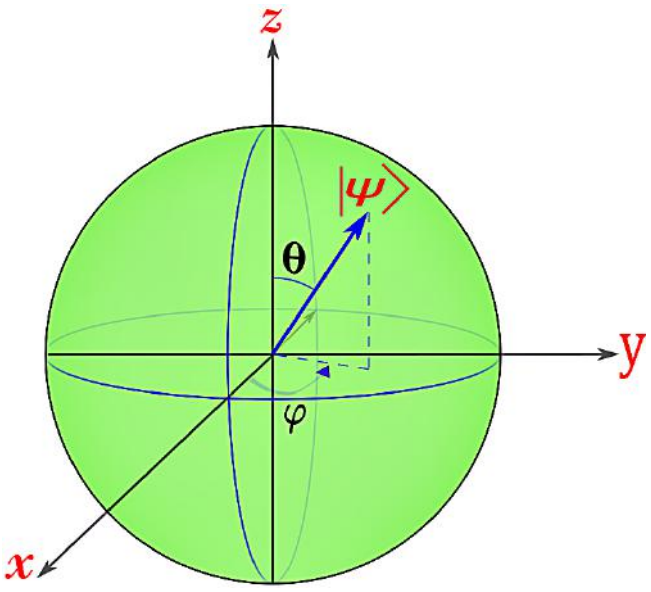

Figure 1.1: Geometrical representation of the Hilbert space of a single qubit. Points on the surface and interior of the Bloch sphere represent density matrices of pure and mixed states.

The state of a quantum system can be easily represented by a density matrix and the density matrix used to describe a two level system can be parametrized as

$$\rho = \begin{pmatrix} \frac{1}{2} + z & x - iy \\ x + iy & \frac{1}{2} - z \end{pmatrix} \tag{1.7}$$

where x, y and z are real numbers.

To better understand the use of Bloch sphere for the geometric representation of two dimensional quantum states, one needs to consider the semi-definite property of the density matrix used to represent the states of the 2D quantum system. If the product of the eigenvalues is greater than or equal to zero, we end up with the inequality, $x^2 + y^2 + z^2 \leq \frac{1}{4}$, that defines the interior of a sphere of unit diameter. This sphere represents all the states of a qubit where the surface points correspond to pure states whereas the interior points in the sphere correspond to the mixed states with the center of the sphere being the maximally mixed state.

Any density operator for a single qubit can be decomposed into a linear combination of three Pauli matrices (σ_x, σ_y and σ_z) and the identity matrix. The Pauli matrices and the identity matrix are the basis

elements of the vector space of 2×2 Hermitian matrices and any 2×2 matrix can then be written as a linear combination of these matrices.

$$\sigma = \begin{pmatrix} \sigma_x \\ \sigma_y \\ \sigma_z \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.8}$$

The σ_x, σ_y and σ_z observables have eigenvalues ± 1 and their eigenstates form a complete basis and can be used as basis states. In the case of σ_z, the eigenstates are $|0\rangle$ and $|1\rangle$ and these two states form a basis generally known as the computational basis. For σ_x, the eigenstates are $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ and these two states form a basis generally known as the Fourier basis. Lastly, for σ_y, the corresponding eigenstates are $\frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$.

The density matrix can then be rewritten as

$$\rho = \frac{1}{2}(1 + \mathbf{r}.\vec{\sigma}) \tag{1.9}$$

Here $\mathbf{r}$ is the Bloch vector and defines any state on the Bloch sphere using θ and ϕ, and in order to represent the pure states on the Bloch sphere, the inequality $|\mathbf{r}| \leq 1$ must hold. Also note that the $\mathbf{r}$-coordinates represent the expectation values of the Pauli operator [8].

$$\mathbf{r} = r \begin{pmatrix} \sin\theta\cos\phi \\ \sin\theta\sin\phi \\ \cos\theta \end{pmatrix} \tag{1.10}$$

As an example, photon's polarization can be used to implement a qubit. This is covered in detail in section 1.2.4. Although quantum states of dimension 2 are the most commonly known quantum states, the work done in the scope of this thesis also involves quantum states of dimensions $d > 2$. The state space postulate allows for general $d-level$ quantum systems also known as *qudit*, which are state vectors on the Hilbert space $\mathbb{C}^d$. Considering the computational basis, a qudit can be written as [9]

$$|\psi\rangle = \sum_{k=0}^{d-1} c_k |k\rangle = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{d-1} \end{pmatrix} \tag{1.11}$$

where $c_0, \ldots, c_{d-1} \in \mathbb{C}$ are subjected to the normalization constraint $|c_0|^2 + |c_1|^2 + \ldots + |c_{d-1}|^2 = 1$.

1.1.3 Measurements on a quantum state

In quantum mechanics, a physical system is represented by its quantum state and measurements on a physical system are associated with observables, where an observable presents some measurable property of the system. In other words, a measurement on the physical system provides us with the knowledge of some physical observable of the system, e.g., position and momentum of a particle, spin or polarization of a photon etc. In the context of a measurement, the term observable is also applied to the associated Hermitian operator. A Hermitian operator has real eigenvalues with orthogonal eigenvectors and their eigenstates form a complete set of basis states. The observables (σ_x, σ_y and σ_z) described above are a good example in this regard and their eigenstates form a complete set of basis states with eigenvalues ± 1. While performing a measurement, the operation of an observable projects the state of a quantum system into one of the associated eigenstates of the operator along with a resulting eigenvalue (± 1 for a qubit).

If the aim of a measurement is to analyse the polarization states of photons in a given basis, this can be implemented through a combination of wave plates and polarising beam splitters (PBS). These optical components and how these measurements for different basis states are performed is explained in the experiments included in this thesis. What is important to state here is that suitable orientations of half-wave plates (HWPs) and quarter-wave plates (QWPs) can be used to project a given state onto the eigenvectors of $\sigma_x\,\sigma_y$ and σ_z observables, making it possible to perform measurements in different measurement bases.

1.2 Experimental quantum state engineering

In this section, we will briefly look at some of the parameters that are important from an experimental point of view. The work presented in this thesis involves physical systems based on single optical photons, as a resource in quantum information processing. It is perhaps important to begin with a brief introduction and formulation regarding single photon sources (SPS). We will start by looking at the basic criteria and demands placed on single photon sources, as single photons are used extensively in this thesis, for the realization of d-dimensional physical systems otherwise known as qudits. This requires the understanding of how physical systems of different dimensions d (d=$\{2, 3, 4\}$) can be implemented using them.

1.2.1 Single photon sources

The concept of photon has been one of the most discussed and hotly debated issues in the history of physical science. The desire to better understand the concept and the debate, has been raging on for decades but even now people are probably as unsure and divided as they ever were. Regardless of the conceptual disagreements, the concept of photon as a quantum of energy hv is essential to the quantum revolution. This definition stems from the quantization of the electromagnetic field, which necessitates the presence of an elementary excitation of a single mode of discrete energy, hence a photon [10]. As this is an experimental thesis that deals in length with the creation and collection of single photons in addition to the use of these photons as flying particles to transmit quantum information, the words of Roy Glauber are probably sufficient for our purpose: "A photon is what a photodetector detects" [11].

It was briefly introduced before that the use of quantum resources can potentially enhance information processing capabilities well beyond classical means. Optical photons have been shown to be ingeniously capable for the realization of such quantum resources due to their information encoding, transfer and manipulation characteristics. In reality, the use of photons or single photon sources more specifically extends beyond the realm of quantum information technologies and they have proven usefulness in a range of diverse modern day applications such as remote sensing and medical sciences [12; 13]. From a quantum information perspective, deterministic on demand generation of indistinguishable single photons is an ideal resource for applications as quantum sensing, quantum metrology and quantum information processing.

An ideal single photon source deterministically emits indistinguishable single photons on demand without the possibility of multiphoton emission, is highly photostable with exactly defined spatial and spectral characteristics. Such a source should have a sub-nanosecond lifetime and must be highly polarized in both emission and absorption [14]. An ideal single photon source (SPS) is extremely hard to realize in practise due to the above stringent requirements, but suitable candidates that meet some key criteria have been realized [12; 13; 15]. The first experimental realization of a single photon emission was demonstrated by Kimble et al. in 1977 using sodium atoms [16] and since then a number of demonstrations employing different approaches have been presented. Examples of systems that have demonstrated similar characteristics include single molecules [17], single atoms, trapped ions [18], artificial atom like structures as quantum dots (QDs) [19] and defect centers in solid state

materials as diamond [20] and silicon carbide [21]. The single photon nature of these sources is confirmed by using a Hanbury Brown and Twiss (HBT) configuration to measure the second order correlation function value that can confirm the presence of a single photon emitter.

Alternate approaches for single photon sources include the heralded single photon sources, which although different in mechanism to the above systems, are commonly used as a robust single photon source in quantum communication protocols. One such source of single photons is used in the experiments performed in this thesis and an overview of which is provided in the next section.

1.2.2 Heralded single photon source

A heralded single photon source from entangled pair of photons generated using spontaneous parametric down conversion (SPDC) in non-linear beta barium borate (BBO) crystals has been used in the experiments covered in this thesis. Such non-linear crystals have proven to be quite efficient for generating entangled photon pairs [22]. In SPDC, a high energy pump photon incident on a non-linear crystal may result in the emission of two photons of lower energies, commonly known as the *signal* and *idler* photons. This conversion of pump laser photon into down converted photons occurs spontaneously, as the name indicates, and strong correlations between the signal and idler photons (energy, momentum, polarization) exist due to energy and momentum conservation. Such sources based on SPDC can produce entanglement directly in the crystal and entangled photons of the same frequency can also be produced.

The laser source used is a Coherent Ti:sapphire femtosecond laser pulsed at 80 MHz with a pulse width of 140 fs and an average power of 3.3 W at 780 nm, translating into an average power of 0.3 MW in each pulse. The laser is then frequency doubled to 390 nm using a bismuth triborate (BIBO) crystal with an average power of around 1.4 W for the frequency doubled UV beam. This extraordinarily [1] polarized UV beam (390 nm) is then used as the pump beam for the BBO crystal to produce degenerate down converted infrared photons (780 nm).

There are two main types of the SPDC processes: type-I where both

[1] In birefringent materials, the refractive index depends upon the polarization and the direction of propagation of the light beam. An incident beam is polarization split into two beams, i.e., extraordinary and ordinary polarized. For normal incidence, the extraordinary polarized light does not obey Snell's law and deviates from the straight path inside the material [23].

the down converted photons have ordinary polarization [1] and have the same polarizations or type-II where one photon is ordinary polarized and the other is extraordinary polarized resulting in orthogonal polarizations of the down converted photons. We have used type-II SPDC where polarization entanglement between photons is created within the crystal due to a blending of the orthogonal polarizations and the energies of the emitted photons are degenerate. Fig. [1.2] shows the non-collinear configuration of the type-II SPDC process where the two emitted cones of orthogonally polarized photons intersect at two points.

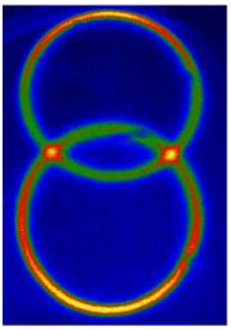

Figure 1.2: Non-collinear type-II SPDC configuration leads to entangled photon pairs at the intersection of the two cones. Reproduced from [23].

It has already been mentioned that we consider the degenerate case where the energies of emitted photons are the same. In addition, for a small thickness of the non-linear crystal the photons are also indistinguishable in timing of their arrival as they were created together. At these intersection points, it is only the polarization of the two photons that is not defined as they could be coming from any of the two intersecting cones, resulting in, e.g., a polarization entangled Bell state $|\psi^+\rangle$.

$$|\psi^+\rangle = \frac{1}{\sqrt{2}} \left(|HV\rangle + |VH\rangle\right) \tag{1.12}$$

A polarization measurement at one of the crossings can only reveal the polarization state of the photon but as these photons are entangled with orthogonal polarization such a measurement also directly reveals the polarization state of the second photon at the other crossing. Such a source of entangled pairs of photons can be employed as a heralded single photon source where the idler photon can be used as a trigger and

[1] For normal incidence, the ordinary polarized light is the one that obeys Snell's law and continues its motion in a straight path inside the material.

the detection of this idler photon using a single photon detector heralds the presence of the other photon which can now be used in experiments requiring single photons. These signal photons are then made to pass through a narrow band interference filter of bandwidth $\approx 3\ nm$. Such a spectral filtering is necessary to increase the coherence length of the photons, which depends upon the spectral range of the filter used. Afterwards, the photons are coupled to single mode fibres (SMF) to obtain a well-defined spatial mode. This is possible as SMF are optical fibres with a very small core ($\approx 5\ \mu m$ diameter) surrounded by a larger cladding of lower refractive index and are commonly used for distributing photons between two points. Light guiding is made possible by total internal reflection (TIR) and for a specific incident wavelength and polarization they can only guide a single spatial propagation mode. Hence a SMF acts as a mode filter providing photons of exactly defined spatial mode at the fibre output.

1.2.3 Implementation of a qudit

We begin by considering the implementation of a qubit before moving on to implementing higher dimensional quantum systems. A quantum bit can be implemented using any quantum system of dimension two. We will use single photons generated through spontaneous parametric down conversion (SPDC) in non-linear crystals for experimentally realizing qubits. Using photons as a candidate for implementing qubits is attractive due to their weak interaction with the environment which reduces the decoherence effect. A photon's spin or polarization can hence be used as a two dimensional quantum system for implementing a qubit.

1.2.4 Different encoding schemes

Using a photon's polarization is probably the most commonly used and yet the simplest method for representing a two level system. The simplest way to demonstrate a two level is to use the two most commonly known orthogonal polarization states, horizontal $|H\rangle$ and vertical $|V\rangle$. The state vectors $|H\rangle$ and $|V\rangle$ are the eigenvectors of the σ_z operator and a qubit basis is defined using $|0\rangle \equiv |H\rangle$ and $|1\rangle \equiv |V\rangle$. In a similar manner, eigenstates of the observable σ_x, which are $\pm 45^\circ$ polarized photons defined by superpositions $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$, and observable σ_y, which are circularly polarized photons defined by superpositions $|L/R\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm i|V\rangle)$, are also used for the implementation of qubits. One can clearly see that the qubit basis defined by state vectors $|H\rangle$ and

$|V\rangle$ is the default basis and all other states can be represented using this basis.

Although commonly used, polarization implementation is not the only way to implement a qubit. Another known method employs the use of two different, well-defined and distinguishable spatial paths a and b. Using this spatial approach of two different paths, a qubit can be defined by choosing $|1\rangle \equiv |a\rangle$ and $|2\rangle \equiv |b\rangle$ where the former indicates the presence of a photon in path a and the latter indicates the presence of a photon in path b. Similar to the polarization approach of implementing qubits, superpositions can also be introduced between the two physical paths.

Previously, we discussed how two level systems defined by photon's polarization or different spatial paths can be used for implementing qubits. As work in this thesis additionally involves the use of quantum systems of higher dimensions as well, it is important to realise quantum systems that can be used for the task. For a ququart ($d = 4$) state, the above two methods can be combined and the two spatial and polarization degrees of freedoms can be used for implementing a physical system of $d = 4$ whereas for a physical system of dimension $d = 3$ (namely qutrit), single photons can be used in a three spatial path encoding scheme. The qutrit encoding scheme is implemented by using the two spatial modes of three polarization beam splitters (PBS). The detailed encoding schemes for preparation of these states will be covered later on when dealing with individual experiments.

2. Random Access Codes (RACs)

Random Access Codes, commonly known as *RACs*, belong to a class of communication tasks where a RAC, generally, represents encoding a number of bits into a single bit and any one of the initial bits can be recovered with a certain probability of success. RACs could also be viewed in a context, where a given user (Alice) possesses some information (a bit string) and another user (Bob) is interested in any arbitrary subset of information (any bit) held by Alice despite limited one way communication between them. RACs are traditionally characterized as $n \mapsto m$, which implies that n bits are encoded into m bits and any one of these n bits can be recovered with an average success probability p.

In terms of implementation through quantum resources, RACs can be classified into two variants: quantum communication random access codes (QRACs) and entanglement assisted random access codes (EARACs). In the QRACs, quantum systems are prepared and communicated from one party to the other through a quantum channels whereas in EARACs, quantum entanglement is shared between the participants through a classical channel. These two types of quantum RACs have proven to be equally efficient and advantageous in many scenarios. However, there do exist specific scenarios where one type has been shown to be better suited as compared to the other. In the context of this thesis, all the presented work has been done using the QRACs variety where the implementation is done in a prepare and measure scenario.

In the one way communication scheme, RACs could be both classical or quantum depending upon the choice of communication used. For a given input string of classical bits, consider a scenario where only a single bit (qubit) is used for encoding the input string, i.e., $m = 1$ (this is the case employed throughout this thesis). In the classical case, Alice encodes her input bit string into a single bit, which is consequently sent to Bob who then tries to recover any of the input bits with either an average success probability p or a worst case probability p depending upon the situation of interest. In any case, the success probability should be greater than $1/n$, which is the most trivial scenario where Bob just tries to guess the sent bit. The quantum counterpart of this RAC employs

a single qubit into which all the input bits are encoded. Bob receives this qubit, performs a measurement on it and tries to recover the bit of interest. The choice of Bob's measurement setting depends upon the bit that he is trying to recover.

The main advantage of *QRAC* over its classical counterpart is that once Bob has performed a measurement on the qubit, to recover the bit of interest, no more information can be extracted from it. This does not hold for the classical RAC though where the recovery of a single bit implies that Bob can essentially recover all of the bits in the input bit string.

The idea of QRAC was initially presented, almost four decades ago, in early 1980s [24] but it has only been recently (in the last fifteen years) that they have been studied extensively. QRACs have found important applications in a range of tasks including machine learning [25–27], in the interest of quantum communication complexity [28] and particularly network coding [29], locally decodable codes [30] along with meaningful applications in quantum information processing (QIP). The QIP applications cover areas such as semi-device independent (SDI) protocols based generation and certification of truly random numbers [31; 32], tests of non-classicality, tests of classical and quantum dimensions of a system as well as semi-device independent quantum cryptography [33]. Results from QRACs have been applied to quantum state learning, super quantum resources [34] and links between QRACs and foundations of quantum mechanics [35] have also been established. Furthermore, QRACs realized by means of entanglement [36], as described above, have found usefulness in real life games [37].

2.1 Commonly known RACs

The first two published articles (I and II) produced during this thesis deal with QRACs of dimension $d = 4$. We will first begin with 2-dimensional QRACs for ease of understanding, before building onto the higher level RACs ($d = 4$) and their optimal strategies required to acquire the highest success probabilities. For this purpose, we will consider both classical and quantum scenarios.

2.1.1 The $2 \mapsto 1$ RAC

The simplest known RAC is the $2 \mapsto 1$ variant where $n = 2$ bits are encoded into a single bit. Alice has an input string of 2 bits, $x = x_1x_2$, which she encodes into a single bit. She is only allowed to communicate

this single bit to Bob, who could be interested in any one of the bits in Alice's string. Firstly, we will analyse the optimal classical strategy that Alice could use to obtain the most efficient scenario of a classical RAC, followed by the presentation of its quantum analogue. Later on a natural performance comparison will be made between the classical and quantum cases.

For the $2 \mapsto 1$ code, the best classical strategy that Alice could employ is to send the same bit all the time. Let x_1 be that bit in this case. The highest classical success probability that Bob can obtain in this case is

$$p^C_{2\mapsto 1} = 3/4. \tag{2.1}$$

This is straight forward as every time Bob is interested in x_1, he will recover it and for every other time when he is interested in x_2, he will have to guess its value. This results in a total classical success probability of $p^C = 3/4$.

On the other hand, in the $2 \mapsto 1$ QRAC, there are 2^n possible values (four in this case) for Alice's input string and she uses a two level quantum system to represent any of these inputs.

$$|\psi_{x_1x_2}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \frac{(-1)^{x_1} + i(-1)^{x_2}}{\sqrt{2}}|1\rangle\right) \tag{2.2}$$

Whereas Bob uses two mutually orthogonal pairs of antipodal Bloch vectors, as measurement bases (M_1 and M_2), to recover his bit of interest. If M_1 and M_2 are the measurements along x and y axes, respectively, with corresponding Bloch vectors $\upsilon_1 = (\pm 1, 0, 0)$ and $\upsilon_2 = (0, \pm 1, 0)$, then the measurement bases [38] are

$$\begin{aligned} M_1 &= \{\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}\} \\ M_2 &= \{\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}\} \end{aligned} \tag{2.3}$$

For a given input string x and encoding states $|\psi_{x_1x_2}\rangle$ in eq. 2.2, Bloch state vectors of the encoding states are given as

$$r\,(x) = \frac{1}{\sqrt{2}}\begin{pmatrix} (-1)^{x_1} \\ (-1)^{x_2} \\ 0 \end{pmatrix} \tag{2.4}$$

From this geometric consideration, the used encoding states are the vertices of a square $\frac{1}{\sqrt{2}}(\pm 1, \pm 1, 0)$ drawn in the unit circle on the xy plane as

shown in Fig. 2.1. These encoding states are symmetrically distributed at the equator, on the surface of the Bloch sphere. They are the best option considering that all the encoding points should be as far as possible from the two planes that are orthogonal to the x and y axes and cut the sphere into four parts [38]. This is vital to maximize the worst case success probability.

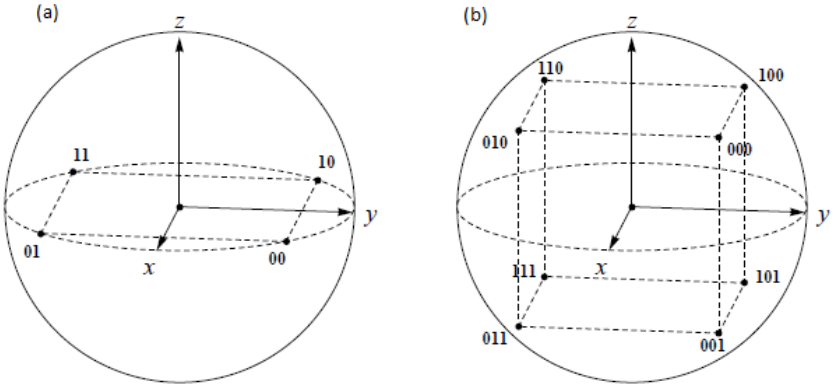

Figure 2.1: Bloch sphere representation of $2 \mapsto 1$ (a) and $3 \mapsto 1$ (b) QRACs. Reproduced from [38].

In order to recover an input bit of interest, Bob performs a measurement using the corresponding measurement basis. He measures in M_1, if he wants to recover x_1 or in M_2 basis, if he wants to recover x_2. Bob's success probability always remains the same and is independent of the measurement he performs or the encoding state he receives.

$$p^{Q}_{2\mapsto 1} = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\right) \approx 0.854 \tag{2.5}$$

2.1.2 The $3 \mapsto 1$ RAC

As in the previous case of a $2 \mapsto 1$ RAC, the success probability for a classical random access code $3 \mapsto 1$ is again

$$p^{C}_{3\mapsto 1} = 3/4 \tag{2.6}$$

albeit with a more elegant strategy (majority encoding scheme, will be explained later) than the prior case. The $3 \mapsto 1$ QRAC is a generalization of the $2 \mapsto 1$ code introduced in the previous section and was first introduced by Chuang [25]. In this class of RACs, three mutually

orthogonal pairs of antipodal Bloch vectors are used instead of two. Alice has an input string of three bits, $x = x_1, x_2, x_3$, and the additional measurement basis available to Bob in this case is

$$M_3 = \{\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\} \tag{2.7}$$

where the third pair of antipodal Bloch vector is $\upsilon_3 = (0, 0, \pm 1)$.

There are eight possible values to Alice's given input string which are encoded into 8, two level, quantum states $|\psi_{x_1 x_2 x_3}\rangle$. These encoding states arise from the three planes that are orthogonal to the x and y axes and cut the Bloch sphere into eight parts. The Bloch vectors of the encoding states for the given string are

$$r\,(x) = \frac{1}{\sqrt{3}} \begin{pmatrix} (-1)^{x_1} \\ (-1)^{x_2} \\ (-1)^{x_3} \end{pmatrix} \tag{2.8}$$

Hence, the optimal encoding states $|\psi_{x_1 x_2 x_3}\rangle$ are symmetrically distributed on the surface of the Bloch sphere and conform with the vertices of a cube, $\frac{1}{\sqrt{3}}(\pm 1, \pm 1, \pm 1)$, as drawn in the unit circle on the xy plane, Fig. 2.1. The optimal encoding states are

$$|\psi_{x_1 x_2 x_3}\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.9}$$

Where the coefficients α and β are given as [25]

$$\begin{aligned} \alpha &= \sqrt{\frac{1}{2} + \frac{(-1)^{x_3}}{2\sqrt{3}}} \\ \beta &= \frac{(-1)^{x_1} + i(-1)^{x_2}}{\sqrt{6 + 2\sqrt{3}(-1)^{x_3}}} \end{aligned} \tag{2.10}$$

Similar to the $2 \mapsto 1$ code, Bob measures in M_1, M_2 or M_3 basis to recover the x_1,x_2 or x_3 bit. Again, Bob's success probability remains the same in all scenarios and is independent of the measurement he performs or the encoding state he receives.

$$p^{Q}_{3\mapsto 1} = \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right) \approx 0.789 \tag{2.11}$$

2.1.3 Quantum versus classical random access codes

As discussed previously, the optimal strategies for classical random access codes lead to a success probability of $p^C = 3/4$ in both types of random

access codes. Whereas, the success probability of a quantum random access code is ≈ 0.854 in the first case and ≈ 0.789 for the second. Hence, in both classes of random access codes, it can be seen that the quantum random access code outperforms its classical counterpart. The apparent advantage of this quantum resource over its classical counterpart can be quantified by calculating the ratio of the quantum to classical success probability (p^Q/p^C).

For the $2 \mapsto 1$ RAC, the quantum advantage is ≈ 1.138 and for the $3 \mapsto 1$ RAC, the quantum advantage is ≈ 1.052. The $3 \mapsto 1$ advantage is comparatively lower than the $2 \mapsto 1$ but still clearly emphasizes the superiority of quantum random access codes over classical codes.

2.2 High-level RACs

The previous section provided a brief outlook and a basic introduction to the commonly known RACs, where the physical systems used for encoding information were two dimensional systems. Here we shall approach random access codes based on physical systems of dimensions greater than two. This generalization enables RACs to find additional applications otherwise not possible in the original context of RACs. This expansion of the conventional RACs is introduced as
Any collaborative task, where a set of parties attempt to randomly access some subset of data held by another set of parties, despite limited one way communication between them, is called a task of random access coding [9].
Such an expansion makes it possible to find implementations in numerous schemes in QIP. One such example is the scenario of multiparty RACs, where both the input and output data sets are subjected to certain probability distributions. Other examples include RACs with arbitrary communication restrictions such as asymmetric encodings and RACs employing high level communication. Initially, despite all these potential advantages, other than the initial steps regarding RACs of high level communication [39], where QRACs of the form $(d+1)^{(d)} \mapsto 1$ for $d = 2, .., 8$ are presented, high level RACs had not seen much attention. Since the publication of our article about the realization of 4-level $2 \mapsto 1$ QRAC (presented in detail in later sections), the higher level RACs have received more attention. In one of these succeeding articles [40], the optimality of majority encoding scheme for classsical RACs is proven for any d, which was an unproven assertion in our case. This will be elaborated on in the upcoming sections.

In the present scenario, Alice has access to an input string of n d-

levels, $x = x_1, x_2, ..., x_n$ and each individual d-level is given as $x_i = \{0, ..., d-1\}$. Bob, on the other hand, has access to settings b, $b \in \{1, ..., n\}$, which he uses to indicate the d-level of his interest, x_b. Similar to the previous cases, Alice can only communicate one d-level to Bob. The notation used for this high level RAC is thus $n^{(d)} \mapsto m$ and $p_{n,d}$ is the average (or worst case) success probability for Bob to recover his preferred d-level. In the succeeding sections, we shall look at the characteristics of high level classical and quantum random access codes of arbitrary dimensions d. We shall also consider the success probabilities achieved for each and a subsequent analysis of results, observing whether a quantum advantage over classical RACs is possible or not. In case of a higher quantum success probability, we shall also try to quantify this quantum advantage but, at the same time, in the scope of this thesis, we will restrict ourselves to scenario of RACs for $n = 2$. All the topics covered in the coming sections are presented in article I [41].

2.2.1 Classical RACs

The aim here is to establish classical RACs of the given form $n^{(d)} \mapsto m$ and present an optimal classical strategy to obtain the average classical success probability for these RACs. A classical approach based on these RACs makes use of pure strategies to estimate the performance of such codes. Such pure strategies are deterministic in nature as the resulting outcome is either correct or incorrect. In this pretext, a deterministic strategy is considered optimal if it yields correct outcomes for the maximum number of $n2^n$ inputs possible. In a pure strategy, Alice uses an encoding function E, $E : \{0, ..., d-1\}^n \rightarrow \{0, ..., d-1\}$, to encode her input string of n d-levels into a single d-level, which is then communicated to Bob. Bob proceeds by using a decoding function D_b, $D_b : \{0, ..., d-1\} \rightarrow \{0, ..., d-1\}$, to decode the d-level communicated by Alice with respect to x_b.

For classical RACs with $d = 2$, it has been shown that the optimal classical strategy for $n \mapsto 1$ RACs employs a majority encoding function, for encoding Alice's input string, and an identity decoding function used by Bob [38]. A generalization of this could easily be seen from the encoding and decoding functions used above, E and D, by Alice and Bob respectively. The operation of both the encoding and decoding functions can be presented as $D_b(E(x))$. Therefore, this joint operation of the two functions can be regarded as a single function and allows Bob to perform identity decoding, $D_b(E(x)) = E$, provided that the range of D_b and E are the same.

For the classical random access codes based on high level communication, the majority encoding and identity decoding strategy is implemented as follows. Alice studies her input string of n d-levels and observes the number of times a given d-level occurs. She stores this information in a frequency table, where she reports how frequently a given d-level occurs in x, and then outputs the consequent d-level that occurs the most number of times. The frequency table, as the name suggests, only contains the occurring frequency of a given d-level and is independent of their values. For a given input string x, the frequency table can also be mathematically viewed as an integer partition of n and all of Alice's d^n possible strings are uniquely associated with a particular partition of n. This set of all positive integer partitions of n is denoted as X, where X_j is the jth partition and $|X|$ is the total number of all partitions of n [9].

Making use of the optimal classical strategy involving majority encoding, Alice's task is to find out the d-level that occurs most frequently. This maximum frequency is represented as $\max\{X_j\}$. The d-level with the highest frequency is then outputted to Bob, where Bob uses identity decoding, to recover the d-level of interest with a success probability of $\max\{X_j\}/n$. The optimal average classical probability achievable for an $n^{(d)} \mapsto 1$ RAC is given as [41]

$$p_{n,d}^{C} = \frac{1}{nd^n} \sum_{j=1}^{|X|} \max\{X_j\} N_{X_j} \tag{2.12}$$

For the high level classical RACs, the cases for $n = 2$ and $n = 3$ are the ones that we are interested in. The average success probabilities in these two cases is computed to be [41]

$$\begin{aligned} p_{2,d}^{C} &= \frac{1}{2}\left(1 + \frac{1}{d}\right) \\ p_{3,d}^{C} &= \frac{1}{3}\left(1 + \frac{3}{d} - \frac{1}{d^2}\right) \end{aligned} \tag{2.13}$$

The classical success probability calculated for both $n = 2$ and $n = 3$ converges to $\frac{1}{n}$ as $d \to \infty$. It is pertinent to mention here that the success probability $\frac{1}{n}$ corresponds to the simplest of strategies, where Bob just guesses which of the n d-levels were communicated to him. Now, we shall proceed to look at the equivalent QRACs of high level communication, for $n = 2$. A performance comparison with the classical RACs is presented in Appendix section 7.1.

2.2.2 Quantum RACs

In the case of $2^{(d)} \mapsto 1$ QRAC, Alice has an input string of two d-levels, $x = x_1, x_2$, and each individual d-level is given as $x_i = \{0, ..., d-1\}$. The given string is encoded into a single quantum d-level, which is then communicated to Bob. Meanwhile, Bob uses two mutually unbiased bases (MUB) [42; 43] as his measurement options to recover the d-level of his choice. The two MUBs used by Bob are otherwise commonly referred to as the Computational $\{|l\rangle\}_l$ and the Fourier basis $\{|e_l\rangle\}_l$ given as

$$|e_l\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kl} |k\rangle \tag{2.14}$$

where $\omega = e^{2\pi i/d}$ is the root of unity. Bob performs a measurement in the $\{|l\rangle\}_l$ basis if he is interested in x_1 or in $\{|e_l\rangle\}_l$, if he is interested in recovering x_2. The success probability for this family of QRACs is thus represented as $p^Q_{2,d}$. For the given input string of 2 d-levels, Alice has available to her d^2 possible encoding states. For the general encoding states $|\psi_{x_1 x_2}\rangle$, it is but logical to begin by considering the encoding of the string $x_0 x_1 = 00$ into the state $|\psi_{00}\rangle$, which is given as

$$|\psi_{00}\rangle = \frac{(|0\rangle + |e_0\rangle)}{N_{2,d}} \tag{2.15}$$

$N_{2,d}$ is the d-dependent normalization and is given as

$$N_{2,d} = \sqrt{2 + \frac{2}{\sqrt{d}}}. \tag{2.16}$$

All the other encoding states are a generalization of the state $|\psi_{00}\rangle$ and in order to define the other possible encoding states of Alice, a generalization of Pauli operators σ_x and σ_z is required. These generalized Pauli operators are defined as X_d and Z_d, where X_d is the generalized form of σ_x and Z_d is the generalized form of σ_z. These generalized Pauli operators are given as

$$\begin{aligned} X_d &= \sum_{k=0}^{d-1} |k+1\rangle\langle k| \\ Z_d &= \sum_{k=0}^{d-1} \omega^k |k\rangle\langle k| \end{aligned} \tag{2.17}$$

The operation of X_d operator is analoguous to σ_x, which acts as a bit flip when acting on a given state $|s\rangle$. This implies that the operation of X_d will raise the state from $|s\rangle$ to $|s+1\rangle$, where the sum is modulo d. Similarly, the operation of Z_d is analoguous to σ_z, which flips the sign of a given state $|s\rangle$. This operation is identical to the phase rotation of the state in two dimensions, which is given as $e^{i\pi}$. Hence the operation of Z_d rotates the phase of any given state $|s\rangle$ with ω^l. The generalized encoding states $|\psi_{x_1x_2}\rangle$ can be defined using with the help of these unitary operators, X_d and Z_d [9].

$$|\psi_{x_1x_2}\rangle = X_d^{x_1} Z_d^{x_2} |\psi_{00}\rangle \tag{2.18}$$

which can be expanded further such that

$$|\psi_{x_1x_2}\rangle = \frac{1}{N_{2,d}} \left(|x_1\rangle + \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{jx_2} |j + x_1\rangle \right) \tag{2.19}$$

This is the generalized encoding state that is used to represent all possible d^2 values of Alice's input string. As described before, when communicated to Bob, Bob measures in the computational basis $\{|l\rangle\}_l$ to recover x_1 or in the Fourier basis $\{|e_l\rangle\}_l$ to obtain x_2. In the scenario of a measurement in $\{|l\rangle\}_l$ basis, the resulting measurement outcome is l and the probability distribution P_Z of this outcome is given as

$$P_Z(l) \equiv |\langle l|\psi_{x_1x_2}\rangle|^2 = \frac{1}{N_{2,d}^2} \left| \delta_{l,x_1} + \frac{\omega^{x_2(l-x_1)}}{\sqrt{d}} \right|^2 \tag{2.20}$$

On the other hand, in the scenario of a measurement in $\{|e_l\rangle\}_l$ basis, the resulting probability distribution P_X of measurement outcome l is given as

$$P_X(l) \equiv |\langle e_l|\psi_{x_1x_2}\rangle|^2 = \frac{1}{N_{2,d}^2} \left| \frac{\omega^{-lx_1}}{\sqrt{d}} + \omega^{-x_1x_2} \delta_{x_1,l} \right|^2 \tag{2.21}$$

Irrespective of the measurement basis used by Bob or the encoding state used by Alice, the quantum success probability depends upon the recovery of the preferred d-level resulting in an outcome of x_1 when measured in computational basis or the outcome x_2 when measured in the Fourier basis. The success probability of Bob's outcome is given in [41] as

$$p_{2,d}^Q = \frac{1}{2} \left(1 + \frac{1}{\sqrt{2}} \right) \tag{2.22}$$

From the above expression, one can deduce that the success probability of recovering a given d-level, x_i, remains the same and is independent of the encoding state used by Alice or the measurement basis used by Bob. Hence, this success probability is both an average and the worst case probability. Additionally, as $p^Q_{2,d}$ is always greater than $1/2$, therefore, the QRAC is non-trivial for any d. Moreover, the quantum success probability $p^Q_{2,d}$ is greater than the classical probability $p^C_{2,d}$ for $d > 1$, which shows the advantage of these quantum resources over their classical counterparts. Furthermore, for $d = 2$, the success probability of a standard $2 \mapsto 1$ QRAC where $p^Q \approx 0.854$ is reproduced.

In section 2.1.3, we quantified the advantage of quantum over classical RACs through the ratio p^Q/p^C. At the same time, while looking at the quantum success probability in eq. 2.22 and the classical success probabilities in eq. 2.13 for $2^{(d)} \mapsto 1$ RACs, one can see that the maximum advantage in terms of difference in numbers, $p^Q_{2,d} - p^C_{2,d}$, is achieved for $d = 4$ when the quantum success probability is $\frac{1}{8}$ times larger than its classical counterpart. An experimental implementation and test of such a $2^{(4)} \mapsto 1$ QRAC is presented in detail in the next section. In 7.1, a comparison of the high level classical RACs with the $(d+1)^{(d)} \mapsto 1$ QRACs of [39] and the advantage of using $n^{(d)} \mapsto 1$ QRACs based on high level systems is provided.

2.3 Experimental implementaion of $2^{(d)} \mapsto 1$ QRACs

In this section, we will look at the experimental demonstration of a $2^{(4)} \mapsto 1$ quantum random access code in the laboratory. In this high level QRAC of dimensions four, Alice has available to her an input string of two 4-levels x_1, x_2, where $x_i \in \{0, 1, 2, 3\}$, which are encoded into a single 4-level quantum system before being communicated to Bob. Bob, has access to two measurement bases, namely the Computational (eigenbasis of Z) and Fourier (eigenbasis of X) bases and depending upon the 4-level system of his interest he performs a measurement in either of these two bases. The success probability in a random access code task depends upon upon his ability to successfully recover the 4-level system of his interest.

2.3.1 State preparation

Before we proceed it is important to understand how are we going to implement these 4-level physical systems using single photons. Such a scheme was briefly presented in section 1.2.4 where it was mentioned

that physical systems of dimensions four can be realized by utilising the polarization and path degrees of freedom of single photons. This is possible as by using the horizontal ($|H\rangle$) and vertical ($|V\rangle$) polarization modes along with two spatial modes ($|a\rangle$ and $|b\rangle$) of single photons we can define the following four basis states, $|1\rangle \equiv |H,a\rangle$, $|2\rangle \equiv |V,a\rangle$, $|3\rangle \equiv |H,b\rangle$ *and* $|0\rangle \equiv |V,b\rangle$. This is usually done by using a combination of half-wave plates (HWPs) and a polarization beam splitter (PBS). Wave plates are optical components made of a birefringent material (quartz) and are one of the most important tools for manipulating a photon's polarization. The polarization state can be transformed to another state through the suitable rotation of a wave plate where this rotation introduces a phase shift (ϕ) between the horizontal and vertical polarizations of photons. Depending on the value of the introduced phase (ϕ), the wave plate can either be termed as a HWP ($\phi = \pi$) or a QWP ($\phi = \frac{\pi}{2}$). In this thesis, both HWPs and QWPs are used for polarization control in the performed experiments. A PBS cube on the other hand is an optical component which splits the incoming light into two separate parts based upon its polarization state as the transmission and reflectance is polarization dependent. The PBSs used in the scope of this thesis are in a cube form and they allow the horizontal polarization to pass through them while reflecting the vertical polarization. This provides an efficient way to map polarization states into paths as the horizontal and vertical polarizations are split into different paths when passing through a PBS. In this configuration, a PBS performs a measurement in the computational basis as the output ports correspond to state vectors $|H\rangle$ and $|V\rangle$. Therefore, information can then be encoded using the four bases states described above and a ququart state can be written as

$$|\psi\rangle = \alpha|H,a\rangle + \beta|V,a\rangle + \gamma|H,b\rangle + \delta|V,b\rangle \tag{2.23}$$

Now that we have presented a method of implementing a 4-level physical system with single photons, we will present how we used this two polarization two path scheme to prepare the $d^n = 16$ encoding states of Alice. To begin with, we required an initial state of the form

$$|\psi\rangle = a|x\rangle \pm b|y\rangle \pm b|z\rangle \pm b|w\rangle \tag{2.24}$$

where $x, y, z, w = \{1, 2, 3, 4\}$ and $a^2 = 0.75$ and $b^2 = 0.083$.

For encoding this state into a two path and two polarization scheme, a $HWP(\theta_1)$ and a PBS were first used to control the population for each path followed by the use of $HWP(\theta_2)$ and $HWP(\theta_3)$ in the two paths to control the population between the different polarization states.

By using these optical components, we achieved the right populations in each path but not the desired phases. This however can be taken care of by the use of phase shifters $PS(\phi)$ that can introduce an arbitrary phase shift between the two paths. In our case, the required phase shift between the two paths is either 0 or π.

In Fig. 2.2, the *state preparation box* shows this configuration of HWPs and PBS used to prepare the 4-level physical system with single photons.

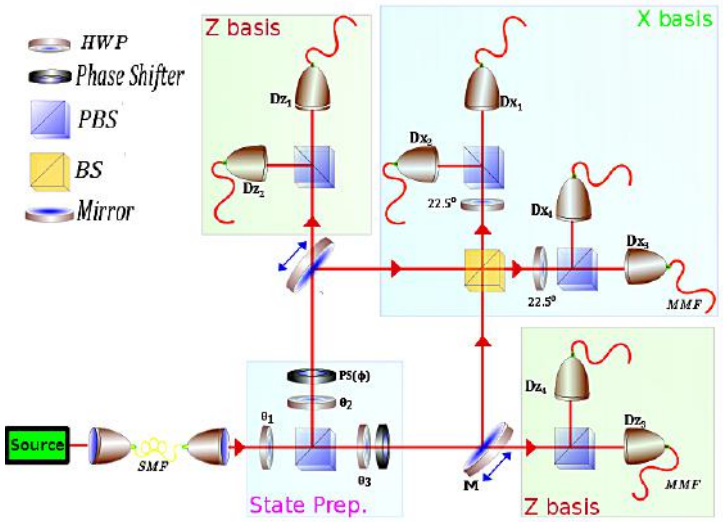

Figure 2.2: Experimental implementation of four-level encoding QRACs. The state preparation box allows to prepare any of the 16 input states through the appropriate orientation angles θ_i of the three HWPs. Mirrors (M) mounted on picometer translation stages can be moved in and out of the photon path enabling a measurement choice between the computational and Fourier bases.

After the first $HWP(\theta_1)$ and PBS, we have $\cos(2\theta_1)|V,a\rangle + \sin(2\theta_1)|H,b\rangle$ whereas after the HWPs and PSs in the two paths the state can be written as

$$\begin{aligned}|\psi_{x_1x_2}\rangle = \cos(2\theta_1) \times \cos(2\theta_2)|H,a\rangle \ + \ \cos(2\theta_1) \times \sin(2\theta_2)|V,a\rangle \\ + \ e^{i\phi}[\sin(2\theta_1) \times \sin(2\theta_3)|H,b\rangle \ - \ \sin(2\theta_1) \times \cos(2\theta_3)|V,b\rangle]\end{aligned} \tag{2.25}$$

By suitably adjusting the orientation angles θ_i of the three HWPs, Alice can prepare any of the 16 encoding states $|\psi_{x_1x_2}\rangle$ where $x_1, x_2 \in \{0,1,2,3\}$. The θ_i settings corresponding to all the three HWPs are shown in table 2.1.

2.3.2 Experimental setup

The experimental setup used for this 4-level encoding QRACs is shown above in Fig. 2.2. The *Source* represents the heralded single photon source presented above in section 1.2.2. The coincidence counts between the signal and idler photons are counted using a homebuilt FPGA based multichannel coincidence unit with a coincidence window of 1.7 ns. We characterized our *Source* to make sure that the ratio between the coincidence photon counting due to single-photon and multiphoton pair emissions is below 0.1%. Before being sent to the *state preparation box*, the single photons are passed through a polarizer oriented such that the photons going to the setup are horizontally polarised. The *state preparation box* depicts the appropriate placement of HWPs, PBS and PSs to prepare all 16 encoding states available to Alice in this $2^{(4)} \mapsto 1$ QRAC. Bob's aim on the other hand is to successfully recover the 4-level he is interested in. For this purpose, he chooses between two measurement settings, a measurement in the computational basis (Z basis) or the Fourier basis (X basis). The implementation of these two measurement choices can be seen in Fig. 2.2 where they are represented in different boxes labelled as *Z basis* or *X basis*. After the state preparation box, the single photons travel in the spatial modes (a and b) of the PBS and are then either sent to, after reflection from two mirrors M, interfere at a non-polarising 50 : 50 beam splitter (BS) where they are then measured in the X basis or are allowed to pass through to the Z basis measurement boxes. The choice of a specific measurement setting is implemented by the use of mirrors M that can be moved in or out of the photon path by the use of picometer motorized translation stages.

2.3.3 Measurements and results

A measurement in Z basis is simpler of the two measurements where a PBS alone in the measurement box performs a measurement of the observable σ_z as explained earlier in the functionality of a PBS. In both the Z basis boxes, the number of photons arriving at the two output ports of the PBS are then recorded by the use of two single photon silicon based avalanche photodiodes (APDs) (D_{zi}). The APDs used in this experiment have an effective detection efficiency $\eta_d = 55\%$, dark counts rate $R_d \approx 400/sec$ and a dead time of 50 ns. Here, dead time is the time during which the bias voltage across the p-n junction of the device is below the breakdown level and no photon can be detected.

The measurement in the Fourier basis requires the application of a quantum interference between the photons travelling in the two spatial

modes of the PBS at a 50/50 BS, which splits light into equal transmission and reflection components irrespective of its polarization state. At both output ports of the BS, a configuration of HWP and PBS is used to perform a measurement of the σ_x observable or in other words a measurement in the X basis. For this purpose the HWPs in the measurement box are set at 22.5° as this HWP setting leads to the projection of a given state onto the eigenvectors of σ_x. Afterwards, photons arriving at the two output ports of both the PBSs in the X basis box are recorded by the use of four APDs D_{xi}. All the probabilities needed for the QRAC in each measurement basis can be calculated from the number of detected photons by the APDs. This is shown below in table 2.1, where the success probabilities in both measurement bases are obtained from the APD detected counts for all 16 states communicated by Alice.

It is important to mention here that the total number of detected photons in each experimental setting was on average ≈2500/sec and the measurements were performed for a total of 10 secs for each experimental setting.

Along with table 2.1, in the appendix section 7.2 a detailed account of measurement of all the 16 states for both measurement bases is presented along with the obtained QRAC probabilities in each individual detector setting corresponding to the initial state shown in eq. 2.24. Quantum mechanics predict that, in the case of an ideal experiment, the maximum success probability that can be obtained for a $2^{(4)} \mapsto 1$ QRAC is $p^Q = 0.75$. On the other hand, the maximum classical success probability is $p^C = 0.625$. Considering the fact that experiments performed in the lab are not ideal and are greatly affected by various sources of error. Such is the case for this experiment as well where the major contributing sources are the systematic errors due to the intrinsic imperfections of the optical components used in the experimental setup. These include mostly the imperfections in HWPs and non-ideal splitting ratios of PBSs and BS used in the setup. Another source of errors is the poissonian counting statistics of the detected photons. The experimental results presented here yield an average quantum success probability of 0.754 ± 0.038 and demonstrate a clear violation of the classical bound. Therefore they are in good agreement with the results predicted by quantum theory, indicating a successful implementation of a $2^{(4)} \mapsto 1$ QRAC.

Table 2.1: The orientation of the three half wave plates θ_i (with $i = 1, 2, 3$) and the phase shift PS (ϕ) for the 16 quantum states ψ_{ij}. The quantum success probabilities P^Z_{exp} and P^X_{exp} for measurements in the computational and Fourier basis respectively. Reproduced from [41].

$\psi_{x_1x_2}$	θ_1	θ_2	θ_3	ϕ	P^Z_{exp}	P^X_{exp}
ψ_{00}	12.05	22.5	-9.22	0	0.747 ± 0.036	0.752 ± 0.038
ψ_{01}	12.05	22.5	-9.22	π	0.748 ± 0.036	0.774 ± 0.038
ψ_{02}	12.05	-22.5	9.22	0	0.749 ± 0.036	0.752 ± 0.039
ψ_{03}	12.05	-22.5	9.22	π	0.753 ± 0.036	0.713 ± 0.039
ψ_{10}	12.05	22.5	-35.78	0	0.766 ± 0.036	0.763 ± 0.038
ψ_{11}	12.05	22.5	-35.78	π	0.767 ± 0.036	0.750 ± 0.038
ψ_{12}	12.05	-22.5	35.78	0	0.764 ± 0.036	0.751 ± 0.039
ψ_{13}	12.05	-22.5	35.78	π	0.764 ± 0.036	0.748 ± 0.039
ψ_{20}	32.95	9.22	-22.5	0	0.755 ± 0.036	0.764 ± 0.038
ψ_{21}	32.95	9.22	-22.5	π	0.761 ± 0.036	0.754 ± 0.038
ψ_{22}	32.95	-9.22	22.5	0	0.786 ± 0.036	0.775 ± 0.039
ψ_{23}	32.95	-9.22	22.5	π	0.786 ± 0.036	0.728 ± 0.039
ψ_{30}	32.95	35.78	-22.5	0	0.742 ± 0.037	0.772 ± 0.038
ψ_{31}	32.95	35.78	-22.5	π	0.743 ± 0.037	0.766 ± 0.038
ψ_{32}	32.95	-35.78	22.5	0	0.732 ± 0.037	0.749 ± 0.039
ψ_{33}	32.95	-35.78	22.5	π	0.733 ± 0.037	0.703 ± 0.039

3. Applications of RACs

In the previous chapter, both classical and quantum random access codes were introduced starting from the simpler and commonly known RACs before building up to RACs of larger dimensions. A short yet concise overview and introduction to these RACs was presented in this regard, which was followed by an optimal performance comparison between classical and quantum RACs for both classes of RACs. The performance comparison was made by comparing optimal success probabilities in each scenario. The QRACs seemed to perform better than the classical RACs and laid claim to the notion that quantum resources enhance information processing beyond classical limitations and are important in QIP. Moreover, this laid the ground work for analyzing and implementing such QRACs in real time experiments so that steps can be taken for actual realization of these claimed potential applications of QRACs.

A few applications of QRACs were briefly touched upon in the previous chapter 2. Here, we will study two such utilizations that have shown importance in a number of fields. We will also discuss methods and protocols necessary for their secure and practical implementation using quantum resources. These applications include certification of true random numbers and test of non-classicality of a system and are perceived important in the field of QIP. Articles II and III produced during this thesis work covers in detail the protocols and quantum implementation for both these applications. For this purpose, device independent (DI) and semi-device independent protocols are also examined for an efficient yet secure practical utilization of these applications.

3.1 Truly random numbers

The idea of randomness coupled with the desire and demand to generate truly random numbers is a fascinating topic of interest. This intriguing property of randomness and the ability to create randomness has found its use in all walks of life from general everyday applications to the more scientifically advanced ones. Purely random numbers have been utilized in a wide range of applications as numerical simulations, lottery games, biological systems, statistical sampling, completely randomized designs and cryptography. In addition, many QIP tasks demand the ability to produce genuinely random numbers as well, e.g., security of QKD protocols is based on a random selection of the state preparation and measurement [32]. True random numbers should be completely unpredictable for any eavesdropper in any scenario [44]. Furthermore, recently demonstrated landmark experiments for the loophole-free test of Bell's theorem [45–47] depended greatly on fast random number generators (RNGs) for generating random input bits for the consequent devices. This would have otherwise been impossible without such fast RNGs for space like separation of the relevant events in the Bell test.

The first and foremost question that arises at this point is how could one go about generating numbers that are genuinely random in nature? Modern day computers make use of carefully designed, sophisticated and advanced algorithms to produce random numbers. Should random numbers generated by these dedicated algorithms be considered truly random? or Is there an underlying argument that leaves this claim implausible? The underlying fact is that computers use deterministic algorithms to produce random numbers and as a result, generated random numbers are essentially pseudo-random numbers and not absolutely random. The use of such a deterministic strategy along with an understanding of the software generating random numbers renders the outcome fundamentally predictable. Hence, by using strong and strict tests one can show that such random numbers are indeed pseudo-random.

Randomness cannot be authentically classified as genuine unless the process used to create randomness is truly random in itself. This is why most true random number generation protocols are based on unpredictable physical processes [48–55]. This is where quantum mechanics comes in handy as the concept of genuine randomness is a fundamental feature of the physical reality of quantum systems and an innate property of quantum theory. A simple yet effective demonstration of this is the example of path-splitting of incident photons [48]. Consider a scenario, where a single photon is made incident on a 50/50 beam splitter (splits

incoming light into two equal intensity parts) followed by two detectors (D_a and D_b) at each output port of the beam splitter. Every time, detector D_a records the detection of a photon event, it is termed as "0" and "1" for the same in the detector D_b. Quantum theory predicts that, in both scenarios, the detection events in either arm are truly random and independent of each other. Therefore, the resulting string of numbers generated by detection of photons in the two detectors is described as truly random by quantum mechanics as the measurement process is essentially random in itself. In this chapter, we will consider our experimentally demonstrated $2^{(4)} \mapsto 1$ QRAC from the previous chapter and shall see how much randomness can be generated and certified from such a high-level code. It would also be interesting to compare the randomness generated from such QRAC against the results of commonly known $d = 2$ QRACs.

3.1.1 Device and semi-device independent protocols

Device independence (DI), as the name indicates, is a scenario where an application/protocol functions successfully on a range of devices regardless of the local hardware used in them. The concept arises originally from computer science where it is used extensively such that a software application is made to function on all platforms regardless of the local hardware on which the software is used [56]. In simple words, it can be considered as a scheme that bears no consideration to the internal hardware and functionality of a device. The idea of device independence can be extended to quantum information science where it may assure the success of a protocol, irrespective of the device functionality, provided that the assumption that no additional classical information leaves the laboratory is upheld. How this is applied successfully is explained below in coming paragraphs.

In quantum information context, the DI approach was first presented in [57] and has been successfully implemented in the field of quantum cryptography [58–60]. The same approach was later extended successfully to randomness generation protocols. It was first used by Colbeck et al. [61; 62] to demonstrate a Greenberger-Horne-Zeilinger (GHZ) test based randomness expansion protocol. Later on, Pironio et al. proposed a true random number generation protocol certified by the violation of a Bell inequality [63]. In this context, the violation of Bell inequality acts as a security parameter for randomness certification. It was shown that we need not make any assumptions about the way the devices work as long as correlations that violate a Bell inequality are upheld. In this way,

classical methods cannot be used for random number generation and the certification of randomness is provided by the Bell inequality violation.

True random number generation protocols must be based on unpredictable physical processes and to certify whether a given set of random numbers is truly random is no easy task. The devices that are used to generate authentic random numbers must in turn operate according to some intrinsically random process. In this scenario, the problem reduces to the certification that the device is performing as it is supposed to, at least within reasonable limits [34]. Bearing this in mind, the device independent approach has attracted great attention recently as it provides a platform for all involved parties to establish the required parameters for randomness certification without making any assumptions about the inner functionality of the devices used. This is important as the internal working of a device could be described using a local hidden variable model. Therefore, one can not be sure if the device is performing as it is supposed to and one needs to assume that the parties have complete control over the state preparation and measurement devices.

In the device independent protocols for randomness generation and certification, the experiment consists of a number of rounds. In each of these rounds, a quantum state is prepared and is subjected to a measurement. Most of these experimental rounds are used for generating randomness whereas a few are used for the estimation of the security parameter (violation of bell inequality). In each individual round, the involved parties generate an input that corresponds to the choice of measurement setting and then observe the resulting outcome. This is in principle very similar to performing a Bell test. It is obvious that if the parties are interested in generating more randomness than what they enter, their input settings cannot be random for every round. In fact, the input setting is usually kept the same for all the randomness generation rounds but is chosen randomly for all the security parameter estimation rounds. The total amount of randomness generated is then estimated from the violation value.

As the DI protocols rely heavily on the violation of a Bell inequality and this requires the involved parties to share entangled states. This makes the implementation of such devices highly complex and negatively influences the rate of randomness generation due to the strict requirements placed on the devices [63]. One can see that, although the DI protocols provide strong security but the complicated experimental setups and the limited efficiency is a big downside to these protocols. Additionally, as the requirement of pre-established true random numbers is necessary to select the measurement bases, the protocols are commonly

termed as randomness-expansion protocols [31].

To improve the rates at which random numbers are generated and making the experimental setups easier to implement, a compromise was proposed in the form of semi-device independent (SDI) protocols. In the SDI protocols, the devices remain untrusted as no assumptions are made about their internal working but an upper bound on the capacity of quantum channel is however assumed. This was first demonstrated in the context of one way QKD [35]. The preparation and measurement devices are kept in a safe area, have no access to side channels or shared quantum entanglement although they may share correlated classical variables but not correlated inputs.

3.1.2 SDI random number generation protocols

SDI protocols employing $n \mapsto 1$ QRACs for the generation and certification of truely random numbers have been shown in [24; 31]. Typical SDI RNG protocols require two black boxes and can be implemented in a simple prepare-and-measure scenario. Such a scenario maintains two devices (black boxes) where one device lets the user to prepare the physical system in different ways and the measurement device is then used to perform a measurement on the prepared physical system. So, the inputs in a SDI protocol correspond to the choice of preparation and measurement for the sender and receiver device. We will now discuss the generation of random numbers using high level QRACs of the form $n^{(d)} \mapsto 1$. Here d is the assumed upper bound on the underlying Hilbert space. The general description of the SDI protocols is as follows.

Similar to the DI protocol, in a SDI random number generation protocol, a given experiment is divided into numerous rounds. These rounds are then categorized into different groups of random sizes. In each of these groups, all the rounds are used for generation of random numbers albeit one particular round. This specific round, the first round in every group, is always used for the calculation of the security parameter T, which is used to certify true randomness and is strongly correlated to the average success probability of a QRAC, in our case The security parameter sets a lower bound on the average amount of randomness of a measurement result in any given round.

Let us suppose that χ is a set of elements that contains all the possible inputs for the preparation and measurement devices. For the rounds used for the security parameter estimation, the inputs are always chosen randomly from χ. Whereas for the randomness generation rounds, an input is chosen from $\chi^{'}$ (a subset of χ) independently of the group.

Traditionally, as mentioned above, RNG protocols use the same input for all randomness generation rounds, i.e., only one element in $\chi^{'}$. This is vital as otherwise more randomness is expended as compared to what the protocol generates.

For implementing the SDI RNG protocol, consider a given input string a of n bits, $a = a_1, ..., a_n$, such that the state preparation black box receives any one of the d^n inputs associated with the input string. For each received input, the preparation box prepares a quantum state ρ_a, only the Hilbert space dimension of which is known. ρ_a is then communicated to the measurement black box. The measurement black box is provided with a set of n measurements where any one of these measurements $y \in \{1, ..., n\}$, when performed, will return an outcome $b \in \{0, ..., d-1\}$. Again, we have no information regarding the prepared state ρ_a or the measurement settings (bases) and the whole preparation and measurement process results in a conditional probability distribution $P(b|a, y)$.

3.1.3 Certification and quantification of randomness

As stated before, security parameter T is important as it is a test of randomness and certifies its generation by setting a lower bound on the average amount of randomness of a measurement result. It also in turn is strongly connected to the average success probability of a QRAC (in our case the multi-dimensional quantum random access code with $d = 4$). The efficiency of this QRAC serves as the security parameter T and is mathematically expressed as

$$T = \frac{1}{nd^n} \sum_{a,y} P(b = a_y|a, y) \tag{3.1}$$

It is important to mention here that the average success probability of a QRAC is a vital parameter in the pretext of randomness generation. For given input random numbers a, y and the resulting measurement outcome b, generation of random numbers is directly related to the average success probability. The success probability parameter guarantees the randomness of the measurement outcome, provided that the classical bound is violated, without making any assumptions about the internal working of the black boxes. This is possible as if a given probability distribution $P(b|a, y)$ violates the classical bound, randomness is certified as it is verified that a classical deterministic strategy can not reproduce this $P(b|a, y)$.

For generation of random numbers, it is important to not only certify but also to quantify the amount of randomness of measurement outcome b. The parameter used commonly for quantifying generated randomness, for random inputs a and y, is the minimum entropy function H_∞ given as

$$H_\infty\left(B|X=a,y\right) = -\log_2 \max_{b,a,y} P\left(B=b|X=a,y\right) \tag{3.2}$$

The aim is to find a lower bound on H_∞ as a function of security parameter T. This is achieved by using methods [64] employing semi definite programs (SDP) [9] that give lower bounds over a quantity by performing optimization over states and measurements from the interior of quantum set of probability distributions [65]. In order to compute a lower bound on quantity of randomness, all parameters that could reproduce the observed data must be optimized whereby the least random result is chosen. In section 3.1.5, it will be shown that the amount of randomness generated from high level QRACs is more than what is generated by 2 dimensional QRACs.

3.1.4 Certification of more randomness

In the preceding section, it was reported that higher-level QRACs can generate more randomness when compared with their lower level counterparts. However, there are ways to certify more randomness, even for higher level QRACs, by utilizing subsets of data alone. One such method is demonstrated in article II, where its shown that the requirements on the used experimental setup can be lowered greatly if the computational capacity available to the user is high. The QRAC used for this purpose is the $2^{(4)} \mapsto 1$ and experimental data from this code is used for the calculation of T. The results presented are both qualitative and quantitative in nature as it is shown that a user with access to large computational capacity can certify the existence of randomness in an experimental setup where another user with lower computational capacity can not. Additionally, for the same setup, the user with large computational capacity can certify more randomness. The ability to certify the existence of randomness and to certify more randomness depends upon the number of settings (elements in $\chi^{'}$) used for the randomness generation round.

It was stated before that traditional SDI RNG protocols use the same input for all randomness generation rounds, i.e., only one element in $\chi^{'}$. However, the number of settings (number of elements in $\chi^{'}$, denoted as K from now on) used for a randomness generation round is a very important parameter in terms of required computational capacity and the amount of randomness generated. The idea behind these protocols (for $K > 1$) is

that for a large number of rounds used for security parameter estimation, the average value of T calculated from these rounds will be approximately similar to the estimated $O\left(\sqrt{N}\right)$ average value for the rest of the rounds provided that K is chosen randomly.

The randomness of measurement outcome B is quantified by average min-entropy function, expressed as

$$H_{\infty}^{av}\left(B|X\right) = -\frac{1}{K}\sum_{x\in\chi'}\log_2\ \left(\max\right)_b\ P\left(B=b|X=a,y\right) \tag{3.3}$$

where optimization over all parameters is done using state-of-the-art SDPs. However, minimization of $log\ max\{.\}$ is not possible using SDP as $\log\max\{.\}$ is a decreasing function, where finding its minimum is equivalent to finding the maximum of the argument. In this regard, the concavity of the $log\left(.\right)$ function can be used such that we get $H_{\infty}^{av}\left(B|X\right) \geq -log\ \frac{1}{K}\ \sum_{x\in\chi'}\ \left(max\right)_b\ P\left(B=b|X=a,y\right)$.

For maximizing the argument, a separate maximization should be executed for all b where a separate value of b is chosen for every round. This leads to optimization over D^K rounds where D is the number of total values that B could have. This is quite complex as the computational capacity required for the task increases exponentially with K. Nonetheless, by exploiting the properties of min-entropy function (depends only on the largest value of $P\left(b|a,y\right)$) and RACs (distinguishes between outcomes $B=a_y$ or $B\neq a_y$), one can use a new binary variable B'. B' can be obtained from B by classical postprocessing and is 0 when $B=a_y$ and 1 otherwise. As B' takes only two values, the number of optimizations required to set a lower bound on min-entropy function are lowered to 2^K. This number remains the same even for scenarios where QRACs of even higher dimensions are considered. In the next section, it will be shown how this method can lead to certification of more randomness along with a lower critical T value.

3.1.5 Randomness generation from $2^{(4)} \mapsto 1$ QRACs

Here, we will consider the possible generation of random numbers from our 4-level QRACs in a semi-device independent scenario. Let Alice and Bob denote the preparation and measurement devices where corresponding to a $2^{(4)} \mapsto 1$ QRAC, Alice′s input numbers a_0 and a_1 can attain values from 0 to $d-1$ and she communicates a 4-level quantum system to Bob who aims to find outcome $B=a_y$. The efficiency (T) of this 4-level QRAC serves as our security parameter, which is the parameter that certifies the randomness of Bob's measurement outcomes by setting

a lower bound on the average amount of randomness in a measurement outcome. The security parameter is given in eq. 3.1 where $nd^n = 32$.

Generation of random numbers is directly dependent on the success probability of a QRAC. By using our experimental results of the $2^{(4)} \mapsto 1$ QRAC, we calculated the value of T where $T = 0.7347$. Bearing in mind the fact that the security parameter T clearly violates the classical bound (0.625), we can certify that the randomness generated is genuine. Now that the randomness in measurement outcomes is certified we can calculate the amount of randomness generated by the use of minimum entropy function as given in eq. 3.2 and is shown below in Fig. 3.1.

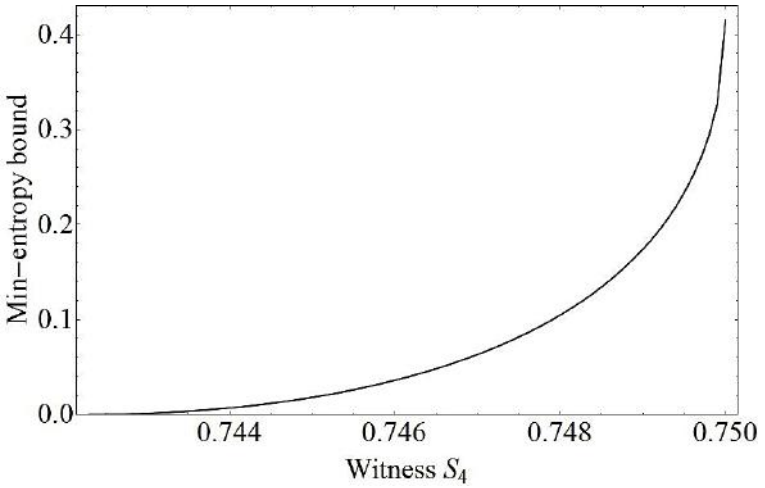

Figure 3.1: Semi-device independent expansion of randomness using $2^{(4)} \mapsto 1$ QRAC. Reproduced from [9].

In quantitative terms, the amount of randomness (0.42) is significantly larger as compared to randomness generated (0.23) for known $n = 2$ QRACs of dimension two [31; 32] leading one to state that more randomness can be generated using random access codes of higher dimensions. It is also apparent from Fig. 3.1 that total randomness produced is very sensitive to the optimal QRAC average success probability of 0.75 as even a very small deviation from the optimal quantum value leads to an incredible change in the amount of randomness produced and below a critical value of T no randomness is produced. Therefore, one can conclude that although more randomness is produced using high-level QRACs but the amount of randomness produced is strongly dependent upon the optimal value of a QRAC.

The experimental results and the security parameter obtained were

then used by our theoretical collaborators who used it to investigate the computational requirements of methods (used for optimization over all involved parameters) on postprocessing of experimental data for randomness certification. It is successfully shown in [66] that for a given experimental setup, by increasing the value of K (no. of possible settings used in randomness generation round) from 1, a user with more computational power can certify not only more randomness but also the existence of randomness where a user with less computational power cannot. $K = 1$ is the case, where the same inputs are used in every randomness generation round shown in Fig. 3.1. For our experiment, the critical value of T is given as $T_K = \frac{16-K}{16}\frac{3}{4} + \frac{K}{16}\frac{5}{8}$. Here K is the number of inputs used for randomness generation rounds, 16 are the number of states that Alice can communicate, 3/4 and 5/8 are the success probabilities for the optimal and non-optimal states. The advantage of using $K > 1$ is clear as critical $T_{K=1} \approx 0.742$ and $T_{K=2} \approx 0.734$ [66].

The method was presented in section 3.1.4 where it was shown that the number of optimizations required to set a lower bound on min-entropy function are lowered to 2^K. In Fig. 3.2 these optimizations are plotted for various values of K as a function of T. It is clearly seen that not only more randomness is certified for increasing values of K but also, at the same time, the critical value of parameter T is lowered.

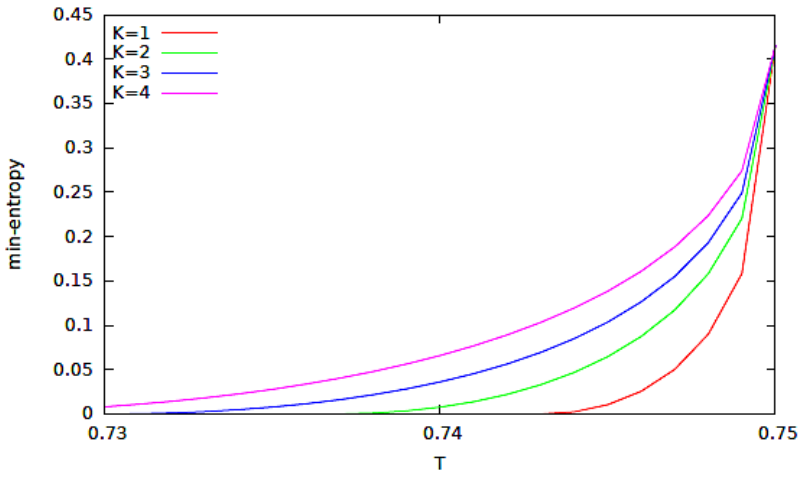

Figure 3.2: A lower bound on min-entropy shown for different values of K as a function of security parameter T. Certification of more randomness is apparent for larger values of K. Reproduced from [66].

Now to compare it with the experimental results, the amount of randomness generated for different K from the experimentally obtained

value of the security parameter is shown below in table 3.1. One look at the table one can see that the amount of randomness increases quickly with K. However, for $K = 1$ no randomness is generated despite the high fidelity of the experiment because only rounds with a specific input setting is used for randomness generation. Hence, no randomness is generated as the measurement outcome can be predicted with certainty. The last column in the table 3.1 shows the time taken for computation, which clearly reflects the increased complexity of larger K. It is estimated that to certify the randomness when all the settings are used for its generation, i.e., $\mathcal{X} = \mathcal{X}'$ it would take 400.000 years on the used machine.

Table 3.1: Randomness generated for different K from the experimentally obtained value of T. Reproduced from [66].

K	$P_{av}(B' = 0)$	H_{∞}^{av}	time taken
1	1	0	c.a. 10 min.
2	1	0	c.a. 20 min.
3	0.99512	0.007058	c.a. 40 min.
4	0.98180	0.026499	c.a. 1.5h.
5	0.96882	0.045699	c.a. 2.5h.
6	0.95565	0.065446	c.a. 5h.
7	0.94628	0.079661	c.a. 11h.

To conclude this section, the 4-level QRAC was used for the estimation of the security parameter that certified the genuineness of randomness by violating the classical bound. Moreover, by increasing the number of possible settings for a randomness generation round, a generalization of SDI random number generation protocols is presented. The advantage is the certification of more randomness for a given experimental setup but on the other hand greater demands are placed on the required computational complexity of the certification.

3.2 Test of non-classicality

In section 3.1 we looked at increased certification of genuine randomness using QRACs. In addition, QRACs can also be useful in testing the non-classicality and measuring the dimensions of a physical system (classical or quantum). Both of these applications play a vital role in communication tasks in QIP as certifying the dimension and non-classicality of a system implies that a classical description of the experiment is indeed

not possible [67]. Here it will be introduced how QRACs can be used as a potent resource for certifying the quantumness or non-classicality of a given physical system.

The potential use of classical communication to simulate quantum communication [68; 69] is an important problem in foundations of quantum theory and communication complexity [65]. Therefore, testing the non-classicality of any given system becomes important as it can help to quantify how much of classical communication is needed for the purpose. We will investigate the problem in a prepare-and-measure implementation based on a SDI scheme where only the observable data is relied upon and an upper bound on the dimension of the system is assumed. The observable data represents the probabilities of obtaining certain measurement outcomes for the chosen preparation and measurement settings. In a simple prepare-and-measure scenario, it has been shown that the use of quantum communication can be guaranteed provided an upper bound on the dimension of system exists [70]. This upper bound on the dimensions of the communication is vital as if the system is not dimensionally bounded then the measurement device will, in principal, can have access to all information about preparation and measurement settings and this information can then be used to reproduce any set of data.

Several tests of non-classicality have been reported already and these include violations of a Bell inequality [71], use of dimension witnesses [70] or success probability in a communication complexity task [72]. Additionally, in [67], optimal quantum dimensional witnesses of dimension d (in a SDI scheme) based on linear inequalities are used for testing the non-classicality of a communication system and several case studies, for deriving dimensional witnesses for simple examples of networks, are discussed. As the quantum dimensional witness violates classical dimensional witnesses of dimension d, the use of a quantum dimensional witness for tests of non-classicality of physical systems of dimension d makes sense. For a given set of data, the violation of a classical dimensional witness establishes the use of quantum systems to reproduce the same data set and this comes essentially from the ability of quantum resources to outperform classical resources of same dimensions.

3.2.1 QRACs for test of non-classicality

Now, we will explore the role of d-dimensional $2 \mapsto 1$ QRACs as a candidate for testing the non-classicality of a communication without any constraints from limited detection efficiency of detectors used and other conditions as the absence of shared randomness. This arises from the

requirement that the parties involved in test must lead to a conclusive result in the absence of the above constraints. Experimentally, this is not so straightforward to achieve as the DI non-classical tests are only conclusive if the detection efficiency used is above a critical value. These minimum values of detection efficiency are known for various tests but are difficult to achieve in practise due to technological limitations. Consequently, it is no coincidence that up until now only a few DI tests have been demonstrated [45–47; 63; 73]. Such a situation can however be avoided by adding additional constraints such as the absence of shared randomness between the preparation and measurement devices, which allows the experimentalist to use any arbitrary detectors of non-zero detection efficiency for DI tests of non-classicality [74]. This certainly makes implementing such DI tests of non-classicality easier and has been recently shown in [75; 76].

A quantum random access codes, employing qubits as the physical quantum system, can also be used as a quantum resource for testing the non-classicality. As established before, for a given input string a of two bits, (a_1, a_2), an information capacity of 1 bit (Alice can only send one bit (qubit) at a time) and measurement settings y of the receiver, the success probability of a QRAC is given as $P\left(b = a_y \mid a, y\right)$. QRACs are a good candidate for SDI tests of non-classicality as the optimal average success probability for a QRAC, when only one qubit of information is communicated, is 0.85 which is significantly larger than the classical case when the avg. success probability for one bit of information capacity is 0.75. This capability of the QRAC to outperform the classical code renders it valuable for such tests of non-classicality.

The aim is to demonstrate the use of QRACs as a resource for a SDI test of non-classicality without the detection loophole or absence of shared randomness conditions. This however does not imply that QRACs are unaffected by the detection efficiency loophole [77] and similar to other similar tests, they are also rendered inconclusive due to low detection efficiencies when the detectors fail to detect in an experimental round. This can be bypassed by using the most generic of approaches where the devices return a random number in all such rounds. The obvious advantage of this approach is that the effective detection efficiency artificially becomes 100% although this comes at a cost of the maximum quantum success probability. The quantum probability that can then be achieved from detectors recording photons in the fraction of rounds η is thus given as

$$Q_\eta = \eta Q + (1 - \eta)\,\frac{1}{2} \tag{3.4}$$

One can see from the above equation that this quantum probability goes to 1 for $\eta \to 1$ and to $\frac{1}{2}$ for $\eta \to 0$. The motivation is to construct a test that is independent of a strict required detection efficiency value, i.e., η is as close to zero as required. This could be achieved if the optimal classical probability is limited to $\frac{1}{2}$.

3.2.2 Probability polytopes

In [78], it was suggested that a Bell inequality defined for a specific experiment can always be extended to situations involving more observers, measurement settings and outcomes. In this way, it was shown that if the original inequality defines a facet of the polytope of the joint outcome probabilities then the lifted ones also define the facet of a more complex polytope. Here, the mentioned polytope can be defined as a geometrical object with flat sides that can exist in n-dimensions. Using this framework of probability polytopes, we can extend our above reflections for QRAC to other tests of non-classicality as well. Now this concept of probability polytopes will be used to demonstrate how it can be used in a QRAC scheme for a non-classical test.

Let $p(\vec{x}, \vec{y})$ be a set of conditional probability distributions obtained in an experiment. Here, $\vec{x}$ and $\vec{y}$ respectively, in an experimental run, represent the total set of outcomes and the inputs for all the devices. Now through the vector $\vec{p}$, consisting of the complete set of $p(\vec{x}, \vec{y})$, one can describe the behavior of any device that makes use of any strategy. Here, the linear combinations of all the conditional probabilities $p(\vec{x}, \vec{y})$ is important as its this parameter that reveals if the device violate Bell inequalities or not. Similarly, one can also describe another vector $\vec{t}$, it exists in the same space as $\vec{p}$, to represent these tests such that the scalar product of $\vec{t}$ and $\vec{p}$ gives the test's result.

One example for such a test is the given by the average success probability of the RAC, which in the case of 2-dimensions is $S = \frac{1}{8} \sum_{a,y} P(b = a_y|a, y)$. For such a RAC, the vector $\vec{t}$ would consist of 16 elements that correspond to the number of possible combinations of all the parameters, i.e., inputs to the preparation and measurement devices (a, y) and the outcomes b. For the successful cases when $b = a_y$, each of these elements correspond to $\frac{1}{8}$ and 0 otherwise. For classical RACs communicating single bits of information, it has already been established that regardless of the strategy used, the success probability corresponds to $S_{av} = \vec{t}_{RAC} \cdot \vec{p}_{cl} \leq 0.75$. Moreover, for classical devices, $\vec{p_{cl}}$ is a polytope where all its vertices conform to strictly deterministic strategies and other strategies are simply their convex combinations thatare represented

by points inside the polytope. For the quantum distributions, this set $p_{\vec{qm}}$ is not as simple to characterize and is usually larger than the classical counterpart albeit with equal dimensions. It has however been reported that there are situations when this is not the case [79] and such a situation points to the presence of a vector $\vec{t_0}$ such that $(\forall_{\vec{p}_{cl}} \quad \vec{t_0} \cdot \vec{p}_{cl} = 0)$. It is straight forward to imagine that the the subspace spanned by this vector must be normal to that of $\vec{p_{cl}}$.

Whereas, on the other hand, the quantum distribution $p_{\vec{qm}}$ must be such that $\vec{t_0} \cdot \vec{p}_{qm} = Q \neq 0$. Now to obtain an expression for the probability distribution as a function of detection efficiency, lets revisit the scenario where an experiment while employing detectors with perfect detection efficiency leads us to the probability distribution $p_{\vec{qm}}$. Again, for all the events when no particle is registered by the detectors, they return a random outcome. The probability distribution observed in the experiment then corresponds to the vector $\vec{p}_\eta = \eta\vec{p}_{qm} + (1-\eta)\vec{p}_{cl}$ and the test's outcome will be $\eta^Q \neq 0$ (for $\eta > 0$). Hence, the aim here is twofold: to construct a game that limits the classical success probability to $\frac{1}{2}$ and to realize experimental setups that allow for different dimensions for the classical and quantum distribution sets.

3.2.3 Parallel implementation of QRACs

A parallel implementation of RACs consists of two preparation and two measurement devices that form two random access codes but the preparation and measurement devices are paired randomly with each other in every round, i.e., in a given round, preparation device P_0 is paired with either measurement device M_0 or measurement device M_1. Similarly, P_1 is paired with M_1 if P_0 is paired with M_0 and vice versa. In this way, in any given experimental round we have two RACs performing in parallel to each other. This switching in pairing of preparation and measurement devices is implemented by parameter x where $x = 0$ corresponds to a pairing of P_0 with M_0 and P_1 with M_1 and vice versa for $x = 1$. The terminology for input settings to the devices follows the previously established terminology such that a_0 and a_1 represent the input settings to P_0 and P_1 while y_0 and y_1 denote the input settings to devices M_0 and M_1. Every possible input i is thus represented as $i = \left(a^0, a^1, y^0, y^1, x\right)$ and a receiver n is considered successful if the outcome is $b^n = a_{y^n}^{n \oplus x}$. A graphical illustration of such an implementation of parallel RACs is demonstrated below in Fig. 3.3.

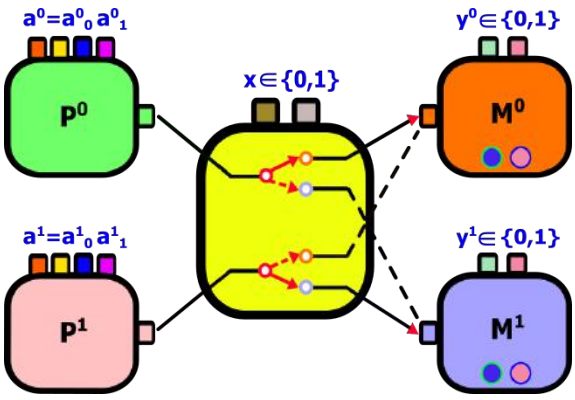

Figure 3.3: A graphical representation of a parallel QRAC implementation. Solid lines represent the coupling of preparation and measurement devices for $x = 0$ whereas the dotted lines represent the corresponding pairing for $x = 1$.

Now, we will discuss how such a parallel implementation of RACs can be used for performing a test of non-classicality without any dependence on a strict detector efficiency or other additional conditions on the devices used. The reasoning is straight forward as the motivation for the parallel RAC scheme arises due to the apparent need for the parties to have coordinated strategies for optimal success in the standard classical RAC. Due to the random pairing of the devices, the parallel implementation rules out this possibility hence the parties must be correlated with each other for their strategies to work every time. Moreover, such correlations must also be visible to the experimentalists. Without using such correlations, the classical devices cannot establish joint strategies and the effect will not be different from the case when the receivers simply return completely random outcomes. To show that this implementation succeeds for our main cause, we make use of the formalism of the conditional probability space.

For our case corresponding to the 16 combinations of a, b and y, there are in total 2^{16} different deterministic strategies. Due to the occurring symmetries between some of them, they correspond to 30496 different points in the conditional probability space however, there are only 125 linearly independent vectors between these points. We define out vector $\vec{t}$ such that it is parallel to the line that connects the point $\vec{p}_{qm}$ and its projection onto the classical subspace. Here, $\vec{p}_{qm}$ corresponds to the set of probability distributions that would arise in the perfect quantum

experiment. We can use the following figure of merit

$$T = \sum_{a_0^0 \oplus a_0^1 \oplus a_1^0 \oplus a_1^1 = 1} \sum_{y^0 \neq y^1} \sum_{b^0, b^1, x} s_0 s_1 p(b^0, b^1 | a^0, a^1, y^0, y^1, x), \qquad (3.5)$$

here s_0 and s_1 are success indicators of the two receives where $s_n = 1$ when $b^n = a_{y^n}^{n \oplus x}$ and -1 otherwise [80]. Here, based on our test, the maximum value of T for the classical case is 0 and the corresponding quantum value is 16. So an experimental $T^Q \neq 0$ value will prove the non-classical behaviour of the communicated systems.

3.2.4 Experimental realization

Now we will look at a simultaneous experimental application of two QRACs working in parallel with each other while employing qubits as their system of communication. In this framework, irrespective of the coupling between them (M^0P^0 and M^1P^1 or vice versa), the state preparation devices look identical to both the measurement devices as single photons sent to them from the two preparation devices have identical polarizations. Hence, the measurement device has no way of telling if they are coupled to P^0 or P^1. In this section, we will see how such a configuration of parallel RACs was implemented experimentally in the laboratory. Probability distributions for all states are measured to demonstrate a test of non-classicality without any requirements for a critical detector efficiency or strong assumptions as the absence of shared randomness. The method for which has already been presented in detail in section 3.2 and [80]. Continuing on the pattern followed in the section 3.2.4, we will begin by considering the state preparation for the experiment, followed by a detailed analysis of the experimental setup and then moving onto experimental results and conclusions.

3.2.4.1 State preparation

The QRACs implmented in the parallel scheme make use of qubit states for information encoding and as a result any quantum system of dimension two will suffice. We have used the two path state preparation method discussed in section 1.2.4 where information is encoded into two different and distinguishable spatial photonic modes $|1\rangle$ and $|2\rangle$. Using the two path encoding, any qubit state can be written as

$$|\psi\rangle = \alpha|1\rangle + \beta|2\rangle \qquad (3.6)$$

This is identical to the qubit state shown in eq. 1.3. The source of single photons here is a heralded single photon source as presented in section 1.2.2. Bearing in mind that we are implementing two RACs here, two different heralded single photon sources are used as input to each preparation device. For input to each preparation device, the heralded single photons are passed through a 3 nm interference filter followed by the coupling of the photon state to a SMF fiber. This is done exactly the same way as it was for the previous experiment. The SMF has a passive polarization controller attached to it such that the photon source can be made to produce horizontally polarized single photons in a single spatial mode of the fiber. Now by making use of a suitably oriented HWP and a PBS, we can expand the state to two spatial modes, whereby the state after the PBS is given as

$$\begin{aligned} |\psi_0\rangle &= \cos(2\theta_0)|1\rangle \ + \ \sin(2\theta_0)|2\rangle \\ |\psi_1\rangle &= \cos(2\theta_1)|1\rangle \ + \ \sin(2\theta_1)|2\rangle \end{aligned} \tag{3.7}$$

Here $|\psi_0\rangle$ and $|\psi_1\rangle$ represent the qubit states for preparation device M^0 and M^1 respectively. It should be noted that the photon polarization in mode $|1\rangle$ is horizontal whereas in mode $|2\rangle$ it is vertical. Rightful orientation of the HWPs ($HWP(\theta_0)$ and $HWP(\theta_1)$) allow us to prepare any qubit state of the above form. The four qubit states used in this experiment are given below

$$\begin{aligned} |\psi_1\rangle &= |2\rangle \\ |\psi_2\rangle &= |1\rangle \\ |\psi_3\rangle &= \frac{1}{\sqrt{2}}\left(|1\rangle + |2\rangle\right) \\ |\psi_4\rangle &= \frac{1}{\sqrt{2}}\left(|1\rangle - |2\rangle\right) \end{aligned} \tag{3.8}$$

Looking at these qubit states, we can see that they can be prepared from eq. 3.7 by orienting the HWPs(θ_0 and θ_1) at $0°, 45°, 22.5°$ and $-22.5°$ respectively. This preparation is figuratively represented by *state preparation box* in the experimental setup described in the next section. The idea behind using two uncorrelated photons, one prepared in P^0 and the other in P^1, passing through the setup at the same time where one will be measured in M^0 and the other in M^1 is to show that the two measurement devices are independent of each other and the preparation devices.

3.2.4.2 Experimental setup

The experimental setup used in the experiment is shown above in Fig. 3.4, whereas Fig. 3.5 shows the setup implemented in the laboratory. The functionality of the state preparation devices and the details about the heralded single photon sources has been presented already. In both the state preparation boxes, one can see an additional HWP in the spatial mode $|2\rangle$. The use of this HWP guarantees that the same polarization can be sent through $|1\rangle$ and $|2\rangle$.

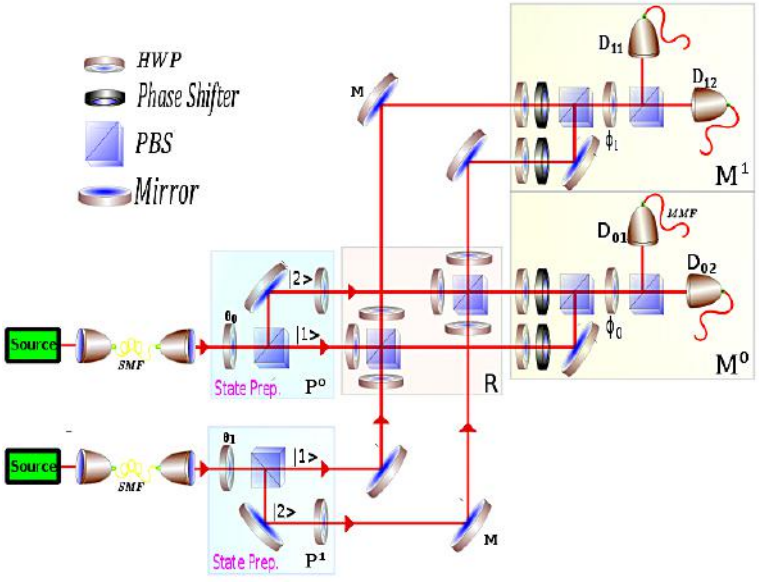

Figure 3.4: Experimental setup for implementation of two parallel RACs. P^0 and P^1 are the two preparation devices, M^0 and M^1 are the measurement devices. Choice of pairing between the preparation and measurement devices is controlled by box R.

The setup consists of three parts: the preparation boxes that encode information into the qubit and send it to the measurement devices. They are followed by a part R that allows the switching and pairing between the preparation and measurement devices followed by M^0 and M^1.

The part of the setup R contains two PBSs surrounded by three HWPs each where two configurations of one PBS surrounded by three HWPs enable pairing of a given preparation device with any measurement device. Suitable orientations of the HWPs allow the PBSs to direct incoming photons to the desired measurement device. In the scope of this experiment, the area R is not considered a device for the purpose

of analysis. The part R could simply be replaced by optical fibers to randomly connect senders and receivers in each round. This would leave R empty but greatly increase the duration of the experiment.

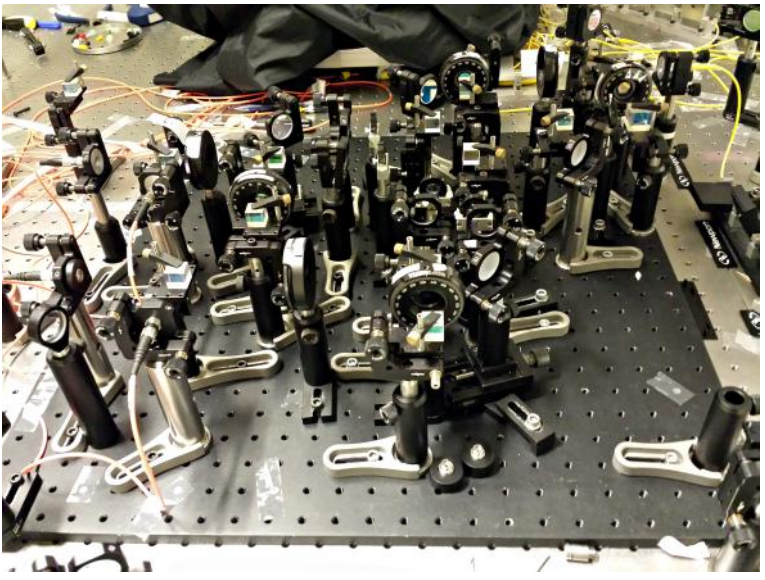

Figure 3.5: Experimental Setup built in the laboratory for implementing the parallel QRAC scheme.

Each measurement device receives incoming photons in two paths from R where they are made to interfere in an interferometric setup. The interferometric setup consists of one HWP and one PS each in both arms. The use of HWPs allow us to control photon polarizations such that incoming photons will leave through the same output port of the BS. The PSs in the two arms make sure that the right phase exists so that a high visibility of interference can be achieved. Upon leaving the interferometer, the photons pass through a HWP(ϕ_i), where $i = 0, 1$, and the adjustment of angle ϕ_i allows us to select the appropriate measurement settings. For the qubit states, the two measurement settings correspond to setting the HWP to an angle $\phi = 11.25°$ and $\phi = 78.75°$ respectively [72]. A PBS placed directly after the HWP splits the polarization modes of the two spatial modes which are then coupled to two multimode fibers (MMF), with a coupling efficiency of $\geq 85\%$, at the two output ports of the PBS. The MMFs in turn are connected to two single photon APDs to register the single photons arriving at both output ports of the PBS. For every setting of the HWP(ϕ_i), the success probability distributions can then be obtained through the photons registered at both the detectors

in each device. The single photon APDs used in this experiment have a detection efficiency of $\approx 65\%$ for 780 nm and are connected to an FPGA based multichannel coincidence unit with a coincidence window of 1.7 ns.

3.2.4.3 Measurements and results

Considering the four states given in eq. 3.8 and the two measurement settings of the HWP in each measurement device, for each pairing of the devices (P^0M^0 and P^1M^1 or vice versa) a total of 64 measurements were performed and the probability distributions were calculated for these measurements. This resulted in a total of 128 measurements for the two pairing rounds of these devices. Tables given in appendix 7.3 show in great detail the measurement order, settings and the registered photon counts for each measurement choice. The first table corresponds to the following pairings P^0 with M^0 and P^1 with M^1. This pairing scheme is viable when $x = 0$. On the other hand, the lower table corresponds to the following pairings P^0 with M^1 and P^1 with M^0. This pairing scheme is viable when $x = 1$. Before proceeding to the experimental data presented in the two tables, it is paramount that the reader understand the following as then the understanding of the tables and the data presented would not be complicated.

For the two preparation (P^0, P^1) and measurement devices (M^0, M^1), if Alice and Alice$'$ are the ones with access to the preparation devices, whereas Bob and Bob$'$ have access to one measurement device each then in the experimental data tables, a^0 is the input available to Alice such that $a^0_0 = 0, 1$ and $a^0_1 = 0, 1$, i.e., there are four possible encoding states available to Alice.

Similarly, a^1 is the input available to Alice$'$ such that $a^1_0 = 0, 1$ and $a^1_1 = 0, 1$, i.e., there are four possible encoding states available to Alice.

y^0 is the input available to Bob (0,1), i.e., there are two possible inputs and two possible measurements.

Similarly, y^1 is the input available to Bob (0,1), i.e., there are two possible inputs and two possible measurements.

The two measurement settings correspond to setting the half-wave plate to $\phi = 11.25°$ and $\phi = 78.75°$ respectively.

The X and Y used in the tables has the following interpretation:

- $X = 0$, $Y = 0$ corresponds to no detection at either Bob or Bob'.
- $X = 1$, $Y = 0$ corresponds to a detection Bob but no detection at Bob'.

- $X = 0$, $Y = 1$ corresponds to no detection at Bob but a detection at Bob'.
- $X = 1$, $Y = 1$ implies detections at both Bob and Bob'.

All the counts given in the two tables are registered in 30 seconds and were registered when the trigger detectors at both Alice and Alice$'$ also registered a count. For each choice of setting $i = (a^0, a^1, y^0, y^1, x)$, a total of ≈ 180.000 counts were registered by the coincidence unit for the two triggers. Out of these total registered counts, $\approx 15\%$ of photons were detected for each pairing, which corresponds to $\approx 2\%$ of simultaneous detection in both measurement devices.

For a test of non-classicality, it is important to make sure that the experimental results are inconsistent with a classical model and can not be reproduced using classical strategies. Whenever, in a given round, no particle was detected by a receiver, a random value was assigned to the outcome. This enabled us to estimate the conditional probability distribution $p(b^0, b^1|a^0, a^1, y^0, y^1, x)$ and, in turn, the value of T. The estimated value of T from our experimental data is 0.172 ± 0.013. The probability that this (or more extreme) value is observed in an experiment in which classical bits are communicated is extremely low. The corresponding p-value is 1.2×10^{-38} leading one to claim that the non-classicality of the communicated physical system is established conclusively.

4. Distributed Tasks with Single Quantum Systems

In this chapter, we will consider two communication tasks that require the distribution of a quantum system between a given number of participants. The first deals with the distributed QRAC, which is an adaptation of a standard $3 \mapsto 1$ QRAC and is based on the work done in article IV. Whereas the 2nd involves the problem of dining cryptographers and anonymous voting where a single quantum system is distributed between a number of participants. This is based on the work in article V.

4.1 Distributed QRACs

In the previous two chapters, we established the classical and quantum RACs before demonstrating an experimental realization of a high-level QRAC that was followed by a demonstration of two QRAC applications. For one of these applications, randomness certification, the results from the experimentally implemented high-level QRAC were used whereas the other, for the test of non-classicality, employed the use of 2-dimensional QRACs. However, both the implemented QRACs were of the $2 \mapsto 1$ type. Here, we will study the $3 \mapsto 1$ QRAC that is implemented in a distributed scheme. In the standard description of the $3 \mapsto 1$ RAC, the implementation is done in a prepare and measure scenario where the preparation device receives an input string $x = (x_0, x_1, x_2)$ and communicates a single physical system to the measurement device. The measurement device, in addition, receives inputs $y \in \{0, 1, 2\}$ and yields an output $b = x_y$. Such a description for this RAC is provided in section 2.1.2 where the success probabilities for retrieving the correct bit (qubit) are also presented.

4.1.1 Distributed QRACs in a one-path communication network

Here, the adaptation of a standard $3 \mapsto 1$ QRAC in a general communication network scenario of [67] will be addressed. The communication

network scheme consists of preparation, transformation and measurement devices where the preparation device prepares quantum systems that are communicated to the transformation devices. Following the processing of these systems in the transformation devices, they are forwarded to the measurement devices where subsequent measurements are performed to retrieve the encoded information. For our purpose, we consider a one-path alternative of such a general communication network, which consists of a single preparation device followed by a transformation and a measurement device. In line with the above description, x_0, x_1 now denote the inputs to the preparation device, x_2 is the input to the transformation device and y is the ternary input to the measurement device.

In the distributed $3 \mapsto 1$ RAC, the preparation device can be divided into two devices that are succeeded by a measurement device. In addition, the communication between the devices is bounded such that it is of unit capacity, i.e., each communication is one bit (qubit). Such a schematic representation for the distributed $3 \mapsto 1$ RAC is provided in Fig. [4.1] and is the simplest non-trivial adaptation of the random access code to the general communication network containing all of the three devices.

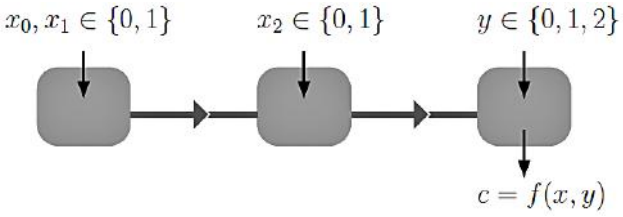

Figure 4.1: A graphical representation of the $3 \mapsto 1$ distributed QRAC. Reproduced from [81].

Like most communication tasks, the average success probability of the RAC defines the efficiency of the task and is given as

$$P = \frac{1}{24} \sum_{x,y} P\left(b = f(x, y)|x, y\right) \tag{4.1}$$

where the output b is a function of the inputs x, y. For the distributed classical RAC, the maximal average success probability that can be achieved is $P^C = \frac{2}{3}$. This happens when $f(x, 0), f(x, 1)$ and $f(x, 2)$ have no information about each other and is obtained by using the following strategy. The preparation device always communicates x_0 to the transformation device that in turn performs an identity transformation

for any of its inputs (0,1) and communicates the same system x_0 to the measurement device. The measurement device in turn outputs $b = x_0$ such that the outcome is $b = x_y$ every time when $y = 0$. Although, for the other two possible inputs of y, the success probability is only $\frac{1}{2}$. This leads to an overall success probability of $\frac{2}{3}$ for the distributed classical RAC, which is lower than the optimal scenario ($\frac{3}{4}$, eq. 2.13) for the standard $3 \mapsto 1$ classical RAC. The optimal classical strategy for the standard case employs the majority encoding scheme where the preparation device uses a majority function to communicate the most frequently occurring bit. This however demands that the preparation device has access to all the input bits in the string x, which however is not the case for any of the involved devices in the distributed scenario.

On the other hand, for the distributed QRAC, there exist tasks where the success probability is maximal ($P^Q \approx 0.79$, eq.2.11). One such example is provided in [67] and will be briefly described here. Consider a QRAC protocol where the output b of the measurement device corresponds to the following three outcomes $f(x,0) = x_0 \oplus x_2, f(x,1) = x_1, f(x,2) = x_2$. The optimal qubit strategy that leads to the maximal success probability involves the encoding states $|\psi_{x_0x_1}\rangle = \cos(\theta)|0\rangle + e^{i\phi}\sin(\theta)|1\rangle$ that correspond to the different inputs given below:

x_0x_1	00	01	11	10
θ	α_+	α_+	α_+	α_+
ϕ	$\pi/4$	$3\pi/4$	$5\pi/4$	$7\pi/4$

here $\alpha_\pm = \cos^{-1}\left(\sqrt{\frac{\sqrt{3}+(-1)^{x_2}}{2\sqrt{3}}}\right)$, $\phi = \frac{\pi}{4}\left(1 + 4(x_0 \oplus x_2) + 2(x_0 \oplus x_2 \oplus x_1)\right)$ and $\alpha\pm$ correspond to $x_2 = \{0,1\}$. Similar to this task, three additional tasks are also constructed and experimentally realized where the resulting (θ,ϕ) settings, for the optimal states in these tasks, can be straightforwardly calculated by replacing x_0, x_1, x_2 with the corresponding $f(x,y)$ using eq. (2) in [81].

The preparation device receives inputs x_0, x_1, assumes that $x_2 = 0$, and prepares one of the corresponding four input states $(\psi_{00}, \psi_{01}, \psi_{10}, \psi_{11})$. The two inputs $x_2 \in \{0,1\}$ of the transformation device are such that, on the incoming state, it performs a π rotation about the x-axis on the Bloch sphere for $x_2 = 1$ or identity transformation for $x_2 = 0$. The qubit state is then communicated to the measurement device. The decoding strategy for the measurement device involves measurements in the three MUBs σ_y, σ_x and σ_z. The basis selection for the measurement device depends on the ternary input y, where σ_y, σ_x and σ_z conform to the inputs $y = 0, 1, 2$ respectively. This described protocol leads to the maximum

success probability for the distributed QRAC and owes its optimality to the fact that the qubit strategies for the distributed and the standard QRAC are essentially the same [38]. Hence, for inputs x_0, x_1, x_2, the qubit states received by the measurement device are the same in both cases and are not disturbed by the distribution between the preparation and transformation devices [67]. Moreover, this leads to a larger quantum over classical advantage ≈ 1.183 for the distributed $3 \mapsto 1$ RAC as compared to the ≈ 1.052 for the standard $3 \mapsto 1$ case.

It is pertinent to stress here that the most important requirement for the above QRAC strategy is that, for $x_2 = 1$, the transformation device applies a unitary rotation in the Bloch sphere such that the four initial states and the four transformed states together form the eight vertices of a cube in the Bloch sphere. This demands that we have the knowledge of all the possible rotations that transform the four vertices of a cube to the other four vertices. From the symmetric rotation group of the cube, the corresponding 15 rotations suitable for the purpose are $R_i(\pi/2), R_i(\pi), R_i(3\pi/2)$ for $i \in \{x, y, z\}$ and $R_{x\pm y}(\pi), R_{y\pm z}(\pi), R_{z\pm x}(\pi)$. Depending upon the initial four vertices, there do exist certain tasks where unitary corresponds to these 15 rotations. This in turn leads to the optimal success probability for the QRAC.

4.1.2 Experimental demonstration of the $3 \mapsto 1$ distributed QRAC

Previously, it was suggested that there exist certain QRAC tasks, based on the above described strategy, where the distributed QRAC gives the maximal success probability. Four such tasks were experimentally realized and their respective success probabilities were estimated from the experimental data. For the sake of clarity, the preparation, transformation and measurement devices from now on will be labelled as Alice, Bob and Charlie. As mentioned previously, the quantum state for the optimal qubit strategy corresponds to the following encoding states of Alice, $\cos(\theta)|0\rangle + e^{i\phi}\sin(\theta)|1\rangle$ with θ, ϕ chosen according to Table 4.1, that lie at the vertices of a cube inside the Bloch sphere (Fig. 2.1).

Table 4.1: All parameters for Alice's state preparation corresponding to the four QRAC tasks. Bob's unitary rotations corresponding to his input values for each task are also presented.

Different Tasks	Alice's encoding state			Unitary by Bob	
$f(x,0), f(x,1), f(x,2)$	x_0x_1	(ϕ)	(θ)	$x_2 = 0$	$x_2 = 1$
$x_0 \oplus x_2, x_1, x_2$	00	$\pi/4$	α_+	$\mathbb{1}$	$R_x(\pi)$
	01	$3\pi/4$	α_+		
	11	$5\pi/4$	α_+		
	10	$7\pi/4$	α_+		
$x_0, x_1, x_2 \oplus x_0$	00	$\pi/4$	α_+	$\mathbb{1}$	$R_x(\frac{3\pi}{2})$
	01	$3\pi/4$	α_+		
	11	$5\pi/4$	α_-		
	10	$7\pi/4$	α_-		
$x_0 \oplus x_2, x_1, x_0$	00	$\pi/4$	α_+	$\mathbb{1}$	$R_x(\frac{\pi}{2})$
	01	$3\pi/4$	α_+		
	11	$5\pi/4$	α_-		
	10	$7\pi/4$	α_-		
$x_0 \oplus x_2, x_1 \oplus x_2, x_0$	00	$\pi/4$	α_+	$\mathbb{1}$	$R_z(\pi)$
	01	$3\pi/4$	α_+		
	11	$5\pi/4$	α_-		
	10	$7\pi/4$	α_-		

Table 4.1 contains a detailed account of the four tasks along with the other parameters that define Alice's encoding states depending upon her inputs x_0, x_1 and the unitary rotations performed by Bob corresponding to his input x_2.

4.1.2.1 State preparation by Alice

For the encoding states of Alice, we needed to prepare a quantum system of two dimensions and similarly to the previous experiments in this thesis, we used the polarization degree of freedoms of a single photon. The source of single photons is the heralded single photon source, described in section 1.2.2. The horizontal ($|H\rangle$) and vertical ($|V\rangle$) polarization states of the single photon allowed us to realize a two level physical system and this polarization encoding preparation was described in section 1.2.4. Using this scheme, a qubit state can then be represented as $a|0\rangle + b|1\rangle$. In order for Alice to prepare any four of the input states for a given task (Table 4.1), she was provided with two half and two quarter-wave plates such that the encoding state is parametrized as

$$|\psi_{x_0x_0}\rangle = \cos(2\alpha)|H\rangle + e^{i\phi}\sin(2\alpha)|V\rangle \tag{4.2}$$

Experimentally, any qubit state can essentially be prepared by using a sequential combination of a QWP, HWP and QWP as this makes it possible to perform arbitrary changes of the photon's polarization state [82]. The reason for providing Alice with four wave plates stemmed from practical simplicity where the HWP setting (α) allowed Alice to control the population between the two polarization states (corresponds to θ in table 4.1) and the QWP(θ_a), HWP(β), QWP(θ_b) configuration enabled to perform any arbitrary rotation along the z-axis in the Bloch sphere (corresponds to ϕ in table 4.1). This 3 WP configuration implements a polarization dependent phase shifter and can be realized by the following wave plate settings: $\theta_a = \theta_b = \pi/4$ and $\beta = (-\phi/4 - \pi/4)$ [23]. Depending on the value of ϕ in Table 4.1, one can calculate β for all of Alice's states.

This robust and elegant scheme enabled Alice to manipulate the photon's polarization making it possible for her to prepare any of the required states $|\psi\rangle_{x_0x_1}$ through the relevant orientations of HWP(α) and HWP(β). For each state preparation, this translated to a rotation of two wave plates instead of rotating three wave plates as is done in the other scheme. This not only made the process easier but also contributed less to the systematic errors. The schematic and the experimental setup are shown in Figs. 4.2 and 4.3 respectively. Table 4.2 lists all the possible settings of HWP(α) and HWP(β) for preparing Alice's input states in each QRAC task.

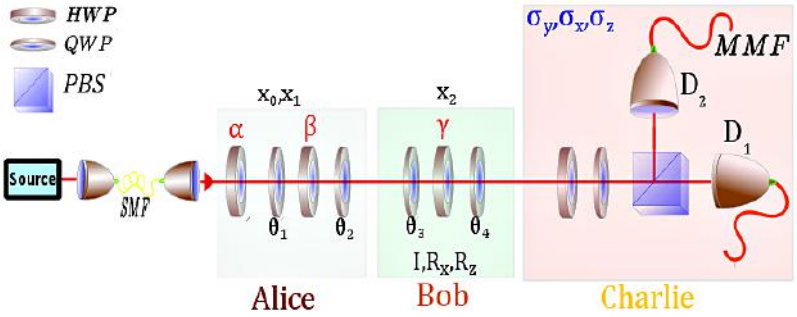

Figure 4.2: Experimental implementation of $3 \rightarrow 1$ distributed QRAC. Alice encodes her states in horizontal and vertical single photon polarization states that are prepared by suitable orientation of HWP(α) and the combination of QWP(θ_1),HWP(β),QWP(θ_2). Unitary rotations by Bob along x-axis, z-axis and I are implemented by a combination of QWP(θ_3),HWP(γ) and QWP(θ_4) respectively. A combination of HWP, QWP and PBS followed by two single photon detectors D_i $(i = 1, 2)$ allow Charlie to perform the measurements in $\sigma_y, \sigma_x, \sigma_z$ bases respectively.

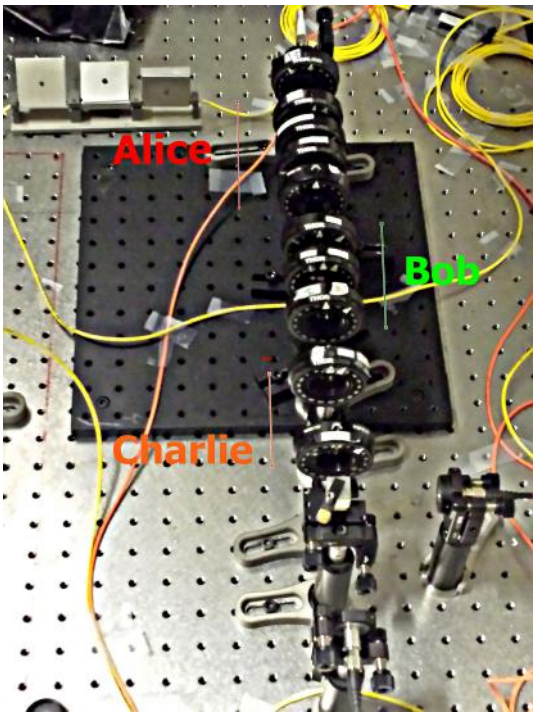

Figure 4.3: Experimental setup built in the lab for the distributed QRAC.

Table 4.2: The complete settings for preparing all the states corresponding to the four QRAC tasks.

Different Tasks	State	Alice's settings			
C					
$f(x,0), f(x,1), f(x,2)$	x_0x_1	$HWP(\alpha)$	$QWP(\theta_a)$	$HWP(\beta)$	$QWP(\theta_b)$
$x_0 \oplus x_2, x_1, x_2$	00	13.6839°	45°	−56.25°	45°
	01	13.6839°	45°	−78.75°	45°
	11	13.6839°	45°	−101.25°	45°
	10	13.6839°	45°	−123.75°	45°
$x_0, x_1, x_2 \oplus x_0$	00	13.6839°	45°	−56.25°	45°
	01	13.6839°	45°	−78.75°	45°
	11	31.3161°	45°	−101.25°	45°
	10	31.3161°	45°	−123.75°	45°
$x_0 \oplus x_2, x_1, x_0$	00	13.6839°	45°	−56.25°	45°
	01	13.6839°	45°	−78.75°	45°
	11	31.3161°	45°	−101.25°	45°
	10	31.3161°	45°	−123.75°	45°
$x_0 \oplus x_2, x_1 \oplus x_2, x_0$	00	13.6839°	45°	−56.25°	45°
	01	13.6839°	45°	−78.75°	45°
	11	31.3161°	45°	−101.25°	45°
	10	31.3161°	45°	−123.75°	45°

4.1.2.2 Unitary rotations by Bob

In this general communications network implementation of a QRAC, Bob would perform a unitary rotation about some Bloch sphere axis if $x_2 = 1$. From table 4.1, we can see that for the first three tasks, Bob would perform a unitary rotation on the qubit state about the x-axis whereas for the last task, a π rotation about the z-axis is performed. Experimentally, one can implement a unitary rotation about any of the Bloch sphere axes by using a configuration of one HWP and two QWPs. Although not necessary, but before presenting the specific wave plate configurations and settings for each axial Bloch sphere rotation, it is perhaps worthwhile to present the generally well known matrix representations of both HWPs and QWPs [23; 82].

$$HWP(\theta) = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix} \tag{4.3}$$

$$QWP(\theta) = \frac{(1+i)}{2} \begin{pmatrix} 1 - i\cos(2\theta) & -i\sin(2\theta) \\ -i\sin(2\theta) & 1 + i\cos(2\theta) \end{pmatrix} \tag{4.4}$$

In [23], some configurations of these wave plates are provided that can implement the rotation of a given input state along the x,y and z-axis of the Bloch sphere. These configurations are presented below and

provide a practically simpler solution for the task but are not unique in purpose.

1. Configuration of wave plates for x-axis rotation:

$$QWP(\frac{\pi}{2})HWP(\gamma)QWP(\frac{\pi}{2}) = \begin{pmatrix} \cos(2\gamma) & -i\sin(2\gamma) \\ -i\sin(2\gamma) & \cos(2\gamma) \end{pmatrix} \tag{4.5}$$

2. Configuration of wave plates for y-axis rotation:

$$HWP(0)HWP(\gamma) = \begin{pmatrix} \cos(2\gamma) & \sin(2\gamma) \\ -\sin(2\gamma) & \cos(2\gamma) \end{pmatrix} \tag{4.6}$$

3. Configuration of wave plates for z-axis rotation:

$$QWP(\frac{\pi}{4})HWP(\gamma)QWP(\frac{\pi}{4}) = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i(4\gamma+\pi)} \end{pmatrix} \tag{4.7}$$

For implementing an R_x rotation, the HWP setting γ can be calculated by simply dividing the given rotation for each task with 4. This division by factor 4 represents the translation of the Bloch sphere rotation angle to the HWP angle. In addition, it is clear from eq. 4.7 that the same configuration was also used for introducing ϕ for a given state of Alice in the state preparation scheme. To implement the desired unitary rotations for R_z, γ is calculated in the same manner as β was calculated in section 4.1.2.1. The complete settings used by Bob in order to perform unitary rotations about x and z-axis are given below in table 4.3.

Table 4.3: The complete settings for Bob to perform $R_x(\pi), R_x(\frac{3\pi}{2}), R_x(\frac{\pi}{2})$ and $R_z(\pi)$ unitary rotations for the four tasks.

Different Tasks	State	Unitary by Bob				
C		$x_2 = 0$	$x_2 = 1$			
	x_0x_1		QWP	$HWP(\gamma)$	QWP	
$x_0 \oplus x_2, x_1, x_2$	00	$\mathbb{1}$	90°	45°	90°	$R_x(\pi)$
	01	$\mathbb{1}$	90°	45°	90°	
	11	$\mathbb{1}$	90°	45°	90°	
	10	$\mathbb{1}$	90°	45°	90°	
$x_0, x_1, x_2 \oplus x_0$	00	$\mathbb{1}$	90°	67.5°	90°	$R_x(\frac{3\pi}{2})$
	01	$\mathbb{1}$	90°	67.5°	90°	
	11	$\mathbb{1}$	90°	67.5°	90°	
	10	$\mathbb{1}$	90°	67.5°	90°	
$x_0 \oplus x_2, x_1, x_0$	00	$\mathbb{1}$	90°	22.5°	90°	$R_x(\frac{\pi}{2})$
	01	$\mathbb{1}$	90°	22.5°	90°	
	11	$\mathbb{1}$	90°	22.5°	90°	
	10	$\mathbb{1}$	90°	22.5°	90°	
$x_0 \oplus x_2, x_1 \oplus x_2, x_0$	00	$\mathbb{1}$	45°	−90°	45°	$R_z(\pi)$
	01	$\mathbb{1}$	45°	−90°	45°	
	11	$\mathbb{1}$	45°	−90°	45°	
	10	$\mathbb{1}$	45°	−90°	45°	

For the case when $x_2 = 0$, no unitary rotation is performed by Bob. Here the orientation of Bob's wave plates is set such that an identity transformation is performed. This corresponds to the following wave plate settings $QWP(\pi/4), HWP(-\pi/4), QWP(\pi/4)$ and the incoming state is communicated to the measurement device as it is.

4.1.2.3 Measurements performed by Charlie

Charlie's task is to perform a measurement in the $\sigma_y, \sigma_x, \sigma_z$ bases depending upon his input y. In the section 2.3.3, it was demonstrated how measurements in the σ_z, σ_x bases can be experimentally applied. However, as the protocol also demands a measurement choice of σ_y, a combination of HWP, QWP and PBS is used to analyze the incoming qubit state into any of the three measurement bases. This is possible as HWP and QWP together can rotate the polarization state $|H\rangle$ to any other pure qubit state. The settings of the HWP and QWP in conjunction with the functionality of the PBS decide the projection of a given state onto the eigenvectors of the measurement basis. For measurements in the $\sigma_y, \sigma_x, \sigma_z$ bases, the corresponding HWP and QWP settings are given in table 4.4.

Table 4.4: HWP and QWP settings to perform a measurement in the $\sigma_y, \sigma_x, \sigma_z$ bases.

HWP	QWP	Measurement Basis
0°	−45°	σ_y
22.5°	0°	σ_x
0°	0°	σ_z

4.1.2.4 Experimental results

The experimental results for the four QRAC tasks will now be presented. The success probabilities for each task were estimated from the detection events in the two APDs at the two output ports of the PBS in the measurement device. The APDs and the electronic photon coincidence counting system used were the same as in the previous experiments. On average, $\approx$ 10,000 cps were recorded for each measurement setting whereas the total measurement time was 10 s. The average experimental results corresponding to each task are listed in table 4.5 and the detailed results for each task are provided in appendix 7.4 in tables 7.2, 7.3, 7.4 and 7.5 respectively.

Table 4.5: Experimentally estimated success probabilities for the four distributed QRAC tasks. P^Q_{exp} represents the experimental values of P and the corresponding uncertainties.

QRAC Task	Transformation	P^Q_{exp}
$x_0 \oplus x_2, x_1, x_2$	$R_x(\pi)$	0.790 ± 0.018
$x_0, x_1, x_2 \oplus x_0$	$R_x(3\pi/2)$	0.787 ± 0.018
$x_0 \oplus x_2, x_1, x_0$	$R_x(\pi/2)$	0.788 ± 0.018
$x_0 \oplus x_2, x_1 \oplus x_2, x_0$	$R_z(\pi)$	0.788 ± 0.017

The estimated results are observed to be in good agreement with the optimal success probability ($P^Q = 0.7887$) for the QRAC.

4.2 Quantum solution to the dining cryptographers problem

Information exchange between people is an extremely common occurrence in our lives and in the context, it is greatly emphasized to establish secure means of information exchange between communicating parties such that only the sender and the receiver are familiar with the contents of the communicated message. In addition, considering another important aspect, in certain scenarios the identities of communicating participants can also be highly sensitive information depending on the of delicacy of the communication. This makes the privacy and protecting the privacy of the communicating participants paramount in such situations. However, to ensure that the secrecy and confidentiality of this information will be upheld upon communication is no easy task. This is in essence due to the source traceability of any information communicated through classical means. The issue becomes highly sensitive especially in situations where a group of people are tasked to mutually agree upon a given option, preferably from a number of possibilities. It should come as no surprise that the topic of anonymous transmission and secrecy of identity is well researched, and is vital for communication protocols such as Byzantine agreement [83], key distribution [84] and digital pseudo signature [85].

One of the most common means for a group of people to collectively decide something is through the act of voting. Regardless of the democratic nature of the process, depending upon circumstances and implications, it is often imperative that the decision of an individual voter is kept confidential despite the overall outcome being known to all. This is almost impossible through classical means of communication. To achieve the secrecy of a voters identity, a number of secret voting protocols, employing cryptographic principles, as anonymous broadcast [86] and blind signatures [87; 88] have been presented.

Anyhow, implementing a trustworthy voting protocol requires that a number of prerequisites are adhered to. Some of these conditions include security, verifiability, and privacy [89]. The security condition establishes honesty with the guarantee that each legitimate voter casts only a single vote with no room for any participant to discover the intermediate result. The verifiability condition, as the name suggests, imposes that the genuineness of the outcome can be verified by any voter without the need to disclose how (s)he voted. The third condition deals with keeping the anonymity of the voters as under no circumstances should the individual choices of the voters be revealed. Voting schemes that satisfy

the first two conditions are easier to implement [90] but maintaining the anonymity of a voter is harder to achieve due to the traceability implications described previously. In the context, both classical and quantum solutions to the anonymity problem have been explored. In the coming sections, a brief introduction to these protocols is provided followed by our approach for a quantum solution, which we believe is novel, efficient and simpler to implement as compared to other classical and quantum solutions.

4.2.1 The dining cryptographers problem and anonymous veto voting

In the context of identity protection, the commonly employed classical means for ensuring anonymity involves the use of trusted third parties to spread information while keeping the identities of the senders a secret [91; 92]. The use of multiple servers to randomize the ordering of the messages is also explored for this purpose [86]. In another approach for anonymous communication of classical messages, Chaum introduced the problem of dining cryptographers and presented a classical protocol that could allow secure transmission of a message while maintaining the sender's anonymity [93]. Before going into any details, it is important to briefly provide an outline to the dining cryptographers problem.

In this problem, three cryptographers that work for the national security agency (NSA) go to a fancy restaurant for dinner. After the dinner, the cryptographers are promptly informed by the waiter that their bill has been anonymously paid. At this point, although they respect each others right for secret generosity, they would like to know if the NSA had anything to do with the payment. Chaum presented the following protocol to resolve the cryptographers dilemma.

The three cryptographers agree on a strategy where they decide to flip an unbiased coin (each of them participates) between them such that only the one flipping the coin and the cryptographer to his right would see the flipping outcome. Afterwards, each of them declares whether the two coins (s)he observed had the same or different outcomes. In the case, where the dinner is paid by one of them, the respective cryptographer states the opposite of what (s)he actually observed. In this strategy, an odd number of reported 'differences' imply that a cryptographer paid for the dinner without giving any information about the cryptographer that actually paid. For even reported 'differences', the payment is attributed to the NSA given that only a single payment for the dinner was made.

At the time, it was claimed that, if all the parties are sincere, then the

protocol is unconditionally secure [93] and in the case when the payment is attributed to the NSA, the issue of anonymity becomes irrelevant. For the sake of understanding, let us consider a scenario where one of the cryptographers, who did not pay, intends to find out which of the other cryptographers had paid. In the first case, let us consider that the two coins he observed had the same outcomes while the others claimed "different" and "same" respectively. If the unknown outcome is the same as what the cryptographer had observed then the one who claimed "different" is the one that paid. On the other hand, if the unknown outcome is different to his outcomes, the one who claimed "same" is the one that paid. The two possibilities though have equal probabilities to occur. In the second case, the two coins that the cryptographer observed had different outcomes. If the other two cryptographers, claimed "different" outcomes then the one who is closest to the coin with the same outcome as the unknown coin, is the one that paid. However, if the two cryptographers claimed the "same" outcomes then the one who is closest to the coin with the opposite outcome as the unknown coin, is the one that paid. But in each of these scenarios, a cryptographer that did not pay gains no information about the cryptographer that paid.

The implementation of this classical protocol is done as follows: The three diners, pairwise, establish secret bits, $k_{ij} = 0, 1$. Every one of them announces the sum (modulo 2) of his/her bits if (s)he did not pay, or the negation of this sum if (s)he did. Afterwards, each cryptographer sums up all of the announced bits and calculates the corresponding XOR. If the result is 1, this implies that the dinner was paid for by one of the diners whereas a result of 0 indicates that the NSA paid for the dinner.

A number of drawbacks were later observed with the protocol rendering it impractical. Along with the drastically increased complexity of implementation that arises as the group of participants enlarges, every time an even number of partners pay this appears as a non-payment as their subsequent alterations cancel each other out. This problem is known as the collision problem and as a consequence, the employer agency is wrongly deduced as the payer. Moreover, the honesty of the involved participants is a significant issue as well as a number of them may conspire to trace the diner who has paid. This is otherwise known as the collision loophole. It is pertinent to mention here that if one eliminates the collision problem, the dining cryptographer question is equivalent to the anonymous veto problem where a group of people unanimously decide something, as described previously.

Later on, another classical solution was presented in [94] where the protocol was shown to overcome all the limitations that are generally as-

sociated with the proposed dining cryptographer networks. These weaknesses include complex key setup, collisions and sensitivity of disruptions. The dining cryptographer problem is reconsidered in a different light as an anonymous veto protocol where the security of this protocol lies in the computational complexity under the Decision Diffie-Hellman (DDH) assumption. The mentioned DDH assumption typifies a computational complexity assumption in a problem that deals with discrete logarithms in cyclic groups. The DDH assumption has been shown to be critical for the strong security of various classical cryptography protocols [95].

The anonymous veto protocol is a consequent variant of the dining cryptographer protocol, where the problem is re-interpreted such that the three diners vote against the statement that "no cryptographer has paid". This is why the term voting is replaced by the term veto. If somebody vetoes then it is implied that a payment is made and if nobody vetoes, then this corresponds to a payment by the NSA.

In the proposed anonymous vetoing protocol, the senders use a Schnorr's signature (zero-knowledge proof) to demonstrate their knowledge of discrete algorithms in each round without disclosing them. The use of these zero-knowledge proofs is quite common in cryptography where it has been used to prevent different attacks [96–98]. By employing the assumption that the broadcast channel available to each voter is reliable and two broadcast rounds, it preserves the sender's anonymity with acceptable security unless all the participants are compromised. In another variant of the protocol, it was also shown that the use of zero-knowledge proofs can be avoided if the parties disclose their announcements before each broadcast round. This though comes at the cost of increased network communication. This simple yet efficient protocol has its security based in the computational hardness that relies on the difficulty in reversing of some calculations or through restrictions on the number of dishonest participants [99]. Bearing in mind the ever increasing available computational power, the former is simply an arbitrary assumption.

In addition to these classical protocols, quantum resources that obey the quantum mechanical laws have also been explored for practical and secure solution to the identity anonymity problem. As the use of quantum resources in a number of communication tasks has demonstrated advantages that extend well beyond the capabilities of the classical systems, intuition strongly suggests that quantum systems are probably better suited in achieving the current goal. The first attempted quantum solution made use of the generalized Greenberger-Horne-Zeilinger (GHZ) states [1] for the traceless communication of bits and qubits [100]. It was

[1] GHZ state is a multiqubit maximally entangled state such that that it leads

suggested that entangled states seem to be a very attractive candidate for traceless unidentifiable transmissions. Since then a number of quantum protocols [101; 102], also employing entangled states for the task, have been reported. Furthermore, other quantum solutions based on correlations of multipartite GHZ states have also been presented [90; 103] where the former proposed protocols to guarantee voting anonymity and the latter proposed secure quantum protocol for both the anonymous veto and dining cryptographer predicaments.

The quantum protocol presented in [103] exploits the multi-qubit GHZ correlation and the GHZ paradox [1] for demonstrating a generalized secure quantum protocol that promises unconditional security while simultaneously prohibiting multiple payments. In a three party description of the protocol, the involved parties share genuine GHZ states where a payment is represented by local unitary operations on the shared states. Randomly selected copies of the shared states can then be used to distinguish the cases of even and odd payments. The final step of the protocol is used to distinguish between zero and double pay scenarios for the even payment case and the single and triple pay scenarios for the odd case. The diners perform different unitary operations in the even and odd cases depending on if they have paid or or not. The product of the local measurements represents if zero or double payments were made in the even case or if single/triple payments were made in the odd case. In the event of double and triple payments, the subsequent payments are cancelled. The protocol can detect events of multiple payments, which is yet to be demonstrated for a classical protocol while promising unconditional security. The generalized protocol however, is based on the assumption that no multiple payments occur. The unconditional security for both the dining cryptographer and the anonymous veto protocols rely on fundamental features of GHZ correlations that are related to quantum nonlocality [103].

Regardless of the unconditional security promise of the protocol, the protocol requires $(N+1)^N$-dimensional Hilbert space for N voters. This is no easy task as generating entangled states of many particles is a nontrivial task and suffers greatly from low generation rates and low state fidelity along with complicated practical difficulties. However, there is an

to a maximum violation of Bell's inequality for a given set of observables. The GHZ states are successfully employed in a wide range of problems in quantum information theory, details of which are beyond the scope of this thesis.

[1] Greenberger, Horne and Zeilinger (GHZ) demonstrated a direct contradiction of quantum mechanics with local realism without using any statistical inequality [104].

alternative solution where the essential correlations of the GHZ states can be effectively simulated by phase shifts performed sequentially by a set of users on a single particle. This is followed by a measurement that is conducted by a receiver. This approach significantly reduces the complexity of the experiment as only a single quantum system is used. In the next section, such a quantum protocol for the dining cryptographer problem, based on the distribution of a single quantum system between N parties, is introduced and experimentally demonstrated.

4.2.2 Sequential one-way quantum protocol

Our novel quantum protocol for the dining cryptographer problem is implemented using a flying particle scheme in a sequential one-way communication and consists of $N + 2$ participants. Here N represents the total number of voters, each provided with sets of phase shifters to perform local unitary transformations on the distributed particle, along with a sender (S) and a receiver (R). S prepares the quantum system that is distributed among the voters before arriving to receiver (R) that performs a measurement on the received particle. A three-voter scheme is shown in Fig. 4.4.

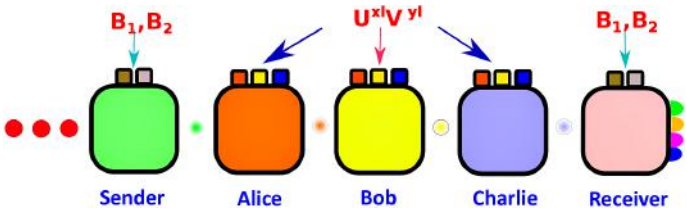

Figure 4.4: A schematic representation of the $(N + 2)$-party protocol where $N = 3$. S prepares a random state, which is propagated through N voters that either perform a unitary transformation ($U^{x_l}V^{y_l}$; $x_l, y_l \in \{0, 1\}$) on it or not. Upon arrival of a particle, the receiver performs a measurement in a randomly chosen basis.

The protocol itself has its foundation in the concept of MUBs. For a d dimensional system, consider the states $\{\{|j, l\rangle\}_j\}_{l=0}^{d-1}$ where j represents the basis and l denotes a corresponding state in the basis. The computational basis corresponds to the case when $j = d$ and the total number of bases depends on the dimension d. For powers of primes, sets of MUBs are informationally complete ($j = 0, 1, ..., d$) as (d+1) MUBs are informationally complete for dimension d [105]. For the case, prime

$d \geq 2$ we have

$$\begin{array}{c} |d,l\rangle = |k\rangle, \\ \forall_{j<d} \quad |j,l\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{kl+jk^2} |k\rangle. \\ \omega = e^{\frac{2\pi i}{d}} \end{array} \tag{4.8}$$

From Eq. (4.8) we can observe that there are two important unitary transformations.

$$V = \mathrm{Diag}(1, \omega, \omega^2, \omega^3, ...) \tag{4.9}$$

permutes the vectors within the basis and corresponds to performing a veto in the scheme, while

$$U = \mathrm{Diag}(1, \omega, \omega^4, \omega^9, ...) \tag{4.10}$$

cyclically changes the bases but neither of these operations affects the computational basis. The operation U transforms the state to an unbiased state and hence is used to safeguard the privacy of a voter in the protocol.

The generalized and finer details of the protocol are part of *article V*, included in this thesis. Here, the attention is instead on providing a three-party description and the corresponding experimental realization of the protocol. In the case of three voters/diners the protocol can be implemented by using a quantum system of dimension $d = 4$.

$$\begin{aligned} B_1 &= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}, \\ B_2 &= \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & i & -1 & i \\ 1 & -1 & 1 & 1 \\ -1 & i & 1 & i \end{pmatrix}. \end{aligned} \tag{4.11}$$

Now, similar to the generalized case of (4.8), there exists a transformation that permutes between the vectors within the basis. This is represented by $V = \mathrm{Diag}(1, i, -1, -i)$ and will be the veto transformation in the protocol. In addition, a transformation that changes one basis into another (non-computational bases) is represented by $U = \mathrm{Diag}(1, 1, 1, -1)$ and will be used for establishing the infrastructure in the protocol. This transformation is important as it protects the user's

privacy and ensures that an eavesdropper has no way of knowing which basis to measure in. Both these transformations are diagonal and as we have only used two bases (B_1 and B_2), this implies that the secret numbers used by the voters in the infrastructure round are simply bits. Moreover, U and V can also be generalized for squares of primes ($d = p^2$) and other powers of prime and an example of this is provided in article V.

4.2.3 The three-party description

To understand how this single photon transmission protocol works, we start with a simplified description for which we assume that S and R are two trustable parties. S randomly prepares a single photon in one of the 8 (4-d) states from (4.11) and we define the computational basis as: $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$. The photon is then passed on to the voters, one by one, before reaching R who randomly chooses between basis B_1 or B_2 to perform a measurement. The complete protocol is implemented in two rounds: the infrastructure establishment round and the voting round. The infrastructure establishment round is important to protect the voter's privacy and in this round each voter upon receiving the photon performs a unitary transformation U^{x_l} where $x_l = \{0, 1\}$ and index l denotes the voter. For $\sum_{l=1}^{N} x_l = 0 \bmod 2$, the overall effect of the U's will be unity. Afterwards, R and S discuss what was prepared and what was measured and if they find a match in their choices, the infrastructure establishment round is complete and the voters choice of x_l is accepted. In case of a disagreement between S and R, the round has to be repeated and voters will have to choose again.

In the voting round, there are two runs and S prepares the following two states $\frac{1}{2}(\{|0\rangle + |1\rangle + |2\rangle \pm |3\rangle\})$ in a random order for these two runs. In other words, it will be one of the two states in each run where the order is chosen randomly for each voting round. All the voters would perform unitary transformation U, if they decided so in the previous round. If they want to perform a veto (a veto implies an admission of payment from the participant), they will also apply the V transformation. For each voting round, R randomly chooses one of the two basis to measure in such that the chosen basis is used in both runs.

Now, S sends a different state in each run whereas R measures in the same basis for the two runs. This implies that they will have an agreement in one of the two runs and only this specific run will be considered a valid run. Exactly which run is relevant will be known once they disclose their choices for the two runs. For the relevant runs, if the state

measured by R is the state that was prepared by S, this implies that no veto was performed by a cryptographer and the diners have come to a unanimous conclusion that its the NSA that has paid for the dinner. However, if R measured a different state to what S communicated, this implies that a veto was performed.

Now that we understand how the dining cryptographer protocol works for three parties, we will consider this three-party protocol in a broader sense such that S and R are not trustable and may conspire or plan individually to produce false results.

The procedure of the infrastructure establishment and voting rounds is the same as described above where $U^{x_l}V$ represents the choice of veto. Here, a veto cast by a participant implies that (s)he paid for the dinner.

For each run of the experiment, each voter will yield a trit where the three different values of the trit correspond to three different scenarios. A value of 0 corresponds to a no action (equivalent to identity transformation) from the voter. A value of 1 corresponds to the infrastructure establishment round where the parties decide to apply a U transformation or not. Lastly, a value of 2 corresponds to the voting round.

In a given run of the protocol, S will randomly prepare any one of the eight states from (4.11) and R randomly chooses between B_1 and B_2 for measurement. Afterwards, they disclose the list of states that were sent and measured in each run to the three voters. The voters however do not reveal anything about their actions and their respective trits. The first step by the observers is to discard all those protocol runs where R chose the wrong measurement basis. Now that only those runs are left when the basis choice of both S and R matched, the voters disclose their random trits but not their choice of action (I, U, V, UV). The first step is to discard all the runs when their respective trits had different values.

All the remaining rounds correspond to the three scenarios when all the parties had same trit values. In the first case, 000, all the parties chose to perform no unitary transformations. These rounds can certify the honesty/dishonesty of S and R. If R measured the same state that S had prepared, they are likely honest and dishonest otherwise. The second case, 111, points to the infrastructure establishment round. Again, If R measured the same state that S had prepared, the voters choice of U is correct and incorrect otherwise. For the final possibility, 222, The voters had the opportunity to perform any desired operation as this is the voting round.

The outcome of the voting round demonstrates the applicability and the success of the protocol. We shall review the possible outcomes while keeping in mind that

1. $\sum_{l=1}^{N} x_l = 0 \bmod 2$ conforms to a unity effect of performed U's.
2. Performing a V transformation permutes between the basis vectors.
3. S and R's choices of basis, for state preparation and measurement, match.
4. The voters are limited to a single veto.

Without knowing the state prepared by S, R cannot identify the number of vetoes casted by the parties from the state (s)he measured. Additionally, if S chooses randomly between B_1 and B_2 for state preparation, this rules out the possibility of the voters to cheat. In principle, the intentions of all involved in the protocol can be validated from the above procedure. Considering that everybody played by the rules and R measured the same state as prepared by S, this follows that the voters actions unanimously point to the conclusion that the dinner was paid by the NSA. However, R's detection of a state that is different to what S prepared concludes that a veto was indeed performed and the information about the number of vetoes can be deduced from the measured state.

4.2.4 Experimental demonstration of the quantum protocol

Now, we will consider the experimental demonstration of this three-party (Alice, Bob and Charlie) dining cryptographer and anonymous veto quantum protocol. A quantum system of four dimensions is required and for our experiment we choose single photons for this task. The source of these single photons is a heralded single photon source, presented in section 1.2.2, where a four level physical system using a single photon is prepared by making use of polarization and path degrees of freedom of the single photon. The four level quantum system is prepared using the 2-path and 2-polarization information encoding scheme, described previously in section 2.3.1 with the notable difference that the two spatial modes are now represented as $|1\rangle$ and $|2\rangle$. The complete experimental setup is shown in Fig. 4.5.

4.2.4.1 State preparation

To prepare a ququart state, we define the following four basis states $|H,1\rangle$, $|V,1\rangle$, $|H,2\rangle$ and $|V,2\rangle$. Using these basis states, we can write a given ququart state as $a|H,1\rangle + b|V,1\rangle + c|H,2\rangle + d|V,2\rangle$.

In this N+2 party protocol, S has a choice to randomly prepare any state from the set 4.11. From now on these states, defined by column

j (where j=1,2,3,4) for a given basis B_i (where i=1,2), will be referred to as $S_{i,j}$. The general state preparation setup required to create any of the eight input states would consist of a 50/50 BS that splits incoming light into the two spatial paths of the BS with equal intensities. Each spatial path of the (50/50) BS would also contain a sequence of a HWP and a QWP to control the population and the respective phase between different polarization states. The two wave plates are followed by a phase plate (PP) to introduce a desired phase shift setting (Φ) between the two paths. In the case of states from set 4.11, this corresponds to a phase shift of either 0 or π between the two paths. Using this experimental scheme (Fig. 4.5), one can create any of the eight states from 4.11 and after the PP in both paths, the state can be written as

$$\begin{aligned} |\psi_{gen}\rangle = \frac{1}{\sqrt{2}}\big((\cos(2\alpha)|H,1\rangle + e^{i\phi_1}\sin(2\alpha)|V,1\rangle) \\ +e^{i\Phi}(\cos(2\beta)|H,2\rangle + e^{i\phi_2}\sin(2\beta)|V,2\rangle)\big) \end{aligned} \tag{4.12}$$

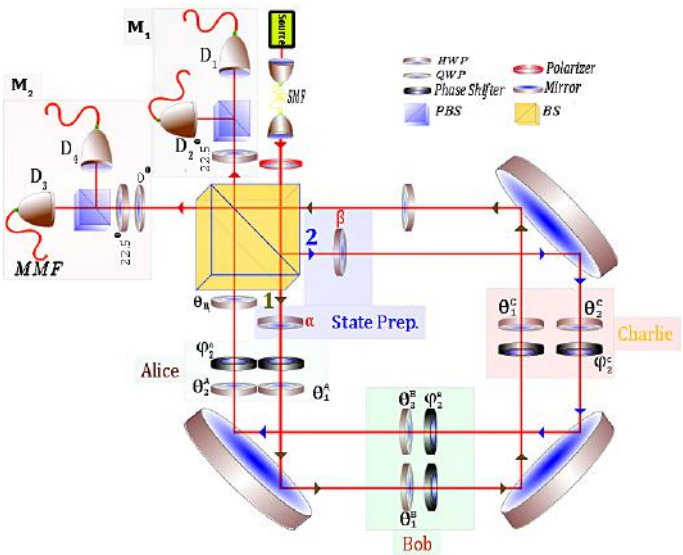

Figure 4.5: Experimental setup: Sender S prepares states $S_{1,1}, S_{1,3}, S_{2,1}$ through suitable orientations of α and β stationed in the two output ports (1), (2) of the BS. The three voters implement their desired transformations through suitable tilting of HWPs in path (1) and (2) and a phase shift setting PP in path (2) by mounting them on rotational stages. A HWP just before the BS in path (2) allows the receiver to choose the measurement basis. To implement the measurement, stations M_1 and M_2.

Considering that S can prepare eight different input states and the two unitary transformation choices for each party along with the two options of basis (B_1 and B_2) to perform a measurement in, this results in a total of 256 measurements for the two stages of the protocol. Bearing this in mind, for a proof of principle demonstration, we opted to prepare the states $S_{1,1} = (1,1,1,1)^T$ and $S_{2,1} = (1,1,1,-1)^T$ for the infrastructure establishment round and the states $S_{1,1} = (1,1,1,1)^T$, $S_{1,3} = (1,-1,1,-1)^T$ for the voting round. These states were only selected as an example and in principle, any of the eight states from the two bases could have been chosen for either round. The complete experimental setup is shown in Fig. 4.5 and now the different experimental parts will be described one by one. For the above four states, the general state preparation setup is reduced to only a single HWP ($\alpha = \beta = \pm 22.5°$) in each of the two ports of the BS and are parametrized as

$$\begin{aligned} |\psi\rangle = \frac{1}{2}\big((\cos(2\alpha)|H,1\rangle \pm \sin(2\alpha)|V,1\rangle) \\ +e^{i\Phi}(\cos(2\beta)|H,2\rangle \pm \sin(2\beta)|V,2\rangle)\big) \end{aligned} \tag{4.13}$$

4.2.4.2 Protocol implementation

The experimental implementation of the protocol requires an interferometric setup. Although, there are a number of choices available for the task, for the sake of high interference stability, practicality and ease of implementation, a Sagnac interferometer with shifted paths was chosen. The advantage is that this scheme allows us to manipulate each path individually. Such interferometers are renowned for their superior stability capabilities and the ease to obtain equal path lengths in the two paths due to the geometrical design.

Each participant, (Alice, Bob and Charlie) can in essence perform four unitary transformations during the complete protocol. These four transformations are $\mathbb{1}$, U, V and UV respectively. Some of these unitary transformations require a certain phase between the two orthogonal polarization states ($|H\rangle$ and $|V\rangle$) in each path. In addition, a relative phase between the two spatial paths may also be required. There are a number of ways to experimentally implement this, for our part, we choose to provide all the three parties with one HWP and a PP in each path (see Fig. 4.5). The two HWPs in each path were permanently oriented at 0° and along with the PP in path (2), were mounted on rotational stages. The PP in path (1) is only for compensation purposes and as such was not mounted on a rotational stage.

Now by appropriately tilting the two HWPs, one can introduce the desired phase between the $|H\rangle$ and $|V\rangle$ polarizations in each path. Let θ_1 denote this phase for path (1) and θ_2 for path (2). The relative phase between the two paths is represented as (ϕ_2) and was implemented by tilting the PP in path (2). For our transformations, ϕ_2 corresponds to either 0 or π. The corresponding θ_1, θ_2 and ϕ_2 values for each transformation is shown in table 4.6.

Table 4.6: Implementation of U, V and UV transformations. θ_1 represents the phase between the two linear polarizations $|H\rangle$ and $|V\rangle$ in path (1). θ_2 represents the same for path (2) and ϕ_2 is the relative phase between the two paths.

Transformation	θ_1	θ_2	ϕ_2
U	0	π	0
V	$\pi/2$	$\pi/2$	π
UV	$\pi/2$	$-\pi/2$	π

The receiver R can choose between the two basis B_1 and B_2 for performing a measurement. To implement the choice of a measurement basis, a HWP was introduced in the path (2) just before the BS where the beams in the two paths recombined. The basis selection was made possible through the appropriate tilting of this HWP (oriented at 0°) to set the required phase θ_{B_i} ($i = \{1, 2\}$) between the polarization states in path (2). This is done in the same manner as the implementation of the unitary transformations above and for this purpose the HWP was also mounted on a rotational stage. A HWP was also added in path (1) for compensation.

Following the output ports of the BS are measurement stations M_1 and M_2 that were used as polarization analysis stations. M_1 consisted of a HWP (22.5°) followed by a PBS. The single photons arriving at the two output ports of the PBS were coupled to multimode fibers that were connected to single photon APDs (D_1 and D_2). The APDs used in this experiment are the same as in every other experiment in this thesis. M_2 is similar to M_1 with the only difference being the presence of a QWP (0°) in the beginning. The two APDs at the output ports of the PBS were denoted as D_3 and D_4. The presence of the QWP in M_2 is important as the four states, in the two bases, are projected onto the four different detectors. In this experiment, the detectors D_1, D_2, D_3 and D_4 correspond to states $S_{1,1}$, $S_{1,3}$, $S_{1,4}$ and $S_{1,2}$ when B_1 is chosen and to states $S_{2,1}$, $S_{2,3}$ $S_{2,4}$ and $S_{2,2}$ for the basis B_2.

All the required probabilities for the protocol were estimated from the

single photon detection counts in each detector. On an average, ≈60,000 cps were detected for each experimental setting with a total measurement time of 10 s. The experimental results are shown in tables 4.7, 4.8 and 4.9. Table 4.7 represents the infrastructure establishment round where S randomly prepares one state from each basis ($S_{1,1}$ and $S_{2,1}$). Table 4.8 represents the voting round where S randomly decides between $S_{1,1}$ and $S_{1,3}$ as the input state. Table 4.9 represents that a wrong measurement basis choice of R leads to inconclusive results as all the detectors click with almost equal probabilities. Our obtained experimental results, for each measurement setting in either round, agree with the expected predictions of quantum mechanics. This validates the successful application of our quantum solution for the 3-party dining cryptographers and anonymous veto problems. In addition, the interferometric visibility of our setup is above 89% for all measurements. This leads to more than 93% success probability in each run of the protocol (see Table 4.8). The estimated errors include Poissonian counting statistics and systematic errors. The innate imperfections of the used optical components as BS, PBSs and HWPs are the main responsible sources of systematic errors in this experiment.

Table 4.7: Infrastructure establishment round. The individual states for each basis correspond to the four detectors as follows: D_1 corresponds to states $S_{1,1}$ and $S_{2,1}$, D_2 corresponds to $S_{1,3}$ and $S_{2,3}$, D_3 corresponds to $S_{1,4}$ and $S_{2,4}$ and D_4 corresponds to $S_{1,2}$ and $S_{2,2}$ respectively. Here, the first index indicates the basis and the second indicates the corresponding state. S prepares randomly $S_{1,1}$ between $S_{2,1}$ while B measures randomly in $B1$ or B_2. The estimated success probabilities from detection events in each detector are also shown.

Sender	*Alice*	*Bob*	*Charlie*	*Receiver*	D_1	D_2	D_3	D_4
$S_{1,1}$	**𝟙**	**𝟙**	**𝟙**	B_1	0.934 ± 0.015	0.006 ± 0.007	0.034 ± 0.007	0.026 ± 0.007
$S_{1,1}$	**𝟙**	**𝟙**	**U**	B_1	0.263 ± 0.022	0.232 ± 0.022	0.231 ± 0.022	0.274 ± 0.022
$S_{1,1}$	**𝟙**	**U**	**U**	B_1	0.975 ± 0.015	0.006 ± 0.007	0.006 ± 0.007	0.013 ± 0.007
$S_{1,1}$	**U**	**U**	**U**	B_1	0.263 ± 0.022	0.244 ± 0.022	0.242 ± 0.022	0.252 ± 0.022
$S_{1,1}$	**𝟙**	**𝟙**	**𝟙**	B_2	0.269 ± 0.022	0.241 ± 0.022	0.243 ± 0.022	0.247 ± 0.022
$S_{1,1}$	**I**	**U**	**U**	B_2	0.240 ± 0.022	0.243 ± 0.022	0.251 ± 0.022	0.266 ± 0.022
$S_{2,1}$	**𝟙**	**𝟙**	**𝟙**	B_1	0.257 ± 0.022	0.245 ± 0.022	0.226 ± 0.022	0.272 ± 0.022
$S_{2,1}$	**I**	**U**	**U**	B_1	0.251 ± 0.022	0.243 ± 0.022	0.242 ± 0.022	0.265 ± 0.022
$S_{2,1}$	**𝟙**	**𝟙**	**𝟙**	B_2	0.952 ± 0.015	0.004 ± 0.007	0.022 ± 0.007	0.022 ± 0.007
$S_{2,1}$	**𝟙**	**𝟙**	**U**	B_2	0.251 ± 0.022	0.235 ± 0.022	0.256 ± 0.022	0.258 ± 0.022
$S_{2,1}$	**I**	**U**	**U**	B_2	0.983 ± 0.015	0.004 ± 0.007	0.002 ± 0.007	0.011 ± 0.007
$S_{2,1}$	**U**	**U**	**U**	B_2	0.240 ± 0.022	0.261 ± 0.022	0.246 ± 0.022	0.253 ± 0.022

Table 4.8: Voting Round. S prepares states $S_{1,1}$ or $S_{1,3}$. The voters choose to perform a veto if they decided in the last round while R measures in B_1 basis. Measurements with $U^{x_l}V^{y_l}$ with $x_l, y_l \in \{0,1\}$ are shown and the success probabilities from the detection events in each detector are estimated for every run.

Sender	*Alice*	*Bob*	*Charlie*	D_1	D_2	D_3	D_4
$S_{1,1}$	𝟙	𝟙	𝟙	0.966 ± 0.015	0.006 ± 0.007	0.010 ± 0.007	0.018 ± 0.007
$S_{1,1}$	𝟙	𝟙	V	0.016 ± 0.007	0.015 ± 0.007	0.008 ± 0.007	0.962 ± 0.015
$S_{1,1}$	𝟙	V	V	0.011 ± 0.007	0.961 ± 0.015	0.011 ± 0.007	0.017 ± 0.007
$S_{1,1}$	V	V	V	0.011 ± 0.007	0.012 ± 0.007	0.974 ± 0.015	0.001 ± 0.007
$S_{1,1}$	𝟙	U	U	0.975 ± 0.015	0.006 ± 0.007	0.006 ± 0.007	0.013 ± 0.007
$S_{1,1}$	V	U	U	0.023 ± 0.007	0.028 ± 0.007	0.006 ± 0.007	0.943 ± 0.015
$S_{1,1}$	𝟙	U	UV	0.032 ± 0.007	0.026 ± 0.007	0.004 ± 0.007	0.938 ± 0.015
$S_{1,1}$	V	U	UV	0.014 ± 0.007	0.94 ± 0.015	0.023 ± 0.007	0.024 ± 0.007
$S_{1,1}$	𝟙	UV	UV	0.004 ± 0.007	0.961 ± 0.015	0.015 ± 0.007	0.020 ± 0.007
$S_{1,1}$	V	UV	UV	0.014 ± 0.007	0.023 ± 0.007	0.956 ± 0.015	0.007 ± 0.007
Sender	*Alice*	*Bob*	*Charlie*	D_1	D_2	D_3	D_4
$S_{1,3}$	𝟙	𝟙	𝟙	0.003 ± 0.007	0.966 ± 0.015	0.015 ± 0.007	0.017 ± 0.007
$S_{1,3}$	𝟙	𝟙	V	0.024 ± 0.007	0.030 ± 0.007	0.941 ± 0.015	0.006 ± 0.007
$S_{1,3}$	𝟙	V	V	0.955 ± 0.015	0.004 ± 0.007	0.022 ± 0.007	0.019 ± 0.007
$S_{1,3}$	V	V	V	0.020 ± 0.007	0.019 ± 0.007	0.015 ± 0.007	0.960 ± 0.015
$S_{1,3}$	𝟙	U	U	0.002 ± 0.007	0.960 ± 0.015	0.022 ± 0.007	0.016 ± 0.007
$S_{1,3}$	V	U	U	0.018 ± 0.007	0.028 ± 0.007	0.946 ± 0.015	0.008 ± 0.007
$S_{1,3}$	𝟙	U	UV	0.018 ± 0.007	0.024 ± 0.007	0.953 ± 0.015	0.006 ± 0.007
$S_{1,3}$	V	U	UV	0.935 ± 0.015	0.012 ± 0.007	0.026 ± 0.007	0.028 ± 0.007
$S_{1,3}$	𝟙	UV	UV	0.954 ± 0.015	0.006 ± 0.007	0.022 ± 0.007	0.018 ± 0.007
$S_{1,3}$	V	UV	UV	0.015 ± 0.007	0.018 ± 0.007	0.004 ± 0.007	0.963 ± 0.015

Table 4.9: Voting Round. S prepares states $S_{1,1}$ or $S_{2,1}$. The voters choose to perform a veto if they decided in the last round while R measures in either of the bases B_1 or B_2. Every time R chooses the wrong basis, all detectors click with equal probabilities.

Sender	*Alice*	*Bob*	*Charlie*	*Receiver*	D_1	D_2	D_3	D_4
$S_{1,1}$	𝟙	𝟙	𝟙	B_2	0.257 ± 0.022	0.255 ± 0.022	0.247 ± 0.022	0.241 ± 0.022
$S_{1,1}$	𝟙	V	V	B_2	0.249 ± 0.022	0.249 ± 0.022	0.249 ± 0.022	0.253 ± 0.022
$S_{2,1}$	𝟙	𝟙	𝟙	B_1	0.252 ± 0.022	0.239 ± 0.022	0.272 ± 0.022	0.237 ± 0.022
$S_{2,1}$	𝟙	𝟙	V	B_1	0.258 ± 0.022	0.256 ± 0.022	0.254 ± 0.022	0.232 ± 0.022
$S_{2,1}$	𝟙	V	V	B_1	0.256 ± 0.022	0.262 ± 0.022	0.241 ± 0.022	0.242 ± 0.022
$S_{2,1}$	V	V	V	B_1	0.251 ± 0.022	0.254 ± 0.022	0.252 ± 0.022	0.244 ± 0.022

5. Color Centers in Diamond

5.1 Introduction

Defect centers in solid state materials, along with other similar systems, have shown traits that make them attractive not only from a single photon emission view point but also from a quantum computation perspective. In the next two chapters, the aim is to study the scope of a specific defect center, namely the nitrogen-vacancy (NV), as a potential single photon emitting source. For this purpose, detailed studies of this color center's properties have been carried out, with a particular emphasis on the single photon emission characteristics.

It is important to mention here that in addition to the color centers in solid state materials, there are a number of other alternatives that have also demonstrated efficient single photon emission. These include isolated systems as single atoms, trapped ions, single molecules and quantum dots, as was introduced in section 1.2.1. For solid state systems, a major advantage lies in their potential scalability through already established and developed fabrication techniques that are used in the semiconductor industry. In diamond, the previously mentioned NV center has recently appeared as a highly promising candidate for applications in quantum information processing and technologies [106–108] and as diamond is host to this and a number of other defect centers, it makes sense to start by briefly discussing what makes diamond such a unique host material.

5.1.1 Diamond

Diamond is a beautiful and exotic structure that has always captured man's imagination. It is a gemstone that has enjoyed a special societal position as a mark of beauty, riches and material wealth. The word diamond comes from the Greek language, meaning *unbreakable*, and it is the hardest, most thermally conductive material known to man. Diamond, although transparent in its purest form, is found in different shapes and colors where the color is a measure of its purity and reveals information about pre-existing impurities (all of which luminesce at dif-

ferent wavelengths). This strong interest in diamond has lead to a great desire in understanding its characteristics, resulting in the extensive use in a wide range of industrial, research and medical applications [109]. So much so that diamond is rigorously studied and investigated in the fields of gemology, material sciences, biology and physics among others. The composition of diamond is rather extraordinary as it consists of the lowest mass element that can form, possess and maintain a symmetric, tightly bounded (covalent) stable lattice structure. It is almost entirely made up of carbon atoms (>99%, a carbon allotrope) that are arranged in a partial variation of a standard face centered cubic structure (FCC). This cubic structure is also commonly referred to as diamond cubic or diamond lattice. The atypical diamond lattice results in extremely strong covalent bonding between adjacent carbon atoms leading to extreme hardness of the structure. In the lattice structure, a basis of two carbon atoms are associated with each lattice point such that the structure itself resembles two inter-penetrating FCC lattices that offset from one another along a body diagonal by one-quarter of its length. The lattice structure of diamond is shown in Fig. 5.1.

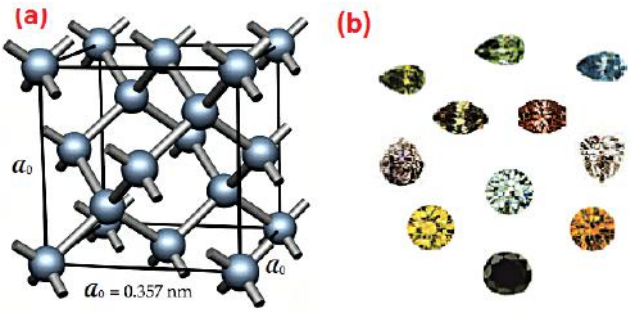

Figure 5.1: (a) Latttice structure of diamond. (b) Different colored diamonds due to various occurring impurities. Figures are reproduced from [110] and [111].

Here, the attributes that make diamond a highly attractive element for several advanced applications are briefly touched upon. It is diamagnetic in nature, has a large band gap of 5.5 eV, corresponding to an ultraviolet wavelength of 225 nm, is a very good insulator and is optically transparent with a broad transmission spectrum. The Debye temperature (T_{debye}) of diamond is 2000 K, which implies that there are almost no optical phonons at room temperature. This leads to the advantage that the spin-orbital coupling and spin relaxation time due to phonons is very low as compared to other materials and compounds, i.e., 10 ms in

diamond at 300 K whereas 10^{-4} s in GaAs at 2 K. Additionally, it possesses inherently the highest thermal conductivity of all elements and provides the maximum resistance to thermal shock. All of the above characteristics make it viable for a wide range of applications ranging from medical, industrial, research, telecommunications, data storage to military applications. Other common applications involve usage in cutting and polishing tools, microwave and infrared applications, high power optical lasers and x-ray applications.

5.1.2 Classification and fabrication of diamond

In its purest form, diamond is originally transparent and colorless due to the large band gap that renders it optically transparent to the visible light. This is not to say that diamond is always colorless and is found in many different colors where the coloration arises due to different crystallographic defects. These defects refer to irregularities in the lattice structure along with the existence of various substitutional impurities (nitrogen, boron, nickel etc.) where a carbon atom is often replaced by an alien impurity atom. This results in defect centers with different energy characteristics such that they are able to absorb and emit at different wavelengths. It is due to this wide emission range that diamond appears in different colors, e.g., yellow (Nitrogen), green (Nickel), blue (Boron), brown (lattice defects) and many other colors (as shown in Fig. 5.1).

For application purposes, diamond is used in both naturally occurring and synthetic forms. Natural diamonds are formed under extremely intense pressure and heat conditions at an approximated depth of almost 200 kilometers, over a period of billions of years ($\sim$3.3), and are brought to the surface due to deep volcanic eruptions. However, to meet the large demand, diamond is also prepared synthetically. Synthetic diamond is prepared in the laboratories using a number of techniques with high-pressure high-temperature synthesis (HPHT) and chemical vapor deposition (CVD) being two of the commonly used methods. HPHT synthesis to produce diamond has been used commercially since 1950 where the process to create natural diamonds is emulated in a laboratory. These extremely high temperature and pressure conditions are vital as they render carbon crystals of diamond structure much more stable compared to other forms of carbon crystals. Diamond produced in this way can either be single crystal or polycrystalline and is mainly classified into type Ib [112]. The HPHT method is the most commonly used method for diamond fabrication but requires large time, energy, space

and monetary investments. Setting up a process with such high pressure and temperature values is no trivial task either.

Another widely used diamond fabrication method is the CVD method. It differs entirely from the HPHT process and is not as commonly used commercially. The growth technique is homoepitaxial and requires a diamond surface as a seed layer [113; 114]. The CVD diamond growth process incorporates a plasma mixture of a hydrocarbon gas (that is rich in carbon content, commonly methane 0.5-5%), and hydrogen gas at low pressure conditions (∼30 mbar) inside a vacuum chamber. The process depends greatly on the role of atomic hydrogen that stops graphite formation and supports diamond growth under these conditions. For this purpose, molecular hydrogen is converted into atomic hydrogen by gas activation through the application of microwaves (hundreds of watts at ∼2 GHz), electric discharge or hot filaments. Atomic hydrogen is important for creating dangling bonds of carbon atoms by breaking the bonds of the reconstructed surface. Methane in this heated gas mixture (between 900°C to 1200°C) is converted to CH_3 where its carbon atom attaches itself to an available carbon atom on the diamond surface. This process continues until a diamond film is grown in a layer by layer manner [111; 115; 116]. Diamond films can be grown with very high purity depending upon the quality of the gas mixture. However the low growth rate of diamond films and the sample quality has been a concern. Using deuterium instead of hydrogen has shown a significant increase in the sample quality [114]. Moreover, the structural defects inside the diamond lattice are shown to be reduced by controlling the growth speed. These different growth methods make it possible to prepare diamond in different, shapes, sizes, thicknesses and grades (quality parameter) to exploit its different properties. Natural diamond has a similar crystalline structure to synthetic diamonds but provides some peculiar advantages compared to its synthetic counterpart. Naturally occurring diamond is rid of metallic inclusions that affect its electrical conductivity. Many synthetic types of diamond contain higher impurity concentrations that lead to discolouration and make diamond more ductile [117].

5.1.3 Different types of diamond

Diamond is commonly classified into two main and further subtypes depending upon the nature of defects and impurities present where the concentration of impurities is generally represented as parts per million (ppm). The two main types are termed as type I and type II where type I is mostly naturally occurring diamond with a higher nitrogen concen-

tration whereas, type II is synthetically produced and is quite rare in nature. This classification of diamond is also indicative of the nitrogen concentration, which is much larger in type I as compared to type II. Type I consists of two subtypes, type Ia and type Ib, where type Ia is further subdivided into two more subtypes; type IaA and type IaB. Table 5.1 represents this classification of diamond based upon nitrogen configuration and concentration.

Table 5.1: Types of diamond with subsequent sub-types [118].

<table>
<tr><td colspan="3">Type I
Naturally occurring (>98%)
High Nitrogen concentration
100 - 3000 ppm</td><td colspan="2">Type II
Synthetically Prepared (rare in nature)
Very low Nitrogen concentration
< 5 ppm</td></tr>
<tr><td colspan="3">Two further subtypes</td><td colspan="2">Two further subtypes</td></tr>
<tr><td colspan="2">Type Ia</td><td>Type Ib</td><td>Type IIa</td><td>Type IIb</td></tr>
<tr><td colspan="2">Aggregated Nitrogen

< 3000 ppm</td><td>Single substitut-
ional Nitrogen
< 500 ppm</td><td>Nitrogen is the
major impurity
<∼1 ppm
Electrically insulating</td><td>Boron is the
major impurity
<∼1 ppm
p-type semiconductor</td></tr>
<tr><td colspan="2">Two further subtypes</td><td></td><td></td><td></td></tr>
<tr><td>Type IaA</td><td>Type IaB</td><td></td><td></td><td></td></tr>
<tr><td>Nitrogen in
A aggregate form</td><td>Nitrogen in
B aggregate form</td><td></td><td></td><td></td></tr>
</table>

5.1.4 Defect centers in diamond

Defect centers in diamond are caused by impurities, lattice irregularities and imperfections. More than 500 different kinds of defect centers have been discovered in diamond and a number of them have been shown to be stable single photon emitters at room temperature. These include Silicon vacancy centers (SiV), Chromium related centers, Nickel related centers (NE8) and the Nitrogen vacancy center (NV) among others. These defect centers are photo-stable at room temperature with emission properties that differ widely from each other. For instance, the NV center has a broad emission range (>100 nm) with a zero phonon line (ZPL) at 637 nm. On the other hand, the NE8 centers and SiV centers have shown narrow ZPLs around 800 and at 738 nm respectively [15]. NE8 centers are hard to fabricate at a single crystal level due to the demand for four nitrogen atoms to form a complex with the nickel atom [119] and are not ideal from a scalability perspective. SiV centers initially suffered from low emission rates due to a high temperature dependent nonradiative decay term, rendering them unattractive from an implementation perspective. However, recently SiV centers in nanodiamond crystals grown using the CVD process have shown exceptional single photon source traits (brightness and narrow linewidth of emission) [120] making them highly attractive for the task. In the same perspective, NV centers have also been observed to be highly stable single photon emitters that do not

photo-bleach under continuous intense optical illumination. In addition, the electronic structure of NV centers has shown aspects that allows its electron spin state to be optically polarized, coherently manipulated using microwave radiations and protectively read out. Even though NV centers have excellent magneto-spin properties that make them attractive for quantum computation and network applications, here NV centers are exclusively studied from the standpoint of a single photon emitter. For this purpose, optical properties of single NV centers in nano and bulk diamond samples have been investigated. Moreover, almost all potential applications depend considerably on increased photon collection efficiency of the NV center emission and different methods to enhance this collection efficiency are also been explored.

5.2 Nitrogen-Vacancy (NV) center

The NV center is a molecular structure in the band gap of diamond that is optically accessible with a ground and excited state gap of around 2 eV. It is shown to be optically stable and does not photo-bleach under continuous optical excitation. This is important for applications that demand high but stable single photon count rates for prolonged periods of time. Moreover, the ground state electronic spin of the NV center is stable at room temperature, can be optically initialized, coherently manipulated and optically read out. In addition, advance fabrication methods for NV creation along with the demonstration of long spin coherence times (≈ 0.6 s [121]) and coupling to surrounding electronic and nuclear spins make NV center a promising qubit candidate and is considered to be a potentially promising building block for a wide range of applications such as quantum computers [122], highly sensitive magnetic [123–125] and electric field [126] sensors, stable single photon sources for quantum communication protocols [20] and in-vivo markers for biological cells [127].

5.2.1 Physical and electronic structure of an NV center

NV centers are usually formed inside a diamond lattice when a substitutional nitrogen atom ends up with a vacancy in one of the adjacent lattice sites (see Fig. 5.2) orientated along the [111] crystalline direction [128]. Nitrogen is a paramagnetic defect and is a major impurity in naturally occurring diamonds where single NV centers are formed overtime due to the migration of vacancies to the nitrogen atom sites [129]. A commonly used method to create NV centers in diamonds with high ni-

trogen concentration is high energy electron irradiation. This results in a homogeneous vacancy density inside the diamond and upon annealing at high temperatures $\sim 800°C$ for a prolonged period of time, these vacancies become mobilized and are trapped by the substitutional nitrogen, forming NV centers [128]. It is a regularly used procedure for creating NV centers in nanodiamonds [130]. Synthetically produced diamonds also contain NV centers that are formed during the growth process. Ultra high purity diamond samples (type IIa) on the other hand, contain a very small quantity of NV centers with apprximately one NV center every 10^4 μm^3 [115]. In these ultra pure samples, one commonly used method to create NV centers is through the implantation of nitrogen ions at high energies (several Kev or MeV) inside an accelerator. Vacancies and carbon interstitials are created through collisions as these ions come to rest inside the sample. Most of these ions stop at interstitial positions and upon annealing, NV centers are locally formed [131].

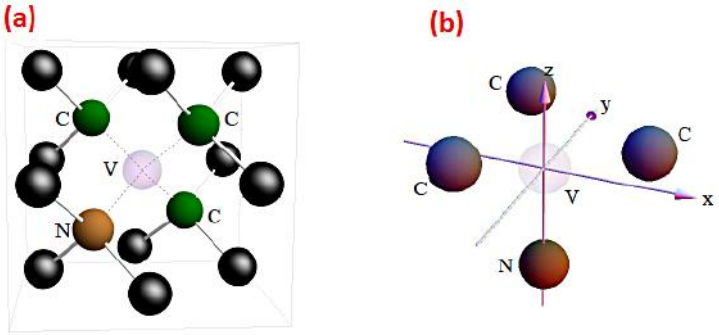

Figure 5.2: (a) Schematic structure of an NV center in the diamond lattice. The substitutional nitrogen atom (brown) is adjacent to the vacancy (pink hollow) and the three nearest carbon atoms in black are shown. (b) The NV center along with the adjacent carbon atoms in the adopted coordinate system where NV center's symmetry axis is along the z-axis. Figures are reproduced from [132]

.

The physical structure of the NV center (Fig. 5.2) is quite important as it determines the nature of its electronic state and the permitted electric dipole-dipole interactions between these electronic states. NV centers have been shown to posess $C_{3\nu}$ symmetry [128] where the nitrogen atom and the vacancy form a symmetry axis. The $C_{3\nu}$ symmetry governs the nature of its electronic states that depends upon their transformation under $C_{3\nu}$ operations. Under these operations, the diamond lattice surrounding the NV center is invarient under rotations of $2\pi n/3$

performed around the vertical symmetry axis (z-axis) of the NV center. It is also invarient under reflections in the three planes containing the vertical symmetry axis and the nearest carbon sites in the diamond lattice [107]. The nature of the electronic states is determined under such operations where both the electronic ground and excited states form spin triplet states (S=1). Likewise, the resulting optical and spin properties of the NV center depend greatly upon the characteristic electronic states structure.

An NV center usually exists in two charge states, the neutral state NV^0 and the negatively charged state NV^-. In the neutral state NV^0, it exhibits a zero phonon line (ZPL) at 574 nm [133] whereas the negatively charged state exhibits a zero phonon line (ZPL) at 637 nm, corresponding to an energy of 1.945 eV [134; 135]. Both charge states are photostable and co-exist [136] but depending on the Fermi level inside the lattice, one of them dominates the other [137; 138]. Moreover, the two charged states have been shown to transform depending upon the excitation energy and intensity. This phenomenon is known as photochromic effect and describes the photon induced change in the state of NV center due to a change in the band gaps between two charge states [133; 139; 140]. The work performed in this thesis targets exclusively the negatively charged state (NV^-) as this is the state with desired properties for many applications [141]. Keeping this in mind, from now on the negatively charged state NV^- will simply be referred to as the NV center.

In the charged state, the NV center has six electrons associated with it and an electron spin of $S = 1$ in the ground and excited states [142]. Out of these six electrons, two are the valence electrons from the nitrogen atom, three are associated with the dangling bonds of the carbon atom surrounding the vacancy [143; 144] and the final electron is trapped from the diamond lattice (from a nearby substitutional nitrogen atom or surface states). The electronic configurations of the ground and excited states are well known and can be explained using either the six-electron model [135; 143; 145] or the two-hole model [146].

The electronic structure of an NV center can be characterized by a three-level energy model (see Fig. 5.3) consisting of a ground state $^3A_2$, excited state ^3E and intermediate singlet states $^1A_1$ and ^1E.

The electronic ground state $^3A_2$ is a spin triplet state where the corresponding spin-spin interactions lead to a first order splitting of the $^3A_2$ [142; 143; 147]. The resulting fine structure levels are denoted by their spin-orbit symmetry and ($m_s = 0, \pm 1$) spin projections [132] where m_s is the quantum number of the spin projection along the symmetry axis of the NV center. D_{gs} represents the splitting between the

$m_s = 0$, $m_s = \pm 1$ spin projections and is equivalent to ~ 2.87 GHz at room temperature. D_{gs}, sensitive to temperature and pressure changes, is commonly referred to as zero field splitting (zfs) in the absence of an external magnetic field or other perturbations. This fine structure splitting of the NV center's ground state was first demonstrated using electron spin resonance (ESR) measurements in the late 1970s [148; 149].

The electronic excited state ^3E can be described as a spin triplet (but an orbital doublet) at room temperature with a zero-field splitting of 1.42 GHz in the absence of any external magnetic field. Moreover, the degeneracy of $m_s = \pm 1$ states for both the $^3A_2$ and ^3E states can be lifted by applying an external magnetic field along the NV center's symmetry axis. This Zeeman splitting appears in the form of two resonances in the ESR measurements and the corresponding frequency splitting is dependent on the strength of the applied field.

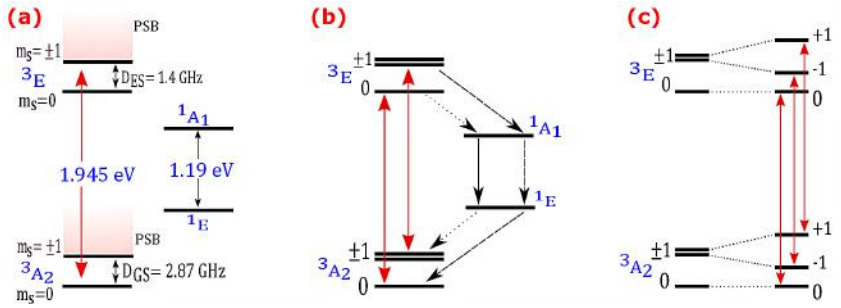

Figure 5.3: (a) Simplified electronic structure of NV center at room temperature with the two ZPL transitions shown in red and black respectively. The PSB is also shown in orange. (b) Six level scheme of the NV center. Solid red lines indicate radiative transitions between the $m_s = 0$ and $m_s = \pm 1$ states. The dashed lines and the dotted lines indicate the strong and weak non-radiative transitions through the singlet states. (c) Zeeman slitting of the $m_s = \pm 1$ spin ground and excited states in the presence of external magnetic field is shown.

The previously stated orbital doublet nature of the excited state is often ignored in the context due to the effective averaging of the spin properties of the orbitals at room temperature, caused by the rapid inter-orbital transitions within the excited state [150]. The room temperature fine structure of ^3E was first experimentally reported by Epstein al. in 2005 using optically detected magnetic resonance (ODMR) studies of single and ensemble color centers [151]. Studies have shown that the ^3E fine structure level is considerably different at cryogenic temperatures as compared to the room temperature fine structure. This is attributed to

the phonon dependent averaging of the low temperature fine structure branches that result in the observed room temperature fine structure [150]. These details however are deemed beyond the scope of this thesis.

Furthermore, there exist metastable spin singlet states ($^1A_1$ and ^1E) between the excited and ground states [142; 152; 153]. These intermediate singlet states play an important role in the spin-dynamics of NV center under optical excitation [154], which will be addressed in the next section. The existence of the intermediate singlet states was first demonstrated in [155] through the observation of a ZPL at 1042 nm (1.190 eV), representing a transition between the $^1A_1$ and ^1E states under optical excitation (excitation energy $>$ 1.945 eV). However, the ZPL associated with the 637 nm transition is approximated to be 10^4 times stronger than the 1042 nm infrared band transition. In comparison to this, the passage through the metastable state can be considered as a dark process and in light of the experimental studies that are carried out in this thesis, it is sufficient to review the intermediate singlet states as one metastable state. The above discussion of NV center's electronic structure would be incomplete without addressing the excited state lifetimes that differ in bulk and nanodiamonds. For nanodiamonds, the reported excited state lifetime is approximately $\sim 25\ ns$ whereas for the bulky counterparts, it is $\sim 12\ ns$ for the $m_s = 0$ spin projection and $\sim 8\ ns$ for the $m_s = \pm 1$ state. The lifetime of the upper intermediate singlet state is reported to be $\ll 30\ ns$ whereas the for longer lived lower intermediate state is about $\sim 300\ ns$ [142].

5.2.2 Accessible optical transitions

The band gap between the ground and excited triplet states is ~2 eV and a ZPL emission at 637 nm (1.945 eV) represents the $^3A_2$ to ^3E transitions (Fig. 5.3). The observed emission spectrum from an optically excited NV center is quite broad (637 nm - 750 nm) with an emission peak around 675 nm. This broadness arises from the presence of a continuum of vibronic states and is attributed to the excitation and absorption of a local vibration of NV center [128]. The vibronic excited states appear at higher frequencies in absorption and lower frequencies in emission such that, under off-resonant laser (above-band excitation with 532 nm) excitation of these vibronic states, the NV center relaxes into one of the electronic excited states through phonon emission [107]. This seems to occur due to the extremely small lifetime of the vibronic states ($\lll 1\ ps$) as compared to the excited state lifetime, which is in nanoseconds and the ensuing emission of an NV center is primarily into the phonon

sideband with a large full width half maximum (FWHM). The emission into the ZPL is very small and even at cryogenic temperatures ($<$ 10 K) accounts for $\sim 4\%$ of the total emission [156]. The detection of NV center fluorescence is made possible due to the high quantum efficiency of radiative relaxation ($\eta \sim 0.99$) and the relatively short excited state lifetime.

5.2.3 Spin dependent optical transitions

Using off-resonant coherent optical excitation at room temperature, both the $m_s = 0$ and $m_s = \pm 1$ transitions can be excited and the corresponding radiative decay from the excited $m_s = (0, \pm 1)$ states is primarily spin conserving (see Fig. 5.3). In addition, there are means for non-radiative decay to the ground state through the intermediate singlet states where the strength of these non-radiative transitions depends on the initial spin projection. The radiative decay from the $m_s = 0$ excited state is spin conserving along with a weak possibility of non-radiative decay through the singlet states. The non-radiative decay through the intermediate singlet states leads to spin-flips under optical cycling [132; 142; 157] but occurs mostly for the $m_s = \pm 1$ states. This leads to a population shelving into the singlet states and creates darker periods between the excited and ground states due to the much larger lifetime of the intermediate state. This behaviour is shown to be especially prominent under intense optical excitation and is also responsible for the bunching effect observed in the fluorescence autocorrelation functions of NV centres [158].

The decay of the singlet states is inherently dark [159] and is mostly into the $m_s = 0$ ground state. This allows for the optical initialization and polarization of the NV electron spin into the $m_s = 0$ state using off-resonant excitation, followed by short durations (μs) of no optical excitation. Published studies have indicated an estimated spin polarization between 80% and 95% using this method [157; 160]. The ground state spin polarization represents the preparation fidelity of the qubit and is an important parameter for the operation of the qubit. In addition, as the non-radiative decay through the singlet states is stronger for the $m_s = \pm 1$ excited states, the resulting fluorescence intensity varies depending on the spin projection. A fluorescence intensity contrast between $20\% - 40\%$ has been reported in different studies [129; 142; 161; 162] for the two spin projections. This spin-dependent change in fluorescence intensity provides a clear information of the spin state of the NV center.

5.2.4 NV center as an electron spin qubit

In the previous section, we discussed the suggested spin state dependent relaxation mechanism of the NV center making it possible to optically initialize and readout the electronic spin state. The electronic spin can also be readily manipulated under an applied microwave field, which is in resonance with the spin transitions ($D_{gs} = 2.87\ GHz$). Continuous off-resonant optical excitation polarizes the spin to the $m_s = 0$ level and a microwave field resonant to the spin transitions (between $m_s = 0$ to $m_s = \pm 1$) shifts the population between these two levels thus effectively enacting a two-level system. This population reorganization results in a decrease in the florescence level (Fig. 5.4a) and can be driven in the absence or presence of an oscillating external magnetic field ($\mathbf{B}$) applied perpendicularly to the spin quantization axis of the NV center. This electron spin resonance can then be optically read out and lies at 2.87 GHz (zero $\mathbf{B}$ field) or is indicated by two frequency separated transitions due to the lifted degeneracy of the $m_s = \pm 1$ states in the presence of an external $\mathbf{B}$ field (Fig. 5.4a). This separation between the transitions depends on the strength of the external magnetic field and is quantified as $2\gamma B$. Here γ is the NV gyromagnetic ratio and is equal to 2.80 MHz G^{-1}.

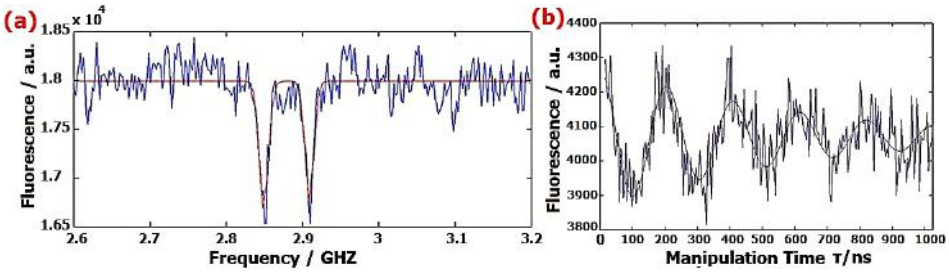

Figure 5.4: (a) Optically detected magnetic resonance (ODMR) spectrum of the NV center showing the two resonances in the presence of a small magnetic field ($\approx 12\ G$) [163]. (b) Induced Rabi oscillations between the electronic spin ground states $m_s = 0$ and $m_s = \pm 1$.

Furthermore, under resonant microwave excitation, one can drive Rabi oscillations (population oscillations [164] between the ground $m_s = 0$ and excited $m_s = \pm 1$ states, indicating a complete state transfer between the two spin states. The Rabi oscillations depend heavily on the applied microwave power and the correct microwave field frequency. An example of these population oscillations is presented in Fig. [5.4b].

It is pertinent to stress here that although preliminary work has

been done in this aspect showing the above optically detected magnetic resonance spectrum and Rabi oscillations, it is merely presented here as an introduction to the suitability and desirability of NV centers as a reliable and attractive electron spin qubit system. For this thesis, we have chosen to focus on the single photon emission attribute of the NV center and exploring different methods to enhance the emission collection efficiency from the NV centers.

5.3 Increased photon collection efficiency

Quantum technologies as secure quantum communication and quantum key distribution require very bright, on-demand and robust single photon sources at room temperatures. Additionally, other targeted applications as quantum networks and quantum computation, sensing and quantum enhanced metrology (QEM) strongly crave that the spin state information is read out before it decoheres. It is therefore not surprising that all these applications place a strong demand on a high photon detection efficiency of the NV center emission.

Even with the use of objectives with high numerical apertures (oil or water), the biggest hindrance in achieving high photon collection efficiency arises from refraction and aberration losses at the air-diamond interface caused by the large refractive index mismatch. The angle for total internal reflection (TIR) at the interface is $\theta_{TIR} = arcsin(1/n_d) \approx 25^{\circ}$ and severely limits the angular collection capacity of the microscope objective by reducing the solid angle between within which emitted photoluminescence can be collected. The goal is to come up with methods that not only lead to a collection enhancement but also do not degrade the spin coherence due to any inherent negative effects. In this regard, a number of different methods have been proposed to increase the collection efficiency. For nanodiamond crystals, it was shown that if the size of nanocrystals is chosen to be small enough then the NV center effectively emits into the free space [165; 166]. This method resulted in an increase in photon collection by a factor of 5 as compared to the previous results. In another scheme, nanodiamonds containing single NV centers were spin coated on the flat surface of commercially available hemispherical lenses (radius=1 mm) made of cubic zirconia (ZrO_2). The emitted photons were collected from the curved side and high saturation counts $\approx$ 850 kcps (stable emitter) and upto 2.4 Mcps (blinking NV) were reported under continuous optical excitation [167].

A number of methods to enhance the photon collection in bulk diamond have also been explored. In one such method, top down fabrcation

of nanowires (∼200 nm diameter and ∼2 μm length) through electron beam lithography (EBL) and reactive ion etching (RIE) in a type Ib diamond was used and a collection improvement by a factor of 10 was reported using this method [168].

Millimeter sized hemispeherical lenses [169; 170] on top of the sample surface and using millimeter scale hemispherical lenses milled in diamond [171] are other examples to improve the collection efficiency. However, there are some downsides as the former suffers from losses due to the hemispherical lens and sample surface mismatch, surface reflections and gaps between the surfaces whereas the latter is highly time consuming, requires extensive machining and is unattractive from a fabrication point of view. One alternate solution is the fabrication of micrometer scale solid immersion lenses (SILs) through focused ion beam (FIB) milling in diamond and an overall increase by a factor 10 has been reported [172; 173] using these micro SILs. In the next section, more details about this method will be provided.

In another method, vertical nanopillars in diamond membranes (30μm thick) were fabricated and structured using EBL and RIE. With a reported photon flux up to 1.7 Mcps at the time, this was the brightest reported monolithic bulk diamond structure based on single NV centers [174]. This is one of the utilized alternatives in this thesis and the fabrication details and photon collection enhancement from such nano-engineered diamond waveguides are covered in detail in the next chapter.

Other examined methods for increased photon flux from NV centers in bulk diamond include the use of optical antennas [175] and silicon dioxide gratings [176] where both these methods reported >0.5 Mcps. Lastly, a recently demonstrated circular diamond "bullseye" grating structure reported the highest recorded photon collection rate from an NV center at saturation (4.56 Mcps) [177]. It is apparent that the advancement in fabrication techniques and technological capacities have greatly contributed to enhancing the photon collection from NV centers making them more viable and thereby increasing their feasibility for implementation in quantum technologies.

5.3.1 Microscale solid immersion lenses (SIL)

Etching micrometer diameter hemispherical lenses, fabricated into a bulk diamond plate, has become one of the most commonly utilized approaches for enhancing photon collection from NVs in bulk diamond. These SILs are milled into the diamond surface using FIB and have been extensively used in recent demonstrations of novel experiments involving NV centers

[45].

In [178], the collection efficiency from an NV center inside a planar diamond surface ($\approx 5.6\%$) and at the centroid of a hemispherical lens ($\approx 28.6\%$) were calculated using the finite-difference time-domain (FDTD) method. Their estimated efficiencies are comparable with the analytical results of [179] and show a large enhancement in collection efficiency by employing microscale etched SILs. Photoluminescence from a color center at the centroid of a hemispherical SIL is perpendicular to the surface over the whole 2π solid angle of the hemisphere. The rays leave SIL in a direction normal to the SIL surface and are not refracted (see Fig. 5.5). The NA of collection is then enhanced by a value equivalent to diamond's refractive index ($n_d = 2.42$) [180]. A micrometer SIL etched into the diamond surface leads to the advantage that the refraction losses from the air-diamond interface can be avoided due to the hemispherical geometry. This considerably enhances the collection efficiency and by etching such micrometer SILs, Hadden et al. [172] reported an enhancement of the photon flux by a factor of 10.

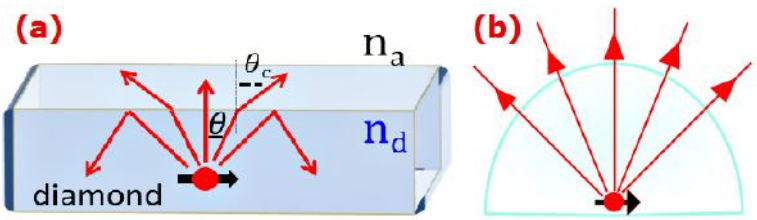

Figure 5.5: (a) Propagation of rays for a dipole (parallel orientation) under planar diamond surface. $n_a = 1$ and $n_d = 2.42$ are the refractive indices of air and diamond respectively. θ_c represents the critical angle of incidence. (b) Ray propagation for a dipole (parallel orientation) at the centroid of a hemispherical lens.

In [178], it was also reported that the position of the defect center with respect to the SIL centroid is an important parameter and the photon collection decreases significantly with a > 1 μm displacement, in any direction, from the focal point of the hemisphere. This is caused by the optical aberrations that occur due to the less than ideal positioning of NV center at the SIL's centroid [181]. For the purpose of increasing collection efficiency, it is thus vital that the fabrication process of a microscale SIL is accurate to about 1 μm. The collection efficiency can be further increased by the use of an anti-reflective (AR) coating on the SIL surface.In the next chapter, a detailed account of accurate fabrication of SILs with respect to single NV centers and the resultant increased

photon flux will be presented.

5.3.2 Nano-pillars in diamond membranes

Another reported method for enhanced photon flux collection involves the fabrication and structuring of nanopillars in diamond using EBL and RIE was presented in [174]. Their fabricated nanopillars were ∼1.2 μm long, with a top diameter of ∼400 nm and a bottom diameter of ∼900 μm. As mentioned above, at the time, this demonstration was the brightest reported monolithic structure for single NV centers. In addition, the defect center's spin coherence properties were observed to be unaffected during the fabrcation of the canonical geometry. An enlarged detection of the photon flux is made possible as the NV emission couples to the fundamental HE_{11} mode of the waveguide, which is then guided backwards and collected by the microscope objective lens (see Fig. 5.6) underneath the thin diamond sample [174; 182]. Hence, this approach is attractive as the nanopillars behave as waveguides that not only allow efficient excitation of the NV but also enhance the emitted photon collection.

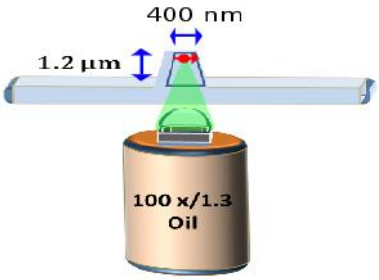

Figure 5.6: A canonical waveguide with top and bottom diameters of ∼400 nm and ∼900 nm. The excitation and PL emission is collected from the bottom surface.

Such structures show great potential and promise significant improvement over other present day capabilities especially concerning the sensing applications (magnetic field [123], electric field [126], temperature [183], strain [184]) and nuclear magnetic resonance (NMR) experiments [185–188] based on NV centers. For greater sensing sensitivity, the positioning of NV center with respect to the surface is important and such nanopillars are fabricated in very thin diamond membranes (<30 μm) where the NV centers are created very close to the surface (shallow NVs) through ion implantation and an annealing process. In this thesis, these tapered

waveguides are fabricated and section 6.4 covers the ion implantation and fabrication procedure followed by the excitation and detection of single NV centers in these nanoengineered waveguides.

6. Experimental Studies of an NV center

In the previous chapter, a brief overview of some of the important properties of NV centers was presented. This allows us to envision the potential role of NV centers in future quantum technologies such as quantum computation, secure quantum communication protocol based devices, stable and robust single photon sources, quantum registers and memories, that will be integral for future photonic networks.

All of these applications require high grade and ultra pure diamond samples along with the capability to precisely control the NV center positioning and scalability. This is vital for the spin coherence properties that are important for many quantum information applications. In addition, we must be able to excite, probe and optically address single NV centers on demand. Confocal microscopy (CM) is a well-known microscopy technique that can be used for this task and allows for efficient excitation of a single NV center, which consequently leads to high resolution imaging and optical detection of the single NV center. It was first used by Gruber et al. for observing individual NV centers in 1997 [129] and since then has emerged as the standard tool used to optically probe single defect centers. In 2000, Kurtsiefer et al. used CM to demonstrate a stable single photon source based on an NV center in diamond [20]. After successfully localizing a single NV center, the individuality of the quantum emitters was confirmed by performing an antibunching measurement using a Hanburry Brown Twiss (HBT) configuration.

6.1 Experimental setup

In the coming sections, an overview of the necessary experimental details and the complete experimental setup used in the laboratory is presented. The working setup consists of a purpose built confocal microscope (for excitation and detection of the NV center) and a HBT setup used for antibunching measurements.

6.1.1 Confocal microscopy of NV centers

Confocal microscope (CM) is a well-known microscopy technique developed for imaging biological samples, living cells and tissues. Invented in 1957 by Marvin Minsky, it increases the contrast of microscope images by restricting the observed volume (collection only from a focused spot) and by discarding the contribution from nearby unfocussed elements.
The basic working principle uses point illumination of a sample and a pinhole in an optically conjugated plane to eliminate contributions arising from the unfocussed specimen. As the corresponding excitation volume coincides with the detection volume, the procedure is termed as confocal microscopy. This is different from conventional wide field microscopy where the whole sample is illuminated at once and the resulting photoluminescence (PL) is collected by a detector [189]. The CM technique results in a slightly better imaging resolution and a higher image contrast albeit at the cost of a longer scanning and interval time. The spatial resolution of CM is diffraction limited to an order of wavelength and hence two neighbouring NV centers can only be individually distinguished if the distance between them is larger than that. Our interest in using CM as a tool solely lies in its capability to selectively excite and probe individual NV centers through optical sectioning and elimination of the defocussed light. As confocal microscopy has been around for a long time, it is a well known and an extensively used imaging procedure whose advantages and general use has been covered in depth in numerous manuscripts and books [190]. In regards to this, only a concise functional insight is provided here and instead the emphasis is to elaborate the technical description and operation of the purpose built confocal microscope setup used in our experiments.
The employed CM setup is different to conventional confocal microscopes in the sense that we have replaced the standard pinhole with a standard single mode fiber (SMF) where the core of the fiber acts as a pinhole to reject any out of focus light. The advantage of using a SMF as a pinhole is twofold. Firstly, it allows for efficient rejection of unwanted light and optimal mode matching between the optical mode collected from the NV center and the mode of the fiber. Secondly, along with ease of alignment, using the SMF enables us to use this single spatial mode efficiently in any scheme possible. The confocal microscope setup used in our experiments is shown in Fig. 6.1. For some measurements, that were performed during my stay at Pi3 institute at the University of Stuttgart (indicated by color scans), the confocal microscope had a standard pinhole of 50 μm diameter instead of a SMF. All the used components utilized for both

CM setups are off the shelf components.

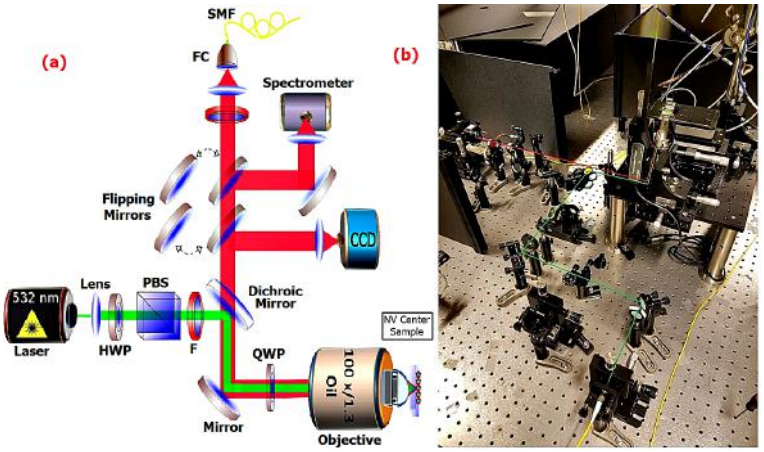

Figure 6.1: (a) Schematic representation for the confocal setup used for optical detection of NV centes in diamond. (b) The experimental setup built in the lab.

Optical probing of a given sample requires an appropriate pump laser. For our setup, the excitation laser is a (25 mW) 532 nm, Cobolt Samba®, continuous-wave (CW) diode-pumped solid state laser (DPSSL). It provides a single longitudinal mode with a high level of stability, low noise, a narrow spectral bandwidth and a long coherence length.

Emitted laser light is coupled into a SMF, using a standard fiber coupling lens. The other end of the SMF lies at the focal point (35 mm) of a plano-convex lens, which collimates the pump beam. Control of beam diameter is important so that it can matched to the aperture of the microscope objective used to image the sample. It is ensured that the excitation beam has well-defined spectral properties by the use of a spatial filter ($\sim$10 nm bandwidth around 532 nm). The laser beam arrives at a dichroic mirror, which separates the incident light from the photoluminescence (PL) of the NV center by reflecting the excitation wavelength but transmits the photoluminescence spectrum through it. A high numerical aperture (NA) microscope objective focuses the incoming light to a diffraction limited spot ($\sim \frac{\lambda_{ex}}{2NA}$) and is used to excite and collect the ensuing fluorescence from a single NV center. This objective is one of the most important components of the microscope where the resolution and photon collection efficiency depends upon its NA. The term numerical aperture is a measure of the acceptance angle of an objective and is defined as $nsin\theta$. n here is the refractive index of the

immersion medium (air, water, glycerol or oil) and θ is the maximum $\frac{1}{2}$ acceptance solid angle of the objective. An oil or water immersion medium is required to achieve numerical apertures greater than 1. An objective lens of larger NA, has higher resolving power, collects more light and therefore provides a brighter image, with a narrower depth of focus as compared to a lens of lower NA. The resolving power is an important parameter as it determines the limit of resolution, i.e., minimum detectable distance between two points. Another important factor for objectives is the magnification (M) of the objective and is defined as ratio of the size of the magnified object image to that of the object.

The microscope objective used in our setup is "Nikon Plan Fluorite", which produces a flat image across the field of view (FOV) and is corrected for aberrations (both spherical and chromatic) for a number of wavelengths. It is an oil immersion objective with a NA of 1.3, a magnification value of 100X and a working distance of 0.16 mm between the front element of the objective and the sample surface. For 3D imaging of the sample, a scanning system with fast and precise positional accuracy (nm range) is required. In our confocal microscope, a high scan rate is achieved through the movement of the sample in the x and y plane with the rest of the optics fixed. The objective is mounted on a high resolution lens positioning system from Jena (MIPOS 100) with a motion range of 100 μm that enables scanning along the z-axis. The lens positioning system is used in a closed loop feedback configuration, has high resolution (2 nm) and provides a positional accuracy of $\pm$6 nm. This positional accuracy is fundamental for the excitation of single NV centers. The samples to be probed are mounted on a 2D xy positioning system from Jena (PXY 201 CAP) that utilizes a capacitive feedback sensor technology to achieve a positional accuracy of 1 nm. It is used in a closed loop feedback configuration and provides a positional repeatability of $\pm$10 nm. This xy scanner facilitates 2D imaging of the sample, with a maximum scanning range of 200×200 μm^2, in a plane normal to the optical path. The closed loop configuration is chosen as it compensates the mechanical drift of the focal plane due to thermal effects.

Upon laser illumination, the PL from the excited NV center is first extracted and then collimated by the same microscope objective exciting the NV center. The emitted fluorescence is transmitted through the dichroic mirror (Fig. 6.1), filtered appropriately to eliminate any contribution from scattered light and to collect emission in a short range (630 - 750 nm). An eyepiece lens with a NA of 0.25 and magnification of 10X efficiently couples the arriving fluorescence light to the core of a SMF (Thorlabs, 600-800 nm). The position dependent PL measured

by the system is mapped onto a single photon counting module (SPCM, Perkin-Elmer SPCM-AQRH-14) by using a SMF. The SPCM used is a silicon avalanche photo diode (APD) and such modules are commonly selected for single photon detection in the near-infrared region. The APDs operate in Geiger mode and the working principle exploits the photoelectric effect such that the detection of a single photon leads to an avalanche breakdown in a reverse biased diode. The used APDs showed dark counts below 100 Hz, a detection efficiency of 65% at 650 nm and a dead time of ∼50 ns between detection events. The setup also contains flipping mirrors that enable optical spectrometer measurements and the visualization of the reflection beam from the sample surface through a μ-eye CCD camera (Thorlabs).

A custom coded software in tool command language (tcl) was used for scanning control of the confocal system. In addition to the on-demand scanning functionality, an automated stabilization module is also incorporated to overcome any mechanical drifts in the system. The stabilization module works by monitoring the position of the single NV center through routinely scheduled scans such that the position of the NV center is periodically updated and the system therefore does not lose focus over time. This module has proven vital in performing longer time measurements on NV centers.

6.1.2 Single photon emission

Fluorescence emission from the excited NV center is used for a range of measurements and can be utilized in different detection schemes. The fluorescence intensity can be measured directly after the SMF especially in cases where the spin state readout of the NV center is desired. This is straightforward considering that the spin of the NV center is initially polarized into the $m_s = 0$ state under constant optical excitation and the fluorescence intensity is dependent upon the spin projection. Many experiments require that the spin state read out is performed at specific times and the fluorescence measurements must be resolved in time. For this purpose, the collected emission is coupled directly to the SPCM for post processing.
In other scenarios, configurations such as the HBT are also used. A stable single photon emitter, upon relaxation, will emit only one photon at a time. The photon statistics of the detected PL must then be analyzed to ensure that it corresponds to that of a single emitter. For a given delay

τ between consecutive photons, time histograms of detected photons can be used to examine the photon distribution close to zero delay. In case of a single quantum emitter, the probability for a delay τ between successive photons should vanish as $\tau \rightarrow 0$ and an estimation of the second order auto-correlation function ($g^2(\tau)$) is pivotal in identifying this behaviour. The measurement yields the probability of detecting a photon at time τ conditional on the detection of another photon at time $\tau = 0$. This leads to a two-time expectation value for the fluorescence intensity, $<I(0)I(\tau)>$ [107]. Normalizing the above expectation value to the overall photon intensity $<I>$ provides the value of the second order correlation function for a stationary process

$$g^2(\tau) = \frac{< I(0)I(\tau) >}{| < I > |^2} \tag{6.1}$$

where $g^2(0)$ reveals the number of simultaneously existing photons. $g^2(0) < 0.5$ is considered a signature of a single photon source as for an n-photon number state $|n>$ and time $\tau \rightarrow 0$, $g^2(0)$ value scales with $(1 - \frac{1}{n})$ [191].

In the lab, $g^2(\tau)$ values can be measured by implementing a HBT configuration that allows the measurement of temporal correlations between arriving photons. At the input of the HBT, a 50/50 beam splitter (BS) splits the incoming photons equally into the two spatial modes of the BS. Afterwards, photons in both modes pass through two identical bandpass filters (SEMROCK 450-750 nm) before being collected by multi-mode fibers (MMF). The MMFs are connected to two independent SPCMs (Perkin-Elmer ARQH-14) that record the arrival of individual photons. Spatial filters are used to suppress any unwanted photons along with any infrared photons generated by the APDs upon breakdown [192]. The outputs of the two SPCMs are connected to the input channels of an autocorrelator instrument (PicoHarp 300) that records the time interval between detection events on the two SPCMs. Whenever a photon is detected at input channel 1 of the autocorrelator, a timer is started and will not be stopped until a photon is detected at the other input channel. Time τ elapsed between the two signals of the SPCMs is measured in this way. By varying the time delay between the detection events in the two detectors and using the data collected by this PicoHarp instrument, the second order correlation function $g^2(\tau)$ can be measured. The HBT setup used for these measurements is shown below in Fig. [6.2].

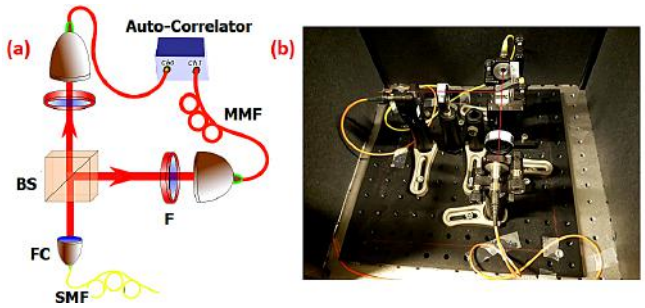

Figure 6.2: (a) Schematic representation for the HBT setup used for measuring the value of normalized second order correlation function ($g^2(\tau)$). (b) The experimental setup built in the lab.

6.2 NV centers in diamond nanocrystals and bulk diamond

In the following sections, NV centers in both diamond nanocrystals and bulk diamond are studied. Excitation and emission from localized NV centers is presented in both cases. Furthemore, antibunching measurements, by the evaluation of $g^2(\tau)$, are performed to confirm that we observing single NV centers.

6.2.1 Diamond nanocrystals

During the course of this work, several NV center samples from both natural and synthetic nanodiamond powders of type Ia and Ib were used. Some of these nanodiamond powder samples include Micron+ MDA (type Ib), from Element 6, produced from selected metal bond diamond raw material and the resulting individual particles are abrasive and blocky [117]. Another sample used is the Liquid Diamond GAF (guaranteed agglomerate-free), from microDiamant (Switzerland), where a liquid-diamond solution is prepared by mixing diamond powder in deionized water. This liquid diamond solution is provided in a high concentration of monocrystalline diamond with a mean diameter of 25 nm. Additionally, SYNDIA® SYP monocrystalline nanodiamonds produced by VAN MOPPES (Switzerland) with a median size of 25 nm were also used. These synthetic nanodiamond crystals are made out of type Ib diamond with a purity $> 99.5\%$.

The use of nanocrystal diamond powder was initially preferred over

bulky diamond substrates. A stable single photon source with a high count rate is highly desirable and the emission rate from nanodiamonds was shown to be more than that of bulky diamonds. Another advantage of nanodiamond crystals is that the reported lifetime of the excited state is ≈ 25 ns whereas the excited state lifetime in bulky diamonds is ≈ 11.6 ns [193]. The lifetime is approximately half in the case of bulk diamonds as the center radiates in a medium of high refractive index (n_d=2.4) whereas for very small nanocrystals, the NV effectively radiates in air. Additionally, the high refractive index of diamond severely limits the photon collection efficiency from bulky diamonds due to the TIR at the air-diamond interface. In order to increase the photon collection efficiency and count rate from bulky diamonds, several enhancement techniques such as solid immersion lenses (SIL) or nanopillars [171; 172; 174] have been used and this was addressed in the previous chapter. The refraction issue can be avoided in very small sized nanodiamond crystals; where a nanodiamond solution is usually spin coated on a standard microscopic glass slide such that a single NV center in a nanocrystal acts as a point source surrounded by air. The emission from this point source can then be easily collected using a microscope objective. Immersion objectives (water and oil) are also used to increase the photon collection efficiency as they provide a high numerical aperture leading to high resolution imagery and increased photon collection efficiency.

6.2.1.1 Sample preparation

The diamond sample used, Syndia SYP 0-0.05 nanodiamond (Fig. 6.3a) by VAN MOPPES (Switzerland), is a synthetic diamond powder prepared by the HPHT process. Diamond crystals are monocrystalline, pure ($> 99.5\%$), with a very low nitrogen concentration ($0.01 - 0.05\%$) [194] and a median diameter of 25 nm. Bearing in mind the lattice constant of diamond (3.57 Å), a single 50 nm nanocrystal would contain about $140^3 \sim 3.10^6$ unit cells in total. Furthermore, considering the relatively low rate of nitrogen impurities and the even lower expected amount of vacancies, most of the single nanocrystals will contain exactly one NV center making them highly ideal for addressing individual NV centers.

A very dilute solution of the nanodiamond powder was prepared with deionized water (to keep the concentration of nanocrystals low). Using a pipette, droplets of the prepared solution were put on a standard microscope glass slide (0.17 mm thickness) before it was spin coated at 2000 rounds per minute (RPM) to obtain a uniform distribution of nanocrystals on the slide. A two step cleaning process (acetone in an ultrasonic

bath followed by cleaning with isopropanol in the ultrasonic bath) was carried out to rid the microscope slide of any additional residue. The sample was then investigated in a scanning confocal microscope setup.

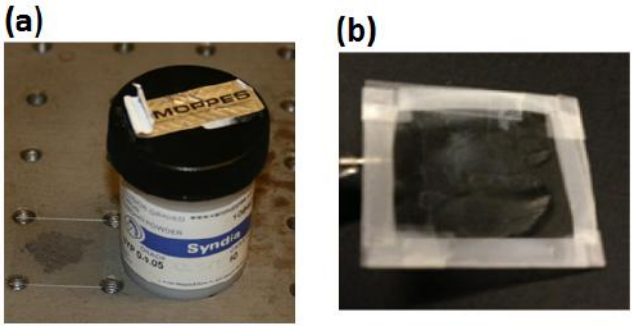

Figure 6.3: (a) Nanocrystal diamond powder from Van Moppes. (b) A microscope glass slide spin coated with a diluted nanodiamond solution in deionised water.

6.2.1.2 Detection of Single NV centers in Nanodiamond Crystals

The prepared sample was securely mounted on a two dimensional xy positioning stage with the help of a specially designed sample holder. The excitation laser beam was focused onto the sample's surface. To estimate the NV center density a broad 2D scan (80×80 μm^2) in x and y orientation is often performed. Fig. 6.4a shows one such example. As the surface scan indicated a reasonable NV center density throughout the scan region, a 10×10 μm^2 scan of a selected area was then performed (see Fig. 6.4b). This scan indicated the presence of a number of bright spots in close proximity to each other and the bright spots showed emission counts matching what would be expected from a single NV center. Afterwards, all the bright spots were confirmed to be single NV centers by performing antibunching measurements and recording the optical spectra of their photoluminescence through a purpose built spectrometer. Three such examples of single NV centers are presented in Fig. 6.5. At $\tau = 0$, the measurements clearly demonstrate a $g^2(0)$ value much smaller than 0.5, confirming this single emission nature. However, for finite delays the $g^2(\tau)$ value goes beyond 1 exhibiting photon bunching [158; 195] due to population shelving into the metastable state before eventually decaying to 1. This electron entrapment by the metastable state prevents photon emission for that period resulting in a bunching effect at longer times.

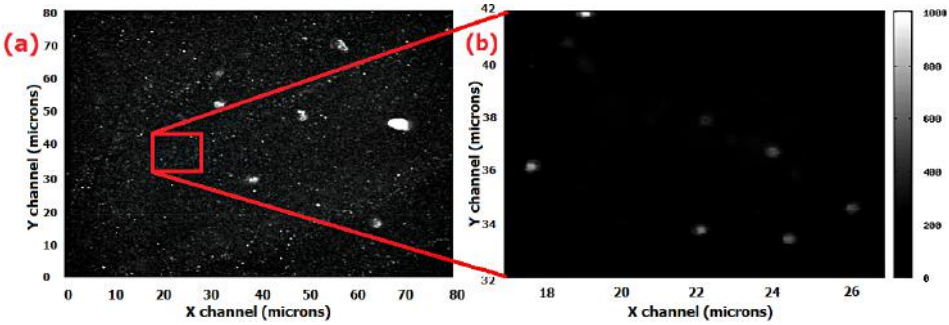

Figure 6.4: (a) A broad, 80×80 μm^2 scan, 50 nm lateral step size and 20 ms integration time, of the nanodiamond sample surface, indicating a dense NV concentration throughout the scanned area. (b) A 10×10 μm^2 scan (20 nm step-width, 40 ms integration time) of a randomly selected area of the sample. Many bright spots with counts matching single NV emission are seen.

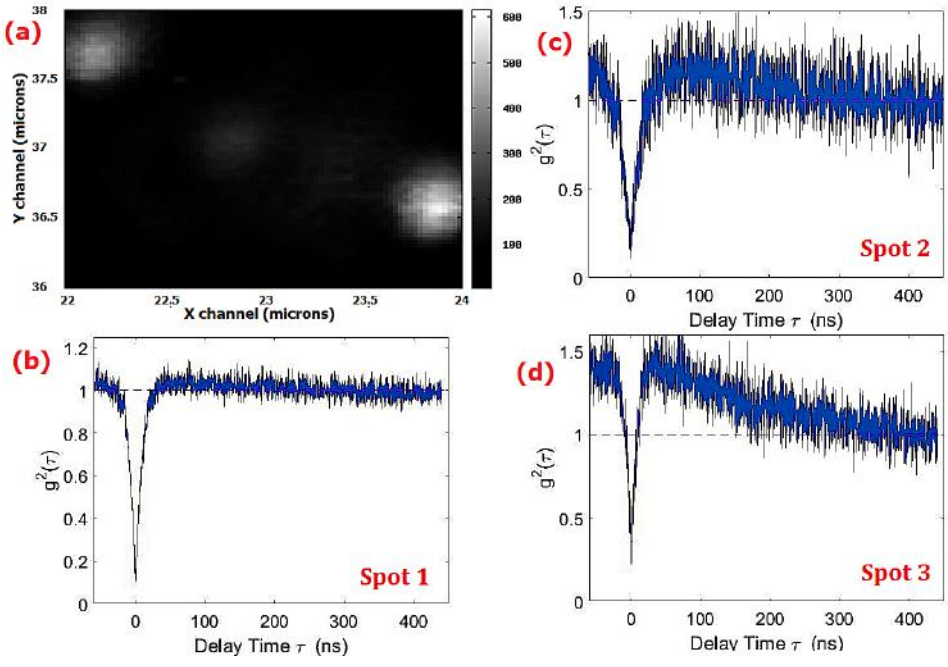

Figure 6.5: (a) A 2×2 μm^2 (20 nm lateral step size, 40 ms integration time) scan displaying 3 single NV centers ≈ 1 μm apart from each other. (b,c,d) Corresponding antibunching measurements from the three spots (left to right) are shown.

The bunching behaviour is power dependent and becomes more prominent with increasing excitation powers (spot 1 (∼0.5 mW), spot 2 (∼1.5 mW) and 3 (∼3.5 mW)) as indicated by much larger $g^2(\tau)$ values around $\tau = 0$. Regardless of the bunching effect, the confirmation of single NV centers validates the choice and functionality of a confocal microscope as a useful tool to excite, probe, isolate and detect individual defect centers in diamond.

6.2.2 Bulk diamond

In this section, single NV centers in bulk diamond samples are investigated in the CM setup. The used diamond samples were of ultra high purity, electronic grade, type IIa single crystal plates ($4.5 \times 4.5 \times 0.50$ mm) from *Element 6* (e6). The diamond surface is cut along the {100} crystal axis with a nitrogen concentration below 5 ppb and a boron concentration $<$1 ppb. Electron irradiation and an annealing were used to create nitrogen vacancy centers in the bulk diamond sample where NV centers were successfully created throughout the diamond surface. The density of NV centers varied greatly at different depths inside the diamond and as an example, one area with a very high NV center density is shown in Fig. 6.6.

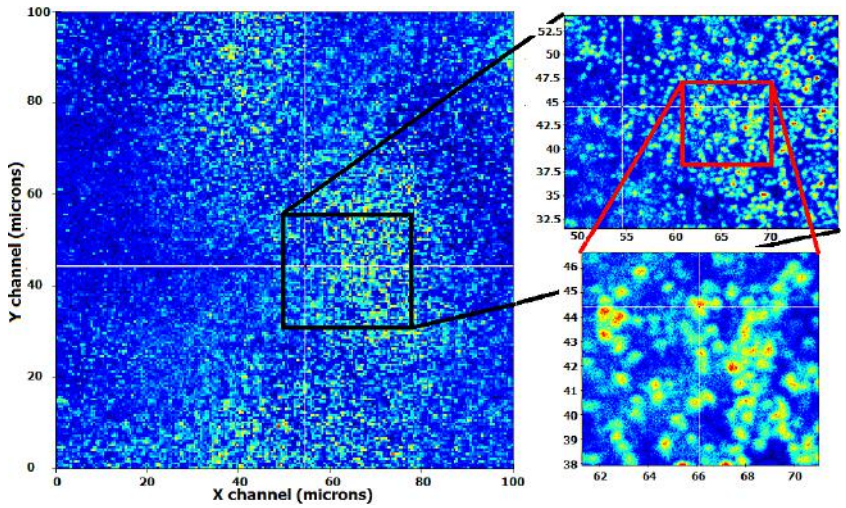

Figure 6.6: A 100×100 μm^2 scan of a densely populated NV region roughly 20 μm below the diamond surface. Zoomed in images of certain regions are provided for clarity.

Before use in a confocal microscope, the samples were thoroughly

cleaned in acetone, then isopropanol followed by cleaning in boiling Piranha solution at 95°C. Piranha solution, 3:1 mixture of sulphuric acid (H_2SO_4) and hydrogen peroxide (H_2O_2), is a very strong oxidizing agent and the treatment is quite common for the removal of organic residues from a substrate surface. A healthy density of single NV centers was observed and this was later confirmed by $g^2(\tau)$ measurements. One such example from a planar single NV center below the diamond surface is shown in Fig. 6.7.

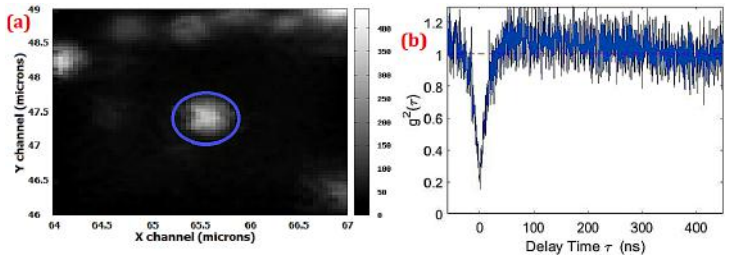

Figure 6.7: (a) A 3×3 μm^2 scan (30 nm step size, 40 ms integrated time) of a randomly selected region roughly 7 μm below the diamond surface. (b) Single emitter presence is confirmed by the $g^2(0) = 0.17$ value.

6.3 Precise SIL fabrication around single NV centers

The step by step procedure for precisely etching a hemispherical SIL with a defect center at its origin will now be presented. The samples used are of the type IIa bulk diamond samples used in 6.2.2. The road map is straight forward as the FIB is used to mill a grid pattern (100×100 μm^2) of periodic holes (20 μm pitch, d= 2 μm). Each grid pattern is marked at the corners by crosses and is labelled alphabetically for easy recognition. Once the sample surface has been etched with multiple such patterned grid squares, a confocal microscope is used to accurately identify and locate single NV centers with respect to the holes location in each grid square. It is important to remember that the placement of NV center at the origin of a milled sil is quite crucial. This requires that the exact lateral whereabouts and depth of the NV center must be known and co-ordinated with surrounding holes before we can proceed to mill a sil on top of the NV. The employed method provides a very efficient way of precisely locating NV centers and accurate milling of a SIL around them and is based on [173]. Before use in the CM setup, the sample is cleaned using acetone, isopropanol and in boiling piranha solution

as before. This is critical as otherwise the background fluorescence from deposits of gallium and other organic contaminants will mask the markers during confocal scans. An example of these FIB milled grid patterns and subsequent confocal microscope imaging of an individual grid pattern is shown in Fig [6.8].

In the next step, an area of $20 \times 20\ \mu m^2$ is chosen within a grid square where the position of these holes is clearly visible.

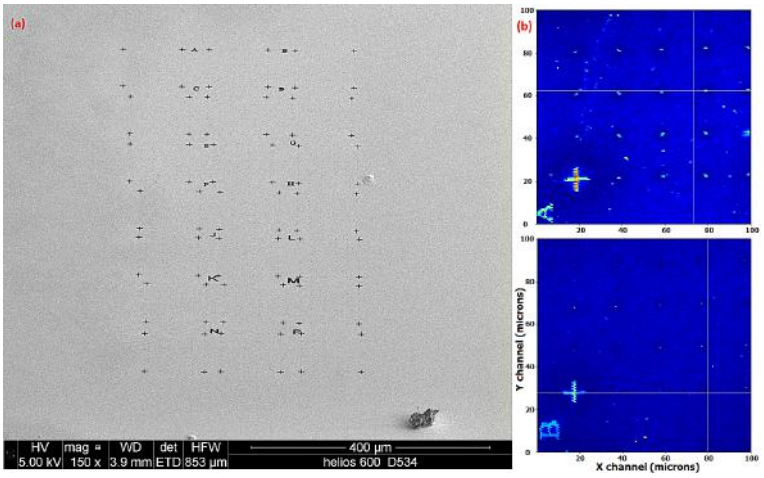

Figure 6.8: (a)A Scanning electron microscope (SEM) image of the alphabatically labeled grid patterns eteched onto the diamond surface using FIB. (b) Confocal microscope scans of 'A' and 'B' marked squares clearly indicating the periodic holes that will be used for definite NV location.

Single NV centers inside this region at a suitable depth are then identified as in Fig. [6.9]b. Once an NV center is found, the confocal co-ordinates of both the NV center and three surrounding holes are accurately recorded. For exact SIL milling, registered to the chosen NV, the same region is then located in FIB system and a python script is used to map the FIB co-ordinates with the confocal co-ordinates.

Along with the SIL diameter, an important parameter is the cone size surrounding the SIL. The radius of this cone is important to avoid any scattering and absorption of the light emitted at high angles and depends upon the SIL radius and the NA of the objective. Once the FIB co-ordinates of the four holes are known and mapped wth the optical co-ordinates, a SIL and the cone are milled by moving the beam along a 'double spiral' path where the dwell time is adjusted at each point to create the desired radial profile.

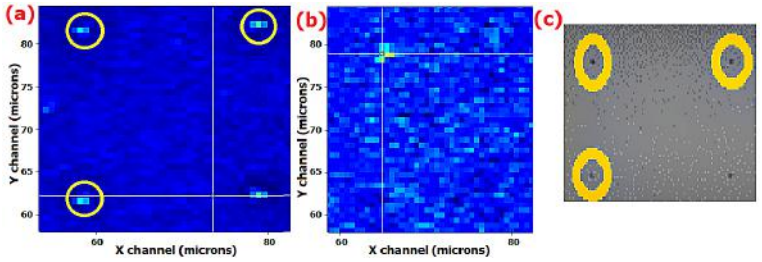

Figure 6.9: (a) Confocal scan of a 20×20 μm^2 region showing four etched holes. (b) A single NV center inside the same region at a depth of $\sim$5 μm. (c) The recognition of the same hole markers on the surface using SEM.

The ion beam starts on the outside, spirals inwards and then spirals outwards again. The same path is written many times with optimal beam focus, resulting in a smooth SIL and cone profile. A number of SILs were milled in this fashion (Fig. [6.10]) and the milling time varied between 40 to 60 minutes depending upon the SIL radius.

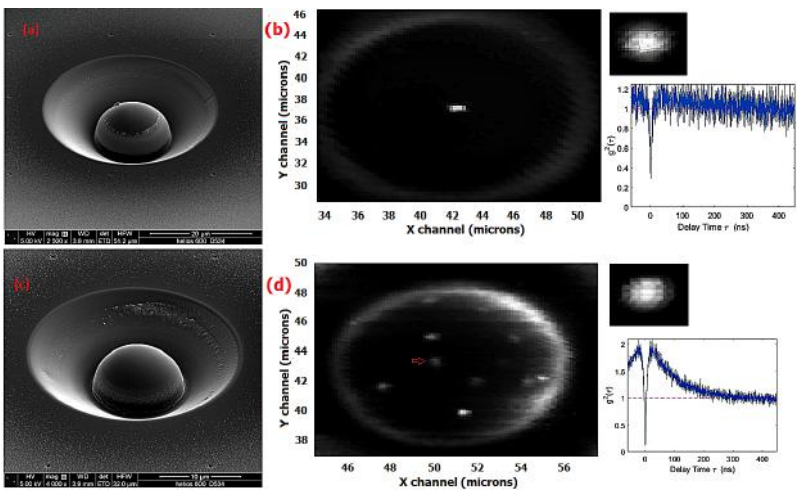

Figure 6.10: (a) A solid immersion lens fabricated with a single NV center at its origin. (b) Confocal scan of the SIL in (a) with a single NV at its centroid. Inset shows a zoom in on the NV and the $g^2(\tau)$ measurement. (c) Another solid immersion lens fabricated containing a number of single NV centers. at its origin. (d) Confocal scan of the SIL in (c), inset shows a zoom in on one of the NVs and the performed $g^2(\tau)$ measurement.

The fabrication of SILs is followed by thorough cleaning of the diamond surface in a boiling triacid solution to remove any graphitic car-

bon, gallium and other organic unwanted contents for atleast three hours. The triacid solution consists of a mixture of sulphuric (H_2SO_4), nitric (HNO_3) and perchloric acid ($HClO_4$) in equal volume concentration ($1:1:1$). After triacid boiling, the sample is ready to be inspected in the CM setup to test the accuracy of the described SIL fabrication process. As an example, two of the milled SILs and the resulting confocal scans are shown in Fig. [6.10]. For the SIL in [6.10]a, the confocal scans show a single NV center right at the origin, validating the precision and accuracy of the fabrication process. Fig. [6.10]c shows a SIL that was milled in area containing multiple single NV centers in close proximity, as can be seen by the following confocal scan in [6.10]d.

6.4 Diamond membranes and NV center creation

The nanopillars used in this thesis were fabricated in a diamond membrane with a $\sim$30 μm thickness. The diamond membrane is created from another ultra high purity, electronic grade, type IIa single crystal plate ($4.5\times4.5\times0.50$ mm) from *Element 6*. The sample is similar in characteristics to the one used in 6.2.2. For membrane formation, the sample was shipped to Applied Diamond, Inc. (US), where it was cut and polished into membranes of dimension ($2.25 \times 2.25 \times 0.030$ mm). The obtained membranes are extremely thin and their treatment requires delicacy.

In order to create single NV centers, the ion implantation facilities at the University of Stuttgart were used to implant the received membranes with nitrogen ions ($^{15}N^{+}$) at energies of 2.5 and 5 KeV and an implantation dose of $100 - 200$ ions/μm^2. Following the implantation process, the diamond sample was annealed at a temperature of 850 °C under high vacuum (Pressure $< 10^{-6}$ mbar) for 10 hours. The annealed sample was then cleaned for any graphite contamination by using a boiling triacid solution (a 1:1:1 mixture of sulfuric, nitric, and perchloric acids). This step ensures the stabilization of the charge state of the shallow NV centers [196]. After NV creation, the sample is ready for EBL and RIE to fabricate nanopillars on top of the shallow NV centers.

6.4.1 Tapered nanopillar fabrication

The canonical geometry of the tapered waveguides plays a vital role in efficient mode guiding and enhanced photon collection [174]. Through precise regulation and control of parameters such as the exposure dose of the resist and the plasma etching parameters, the desired pillar geometry can be achieved. Fig. 6.11 represents the schematic scheme for the

complete fabrication process. The fabrication process for the tapered nanopillars is followed from [174] and for ease of understanding, a brief and concise description of the process is provided here.

The membrane was glued on top of a silicon wafer using epoxy glue for structural support during the preparation steps. For electron beam writing of the nanopillars, Hydrogen Silsesquioxane (HSQ) FOX®25, a negative resist, was used. This resist has many attractive properties and provides a uniform and well-controlled thickness. Moreover, it offers high resolution, a good resistance to plasma etching and can be directly used as an etch mask for pattern transfer [197]. For the sample preparation, due to the poor adhesion of FOX®25 on diamond, a 5 nm layer of chromium (Cr) was thermally evaporated at a rate of 1 Å/s on top of the substrate as an adhesion layer. A ∼450 nm thick layer of the HSQ resist is then deposited on top of the adhesion layer through spin coating at 6 KRPM (45 sec) followed by a soft bake (1 min) at 90 °C. In the next step, another 5 nm layer of Cr was deposited on top of the HSQ resist as an anti-charging layer to avoid any charging effects under electron beam exposure (see Fig. 6.11).

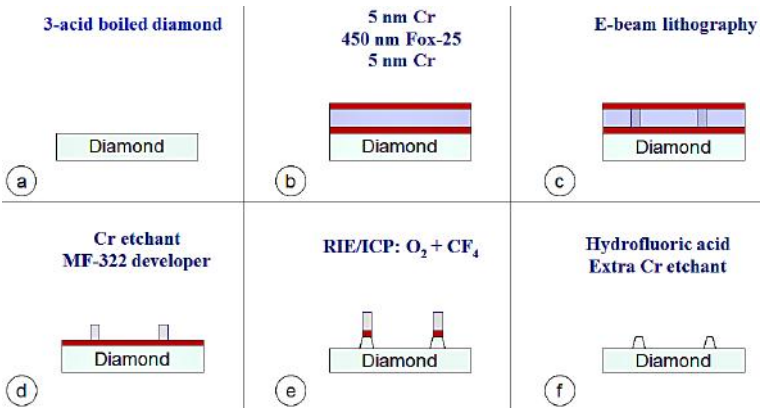

Figure 6.11: (a)-(e) is a schematic representation of all the steps for nanopillar fabrication using electron beam lithography and RIE/ICP etching processes.

For electron beam writing of the nanopillars, a Raith Eline system (20 kV acceleration voltage, 10 μm aperture and an exposure dose of 3000-4000 μC/cm^2) at the Max Planck institute, Stuttgart was used. The sample was then exposed to the electron beam for nanopillar writing in the area of the sample that was nitrogen implanted. Afterwards, the anti-charging Cr layer was chemically etched away and the exposed mask

was then developed in an MF-322 developer for 8 minutes.

To structure the nanopillars into their final shape (top diameter ∼400 nm, bottom diameter ∼900 nm) a reactive ion etching (RIE) and inductively coupled plasma (ICP) process was performed. An Oxford PlasmaPro NGP80 system was used for the RIE-ICP etching. The etching process involves three repeated cycles in an oxygen plasma at a constant RIE power (100 W) and pressure (10 mTorr). To obtain the desired canonical nanopillar geometry, ICP power was regulated to 600 W in each cycle. In-between each etching cycle, a quick 7 second interval of O_2/CF_4 was used to etch out any resist particles from the membrane surface. The complete etching recipe is provided in detail in [174].

After the etching process, the HSQ mask from the top of the pillars was completely removed by drowning the sample in a buffered hydrofluoric acid (BHF) solution. The sample was then boiled in the triacid solution and properly cleaned to remove any unwanted contaminants on the surface before using it in CM setup. The fabricated nanopillars are shown below in Fig. 6.12.

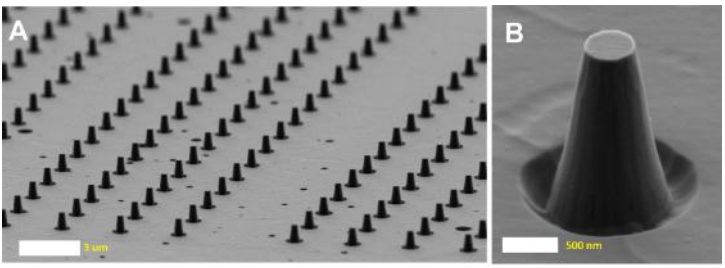

Figure 6.12: (a) SEM image of arrays of nanopillars tapered to the desired canonical geometry through EBL and RIE. (b) SEM image of a single tapered diamond nanopillar. The images are used as an example and are reproduced from [174].

6.4.2 Optical detection of NV centers in nanopillars

For confocal microscopy of the diamond membrane, the membrane sample is mounted such that the shallow NV centers inside the tapered nanopillars are optically excited from the other (non-pillar) side using a microscope objective. The emission from the NV center is collected by the same microscope objective due to the preferred HE_{11} mode guiding characteristics of the waveguide. Fig [6.13] shows a 20×20 μm^2 confocal scan of a pillar fabricated region of the waveguides.

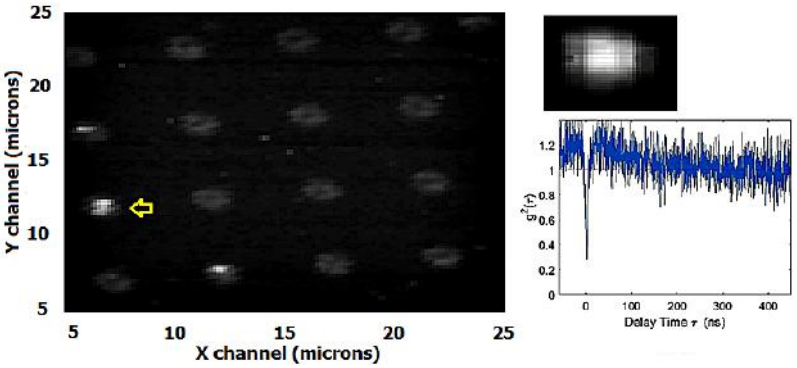

Figure 6.13: Confocal image of a 20×20 μm^2 area showing arrays of fabricated nanopillars with three of the pillars containing single NV centers. Single photon emission is confirmed and a zoomed in image of the marked pillar is also shown.

Arrays of pillars with a 5 μm pitch can be easily seen with three such pillars containing single NV centers. Overall scanning of the sample indicated around ~20% of the tapered nanopillars hosting single NV centers, giving rise to a considerably enhanced photon collection as compared to a single NV under a planar diamond surface.

6.5 Comparison between the collection enhancement methods

In the previous two sections, two of the explored methods that have demonstrated enhanced photon collection of the NV center emission were presented. Successful excitation and optical detection of a single NV center in the fabricated photonic structures was validated. Here, we will present and compare the observed increased photon collection capabilities of each method not only over a single NV in planar diamond sample containing no structures but also with respect to each other.

In Fig. [6.14], the detected photon counts (cps) by a single NV center are plotted as a function of the excitation intensity. The blue line represents a single NV center under a planar diamond surface. The detected photon counts, in the absence of a photonic structure to enhance collection, is low as the collection suffers greatly due to refraction losses at the air-diamond interface. The red line represents photon counts of a single NV center in SIL 2 (Fig. 6.9c), indicated by an arrow. The single NV center is not at the origin of the SIL but a factor of 4 increase

in saturation counts can be observed. As mentioned before, the photon collection suffers if the NV is not at the SIL centroid. The NV center showed stable counts under continuous excitation for a prolonged period of time.

The cyan line is the photon counts of a single NV center in SIL 1 (Fig. 6.9a). The NV center is at the center of the etched SIL and a factor of 5 increase in saturation counts is observed. Keeping in mind that the NV center is approximately at the origin of the SIL, a larger increase in comparison to the detected counts from the previous SIL was expected. It is important to mention that the NV center showed greater counts in general but suffered from blinking. The reason for this blinking behaviour is yet unknown [167].

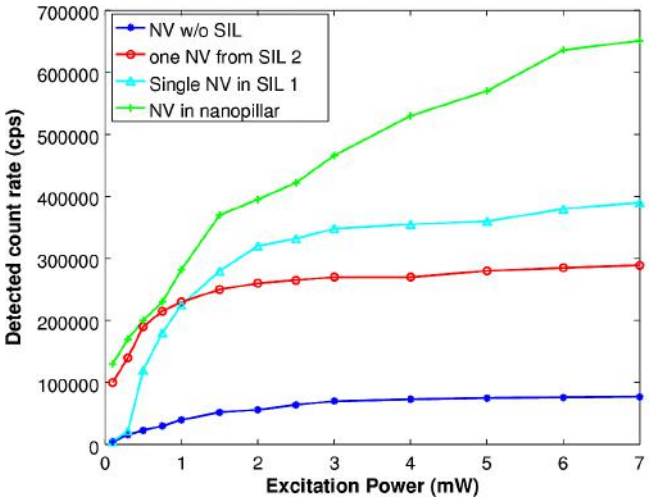

Figure 6.14: Comparison of observed time averaged photon flux from single NV centers under planar diamond surface, inside two SILs and a fabricated nanopillar. A clear enhancement in the photon collection can be observed using SILs and canonically tapered nanopillar, with the nanopillar providing the largest enhancement. The fit of the data points is only for the eye.

Lastly, the green line curve represents the counts detected from a single NV center in a fabricated nanopillar. The detected photon rate is by far the greatest using the nanopillars by a factor of $\sim$9. It is pertinent to mention that due to the small thickness of the diamond membrane, for ease of handling, the membrane was glued on top of a microscope glass slide creating a diamond-air-glass interface. The photon collection suffers from this diamond-air-glass interface and even higher photon collection

rates may be achieved if this interface was eliminated. AR coating of the glass surface may prove helpful in this regard.

6.6 Conclusions

Experimental identification, excitation and detection of a single NV center, both in nanodiamond crystals and bulk diamond, is reported using a confocal microscope setup. The single emitter nature is confirmed by measuring the value of second order correlation function ($g^2(\tau)$) using a Hanburry Brown Twiss configuration. Furthermore, two different methods to enhance photon collection from the emitted NV fluorescence in bulk diamond were described. Both these methods demonstrated a significant increase in the detected photon counts in comparison to a single NV center under a planar diamond surface. The nanofabricated diamond waveguides in particular demonstrated a larger enhancement in the detected optical photon rate. These two explored methods, along with many others, can prove to be important stepping stones for future devices and applications employing single NV centers.

7. Appendix

7.1 Quantum versus classical high level RACs

In section 2.2, QRACs of the form $(d+1)^{(d)} \mapsto 1$, for $d \in \{2,..,8\}$ were mentioned [39]. It was reported that despite their potential, high level RACs have not seen much attention otherwise. In [**?**], the average success probability of these $(d+1)^{(d)} \mapsto 1$ QRACs is derived but they were unable to test their resourcefulness as no optimal classical model for such high level RACs was available. In 2.2.1, such a model of optimal classical RAC $n^{(d)} \mapsto 1$ is presented, where the average success probability of these RACS, for $n = 2$ and $n = 3$, is shown in eq. 2.13. This optimal classical RAC can be used together with the $(d+1)^{(d)} \mapsto 1$ QRACs to calculate the respective quantum advantage (p^Q/p^C). Such a comparison is presented below in Table 7.1, where its apparent that the quantum success probability outscores the classical probability for all d. Increasing the dimension of the RAC evidently leads to superior and more resourceful QRACs. The first case, when $d = 2$, is the well-known case of $3^2 \mapsto 1$ QRAC reported by Chuang [38]. It is clear from the table that the quantum advantage is enlarged for all $d > 2$ when compared to the standard well known case of $d = 2$ with the maximum advantage seen at $d = 5$, $(p^Q/p^C) = 1.0953$.

Table 7.1: Performance comparison of $(d+1)^{(d)} \mapsto 1$ QRACs reported in [39] against high level classical codes. Reproduced from [41].

d	p^Q	p^C	p^Q/p^C
2	0.789	0.75	1.052
3	0.637	0.593	1.075
4	0.5424	0.4961	1.0933
5	0.4700	0.4291	1.0953
6	0.3720	0.3420	1.0876
7	0.3372	0.3118	1.0815

Now that we have compared the performance of our classical RACs with already known QRACs of dimensions greater than 2, we will com-

pare these classical RACs with the high level QRACs $n^d \mapsto 1$, presented in the section 1.2.2 for $n = 2$ case. Such a quantum advantage p^Q/p^C computed from eq. 2.22 when $n = 2$ is shown in Fig. 7.1 for $d \in \{0, ..., 50\}$. The quantum advantage increases with d and reaches its peak when $d = 6$ with the largest quantum advantage of $p^Q/p^C \approx 1.207$. For the well known $2^2 \mapsto 1$ code, the corresponding quantum advantage is $p^Q_{2,2}/p^C_{2,2} \approx 1.138$. After $d = 6$, it starts to decrease with increasing d and eventually falls off to unity when the average quantum success probability matches the classical for very large d. In terms of absolute numbers, it is already shown that the difference between the two success probabilities, $p^Q_{2,d} - p^C_{2,d}$, is maximum for $d = 4$ and an experimental demonstration of such a $2^4 \mapsto 1$ QRAC is shown in chapter 6. Although

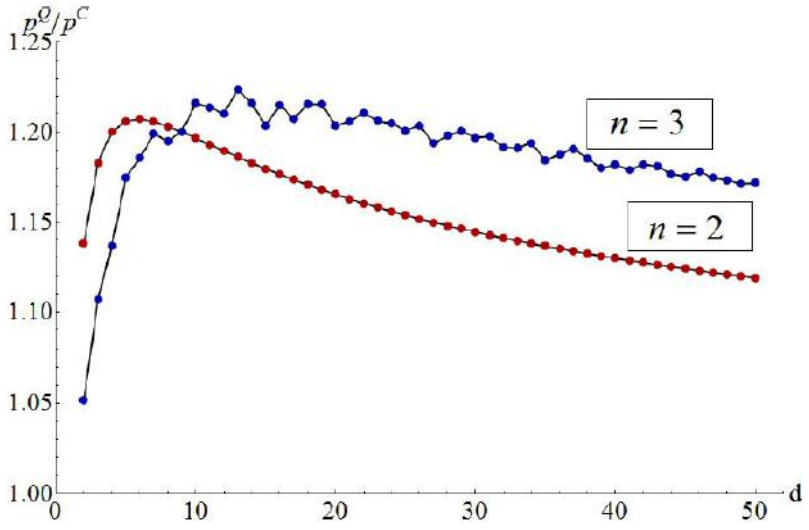

Figure 7.1: The ratio between quantum and classical success probabilities as a function of d for the $2^d \mapsto 1$ and $3^d \mapsto 1$ QRACs. Reproduced from [41].

not in the scope of this thesis but in the paper [41] the case of $3^d \mapsto 1$ QRAC is also considered. The optimal or maximum quantum advantage of $p^Q/p^C \approx 1.224$ is achieved for $d = 13$. For the corresponding $3^2 \mapsto 1$ code [39], the respective quantum advantage is $p^Q_{3,2}/p^C_{3,2} \approx 1.052$, which is four times smaller than $p^Q_{3,13}/p^C_{3,13}$. In both cases of $n^d \mapsto 1$ QRACs considered, the optimal quantum advantage is significantly larger than the $n^2 \mapsto 1$ QRACs. This clearly depicts the point that single qudit communication using a system with dimensions greater than two considerably demonstrates the superiority of such quantum resources not only

over their classical contemporaries but also over the $d = 2$ families of QRACs. The advantage of using higher dimensional quantum systems is clearly established over similar known quantum resources of dimensions two. For the $n^d \mapsto 1$ QRACs, the optimal advantage of $n = 3$ class of QRACs is also shown to be higher than the $n = 2$ class.

7.2 Experimental measurements of $2^4 \mapsto 1$ QRAC

The experimental implementation and results for $2^4 \mapsto 1$ QRAC were presented in ch. 2.3.3. Here, I will give a detailed account of measurements for all the 16 states for both measurement bases along with the obtained QRAC probabilities in each individual detector setting corresponding to the initial state shown in eq. 2.24.

Measurements in Computational basis for all 16 states

Probabilities obtained for individual detectors

Ψ_{00}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,05	22,5	-9,22	0
Detectors	D_1	D_2	D_3	D_4
	0.059 ± 0.027	0.084 ± 0.027	0.110 ± 0.027	0.747 ± 0.036

Ψ_{01}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,05	22,5	-9,22	π
Detectors	D_1	D_2	D_3	D_4
	0.058 ± 0.027	0.083 ± 0.027	0.111 ± 0.027	0.748 ± 0.027

Ψ_{02}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,05	-22,5	9,22	0
Detectors	D_1	D_2	D_3	D_4
	0.046 ± 0.026	0.110 ± 0.027	0.094 ± 0.027	0.749 ± 0.036

Ψ_{03}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,05	-22,5	9,22	π
Detectors	D_1	D_2	D_3	D_4
	0.048 ± 0.026	0.107 ± 0.027	0.093 ± 0.027	0.753 ± 0.027

Ψ_{10}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,05	22,5	-35,78	0
Detectors	D_1	D_2	D_3	D_4
	0.056 ± 0.027	0.083 ± 0.027	0.766 ± 0.036	0.095 ± 0.027

Ψ_{11}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,05	22,5	-35,78	π
Detectors	D_1	D_2	D_3	D_4
	0.059 ± 0.027	0.082 ± 0.027	0.767 ± 0.036	0.092 ± 0.027

Ψ_{12}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,05	-22,5	35,78	0
Detectors	D_1	D_2	D_3	D_4
	0.047 ± 0.026	0.10 ± 0.027	0.764 ± 0.036	0.089 ± 0.027

Ψ_{13}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,05	-22,5	35,78	π
Detectors	D_1	D_2	D_3	D_4
	0.045 ± 0.026	0.103 ± 0.027	0.764 ± 0.036	0.089 ± 0.027

Ψ_{20}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,95	-22,5	9,22	0
Detectors	D_1	D_2	D_3	D_4
	0.081 ± 0.027	0.755 ± 0.036	0.084 ± 0.027	0.079 ± 0.027

Ψ_{21}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,95	-22,5	9,22	π
Detectors	D_1	D_2	D_3	D_4
	0.081 ± 0.027	0.761 ± 0.036	0.082 ± 0.027	0.077 ± 0.027

Ψ_{22}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,95	22,5	-9,22	0
Detectors	D_1	D_2	D_3	D_4
	0.076 ± 0.027	0.786 ± 0.036	0.067 ± 0.027	0.071 ± 0.027

Ψ_{23}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,95	22,5	-9,22	π
Detectors	D_1	D_2	D_3	D_4
	0.076 ± 0.027	0.786 ± 0.036	0.067 ± 0.027	0.070 ± 0.027

Ψ_{30}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,95	-22,5	35,78	0
Detectors	D_1	D_2	D_3	D_4
	0.742 ± 0.037	0.110 ± 0.027	0.074 ± 0.027	0.074 ± 0.027

Ψ_{31}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,95	-22,5	35,78	π
Detectors	D_1	D_2	D_3	D_4
	0.743 ± 0.037	0.107 ± 0.027	0.077 ± 0.027	0.072 ± 0.027

Ψ_{32}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,95	22,5	-35,78	0
Detectors	D_1	D_2	D_3	D_4
	0.732 ± 0.037	0.099 ± 0.027	0.080 ± 0.027	0.089 ± 0.027

Ψ_{33}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,95	22,5	-35,78	π
Detectors	D_1	D_2	D_3	D_4
	0.733 ± 0.037	0.103 ± 0.027	0.082 ± 0.027	0.082 ± 0.027

Measurements in Fourier basis for all 16 states

Probabilities obtained for individual detectors

Ψ_{00}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,050	22,500	-9,220	0,000
Detectors	D1	D2	D3	D4
	0.752 ± 0.038	0.078 ± 0.027	0.062 ± 0.027	0.108 ± 0.028

Ψ_{01}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,050	22,500	-9,220	π
Detectors	D1	D2	D3	D4
	0.067 ± 0.027	0.077 ± 0.027	0.082 ± 0.027	0.774 ± 0.038

Ψ_{02}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,050	-22,500	9,220	0,000
Detectors	D1	D2	D3	D4
	0.0756 ± 0.028	0.753 ± 0.039	0.083 ± 0.028	0.089 ± 0.028

Ψ_{03}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,050	-22,500	9,220	π
Detectors	D1	D2	D3	D4
	0.113 ± 0.028	0.068 ± 0.028	0.714 ± 0.039	0.105 ± 0.028

Ψ_{10}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,050	22,500	-35,780	0,000
Detectors	D1	D2	D3	D4
	0.763 ± 0.038	0.071 ± 0.027	0.072 ± 0.027	0.094 ± 0.028

Ψ_{11}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,050	22,500	-35,780	π
Detectors	D1	D2	D3	D4
	0.087 ± 0.028	0.093 ± 0.028	0.071 ± 0.027	0.750 ± 0.038

Ψ_{12}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,050	-22,500	35,780	0,000
Detectors	D1	D2	D3	D4
	0.080 ± 0.028	0.751 ± 0.039	0.073 ± 0.028	0.095 ± 0.028

Ψ_{13}	HWP θ_1	HWP θ_2	HWP θ_3	Phase
Angles	12,050	-22,500	35,780	π
Detectors	D1	D2	D3	D4
	0.061 ± 0.028	0.087 ± 0.028	0.748 ± 0.039	0.104 ± 0.028

Ψ_{20}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,950	-22,500	9,220	0,000
Detectors	D1	D2	D3	D4
	0.764 ± 0.038	0.107 ± 0.028	0.066 ± 0.027	0.063 ± 0.027

Ψ_{21}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,950	-22,500	9,220	π
Detectors	D1	D2	D3	D4
	0.070 ± 0.027	0.095 ± 0.028	0.081 ± 0.027	0.754 ± 0.028

Ψ_{22}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,950	22,500	-9,220	0,000
Detectors	D1	D2	D3	D4
	0.070 ± 0.028	0.775 ± 0.039	0.079 ± 0.028	0.077 ± 0.028

Ψ_{23}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,950	22,500	-9,220	π
Detectors	D1	D2	D3	D4
	0.076 ± 0.028	0.114 ± 0.028	0.728 ± 0.039	0.082 ± 0.028

Ψ_{30}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,950	-22,500	35,780	0,000
Detectors	D1	D2	D3	D4
	0.772 ± 0.038	0.086 ± 0.028	0.068 ± 0.027	0.074 ± 0.027

Ψ_{31}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,950	-22,500	35,780	π
Detectors	D1	D2	D3	D4
	0.082 ± 0.028	0.091 ± 0.028	0.061 ± 0.028	0.766 ± 0.038

Ψ_{32}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,950	22,500	-35,780	0,000
Detectors	D1	D2	D3	D4
	0.086 ± 0.028	0.749 ± 0.039	0.067 ± 0.028	0.098 ± 0.028

Ψ_{33}	HWP θ1	HWP θ_2	HWP θ_3	Phase
Angles	32,950	22,500	-35,780	π
Detectors	D1	D2	D3	D4
	0.079 ± 0.028	0.109 ± 0.028	0.703 ± 0.039	0.109 ± 0.028

7.3 Experimental measurements of test of non-classicality

In section 3.2.4.3, the measurements and the results of the experiment were presented. Here, in this section, All the measurements settings and results for the 128 measurements are presented. The probabilities are estimated from the corresponding detection events.

A,A'	B,B'	X = 0, Y = 0 (TT')	X = 1, Y = 0 (AB)		X = 0, Y = 1 (A'B')		X = 1 (AB) & Y = 1 (A'B') (Counts/30 secs)					T,T' = 1 & C = 0	
		Counts (N/30 secs)	Probabilities (P)	Counts (N/30 secs)	Probabilities (P)	Counts (N/30 secs)	D1D3TT'	D2D3TT'	D1D4TT'	D2D4TT'	Total Counts (SUM)	Preparing in A & Measuring in B	
1.1	1.1	194082	0.6486	27062	0.6710	28526	505	110	2898	517	4030	Preparing in A' & Measuring in B'	
1.2		143607	0.6960	19973	0.6568	19325	82	325	368	1884	2659	A & A'	1 = Psi(1)
1.3		193414	0.6538	23150	0.6806	24243	498	93	2804	472	3867		2 = Psi(2)
1.4		195490	0.6924	26631	0.6404	26645	105	423	538	2523	3589		3 = Psi(3)
2.1		193019	0.6752	27213	0.6887	28508	2774	507	489	91	3861		4 = Psi(4)
2.2		194327	0.7451	27531	0.6800	26130	500	2603	101	466	3670		
2.3		194445	0.6945	27087	0.6459	27776	2612	559	461	120	3752	B & B'	1 = M1
2.4		193721	0.7293	27204	0.6126	25868	583	2537	102	452	3674		2 = M2
3.1		191696	0.6521	26585	0.7032	27993	2747	497	529	86	3859		
3.2		192386	0.7458	27175	0.6424	25817	460	2423	97	434	3414		
3.3		188049	0.6506	26262	0.6907	27085	2651	487	492	103	3733		
3.4		191772	0.7366	26698	0.5930	25862	596	2426	103	425	3550		
4.1		191745	0.6618	26004	0.6753	27558	488	76	2673	484	3721		
4.2		194296	0.6645	26285	0.6595	25843	101	480	453	2496	3530		
4.3		189054	0.6681	25712	0.7176	27180	463	62	2618	433	3576		
4.4		189598	0.7073	25861	0.6528	25328	94	427	511	2438	3470		
1.1	1.2	184814	0.6410	24752	0.6854	26409	449	71	2541	449	3510		
1.2		190079	0.6968	25435	0.7064	24909	64	426	398	2302	3190		
1.3		186877	0.6962	25244	0.5917	24979	126	421	539	2346	3432		
1.4		178775	0.6528	23864	0.6086	24975	436	91	2161	485	3173		
2.1		180098	0.7520	24359	0.7427	25271	2507	388	341	42	3278		
2.2		181164	0.8088	24538	0.6013	22726	521	2216	91	324	3152		
2.3		179179	0.6852	24274	0.5589	23307	564	2026	108	364	3062		
2.4		179056	0.6305	24391	0.6283	24380	2238	505	467	99	3309		
3.1		176223	0.6848	23993	0.6990	24229	2394	412	394	64	3264		
3.2		178847	0.8729	24242	0.6341	22305	489	2262	70	258	3079		
3.3		178477	0.8392	24258	0.6292	22951	516	2189	56	278	3039		
3.4		176409	0.7877	23726	0.6501	23901	2303	549	326	56	3234		
4.1		175855	0.6858	22874	0.6940	24336	389	61	2215	400	3065		
4.2		177649	0.8004	23169	0.6368	22300	67	312	457	1996	2832		
4.3		176780	0.7463	22980	0.5778	22290	88	348	453	1924	2813		
4.4		176892	0.7136	23087	0.6388	24009	379	90	2190	421	3080		
1.1	2.1	154376	0.5906	18706	0.7088	19761	348	59	1548	295	2250		
1.2		159193	0.6567	19165	0.7144	18350	47	352	277	1481	2157		
1.3		156192	0.6102	18929	0.6486	19548	346	81	1534	310	2271		
1.4		160310	0.6463	19125	0.6503	18737	63	291	292	1533	2179		
2.1		159654	0.6683	19836	0.6169	20374	1769	356	305	69	2499		
2.2		131476	0.7297	19975	0.6584	18509	317	1588	58	289	2252		
2.3		156215	0.6524	19397	0.7142	20016	1735	327	326	56	2444		
2.4		158735	0.7143	19622	0.6534	18538	310	1573	69	295	2247		
3.1		158732	0.6250	19412	0.5810	20347	348	84	1663	393	2488		
3.2		160976	0.6200	19802	0.6367	18935	76	338	326	1573	2313		
3.3		161359	0.6740	19848	0.6791	20434	341	57	1711	344	2453		
3.4		161988	0.6648	19917	0.6923	19559	59	316	291	1622	2288		
4.1		163780	0.6128	20684	0.7036	21348	1854	319	337	61	2571		
4.2		162693	0.7481	20383	0.6745	19306	347	1771	60	316	2494		
4.3		162336	0.7306	20694	0.6350	19506	404	1711	67	317	2499		
4.4		161159	0.6832	19799	0.6816	20510	1814	338	314	54	2520		
1.1	2.2	168739	0.5917	21515	0.6207	22741	399	88	1935	410	2832		
1.2		168947	0.6430	21214	0.5651	20581	81	385	456	1545	2467		
1.3		170849	0.6195	21729	0.6762	22454	426	82	1864	344	2716		
1.4		172264	0.6462	21540	0.7060	21068	62	371	309	1735	2477		
2.1		166051	0.6616	21410	0.6901	21826	1950	345	360	67	2722		
2.2		170858	0.7132	22063	0.6663	20636	325	1833	71	340	2569		
2.3		167089	0.6303	21354	0.6543	22022	1882	402	394	76	2754		
2.4		170103	0.7061	21964	0.6850	20501	325	1810	68	339	2542		
3.1		168453	0.6519	17355	0.6607	18505	353	67	1940	363	2723		
3.2		168358	0.7302	17252	0.6909	16793	59	329	340	1782	2510		
3.3		164277	0.6907	17399	0.7003	17885	339	52	1872	358	2621		
3.4		168854	0.7136	20865	0.7160	16695	81	315	330	1755	2481		
4.1		162803	0.6059	20583	0.6172	21237	1805	378	394	84	2661		
4.2		166381	0.7690	21250	0.5965	20071	416	1817	68	269	2570		
4.3		166303	0.6603	21169	0.7010	21514	1887	351	365	60	2663		
4.4		165605	0.7657	21071	0.6961	19929	321	1802	57	317	2497		

A',A	B,B'	X = 0, Y = 0 [TT']	X = 1, Y = 0 [A'B]		X = 0, Y = 1 [AB']		X = 1 [A'B] & Y = 1 [AB'] [Counts/30 secs]					T,T' = 1 & C = 1	
		Counts [N/30 secs]	Probabilities [P]	Counts [N/30 secs]	Probabilities [P]	Counts [N/30 secs]	D1D3TT'	D2D3TT'	D1D4TT'	D2D4TT'	Total Counts [SUM]	Preparing in A' & Measuring in B	
1.1	1.1	285217	0.6410	40209	0.6765	28262	572	106	2749	483	3910	Preparing in A & Measuring in B'	
1.2		285611	0.6196	40284	0.6338	26372	131	534	524	2525	3714	A & A'	1 = Psi(1)
1.3		283504	0.6586	39663	0.6506	27477	541	99	2704	563	3907		2 = Psi(2)
1.4		282865	0.7705	39762	0.6618	26534	59	378	532	2748	3717		3 = Psi(3)
2.1		280248	0.7289	39887	0.6495	27852	2863	538	428	92	3921		4 = Psi(4)
2.2		281428	0.7251	40221	0.6512	26053	525	2781	97	441	3844		
2.3		279742	0.7231	40081	0.6901	27457	2823	489	469	71	3852	B & B'	1 = M1
2.4		283803	0.7313	40351	0.6620	26413	521	2730	88	452	3791		2 = M2
3.1		280244	0.6159	39405	0.6735	27999	571	123	2738	515	3947		
3.2		282782	0.5811	39521	0.6359	26313	137	580	534	2362	3613		
3.3		281096	0.6232	39358	0.6349	27337	604	125	2490	509	3728		
3.4		281755	0.6150	39030	0.6383	26384	113	603	524	2390	3630		
4.1		277009	0.6650	38731	0.6716	27600	2701	534	569	99	3903		
4.2		280907	0.6588	39346	0.6708	26104	435	2563	87	512	3597		
4.3		278970	0.6621	39384	0.6956	27366	2672	485	515	99	3771		
4.4		279914	0.6590	39445	0.6450	26557	497	2513	102	490	3602		
1.1	1.2	278259	0.6963	38639	0.7485	27811	525	76	2882	418	3901		
1.2		279678	0.6951	38773	0.7267	25893	79	463	391	2601	3534		
1.3		281501	0.6925	38738	0.7116	26129	65	467	452	2632	3616		
1.4		278796	0.6995	38829	0.6605	27335	468	96	2566	529	3659		
2.1		277062	0.7059	39161	0.6258	27541	2709	562	445	110	3826		
2.2		280601	0.7018	39505	0.5997	25794	577	2481	80	419	3557		
2.3		279325	0.7028	39706	0.6901	25981	449	2608	82	455	3594		
2.4		278652	0.6928	39495	0.7083	27260	2737	468	493	78	3776		
3.1		278397	0.6455	38823	0.6170	27594	569	112	2619	566	3866		
3.2		281138	0.5798	38795	0.6275	25708	136	560	507	2382	3585		
3.3		279875	0.6304	38998	0.6819	26151	88	512	482	2566	3648		
3.4		278333	0.6426	38580	0.6900	27443	504	95	2831	469	3899		
4.1		278810	0.6242	38968	0.6224	27703	2597	614	538	118	3867		
4.2		279817	0.6652	38980	0.6047	25907	549	2360	100	458	3467		
4.3		280031	0.6549	39220	0.6887	26270	449	2569	91	491	3600		
4.4		278865	0.6449	39012	0.6646	27508	2724	509	588	101	3922		
1.1	2.1	275653	0.6906	37979	0.6690	27077	489	81	2734	497	3801		
1.2		277858	0.6951	38245	0.6493	25441	80	407	475	2526	3488		
1.3		276015	0.6913	38403	0.6774	27095	75	2581	514		3170		
1.4		276477	0.6881	38269	0.6684	25942	84	424	494	2545	3547		
2.1		274218	0.6410	38591	0.6688	26933	2673	501	563	101	3838		
2.2		275733	0.6480	39024	0.6391	25403	474	2390	107	477	3448		
2.3		273844	0.6499	38451	0.6796	26615	2547	493	558	81	3679		
2.4		274869	0.6531	38723	0.6450	25652	486	2482	100	531	3599		
3.1		275131	0.6752	38339	0.6491	26895	2592	506	505	101	3704		
3.2		275061	0.6660	38815	0.6193	25092	503	2597	105	487	3692		
3.3		274394	0.6834	38374	0.6953	26522	2662	438	486	73	3659		
3.4		275781	0.6907	38308	0.6647	25487	428	2549	84	454	3515		
4.1		274591	0.6755	38024	0.6724	26978	455	94	2614	489	3652		
4.2		275472	0.6766	37926	0.6601	25170	72	451	462	2441	3426		
4.3		273026	0.6624	38393	0.6680	26409	489	90	2637	485	3701		
4.4		275725	0.6740	38011	0.6623	25682	95	475	473	2463	3506		
1.1	2.2	273129	0.7009	37741	0.6224	27048	458	109	2630	552	3749		
1.2		276832	0.6923	38325	0.5940	25630	109	467	542	2406	3524		
1.3		277631	0.6934	38688	0.6784	25802	86	419	481	2523	3509		
1.4		276805	0.6876	38412	0.7088	27174	491	79	2715	470	3755		
2.1		277254	0.6737	38934	0.6456	27231	2612	562	542	114	3830		
2.2		277528	0.6677	39453	0.6270	25647	494	2501	99	481	3575		
2.3		278228	0.6634	39230	0.6867	25724	470	2628	98	478	3674		
2.4		275464	0.6619	39012	0.7071	26474	2683	463	480	89	3715		
3.1		275865	0.6762	39155	0.6206	27412	2633	582	510	95	3820		
3.2		277635	0.6667	38779	0.6517	25812	491	2396	96	469	3452		
3.3		276791	0.6822	38700	0.7075	25732	430	2643	73	479	3625		
3.4		274772	0.6920	38549	0.7087	26934	2731	440	488	68	3727		
4.1		275600	0.5784	38750	0.6514	27253	640	130	2593	545	3908		
4.2		276009	0.6867	38971	0.7089	25495	82	469	423	2647	3621		
4.3		276348	0.6808	38573	0.6657	27069	522	101	2728	499	3850		
4.4		279012	0.6813	38815	0.6403	25737	98	460	535	2522	3615		

7.4 Experimental measurements for the $3 \mapsto 1$ distributed QRAC

Table 7.2: Experimentally estimated probabilities for the QRAC task, $x_0 \oplus x_2, x_1, x_2$, for measurements performed in the $\sigma_y, \sigma_x, \sigma_z$ bases.

		Unitary by Bob ($\mathbb{1}$)					
Different Tasks	State	σ_y		σ_x		σ_z	
$f(x,0), f(x,1), f(x,2)$	x_0x_1	D_1	D_2	D_1	D_2	D_1	D_2
	00	0.211 ± 0.014	0.789 ± 0.014	0.788 ± 0.016	0.212 ± 0.016	0.789 ± 0.020	0.211 ± 0.020
$x_0 \oplus x_2, x_1, x_2$	01	0.212 ± 0.014	0.788 ± 0.014	0.214 ± 0.016	0.786 ± 0.017	0.786 ± 0.018	0.214 ± 0.018
	11	0.788 ± 0.014	0.212 ± 0.013	0.209 ± 0.018	0.791 ± 0.018	0.790 ± 0.020	0.210 ± 0.020
	10	0.800 ± 0.013	0.200 ± 0.013	0.785 ± 0.019	0.215 ± 0.019	0.787 ± 0.018	0.213 ± 0.018
		Unitary by Bob ($R_x(\pi)$)					
	00	0.797 ± 0.017	0.203 ± 0.017	0.786 ± 0.019	0.214 ± 0.018	0.212 ± 0.023	0.788 ± 0.023
$x_0 \oplus x_1, x_0, x_1$	01	0.789 ± 0.017	0.211 ± 0.017	0.210 ± 0.020	0.790 ± 0.020	0.213 ± 0.020	0.787 ± 0.021
	11	0.211 ± 0.016	0.789 ± 0.017	0.209 ± 0.017	0.791 ± 0.017	0.206 ± 0.023	0.794 ± 0.023
	10	0.207 ± 0.017	0.793 ± 0.017	0.795 ± 0.016	0.205 ± 0.016	0.214 ± 0.020	0.786 ± 0.020

Table 7.3: Experimentally estimated probabilities for the QRAC task, $x_0, x_1, x_2 \oplus x_0$, for measurements performed in the $\sigma_y, \sigma_x, \sigma_z$ bases.

Different Tasks	State	σ_y		σ_x		σ_z	
$f(x,0), f(x,1), f(x,2)$	x_0x_1	D_1	D_2	D_1	D_2	D_1	D_2
	00	0.211 ± 0.013	0.789 ± 0.014	0.788 ± 0.016	0.212 ± 0.016	0.789 ± 0.021	0.211 ± 0.021
$x_0, x_1, x_2 \oplus x_0$	01	0.212 ± 0.013	0.788 ± 0.014	0.214 ± 0.016	0.786 ± 0.016	0.786 ± 0.017	0.214 ± 0.017
	11	0.783 ± 0.013	0.217 ± 0.013	0.208 ± 0.016	0.792 ± 0.017	0.216 ± 0.020	0.784 ± 0.020
	10	0.789 ± 0.014	0.211 ± 0.013	0.788 ± 0.016	0.212 ± 0.016	0.213 ± 0.017	0.787 ± 0.017
		Unitary by Bob ($R_x(3\pi/2)$)					
	00	0.796 ± 0.019	0.204 ± 0.019	0.787 ± 0.015	0.213 ± 0.015	0.790 ± 0.022	0.210 ± 0.022
$x_0, x_1, x_2 \oplus x_0$	01	0.791 ± 0.018	0.209 ± 0.018	0.214 ± 0.016	0.786 ± 0.016	0.782 ± 0.019	0.218 ± 0.019
	11	0.214 ± 0.019	0.786 ± 0.019	0.214 ± 0.016	0.786 ± 0.016	0.218 ± 0.022	0.782 ± 0.022
	10	0.219 ± 0.018	0.781 ± 0.018	0.788 ± 0.016	0.212 ± 0.016	0.214 ± 0.019	0.786 ± 0.020

Table 7.4: Experimentally estimated probabilities for the QRAC task, $x_0 \oplus x_2, x_1, x_0$, for measurements performed in the $\sigma_y, \sigma_x, \sigma_z$ bases.

		Unitary by Bob ($\mathbb{1}$)					
Different Tasks	State	σ_y		σ_x		σ_z	
$f(x,0), f(x,1), f(x,2)$	x_0x_1	D_1	D_2	D_1	D_2	D_1	D_2
	00	0.211 ± 0.013	0.789 ± 0.014	0.788 ± 0.016	0.212 ± 0.016	0.789 ± 0.021	0.211 ± 0.021
$x_0 \oplus x_2, x_1, x_0$	01	0.212 ± 0.013	0.788 ± 0.014	0.214 ± 0.016	0.786 ± 0.017	0.786 ± 0.018	0.214 ± 0.018
	11	0.783 ± 0.014	0.217 ± 0.014	0.208 ± 0.016	0.792 ± 0.016	0.216 ± 0.020	0.784 ± 0.021
	10	0.789 ± 0.014	0.211 ± 0.013	0.788 ± 0.016	0.212 ± 0.016	0.213 ± 0.017	0.787 ± 0.018
		Unitary by Bob ($R_x(\pi/2)$)					
	00	0.221 ± 0.017	0.779 ± 0.017	0.798 ± 0.017	0.202 ± 0.016	0.214 ± 0.018	0.786 ± 0.019
$x_0 \oplus x_2, x_1, x_0$	01	0.215 ± 0.018	0.785 ± 0.018	0.212 ± 0.016	0.788 ± 0.017	0.208 ± 0.021	0.792 ± 0.021
	11	0.784 ± 0.019	0.216 ± 0.019	0.211 ± 0.016	0.789 ± 0.016	0.784 ± 0.019	0.216 ± 0.019
	10	0.795 ± 0.019	0.205 ± 0.019	0.788 ± 0.016	0.212 ± 0.016	0.796 ± 0.022	0.204 ± 0.021

Table 7.5: Experimentally estimated probabilities for the QRAC task, $x_0 \oplus x_2, x_1 \oplus x_2, x_0$, for measurements performed in the $\sigma_y, \sigma_x, \sigma_z$ bases.

		Unitary by Bob ($\mathbb{1}$)					
Different Tasks	**State**	σ_y		σ_x		σ_z	
$f(x,0), f(x,1), f(x,2)$	x_0x_1	D_1	D_2	D_1	D_2	D_1	D_2
	00	**0.211 ± 0.013**	**0.789 ± 0.014**	**0.788 ± 0.016**	**0.212 ± 0.016**	**0.789 ± 0.021**	**0.211 ± 0.021**
$x_0 \oplus x_2, x_1 \oplus x_2, x_0$	**01**	**0.212 ± 0.013**	**0.788 ± 0.014**	**0.214 ± 0.016**	**0.786 ± 0.017**	**0.786 ± 0.017**	**0.214 ± 0.017**
	11	**0.783 ± 0.014**	**0.217 ± 0.013**	**0.208 ± 0.016**	**0.792 ± 0.016**	**0.216 ± 0.021**	**0.784 ± 0.021**
	10	**0.789 ± 0.014**	**0.211 ± 0.013**	**0.788 ± 0.016**	**0.212 ± 0.016**	**0.213 ± 0.018**	**0.787 ± 0.019**
		Unitary by Bob ($R_z(\pi)$)					
	00	**0.785 ± 0.016**	**0.215 ± 0.016**	**0.209 ± 0.015**	**0.791 ± 0.015**	**0.789 ± 0.022**	**0.211 ± 0.022**
$x_0 \oplus x_2, x_1 \oplus x_2, x_0$	**01**	**0.795 ± 0.016**	**0.205 ± 0.015**	**0.785 ± 0.016**	**0.215 ± 0.016**	**0.788 ± 0.021**	**0.212 ± 0.021**
	11	**0.213 ± 0.015**	**0.787 ± 0.016**	**0.789 ± 0.015**	**0.211 ± 0.015**	**0.211 ± 0.021**	**0.789 ± 0.021**
	10	**0.211 ± 0.016**	**0.789 ± 0.016**	**0.213 ± 0.015**	**0.787 ± 0.015**	**0.218 ± 0.022**	**0.782 ± 0.022**

Summary

This thesis covers the the work produced in the articles **I-V** based on single quantum system enabled communication. In addition, single photon emission from NV centers in diamond along with different alternatives to enhance the photon collection efficiency are explored.

Article **I** introduced and laid down the theoretical ground work for a class of quantum random access codes with dimensions d greater than 2. In such class of d-level QRACs, Alice can only communicate one bit at a time to Bob who then performs a measurement depending upon his bit of interest. To test the results predicted by theory, an experiment was designed where $2^{(4)} \mapsto 1$ was implemented experimentally in the laboratory. All 16 encoding states of Alice were prepared and were measured by Bob in both the computational and Fourier basis. From the measurement results and recorded data, the success probabilities were calculated. The results of the experiment are in good agreement with the predictions of quantum mechanics and the average success probability ($P^{Q}_{2,4} \approx 0.754 \pm 0.038$) violates the classical bound ($P^{C}_{2,4} \approx 0.625$). In article **I**, it was also shown that high-level QRACs of dimension d provide a significant advantage over not only classical RACs of equivalent dimensions but also the commonly used QRACs of dimensions 2.

Article **II** focussed on the amount of randomness certified by using the experimentally demonstrated $2^{(4)} \mapsto 1$ QRAC in a semi-device independent (SDI) scheme. The security parameter (T) was used to certify the amount of randomness generated, which was then quantified by the minimum entropy function (H_{∞}). A method is presented based on the generalization of SDI random number generation protocols of the case in which the randomness is extracted from more than one choice of inputs. The computational capacity required for the task is however very large but a method to drastically reduce these strong demands on computational requirements was also presented in the regard. By using this approach, it was shown that more randomness can be certified without altering or placing stringent demands on the experimental setup.

Article **III** presented a parallel implementation of two 2-dimensional QRACs in a SDI scenario for performing a test of non-classicality with-

out any dependence on detector efficiency or other additional conditions on the devices. This test of non-classicality conclusively proved the non-classicality of the 2-dimensional quantum system communicated between preparation and measurement devices. The main advantage of such a test is the simplicity of implementation. It is also not limited by high detection efficiencies or strong assumptions as independence of the devices.

Article **IV** focuses on the adaptation of a $3 \mapsto 1$ QRAC to a one-path communication network consisting of a single preparation, transformation and measurement device. This distributed QRAC is the simplest such adaptation of the QRAC for the purpose. Four tasks that lead to optimal success probabilities for the distributed QRAC are presented and experimentally demonstrated. The obtained experimental results for each task are in good agreement with the optimal case and validate the successful adaptation of a standard $3 \mapsto 1$ QRAC to a one-path general communication network.

Article **V** presents a novel quantum solution to the known problems of dining cryptographers and anonymous voting. The protocol is based on a flying particle implementation and a single quantum system is distributed between $N+2$ parties where N, represents the number of voting participants. The protocol consists of two rounds where one round is used to establish the infrastructure necessary for voter's privacy and the second round is the actual voting round. A 3-party experimental demonstration of the protocol is provided for this purpose. The experimental results validate the successful application of our quantum solution for the 3-party dining cryptographers and anonymous veto voting problems.

Chapter 5 contains a theoretical introduction of NV center characteristics, where this defect center in diamond is studied as a resource for single photon emission. In addition, a brief account of some of the methods utilized to enhance the photon collection efficiency from the NV center is also provided.

In chapter 6, single photon emission was observed using a purpose built confocal microscope setup, from NV centers in nanodiamond crystals and bulk diamond samples. To enhance the photon collection efficiency from NV centers in bulk diamond, micrometer SILs and tapered nanopillars were fabricated. A significant enhancement in the collected photon flux, as compared to a single NV center under planar diamond surface, was observed in both cases. The nanopillar geometry provided the highest collection efficiency of the two methods. With this enhancement in photon collection, single photons from an NV center may also be used in similar single quantum system based communication experiments.

References

[1] Claude Elwood Shannon. **A mathematical theory of communication**. *ACM SIGMOBILE Mobile Computing and Communications Review*, **5**(1):3–55, 2001. 29

[2] Magnus Rådmark. **Photonic quantum information and experimental tests of foundations of quantum mechanics**. 2010. 30

[3] Charles H Bennett. **Quantum cryptography: Public key distribution and coin tossing**. In *International Conference on Computer System and Signal Processing, IEEE, 1984*, pages 175–179, 1984. 30

[4] Artur K Ekert. **Quantum cryptography based on Bell's theorem**. *Physical review letters*, **67**(6):661, 1991.

[5] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. **Quantum cryptography**. *Reviews of modern physics*, **74**(1):145, 2002. 30

[6] Charles H Bennett and Stephen J Wiesner. **Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states**. *Physical review letters*, **69**(20):2881, 1992. 30

[7] Klaus Mattle, Harald Weinfurter, Paul G Kwiat, and Anton Zeilinger. **Dense coding in experimental quantum communication**. *Physical Review Letters*, **76**(25):4656, 1996. 30

[8] Michael A Nielsen and Isaac Chuang. **Quantum computation and quantum information**, 2002.

[9] Armin Tavakoli. **The Single d-level Quantum System as a Resource for Information Processing**. *Master thesis, Stockholm University*, 2015.

[10] Chandra Roychoudhuri, Al F Kracklauer, and Kathy Creath. *The nature of light: what is a photon?* CRC Press, 2008. 36

[11] Chandra Roychoudhuri, Al F Kracklauer, and Kathy Creath. *The nature of light: what is a photon?* CRC Press, 2008.

[12] MD Eisaman, J Fan, A Migdall, and SV Polyakov. **Invited review article: Single-photon sources and detectors**. *Review of scientific instruments*, **82**(7):071101, 2011. 36

[13] Christopher J Chunnilall, Ivo Pietro Degiovanni, Stefan Kück, Ingmar Müller, and Alastair G Sinclair. **Metrology of single-photon sources and detectors: a review**. *Optical Engineering*, **53**(8):081910–081910, 2014. 36

[14] Hatim Azzouz. **Creation and Detection of Single Photons**. 2016. 36

[15] I Aharonovich, S Castelletto, DA Simpson, CH Su, AD Greentree, and S Prawer. **Diamond-based single-photon emitters**. *Reports on progress in Physics*, **74**(7):076501, 2011. 36

[16] H Jeff Kimble, Mario Dagenais, and Leonard Mandel. **Photon antibunching in resonance fluorescence**. *Physical Review Letters*, **39**(11):691, 1977.

[17] Th Basché, WE Moerner, M Orrit, and H Talon. **Photon antibunching in the fluorescence of a single dye molecule trapped in a solid**. *Physical review letters*, **69**(10):1516, 1992.

[18] Frank Diedrich and Herbert Walther. **Nonclassical radiation of a single stored ion**. *Physical review letters*, **58**(3):203, 1987.

[19] P Michler, A Kiraz, C Becher, WV Schoenfeld, PM Petroff, Lidong Zhang, E Hu, and A Imamoglu. **A quantum dot single-photon turnstile device**. *Science*, **290**(5500):2282–2285, 2000.

[20] Christian Kurtsiefer, Sonja Mayer, Patrick Zarda, and Harald Weinfurter. **Stable solid-state source of single photons**. *Physical review letters*, **85**(2):290, 2000.

[21] S Castelletto, BC Johnson, Viktor Ivády, N Stavrias, T Umeda, A Gali, and T Ohshima. **A silicon carbide room-temperature single-photon source**. *Nature materials*, **13**(2):151–156, 2014.

[22] Paul G Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V Sergienko, and Yanhua Shih. **New high-intensity source of polarization-entangled photon pairs**. *Physical Review Letters*, **75**(24):4337, 1995.

[23] Muhammad Sadiq. **Experiments with Entangled Photons: Bell Inequalities, Non-local Games and Bound Entanglement**. 2016.

[24] Stephen Wiesner. **Conjugate coding**. *ACM Sigact News*, **15**(1):78–88, 1983.

[25] Andris Ambainis, Ashwin Nayak, Ammon Ta-Shma, and Umesh Vazirani. **Dense quantum coding and a lower bound for 1-way quantum automata**. In *Proceedings of the thirty-first annual ACM symposium on Theory of computing*, pages 376–383. ACM, 1999.

[26] Andris Ambainis, Ashwin Nayak, Amnon Ta-Shma, and Umesh Vazirani. **Dense quantum coding and quantum finite automata**. *Journal of the ACM (JACM)*, **49**(4):496–511, 2002.

[27] Ashwin Nayak. **Optimal lower bounds for quantum automata and random access codes**. In *Foundations of Computer Science, 1999. 40th Annual Symposium on*, pages 369–376. IEEE, 1999.

[28] Ernesto F Galvao. **Foundations of quantum theory and quantum information applications**. *arXiv preprint quant-ph/0212124*, 2002.

[29] Masahito Hayashi, Kazuo Iwama, Harumichi Nishimura, Rudy Raymond, and Shigeru Yamashita. **Quantum network coding**. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 610–621. Springer, 2007.

[30] Iordanis Kerenidis. *Quantum encodings and applications to locally decodable codes and communication complexity*. PhD thesis, University of California at Berkeley, 2004.

[31] Hong-Wei Li, Zhen-Qiang Yin, Yu-Chun Wu, Xu-Bo Zou, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. **Semi-device-independent random-number expansion without entanglement**. *Physical Review A*, **84**(3):034301, 2011.

[32] Hong-Wei Li, Marcin Pawłowski, Zhen-Qiang Yin, Guang-Can Guo, and Zheng-Fu Han. **Semi-device independent random number expansion protocol with n to 1 quantum random access codes**. *arXiv preprint arXiv:1109.5259*, 2011.

[33] Marcin Pawłowski and Nicolas Brunner. **Semi-device-independent security of one-way quantum key distribution**. *Physical Review A*, **84**(1):010302, 2011.

[34] Andrzej Grudka, Karol Horodecki, Michał Horodecki, Waldemar Kłobus, and Marcin Pawłowski. **When are Popescu-Rohrlich boxes and random access codes equivalent?** *Physical review letters*, **113**(10):100401, 2014.

[35] Marcin Pawłowski, Tomasz Paterek, Dagomir Kaszlikowski, Valerio Scarani, Andreas Winter, and Marek Żukowski. **Information causality as a physical principle**. *Nature*, **461**(7267):1101–1104, 2009.

[36] Marcin Pawłowski and Marek Żukowski. **Entanglement-assisted random access codes**. *Physical Review A*, **81**(4):042326, 2010.

[37] Sadiq Muhammad, Armin Tavakoli, Maciej Kurant, Marcin Pawłowski, Marek Żukowski, and Mohamed Bourennane. **Quantum bidding in Bridge**. *Physical Review X*, **4**(2):021047, 2014.

[38] Andris Ambainis, Debbie Leung, Laura Mancinska, and Maris Ozols. **Quantum random access codes with shared randomness**. *arXiv preprint arXiv:0810.2937*, 2008.

[39] Andrea Casaccino, Ernesto F Galvao, and Simone Severini. **Extrema of discrete Wigner functions and applications**. *Physical Review A*, **78**(2):022310, 2008.

[40] Andris Ambainis, Dmitry Kravchenko, and Ashutosh Rai. **Optimal Classical Random Access Codes Using Single d-level Systems**. *arXiv preprint arXiv:1510.03045*, 2015.

[41] Armin Tavakoli, Alley Hameedi, Breno Marques, and Mohamed Bourennane. **Quantum random access codes using single d-level systems**. *Physical review letters*, **114**(17):170502, 2015.

[42] ID Ivonovic. **Geometrical description of quantal state determination**. *Journal of Physics A: Mathematical and General*, **14**(12):3241, 1981.

[43] William K Wootters and Brian D Fields. **Optimal state-determination by mutually unbiased measurements**. *Annals of Physics*, **191**(2):363–381, 1989.

[44] M Peev, M Nölle, O Maurhardt, T Lorünser, M Suda, A Poppe, R Ursin, A Fedrizzi, and A Zeilinger. **A novel protocol-authentication algorithm ruling out a man-in-the middle attack in quantum cryptography**. *International Journal of Quantum Information*, **3**(01):225–231, 2005.

[45] Bas Hensen, H Bernien, AE Dréau, A Reiserer, N Kalb, MS Blok, J Ruitenberg, RFL Vermeulen, RN Schouten, C Abellán, et al. **Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres**. *Nature*, **526**(7575):682–686, 2015.

[46] Marissa Giustina, Marijn AM Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, et al. **Significant-loophole-free test of Bell's theorem with entangled photons**. *Physical review letters*, **115**(25):250401, 2015.

[47] Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. **Strong loophole-free test of local realism**. *Physical review letters*, **115**(25):250402, 2015.

[48] Thomas Jennewein, Ulrich Achleitner, Gregor Weihs, Harald Weinfurter, and Anton Zeilinger. **A fast and compact quantum random number generator**. *Review of Scientific Instruments*, **71**(4):1675–1680, 2000.

[49] André Stefanov, Nicolas Gisin, Olivier Guinnard, Laurent Guinnard, and Hugo Zbinden. **Optical quantum random number generator**. *Journal of Modern Optics*, **47**(4):595–598, 2000.

[50] James F Dynes, Zhiliang L Yuan, Andrew W Sharpe, and Andrew J Shields. **A high speed, postprocessing free, quantum random number generator**. *applied physics letters*, **93**(3):031109, 2008.

[51] Atsushi Uchida, Kazuya Amano, Masaki Inoue, Kunihito Hirano, Sunao Naito, Hiroyuki Someya, Isao Oowada, Takayuki Kurashige, Masaru Shiki, Shigeru Yoshimori, et al. **Fast physical random bit generation with chaotic semiconductor lasers**. *Nature Photonics*, **2**(12):728–732, 2008.

[52] M Fiorentino, C Santori, SM Spillane, RG Beausoleil, and WJ Munro. **Secure self-calibrating quantum random-bit generator**. *Physical Review A*, **75**(3):032334, 2007.

[53] Yong Shen, Liang Tian, and Hongxin Zou. **Practical quantum random number generator based on measuring the shot noise of vacuum states**. *Physical Review A*, **81**(6):063814, 2010.

[54] Wei Wei and Hong Guo. **Bias-free true random-number generator**. *Optics letters*, **34**(12):1876–1878, 2009.

[55] Min Ren, E Wu, Yan Liang, Yi Jian, Guang Wu, and Heping Zeng. **Quantum random-number generator based on a photon-number-resolving detector**. *Physical Review A*, **83**(2):023820, 2011.

[56] Roger Gimson, S Finkelstein, S Maes, and L Suryanarayana. **Device independence principles**. *W3C Working Group Note*, **1**, 2003.

[57] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. **Device-independent security of quantum cryptography against collective attacks**. *Physical Review Letters*, **98**(23):230501, 2007.

[58] Jonathan Barrett, Lucien Hardy, and Adrian Kent. **No signaling and quantum key distribution**. *Physical review letters*, **95**(1):010503, 2005.

[59] Esther Hänggi and Renato Renner. **Device-independent quantum key distribution with commuting measurements**. *arXiv preprint arXiv:1009.1833*, 2010.

[60] Lluís Masanes, Stefano Pironio, and Antonio Acín. **Secure device-independent quantum key distribution with causally independent measurement devices**. *Nature communications*, **2**:238, 2011.

[61] Roger Colbeck and Adrian Kent. **Private randomness expansion with untrusted devices**. *Journal of Physics A: Mathematical and Theoretical*, **44**(9):095305, 2011.

[62] Roger Colbeck. **Quantum and relativistic protocols for secure multi-party computation**. *arXiv preprint arXiv:0911.3814*, 2009.

[63] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzimitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. **Random numbers certified by Bell's theorem**. *Nature*, **464**(7291):1021–1024, 2010.

[64] Miguel Navascués and Tamás Vértesi. **Bounding the set of finite dimensional quantum correlations**. *Physical review letters*, **115**(2):020501, 2015.

[65] Harry Buhrman, Richard Cleve, Serge Massar, and Ronald de Wolf. **Nonlocality and communication complexity**. *Reviews of modern physics*, **82**(1):665, 2010.

[66] Piotr Mironowicz, Armin Tavakoli, Alley Hameedi, Breno Marques, Marcin Pawłowski, and Mohamed Bourennane. **Increased certification of semi-device independent random numbers using many inputs and more post-processing**. *New Journal of Physics*, **18**(6):065004, 2016.

[67] Joseph Bowles, Nicolas Brunner, and Marcin Pawłowski. **Testing dimension and nonclassicality in communication networks**. *Physical Review A*, **92**(2):022351, 2015.

[68] Ernesto F Galvao and Lucien Hardy. **Substituting a qubit for an arbitrarily large number of classical bits**. *Physical review letters*, **90**(8):087902, 2003.

[69] Nicholas Harrigan, Terry Rudolph, and Scott Aaronson. **Representing probabilistic data via ontological models**. *arXiv preprint arXiv:0709.1149*, 2007.

[70] Rodrigo Gallego, Nicolas Brunner, Christopher Hadley, and Antonio Acín. **Device-independent tests of classical and quantum dimensions**. *Physical review letters*, **105**(23):230501, 2010.

[71] John S Bell. **On the einstein podolsky rosen paradox**, 1964.

[72] Johan Ahrens, Piotr Badziąg, Marcin Pawłowski, Marek Żukowski, and Mohamed Bourennane. **Experimental tests of classical and quantum dimensionality**. *Physical review letters*, **112**(14):140401, 2014.

[73] BG Christensen, KT McCusker, JB Altepeter, B Calkins, T Gerrits, AE Lita, A Miller, LK Shalm, Y Zhang, SW Nam, et al. **Detection-loophole-free test of quantum nonlocality, and applications**. *Physical review letters*, **111**(13):130406, 2013.

[74] Joseph Bowles, Marco Túlio Quintino, and Nicolas Brunner. **Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices**. *Physical review letters*, **112**(14):140407, 2014.

[75] Gustavo Cañas, Jaime Cariñe, Esteban S Gómez, Johanna F Barra, Adán Cabello, Guilherme B Xavier, Gustavo Lima, and Marcin Pawłowski. **Experimental quantum randomness generation invulnerable to the detection loophole**. *arXiv preprint arXiv:1410.3443*, 2014.

[76] Tommaso Lunghi, Jonatan Bohr Brask, Charles Ci Wen Lim, Quentin Lavigne, Joseph Bowles, Anthony Martin, Hugo Zbinden, and Nicolas Brunner. **Self-testing quantum random number generator**. *Physical review letters*, **114**(15):150501, 2015.

[77] Michele Dall'Arno, Elsa Passaro, Rodrigo Gallego, Marcin Pawlowski, and Antonio Acin. **Detection loophole attacks on semi-device-independent quantum and classical protocols**. *Quantum Information & Computation*, **15**(1-2):37–49, 2015.

[78] Stefano Pironio. **Lifting bell inequalities**. *Journal of mathematical physics*, **46**(6):062112, 2005.

[79] Lucas Clemente and Johannes Kofler. **No Fine Theorem for Macrorealism: Limitations of the Leggett-Garg Inequality**. *Physical review letters*, **116**(15):150401, 2016.

[80] A Hameedi, B Marques, P Mironowicz, D Saha, M Pawlowski, and M Bourennane. **An unconditional experimental test of Nonclassicality**. *arXiv preprint arXiv:1511.06179*, 2015.

[81] A Hameedi, D Saha, P Mironowicz, M Pawlowski, and M Bourennane. **Distributed random access code with quantum resources**. *arXiv preprint arXiv:1701.08713*, 2017.

[82] Berthold-Georg Englert, Christian Kurtsiefer, and Harald Weinfurter. **Universal unitary gate for single-photon two-qubit states**. *Physical Review A*, **63**(3):032303, 2001.

[83] Birgit Pfitzmann and Michael Waidner. **Unconditional Byzantine agreement for any number of faulty processors**. In *Annual Symposium on Theoretical Aspects of Computer Science*, pages 337–350. Springer, 1992.

[84] Zhengchao Wei, Weilong Wang, Zhen Zhang, Ming Gao, Zhi Ma, and Xiongfeng Ma. **Decoy-state quantum key distribution with biased basis choice**. *Scientific reports*, **3**, 2013.

[85] David Chaum and Sandra Roijakkers. **Unconditionally-secure digital signatures**. In *Conference on the Theory and Application of Cryptography*, pages 206–214. Springer, 1990.

[86] David L Chaum. **Untraceable electronic mail, return addresses, and digital pseudonyms**. *Communications of the ACM*, **24**(2):84–90, 1981.

[87] Jurjen Norbert Eelco Bos. *Practical privacy*. Citeseer, 1992.

[88] Birgit Pfitzmann and Michael Waidner. **Unconditionally untraceable and fault-tolerant broadcast and secret ballot election**. In *Communications of the ACM*. Citeseer, 1992.

[89] Bruce Schneier. **Applied Cryptography, 1996**. *Cover and title pages*, pages 125–147, 1997.

[90] Mark Hillery, Mário Ziman, Vladimír Bužek, and Martina Bieliková. **Towards quantum-based privacy and voting**. *Physics Letters A*, **349**(1):75–81, 2006.

[91] Justin Boyan. **The anonymizer-protecting user privacy on the web**. 1997.

[92] Eran Gabber, Phillip B Gibbons, David M Kristol, Yossi Matias, and Alain Mayer. **Consistent, yet anonymous, Web access with LPWA**. *Communications of the ACM*, **42**(2):42–47, 1999.

[93] David Chaum. **The dining cryptographers problem: Unconditional sender and recipient untraceability**. *Journal of cryptology*, **1**(1):65–75, 1988.

[94] Feng Hao and Piotr Zieliński. **A 2-round anonymous veto protocol**. In *International Workshop on Security Protocols*, pages 202–211. Springer, 2006.

[95] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. CRC press, 2014.

[96] Oded Goldreich, Silvio Micali, and Avi Wigderson. **How to play any mental game**. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 218–229. ACM, 1987.

[97] Aggelos Kiayias and Moti Yung. **Non-interactive zero-sharing with applications to private distributed decision making**. In *International Conference on Financial Cryptography*, pages 303–320. Springer, 2003.

[98] Jens Groth. **Efficient maximal privacy in boardroom voting and anonymous broadcast**. In *International Conference on Financial Cryptography*, pages 90–104. Springer, 2004.

[99] Anne Broadbent and Alain Tapp. **Information-theoretic security without an honest majority**. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 410–426. Springer, 2007.

[100] P Oscar Boykin. **Information security and quantum mechanics: security of quantum protocols**. *arXiv preprint quant-ph/0210194*, 2002.

[101] Matthias Christandl and Stephanie Wehner. **Quantum anonymous transmissions**. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 217–235. Springer, 2005.

[102] P Werbos. **In Bell's theorem, quantum theory, and conceptions of the universe**, 1989.

[103] Ramij Rahaman and Guruprasad Kar. **GHZ correlation provides secure Anonymous Veto Protocol**. *arXiv preprint arXiv:1507.00592*, 2015.

[104] Joan Alfina Vaccaro, Joseph Spring, and Anthony Chefles. **Quantum protocols for anonymous voting and surveying**. *Physical Review A*, **75**(1):012333, 2007.

[105] William K Wootters and Brian D Fields. **Optimal state-determination by mutually unbiased measurements**. *Annals of Physics*, **191**(2):363–381, 1989.

[106] Jeronimo Maze Rios. *Quantum manipulation of nitrogen-vacancy centers in diamond: from basic properties to applications*. PhD thesis, Harvard University Cambridge, Massachusetts, 2010.

[107] Lilian Isabel Childress. *Coherent manipulation of single quantum systems in the solid state*. PhD thesis, Harvard University Cambridge, Massachusetts, 2007.

[108] Emre Togan. *Optical Control of Individual Nitrogen-Vacancy Centers in Diamond*. PhD thesis, 2013.

[109] John Wilks and Eileen Wilks. *Properties and applications of diamond*. Butterworth-Heinemann Oxford, 1991.

[110] Stephen John Sque. *A first-principles study on bulk and transfer doping of diamond*. University of Exeter, 2005.

[111] Dingwei Zheng. **Study and manipulation of photoluminescent NV color center in diamond**. 2010.

[112] RS Balmer, JR Brandon, SL Clewes, HK Dhillon, JM Dodson, I Friel, PN Inglis, TD Madgwick, ML Markham, TP Mollart, et al. **Chemical vapour deposition synthetic diamond: materials, technology and applications**. *Journal of Physics: Condensed Matter*, **21**(36):364221, 2009.

[113] Jan Isberg, Johan Hammersberg, Erik Johansson, Tobias Wikström, Daniel J Twitchen, Andrew J Whitehead, Steven E Coe, and Geoffrey A Scarsbrook. **High carrier mobility in single-crystal plasma-deposited diamond**. *Science*, **297**(5587):1670–1672, 2002.

[114] N Mizuochi, J Isoya, J Niitsuma, T Sekiguchi, H Watanabe, H Kato, T Makino, H Okushi, and S Yamasaki. **Isotope effects between hydrogen and deuterium microwave plasmas on chemical vapor deposition homoepitaxial diamond growth**. *Journal of applied physics*, **101**(10):103501, 2007.

[115] Philipp Neumann. **Towards a room temperature solid state quantum processor-the nitrogen-vacancy center in diamond**. 2012.

[116] Wuyi Wang, Thomas Moses, Robert C Linares, James E Shigley, Matthew Hall, and James E Butler. **Gem-quality synthetic diamonds grown by a chemical vapor deposition (CVD) method**. *Gems Gemol*, **39**(4):268–83, 2003.

[117] Element 6. *THE ELEMENT SIX CVD DIAMOND HANDBOOK*.

[118] John Walker. **Optical absorption and luminescence in diamond**. *Reports on Progress in Physics*, **42**(10):1605, 1979.

[119] I Aharonovich, S Castelletto, BC Johnson, JC McCallum, and S Prawer. **Engineering chromium-related single photon emitters in single crystal diamonds**. *New Journal of Physics*, **13**(4):045015, 2011.

[120] Elke Neu, David Steinmetz, Janine Riedrich-Möller, Stefan Gsell, Martin Fischer, Matthias Schreck, and Christoph Becher. **Single photon emission from silicon-vacancy colour centres in chemical vapour deposition nanodiamonds on iridium**. *New Journal of Physics*, **13**(2):025012, 2011.

[121] Nir Bar-Gill, Linh M Pham, Andrejs Jarmola, Dmitry Budker, and Ronald L Walsworth. **Solid-state electronic spin coherence time approaching one second**. *Nature communications*, **4**:1743, 2013.

[122] Norman Y Yao, Liang Jiang, Alexey V Gorshkov, Peter C Maurer, Geza Giedke, J Ignacio Cirac, and Mikhail D Lukin. **Scalable architecture for a room temperature solid-state quantum information processor**. *Nature communications*, **3**:800, 2012.

[123] Gopalakrishnan Balasubramanian, IY Chan, Roman Kolesov, Mohannad Al-Hmoud, Julia Tisler, Chang Shin, Changdong Kim, Aleksander Wojcik, Philip R Hemmer, Anke Krueger, et al. **Nanoscale imaging magnetometry with diamond spins under ambient conditions**. *Nature*, **455**(7213):648–651, 2008.

[124] JR Maze, PL Stanwix, JS Hodges, S Hong, JM Taylor, P Cappellaro, L Jiang, MV Gurudev Dutt, E Togan, AS Zibrov, et al. **Nanoscale magnetic sensing with an individual electronic spin in diamond**. *Nature*, **455**(7213):644–647, 2008.

[125] JM Taylor, P Cappellaro, L Childress, L Jiang, D Budker, PR Hemmer, A Yacoby, R Walsworth, and MD Lukin. **High-sensitivity diamond magnetometer with nanoscale resolution**. *Nature Physics*, **4**(10):810–816, 2008.

[126] Florian Dolde, Helmut Fedder, Marcus W Doherty, Tobias Nöbauer, Florian Rempp, Gopalakrishnan Balasubramanian, Thomas Wolf, Friedemann Reinhard, Lloyd CL Hollenberg, Fedor Jelezko, et al. **Electric-field sensing using single diamond spins**. *Nature Physics*, **7**(6):459–463, 2011.

[127] Yi-Ren Chang, Hsu-Yang Lee, Kowa Chen, Chun-Chieh Chang, Dung-Sheng Tsai, Chi-Cheng Fu, Tsong-Shin Lim, Yan-Kai Tzeng, Chia-Yi Fang, Chau-Chung Han, et al. **Mass production and dynamic imaging of fluorescent nanodiamonds**. *Nature nanotechnology*, **3**(5):284–288, 2008.

[128] Gordon Davies and MF Hamer. **Optical studies of the 1.945 eV vibronic band in diamond**. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, **348**, pages 285–298. The Royal Society, 1976.

[129] A Gruber, A Dräbenstedt, C Tietz, L Fleury, J Wrachtrup, and C Von Borczyskowski. **Scanning confocal optical microscopy and magnetic resonance on single defect centers**. *Science*, **276**(5321):2012–2014, 1997.

[130] Jean-Paul Boudou, Patrick A Curmi, Fedor Jelezko, Joerg Wrachtrup, Pascal Aubert, Mohamed Sennour, Gopalakrischnan Balasubramanian, Rolf Reuter, Alain Thorel, and Eric Gaffet. **High yield fabrication of fluorescent nanodiamonds**. *Nanotechnology*, **20**(23):235602, 2009.

[131] P Reichart, G Tamanyan, DN Jamieson, S Prawer, F Jelezko, T Gaebel, I Popa, M Domhan, J Wrachtrup, et al. **Implantation of labelled single nitrogen vacancy centers in diamond using 15N**. *arXiv preprint cond-mat/0511722*, 2005.

[132] Marcus W Doherty, Neil B Manson, Paul Delaney, Fedor Jelezko, Jörg Wrachtrup, and Lloyd CL Hollenberg. **The nitrogen-vacancy colour centre in diamond**. *Physics Reports*, **528**(1):1–45, 2013.

[133] T Gaebel, M Domhan, C Wittmann, I Popa, F Jelezko, J Rabeau, A Greentree, S Prawer, E Trajkov, PR Hemmer, et al. **Photochromism in single nitrogen-vacancy defect in diamond**. *Applied Physics B*, **82**(2):243–246, 2006.

[134] Yoshimi Mita. **Change of absorption spectra in type-Ib diamond with heavy neutron irradiation**. *Physical Review B*, **53**(17):11360, 1996.

[135] PR Briddon G Davies AT Collins-A Mainwood JA van Wyk JM Baker ME Newton AM Stoneham JP Goss, R Jones and SC Lawson. **Comment on Electronic structure of the NV center in diamond Theory**. *Physical Review B*, **56**.

[136] Simon C Lawson, David Fisher, Damian C Hunt, and Mark E Newton. **On the existence of positively charged single-substitutional nitrogen in diamond**. *Journal of Physics: Condensed Matter*, **10**(27):6171, 1998.

[137] MV Hauf, B Grotz, B Naydenov, M Dankerl, S Pezzagna, J Meijer, F Jelezko, J Wrachtrup, M Stutzmann, F Reinhard, et al. **Chemical control of the charge state of nitrogen-vacancy centers in diamond**. *Physical Review B*, **83**(8):081304, 2011.

[138] L Rondin, G Dantelle, A Slablab, F Grosshans, F Treussart, P Bergonzo, S Perruchas, T Gacoin, M Chaigneau, H-C Chang, et al. **Surface-induced charge state conversion of nitrogen-vacancy defects in nanodiamonds**. *Physical Review B*, **82**(11):115449, 2010.

[139] Y Dumeige, F Treussart, R Alléaume, T Gacoin, J-F Roch, and P Grangier. **Photo-induced creation of nitrogen-related color centers in diamond nanocrystals under femtosecond illumination**. *Journal of luminescence*, **109**(2):61–67, 2004.

[140] NB Manson and JP Harrison. **Photo-ionization of the nitrogen-vacancy center in diamond**. *Diamond and related materials*, **14**(10):1705–1710, 2005.

[141] MD Lukin and PR Hemmer. **Quantum entanglement via optical control of atom-atom interactions**. *Physical review letters*, **84**(13):2818, 2000.

[142] NB Manson, JP Harrison, and MJ Sellars. **Nitrogen-vacancy center in diamond: Model of the electronic structure and associated dynamics**. *Physical Review B*, **74**(10):104303, 2006.

[143] A Lenef and SC Rand. **Electronic structure of the N-V center in diamond: Theory**. *Physical Review B*, **53**(20):13441, 1996.

[144] Adam Gali, Maria Fyta, and Efthimios Kaxiras. **Ab initio supercell calculations on nitrogen-vacancy center in diamond: Electronic structure and hyperfine tensors**. *Physical Review B*, **77**(15):155206, 2008.

[145] A. Lenef and S. C. Rand. **Reply to "Comment on 'Electronic structure of the NV center in diamond: Theory'"**. *Physical Review B*, **56**(24):16033–16034, 1997.

[146] JR Maze, Adam Gali, Emre Togan, Yiwen Chu, Alexei Trifonov, Efthimios Kaxiras, and MD Lukin. **Properties of nitrogen-vacancy centers in diamond: the group theoretic approach**. *New Journal of Physics*, **13**(2):025025, 2011.

[147] JPD Martin. **Fine structure of excited 3E state in nitrogen-vacancy centre of diamond**. *Journal of luminescence*, **81**(4):237–247, 1999.

[148] JHN Loubser and JA Van Wyk. **Optical spin-polarisation in a triplet state in irradiated and annealed type 1b diamonds**. *Diamond Research*, pages 11–14, 1977.

[149] JoHoNo Loubser and JoA van Wyk. **Electron spin resonance in the study of diamond**. *Reports on Progress in Physics*, **41**(8):1201, 1978.

[150] LJ Rogers, RL McMurtrie, MJ Sellars, and NB Manson. **Time-averaging within the excited state of the nitrogen-vacancy centre in diamond**. *New Journal of Physics*, **11**(6):063007, 2009.

[151] RJ Epstein, FM Mendoza, YK Kato, and DD Awschalom. **Anisotropic interactions of a single spin and dark-spin spectroscopy in diamond**. *Nature physics*, **1**(2):94–98, 2005.

[152] JPD Martin, NB Manson, DC Doetschman, MJ Sellars, R Neuhaus, and E Wilson. **Spectral hole burning and Raman heterodyne signals associated with an avoided crossing in the NV centre in diamond**. *Journal of Luminescence*, **86**(3):355–362, 2000.

[153] Joanne Harrison, MJ Sellars, and NB Manson. **Optical spin polarisation of the NV centre in diamond**. *Journal of luminescence*, **107**(1):245–248, 2004.

[154] A Dräbenstedt, L Fleury, C Tietz, F Jelezko, S Kilin, A Nizovtzev, and J Wrachtrup. **Low-temperature microscopy and spectroscopy on single defect centers in diamond**. *Physical Review B*, **60**(16):11503, 1999.

[155] LJ Rogers, S Armstrong, MJ Sellars, and NB Manson. **Infrared emission of the NV centre in diamond: Zeeman and uniaxial stress studies**. *New Journal of Physics*, **10**(10):103024, 2008.

[156] F Jelezko, C Tietz, A Gruber, I Popa, A Nizovtsev, S Kilin, and J Wrachtrup. **Spectroscopy of single NV centers in diamond**. *Single Molecules*, **2**(4):255–260, 2001.

[157] Lucio Robledo, Hannes Bernien, Toeno van der Sar, and Ronald Hanson. **Spin dynamics in the optical cycle of single nitrogen-vacancy centres in diamond**. *New Journal of Physics*, **13**(2):025013, 2011.

[158] Alexios Beveratos, Rosa Brouri, J-P Poizat, and Philippe Grangier. **Bunching and antibunching from single NV color centers in diamond**. In *Quantum Communication, Computing, and Measurement 3*, pages 261–267. Springer, 2002.

[159] Gijsbertus De Lange. *Quantum control and coherence of interacting spins in diamond*. TU Delft, Delft University of Technology, 2012.

[160] T Van der Sar, ZH Wang, MS Blok, H Bernien, TH Taminiau, DM Toyli, DA Lidar, DD Awschalom, R Hanson, and VV Dobrovitski. **Decoherence-protected quantum gates for a hybrid solid-state spin register**. *Nature*, **484**(7392):82–86, 2012.

[161] Lilian Childress, JM Taylor, Anders Søndberg Sørensen, and MD Lukin. **Fault-tolerant quantum communication based on solid-state photon emitters**. *Physical review letters*, **96**(7):070504, 2006.

[162] L Childress, MV Gurudev Dutt, JM Taylor, AS Zibrov, F Jelezko, J Wrachtrup, PR Hemmer, and MD Lukin. **Coherent dynamics of coupled electron and nuclear spin qubits in diamond**. *Science*, **314**(5797):281–285, 2006.

[163] Christoph Dittel. **Spin Manipulation of Nitrogen-Vacancy Color Centers in Diamond**. *Master thesis, Stockholm University*, 2014.

[164] Marlan O Scully and M Suhail Zubairy. *Quantum optics*. Cambridge university press, 1997.

[165] Alexios Beveratos, Sergei Kühn, Rosa Brouri, Thierry Gacoin, J-P Poizat, and Philippe Grangier. **Room temperature stable single-photon source**. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, **18**(2):191–196, 2002.

[166] Eric Ampem-Lassen, DA Simpson, BC Gibson, S Trpkovski, FM Hossain, ST Huntington, K Ganesan, LC Hollenberg, and S Prawer. **Nano-manipulation of diamond-based single photon sources**. *Optics express*, **17**(14):11287–11293, 2009.

[167] Tim Schröder, Friedemann Gädeke, Moritz Julian Banholzer, and Oliver Benson. **Ultrabright and efficient single-photon generation based on nitrogen-vacancy centres in nanodiamonds on a solid immersion lens**. *New Journal of Physics*, **13**(5):055017, 2011.

[168] Thomas M Babinec, Birgit JM Hausmann, Mughees Khan, Yinan Zhang, Jeronimo R Maze, Philip R Hemmer, and Marko Lončar. **A diamond nanowire single-photon source**. *Nature nanotechnology*, **5**(3):195–199, 2010.

[169] Valery Zwiller, Hans Blom, Per Jonsson, Nikolay Panev, Sören Jeppesen, Tedros Tsegaye, Edgard Goobar, Mats-Erik Pistol, Lars Samuelson, and Gunnar Björk. **Single quantum dots emit single photons at a time: Antibunching experiments**. *Applied Physics Letters*, **78**(17):2476–2478, 2001.

[170] Zhiheng Liu, Bennett B Goldberg, Stephen B Ippolito, Anthony N Vamivakas, M Selim Ünlü, and Richard Mirin. **High resolution, high collection efficiency in numerical aperture increasing lens microscopy of individual quantum dots**. *Applied Physics Letters*, **87**(7):071905, 2005.

[171] P Siyushev, F Kaiser, V Jacques, I Gerhardt, S Bischof, H Fedder, J Dodson, M Markham, D Twitchen, F Jelezko, et al. **Monolithic diamond optics for single photon detection**. *Applied physics letters*, **97**(24):241902, 2010.

[172] JP Hadden, JP Harrison, AC Stanley-Clarke, L Marseglia, Y-LD Ho, BR Patton, JL O'Brien, and JG Rarity. **Strongly enhanced photon collection from diamond defect centers under microfabricated integrated solid immersion lenses**. *Applied Physics Letters*, **97**(24):241901, 2010.

[173] Mohammad Jamali, Ilja Gerhardt, Mohammad Rezai, Karsten Frenner, Helmut Fedder, and Jörg Wrachtrup. **Microscopic diamond solid-immersion-lenses fabricated around single defect centers by focused ion beam milling**. *Review of Scientific Instruments*, **85**(12):123703, 2014.

[174] S Ali Momenzadeh, Rainer J Stohr, Felipe Favaro de Oliveira, Andreas Brunner, Andrej Denisenko, Sen Yang, Friedemann Reinhard, and Jorg Wrachtrup. **Nanoengineered diamond waveguide as a robust bright platform for nanomagnetometry using shallow nitrogen vacancy centers**. *Nano letters*, **15**(1):165–169, 2014.

[175] D Riedel, D Rohner, M Ganzhorn, T Kaldewey, P Appel, E Neu, RJ Warburton, and P Maletinsky. **Low-loss broadband antenna for efficient photon collection from a coherent spin in diamond**. *Physical Review Applied*, **2**(6):064011, 2014.

[176] Jennifer T Choy, Irfan Bulu, Birgit JM Hausmann, Erika Janitz, I-Chun Huang, and Marko Lončar. **Spontaneous emission and collection efficiency enhancement of single emitters in diamond via plasmonic cavities and gratings**. *Applied Physics Letters*, **103**(16):161101, 2013.

[177] Luozhou Li, Edward H Chen, Jiabao Zheng, Sara L Mouradian, Florian Dolde, Tim Schroder, Sinan Karaveli, Matthew L Markham, Daniel J Twitchen, and Dirk Englund. **Efficient photon collection from a nitrogen vacancy center in a circular bullseye grating**. *Nano letters*, **15**(3):1493–1497, 2015.

[178] L Marseglia A C Stanley-Clarke B C Gibson B A Fairchild J P Hadden Y-L D Ho M P Hiscocks K Ganesan S Castelletto1, J P Harrison. **Diamond-based structures to collect and guide light**. *New Journal of Physics*, **13**.

[179] J. M. Gerard P. Jonsson-J. A.E. Wasey P. T. Worthing W. L. Barnes, G. Bjork and V. Zwiller. **Solid-state single photon sources: light collection strategies**. *Eur. Phys. J. D*, **18**.

[180] T. R. Corle and G.S. Kino. *Confocal scanning optical microscopy and related imaging systems*.

[181] Motoyoshi Baba, Takeaki Sasaki, Masahiro Yoshita, and Hidefumi Akiyama. **Aberrations and allowances for errors in a hemisphere solid immersion lens for submicron-resolution photoluminescence microscopy**. *Journal of applied physics*, **85**(9):6923–6925, 1999.

[182] Patrick Maletinsky, Sungkun Hong, Michael Sean Grinolds, Birgit Hausmann, Mikhail D Lukin, Ronald L Walsworth, Marko Loncar, and Amir Yacoby. **A robust scanning diamond sensor for nanoscale imaging with single nitrogen-vacancy centres**. *Nature nanotechnology*, **7**(5):320–324, 2012.

[183] Philipp Neumann, Ingmar Jakobi, Florian Dolde, Christian Burk, Rolf Reuter, Gerald Waldherr, Jan Honert, Thomas Wolf, Andreas Brunner, Jeong Hyun Shim, et al. **High-precision nanoscale temperature sensing using single defects in diamond**. *Nano letters*, **13**(6):2738–2742, 2013.

[184] S Ali Momenzadeh, Felipe Fávaro de Oliveira, Philipp Neumann, DD Rao, Andrej Denisenko, Morteza Amjadi, Sen Yang, Neil B Manson, Marcus W Doherty, and Jörg Wrachtrup. **Development of a high quality thin diamond membrane with embedded nitrogen-vacancy centers for hybrid spin-mechanical quantum systems**. *arXiv preprint arXiv:1602.08320*, 2016.

[185] Tobias Staudacher, Fazhan Shi, S Pezzagna, Jan Meijer, Jiangfeng Du, Carlos A Meriles, Friedemann Reinhard, and Joerg Wrachtrup. **Nuclear magnetic resonance spectroscopy on a (5-nanometer) 3 sample volume**. *Science*, **339**(6119):561–563, 2013.

[186] M Loretz, S Pezzagna, J Meijer, and CL Degen. **Nanoscale nuclear magnetic resonance with a 1.9-nm-deep nitrogen-vacancy sensor**. *Applied Physics Letters*, **104**(3):033102, 2014.

[187] T Häberle, D Schmid-Lorch, F Reinhard, and J Wrachtrup. **Nanoscale nuclear magnetic imaging with chemical contrast**. *Nature nanotechnology*, **10**(2):125–128, 2015.

[188] HJ Mamin, M Kim, MH Sherwood, CT Rettner, K Ohno, DD Awschalom, and D Rugar. **Nanoscale nuclear magnetic resonance with a nitrogen-vacancy spin sensor**. *Science*, **339**(6119):557–560, 2013.

[189] Rajesh Babu Sekar and Ammasi Periasamy. **Fluorescence resonance energy transfer (FRET) microscopy imaging of live cell protein localizations**. *The Journal of cell biology*, **160**(5):629–633, 2003.

[190] JB Pawley and Barry R Masters. **Handbook of biological confocal microscopy**. *Optical Engineering*, **35**(9):2765–2766, 1996.

[191] Shigeki Takeuchi. **Recent progress in single-photon and entangled-photon generation and applications**. *Japanese Journal of Applied Physics*, **53**(3):030101, 2014.

[192] Christian Kurtsiefer, Patrick Zarda, Sonja Mayer, and Harald Weinfurter. **The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?** *Journal of Modern Optics*, **48**(13):2039–2047, 2001.

[193] Alexios Beveratos, Rosa Brouri, Thierry Gacoin, Jean-Philippe Poizat, and Philippe Grangier. **Nonclassical radiation from diamond nanocrystals**. *Physical Review A*, **64**(6):061802, 2001.

[194] Inga A Dobrinets, Victor G Vins, and Alexander M Zaitsev. *HPHT-treated diamonds*. Springer, 2013.

[195] Martin Berthel, Oriane Mollet, Géraldine Dantelle, Thierry Gacoin, Serge Huant, and Aurélien Drezet. **Photophysics of single nitrogen-vacancy centers in diamond nanocrystals**. *Physical Review B*, **91**(3):035308, 2015.

[196] MV Hauf, B Grotz, B Naydenov, M Dankerl, S Pezzagna, J Meijer, F Jelezko, J Wrachtrup, M Stutzmann, F Reinhard, et al. **Chemical control of the charge state of nitrogen-vacancy centers in diamond**. *Physical Review B*, **83**(8):081304, 2011.

[197] Vikram Passi, Aurelie Lecestre, Christophe Krzeminski, Guilhem Larrieu, Emmanuel Dubois, and Jean-Pierre Raskin. **A single layer hydrogen silsesquioxane (HSQ) based lift-off process for germanium and platinum**. *Microelectronic Engineering*, **87**(10):1872–1878, 2010.