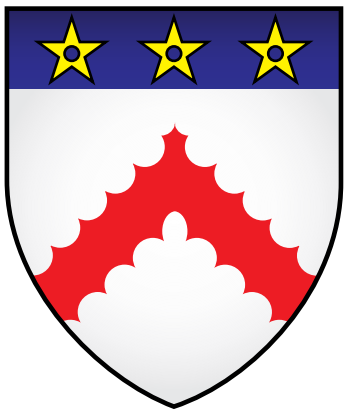
Towards Practical Applications of Quantum Optics

David Drahi

Keble College
University of Oxford



A thesis submitted for the degree of
Doctor of Philosophy

Trinity Term 2019

Supervised by
Prof. Alex I. Lvovsky

Clarendon Laboratory
University of Oxford
United Kingdom

Pour Maman et Papa
sans qui rien n'aurait été possible

Towards Practical Applications of Quantum Optics

David Drahi
Keble College, Oxford

Submitted for the degree of Doctor of Philosophy
Trinity Term 2019

Abstract

This DPhil thesis presents two key works towards practical applications of quantum optics. Both works are novel and achieve competitive state-of-the-art results.

Today's most widely used method of encoding quantum information in optical qubits is the dual-rail basis, often carried out through the polarisation of a single photon. On the other hand, many stationary carriers of quantum information — such as atoms — couple to light via the single-rail encoding in which the qubit is encoded in the number of photons. As such, interconversion between the two encodings is paramount in order to achieve cohesive quantum networks. In the first part of this thesis, we demonstrate this by generating a hybrid entangled resource between the two encodings and using it to teleport a dual-rail qubit onto its single-rail counterpart. Our key results yield an average fidelity of $\mathcal{F} = (92.8 \pm 2.2)\%$ for the teleportation and $\mathcal{F} = (89.7 \pm 2.1)\%$ for entanglement swapping, thus confirming the applicability of this scheme towards a real-world implementation. This work completes the set of tools necessary for the interconversion between the three primary encodings of a qubit in the optical field: single-rail, dual-rail and continuous-variable.

A remarkable aspect of quantum theory is that certain measurement outcomes are entirely unpredictable to all possible observers. Such quantum events can be harnessed to generate numbers whose randomness is asserted based upon the underlying physical processes. In the second part of this thesis, we formally introduce and experimentally demonstrate an ultrafast optical quantum randomness generator that uses a totally untrusted photonic source and whose idea we have patented. While considering completely general quantum attacks, we certify randomness at a rate of 1.1 Gbps with a rigorous security parameter of 10^{-20}. Our security proof is entirely composable, thereby allowing the generated randomness to be utilised for arbitrary applications in cryptography and beyond.

Preface

Thus, gentle Reader, has come the moment for me to address myself directly to *you*. Following a long-standing practice of sheer academic tradition, it is now expected of me to utter my Acknowledgements. However, after having long reveled at the arrival of this precise moment of my DPhil for the last three years and having carefully thought about what I would write within it, I have decided to share with you some personal thoughts in this Preface that I chose to insert prior to the Acknowledgements. Indeed, very seldom was I given the chance to write on paper my personal convictions and ideas acquired over time, and after the completion of my DPhil thesis, the occasion simply craves for it. Moreover, you will find in the body of this DPhil thesis a myriad of scientific explanations, equations and technicalities such that one's intrinsic human soul might be left wondering what there is for itself in this particular document. As such, it is in the hope of encompassing the humanity within us all that I chose to include this specific part in an otherwise predominantly scientific work. My sincere wish, dear Reader, is that the ideas shared here will genuinely help you find your way just like I found my own, no matter who you are. Therefore, please allow me to do so.

By dismissing few exceptional cases, one can safely assume that men, throughout the planet and the history of modern times, have experienced similar settings for what we generally call Life. Usually, it begins with birth somewhere in a family with parents and potentially some siblings, and then is followed by the key stages that are education, work, the making of a family and nurturing it and — alas — death. Yet, given these ubiquitous settings, what is it that makes some men more accomplished than others? You might wonder, perhaps, why should we even bother thinking about accomplishment and live in a society underlain by comparison when death meets us all in the end? In fact, this critical and completely justified train of thoughts must lead oneself to the following two important questions: what purpose shall be sought in Life and, given one such purpose, how can one perfect its realisation to the fullest?

Well, courteous Reader, while I am no philosopher, I should still like to attempt and provide you with an answer to the first question. Obviously, as you might expect from the first paragraphs, this present text will mainly focus on the latter of the two questions.

In my humble opinion, my fair Reader, the purpose of Life for us humans is none other than dedicating ourselves — with the fullest of our force and intellect — to our own passions. You may rightly so ask what these passions are and how we may find them ourselves? To this, I advise you listen to your heart and your boiling curiosity

that, akin to steam constrained in a closed environment, awaits nothing but to be expanded upon. And by fervently abiding by your own curiosity, you will quench the insatiable desire for freedom that yearns in every human being such that one day, you will realise by yourself what you truly care about and may henceforth call *your passion*. For some, it might be domains as well defined as physics or classical music or playing tennis, while others might claim their passion to be about broader actions such as taking care of others and being a good civilian. Overall, no matter the passion, it must be yours and yours only.

Now, enough of the general talk and philosophical questioning. You should have by then found your passion and entered the realm of the second question posed above: how to perfect its realisation? You see, while the reasoning presented above was heavily marked by questions and thinking for yourself, this new realm abides by the laws of doing and pragmatism. Indeed, Shakespeare brilliantly put it in "Hamlet" wherein the Danish Prince pronounces:

"Thus conscience does make cowards of us all,
And thus the native hue of resolution
Is sicklied o'er with the pale cast of thought,
And enterprises of great pitch and moment
With this regard their currents turn awry
And lose the name of action."

Here, to prevent oneself from becoming a coward, one is advised to thwart his own ever-questioning conscience, thereby allowing him to steer his enterprises steadfast in the direction given by his own native resolution. In other words, instead of pondering endlessly, Hamlet should simply have *done* and avenged his father.

And this is chiefly what I advise you to do, my dear Reader: listen to your natural confidence, deliver and never allow self-doubt for a single moment. Let the doubting be for others: the natural course of Life already will show you how much people and situations will doubt of you when you are willing to perfect your passion. Arthur Miller summarised it perfectly in this fine line found in his family drama "All my Sons" where Kate Keller tells her son the naive Chris:

"You don't realize how people can hate, they can hate so much they'll tear the world to pieces."

Of course, wise Reader, it should be said as an obvious caveat that you must invest in those passions of yours for which you have some innate degree of talent. Indeed, while the act of striving is noble nevertheless, you will not achieve a Nobel Prize in physics if your mind is not mathematical from birth, nor will you become the best tennis player on Earth if your motor skills are not naturally good. Ensuing this judgement of pure common sense, it is paramount for you to aim to excel at one aspect of your passion at a time rather than mediocrely trying to master its entirety directly. For this, you will find that the concept of basics, or principles, is of utmost importance. I believe in the approach of René Descartes: if you wish to understand a complex idea or master a challenging skill, you must start by dividing it into smaller pieces of lesser complexity. And — ask yourself — what happens when one continuously subdivides anything? Well, one ends up reaching its basics and thus, as

a natural corollary to the cartesian method, you must perfectly assimilate the basics and principles defining the particular aspect of this passion of yours. In the context of physics for example, this means an understanding and ease in mathematics; for classical music it suggests that one should start by knowing very well the works of the greats like Mozart and Bach before composing one's own music. No matter what task lies ahead of you in order to perfect the realisation of your passion, it will always fall into one of two categories: to either create something new or improve upon something that already exists. And in my opinion, basics will always serve you well when facing such task, no matter the category it assimilates the most to. Learn and master your basics before you can ever reach further.

Now, what follows, esteemed Reader, when you have both found your passion and grasped the importance of basics? Well, beyond the initial excitement of that newly-found fire inside you and its defining principles, you shall now enter the stage in which you must truly perfect your art. For that, there are few ideas and tips I should like to share with you. The first is that you must use your excitement and curiosity to learn all you can in that passion of yours. Never leave hanging anything that you cannot understand, for you should treat your own ignorance with complete abhorrence. This discipline of constantly learning and inquiring requires a lot of work and might discourage you at times, yet its essence is easily justified since when you have reached a stage of deep and total understanding of your art, you are more likely to share and perform it best.

And adding to this perfectionism, I advise you — as a second idea — to surround yourself with like-minded people, those that share the same enthusiasm for Life and have similar passions to yours. Indeed, very seldom is any individual achievement the result of one person's work or thoughts. Instead, by being with people similar to you, constantly engaging with them and listening to them, you can learn greatly, discuss and quickly expand on your knowledge required to perfect the realisation of your passion. These interactions are eminently important, cherish them and they will give you more than you would have hoped.

Finally, as a third idea, perhaps the most important eventually, I say you must be true to yourself at all times. You see, everyone, no matter who they are, has their own natural ways of thinking and being. Yet, the more you progress in Life, the more you will find yourself in situations in which the natural expression of yourself will be challenged by the views of others. May it be when you are stating your own opinion and taste about a topic, or addressing yourself to an audience or simply expressing your feelings to someone: you must obey your own nature and never fear clearly exposing it. If you let your original message or action be modified — by fear of others' rejection or by wish to be *liked or praised* by them — then I am afraid, honest Reader, that whatever message you will try to convey will inevitably become insipid. Worse even, you might change as a person and the glorious fires from which all your enthusiasm originated will be forever lost. Of course, applying this maxim in daily Life requires immense courage as, naturally, it will lead to you facing constant challenges and questioning. However, by remaining true to yourself, you will become a much stronger and more resilient person since your mind will not be corrupt. And as a result, you will perfect your passion like no others and the dreams that are yours would have been kept intact. About this, the illustrious

Albert Einstein, arguably the greatest physicist that ever lived, said:

"Great spirits have always encountered opposition from mediocre minds. The mediocre mind is incapable of understanding the man who refuses to bow blindly to conventional prejudices and chooses instead to express his opinions courageously and honestly."

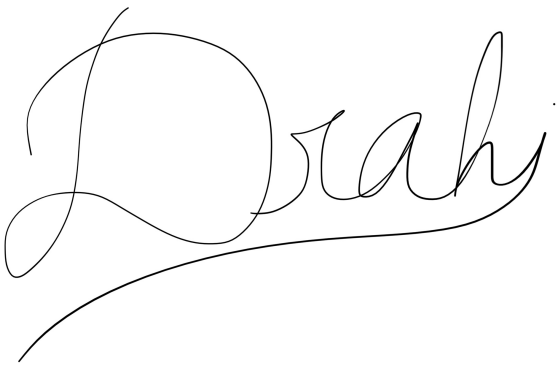
Thus far, my kind Reader, most of what has been described to you belongs to the educational stage of Life previously introduced. And it is my conviction that, by the end of your own education and formation, you must be well-versed in the principles and ideas described above if you ever wish to set yourself on the track of becoming an accomplished man. By following the advices in this text, you will find no limit to what you can achieve, learn or enjoy in this world. Many successes will come greet you and people will deeply respect you as a consequence and aspire to becoming like you since you would have lead by the noblest of example. Yet, is this simply it? Is that all there is to Life? Is Life merely *about you* constantly perfecting the realisation of your passions through whatever maxim or principle you might have derived, read or heard from someone else? Do accomplishments and successes suffice?

My fair and educated Reader, I hereby addressed myself directly to *you* and now stand before you like the great roman politician and general Mark Antony in front of the people of Rome on the day he defended the defiled and lifeless body of Julius Caesar, his most noble friend and source of his inspiration and convictions. And akin to him needing to *pause till his heart comes back to him*, as was put so eloquently by Shakespeare at the end of "Julius Caesar"'s central speech, I must too pause and leave it to *you* to answer those above-mentioned questions. Fight for your dreams, trust yourself and never doubt your heart, for all the answers required lie within it. You are what you choose to be.

Wishing you the most glorious and insightful journey along this beautiful path we call Life on Earth.

Yours most philosophically,

David Drahi



Acknowledgements

Throughout the completion of my DPhil at the University of Oxford, there are many people to whom I am eminently thankful. May it be someone that provided help in science and beyond, has given me support by lending an ear (or two), or simply a person with whom I was lucky enough to have shared educational life experiences, I should like to dedicate the following few words to them all.

The first person I wish to thank is my supervisor Professor Alex Lvovsky. Alex, you may not realise how much it meant to me back then but where should I start? A Skype call on Tuesday the 24th of April 2018. Coming from my situation after a year and a half without supervision in a disastrous and crumbling group, you opened up doors that I had dreamt of for years, and some that I hadn't even imagined. Indeed, going to work for half a year in your group at the Russian Quantum Center in Moscow was by far the best life experience I've had over my 24 years of age. In addition to the fact that I can now proudly claim to have survived through the four seasons of the notoriously tough Russian weather (which in reality is absolutely adorable, especially... winter!), the atmosphere in your group — perhaps a direct image of you in the Fourier plane — was a pure quantum superposition of brilliant scientists with limitless curiosity and people with kind hearts whose Russian souls I have been grateful to discover. Also, what on Earth can be said about the lab downstairs and the quantum teleportation experiment undertaken therein?! Arguably the most exciting setup I've laid hands on (provided you've correctly aligned it all... yes, you guys know what I'm talkin' about) and gratifying intellectual journey I have ever undertaken. Alex, as a physics undergraduate student, it was my dream to explore experimental Quantum Optics and thanks to you, it was made true in ways I would never have conceived. From you, I have learned the importance of diplomacy and I will keep fond memories of those days we spent together towards the end of May 2019 amending the H1V0 paper, scientifically arguing over it (where I have to admit that your rhetoric always seemed much stronger than mine) and sharing each other's personal views on life as well as our belonging to the same obscure yet ubiquitously successful sect... It was a pleasure to be your student and mentee and I truly wish you all the best of success in your exciting Machine Learning and Robotics endeavors!

Coming up, the very two people I will forever be grateful to and without whom the work presented here wouldn't have been: Nathan (Walk) and Demid. I oftentimes tell myself that in $20-30$ years, I will probably forget most of the scientific content and achievements made throughout my DPhil. However, if there is something that will vividly be remembered, it is the exciting journey and human experiences shared

with you two. Reminiscing them tempts me to cite some of Reagan's famous conclusions at his farewell address to the Nation: "My friends, we did it" and "All in all, not bad. Not bad at all." Indeed, Nathan, how can effort and resilience better be embodied than by what we went through together to get this QRNG working and write its titanic 27 pages long paper? You will agree this is especially true given the many ups and downs we faced over years and the key existential questionings that arose along the way concerning our QRNG (do you remember the panic ensuing the temporal detection issue with Eve making infinitely narrow pulses in time leading to a complete predictability of our difference measurement?!). Over the two and a half years since I've met you, I cannot be thankful enough for your time, devotion to this project and your constant and altruistic generosity in explaining quantum informational concepts to me. Even more important, during the darkest times of this long-running project where nothing seemed like progressing, the directions were unclear and the group situation unpleasant, you were the only one in Oxford to provide an attentive ear to my complains and questions. These moments of key importance kept my enthusiasm going and together we concluded the work I'm the proudest of. And speaking of milestones, I want to pay a tribute to the nearly 48 hours we spent together on Skype restructuring the paper after I came back from Russia. This was colossal work, full of some of the most insightful scientific discussions of my DPhil (it surely felt good to solve that wicked temporal issue...) and I will particularly remember the times during these Skype calls in which we both shared our taste for literature and Arthur Miller. Thank you Nathan, may you and Helen be the happiest Aussies in Berlin and I hope you will soon become a Professor back home. Now Demid, my dear brother-in-arms, words cannot express the affection and respect I have earned for you. My most exciting moments in science have taken place when working with you in that impressive lab downstairs in Moscow. May it be when I first experienced the quantum regime and you had the SPDC crystals emit single photons, when we were enthusiastically optimising — late at night after much toil — the single-photon quantum efficiency (and breaking the group's records!), when I first witnessed a Hong-Ou-Mandel dip thanks to you having cleverly thought about adding that paramount quarter wave plate for the Bell projector to correctly function, or when we both euphorically retrieved those tremendously good-looking teleportation density matrices during the data analysis; you have continually lead by example. To me, you symbolised the role model of what a great scientist should be: someone that keeps his cool and solves problems by incessantly trying, failing and eventually prevailing. In addition to that, I deeply thank you for your patience as well as calm and pedagogical approach when explaining the myriad of technicalities associated with our setup. Demid, there are two souvenirs I wish to write down here in order to both honour and ponder over the good old muscovite days. The first was meaningful and happened on that day we went ice skating at VDNKh on the 14th of February 2019 — it was exactly the day I had successfully obtained all the results for the experiment — and I recall experiencing and sharing with you the comforting feeling that our work on that experiment was done just right. It then seemed extremely clear what path I was going to follow to complete this DPhil and tackle my new challenges thereafter. The second moment was more of a poetical synesthesia that occurred earlier on the night of Thursday the 22nd of November 2018. It was right after our Chinese dinner in Kitay Gorod with Egor. You might remember that this night, we walked through Zaryadye Park with its stunning panoramic view of

Moscow under the sweet carpet of freshly fallen snow. In this precise situation, we three discussed the meaning of life and I remember you said that our purpose was "to build something greater than us". We later philosophised about the need for total immersion in our work in order to do meaningful science while walking across the Red Square full of its eponym color whose name stands for beauty (krasnaye) in Russian. The full moon was casting its gleaming white light upon the Square, revealing all its magnificence, and when I stepped into the metro from Okhotny Ryad to Ploschad Revolutsii, hearing the melancholic soviet tunes played by the guitarist in the long and lonely corridor, I realised how lucky I was to be part of this great adventure that the H1V0 experiment turned out to be. Being now nostalgic of my Russian adventures, I thank you Demid for your help and wish you live the true American dream in Purdue prior to becoming soon a great Professor yourself.

I would then like to acknowledge the people at the Russian Quantum Center and especially him that once said "David, you're maximally entangled with the setup downstairs" on a late evening the 16th of November 2018, and after whose comment we both shared a huge laughter of excitement revealing the full range of complicity and camaraderie that had been weaving since we had met and immediately sympathised. Yes, Egor, that's precisely you. And while I recall soothing and fun memories with you playing ping-pong next to the lab after long and hard working days, enjoying tasty food together (remember those spaghetti carbonara dude? Wow, that was a change for the canteen!), or deeply discussing about "the machine being intelligent" on our way from the canteen back to the office; I wish you "Bonne Chance" (it needs to be read with that Albanian accent) starting a beautiful family with Vera and getting that Machine Learning postdoc in the best place possible.

The next important place with people that deserve a big mention is Oxford and in it, my College Keble. Starting with my loyal friends Shaobo and Clemens. I thank you guys for being there when it mattered and spending such good times together during those innumerable, yet crucially important, lunches and dinners at New and Christ Church (by the way, I can only admit now that they both are overall better looking than Keble... especially New!), Sasi's Thai or the various Chinese restaurants we tried where Shaobo masterfully chose the food for us. Shaobo, thank you for the Niu Lan Keng Rougui from the Wuyi Mountains — by far the best I've ever had. Our discussion that day where you told me your life aspirations will be remembered. Clemens, thank you for the many rowing tips you gave me when I got started (although these came from back when you were a Tab... I hope you are now a convinced dark blue). I look forward to baking that Sachertorte with you as our chef and Shaobo. From the Physics department and my old group: William for your immense generosity and unwavering kindness, Patrick for having been the only honest person with me in the group when the event happened and being so nice and positive all the time, Raj for helping out with that sick 3D figure, Magda for having been such an attentive office mate for months, Professor Peter Norreys for always having your door open and given the advices that helped me get through, and all the people that provided scientific help along the way. Now comes Keble and as a true Keblite, I owe the unsung heroes of our College the recognition they deserve. Felipe (now gone at Univ... but you'll remain a Keblite to me), Bas, Conor, Patrick, Ken and the rest: your job was never easy, yet know that you are the College's main artery. I'll keep warm memories of some of those late night discussions we had.

Then my good friends Imanol, Subhayan and Joe (by the way, how on Earth did I manage to be friends with so many mathematicians and theoretical physicists?) and all the members from the MCR, we had such a great time together. Imanol, may it be chess, pool, foosball, squash or anything else, it was a pleasure to be your noble adversary and I hope that one day you get that successful hedge fund of yours living in London with Marina. Subhayan, thank you for having initiated me to the awesomeness of the American golf at Oxford — it certainly was nice hitting some balls together. Also, that Sunday morning discussion at George's social was helpful and very considerate from you. To you, I can only wish one thing (and you'll know what I'm talking about): "just take that rifle and shoot man". Joe, it was such an honour to live with you some of my most exciting and labourious times in Oxford in that eight — we truly were the boys in the boat mate. Kudos to us for having been that legendary stern pair of M1, even if it was ephemeral! I wish you to be happy forever with Archna. From the boat club at Keble, I wish to acknowledge Callum and John for having instilled in me the true spirit of hard work and brotherhood in rowing. Finally, a shout-out to Irina for having helped me move out of Oxford — much appreciated.

Now, if there is heaven on Earth, I would then like to utter this special and particularly personal mention to Mozart. Akin to Mahler whose symbolic last words indeed were "Mozart! Mozart!", I want to thank the greatest genius that ever existed. His music not only speaks with the very voice of God but it also brings out the sheer humanity encompassing us all. Mozart, you have countlessly filled me with the emotions that are most noble in a man and for that, I thank you and will continue cherishing as well as breathing your music for the rest of my life.

Finally, none of what I did would have been possible without the constant love and support from my dear family. Nathan, thank you for being my best friend and confidant. We two are very young and yet we've achieved so much. It is my deepest conviction that we are currently confidently staring straight ahead at a life full of accomplishments and joys: let it be ours. Angelina, I am so proud of you. The courage required to move across the Pond and settle there is the very testament of your genuine qualities. Your wedding was the best celebration on this planet and I wish you and Dan the happiest life with many children. Graziella, you have showed everyone how tough you were throughout the many challenges you had to face. Being confident that you will prevail everywhere, I wish you the best with your current job. And most importantly, Mum and Dad. This thesis is dedicated to you. You have taught me the values that define my jewish identity and from which I constantly draw my strength and soul. Mum, you truly are the family's spine and my biggest supporter. Thank you so much for showing me the way of the heart. Dad, you are my role model and your passion for everything you do in this world is a huge inspiration to me. Thank you for having taught me so much and taken me to all these wonderful places full of inspiring people, I look forward to our glorious days ahead. And thus it is finally done... you now have a doctor in the family! Mazel tov!

Publications

Journal Publications

1. D. Drahi, D. V. Sychev, K. K. Pirov, E. A. Sazhina, V. A. Novikov, I. A. Walmsley, and A. I. Lvovsky. "**Quantum Interface Between Single- and Dual-Rail Optical Qubits**" *ArXiv* preprint arXiv:1905.08562 (2019).

2. D. Drahi, N. Walk, M. J. Hoban, W. S. Kolthammer, J. Nunn, J. Barrett, and I. A. Walmsley. "**Certified Quantum Randomness from Untrusted Light**" *ArXiv* preprint arXiv:1905.09665 (2019).

3. B. Rigal, D. Drahi, C. Jarlov, B. Dwir, A. Rudra, A. Lyasota, and E. Kapon. "**Probing Disorder and Mode Localization in Photonic Crystal Cavities using Site-Controlled Quantum Qots**" *Journal of Applied Physics*, **123**(4), 043109 (2018).

Conference Presentations

1. D. Drahi, D. V. Sychev, A. E. Ulanov, E. S. Tiunov, A. A. Pushkina, A. Kuzhamuratov, V. A. Novikov, E. A. Sazhina, K. K. Pirov, I. A. Walmsley, and A. I. Lvovsky. "**The Three Qubits in Quantum Optics**" *The International Laser Physics Workshop (LPHYS'19)*, July 2019.

2. D. V. Sychev, D. Drahi, A. E. Ulanov, E. A. Sazhina, A. A. Pushkina, E. S. Tiunov, V. A. Novikov, I. A. Fedorov, A. Kuzhamuratov, K. K. Pirov, I. A. Walmsley, and A. I. Lvovsky. "**Entanglement between Continuous Variables and Discrete Variables**" *International Conference on Quantum Technologies (ICQT 2019)*, July 2019.

'And as I sat there brooding on the old, unknown world, I thought of Gatsby's wonder when he first picked out the green light at the end of Daisy's dock. He had come a long way to this blue lawn, and his dream must have seemed so close that he could hardly fail to grasp it. He did not know that it was already behind him, somewhere back in that vast obscurity beyond the city, where the dark fields of the republic rolled on under the night.

Gatsby believed in the green light, the orgastic future that year by year recedes before us. It eluded us then, but that's no matter—to-morrow we will run faster, stretch out our arms farther. . . . And one fine morning––

So we beat on, boats against the current, borne back ceaselessly into the past.'

Nick Carraway from F. Scott Fitzgerald's "The Great Gatsby"

Contents

List of Figures

List of Tables

Chapter 1

Introduction

'Soldats, vous avez en quinze jours remporté la victoire, pris 21 drapeaux, 55 pièces de canon, plusieurs places fortes, conquis la partie la plus riche du Piémont; vous avez fait 15000 prisonniers, tué ou blessé près de 10000 hommes.

Vous vous étiez jusqu'ici battus pour des rochers stériles. Dénués de tout vous avez supplée à tout. Vous avez gagné des batailles sans canons, passé des rivières sans pont, fait des marches forcées sans souliers, bivouaqué sans eau-de-vie et souvent sans pain. Les phalanges républicaines, les soldats de la liberté étaient seuls capables de souffrir ce que vous avez souffert.

Mais soldats, vous n'avez rien fait, puisqu'il vous reste encore à faire. Ni Turin, ni Milan ne sont à vous. La patrie a droit d'attendre de vous de grandes choses: justifierez vous son attente ? Vous avez encore des combats à livrer, des villes à prendre, des rivières à passer. Tous brûlent de porter au loin la gloire du peuple français; tous veulent dicter une paix glorieuse, tous veulent, en rentrant dans leurs villages, pouvoir dire avec fierté: "J'étais de l'armée conquérante d'Italie!".

Amis, je vous la promets, cette conquête; mais il est une condition qu'il faut que vous juriez de remplir, c'est de respecter les peuples que vous délivrerez, c'est de réprimer les pillages horribles. Les pillards seront impitoyablement fusillés.

Peuple d'Italie, l'armée française vient rompre vos chaînes; venez en confiance au devant d'elle.'

Discours du Général Napoléon Bonaparte lors de la Campagne d'Italie

The theory of quantum physics is arguably one of the greatest intellectual achievements of mankind. Despite appearing oftentimes counterintuitive, it rigorously describes phenomena such as superposition [1] and entanglement [2] within systems of atomic and subatomic scales. Such instances of quantum physics are not observable in our daily lives, abiding by the laws of classical physics, yet quantum physics deserves its fame for being one of the most successful scientific theories ever put to continuous test [3]. From solving the *ultraviolet catastrophe* by coming up with Planck's law [4] for the black body radiation, to describing the exceptionally important photoelectric effect [5], correctly predicting the energy levels of atoms [6] and proposing the uncanny wave-particle duality [7], its triumphs were many, leading to *"enterprises of great pitch and moment"*.

However, amongst the various fields of quantum physics, quantum optics reigns supreme. Seldom has a physical domain featured such a sheer duality between its scientific fundamentality and the ensuing practical applicability.

Indeed, it is within quantum optics that Einstein's famously enunciated *"spooky action at a distance"* [8] was first experimentally demonstrated [9] to be arising from the truly non-local nature of quantum physics via the violation of Bell's inequality [10] in the CHSH form [11]. Moreover, the wave-particle duality of quantum physics is readily observable for light, wherein the wave-like behaviour is found in the interference of a single photon with itself in a Mach-Zehnder interferometer [12, 13, 14], while the Hong-Ou-Mandel interference [15] and photon anti-bunching effect [16] provide strong experimental evidence for a quantised nature of the electromagnetic field with bosons. Another fundamentally important contribution of quantum optics is in metrology [17], where the use of squeezed light [18] in an optical interferometer enables measurements beyond the shot-noise limit [19, 20], thereby leading to enhanced sensitivity detection schemes [21, 22] for the successful and groundbreaking first observation of gravitational waves [23] in 2016, as was eminently surmised by Einstein [24, 25] a century ago in 1916. Furthermore, the experimental proof of micro-macro entanglement — an idea that was a mere *Gedankenexperiment*

for Schrödinger in 1935 [1] — for light [26, 27] has enlightened the hypothesis of whether quantum physics could be applied to macroscopic systems. Finally, in the continuously-explored paradigm of quantum computing [28, 29, 30, 31, 32], quantum optics may offer a solution exploiting non-classical states of light in the framework of linear optics [33, 34] and so-called one-way quantum computing [35].

On the other hand, the applicability of quantum optics is outstandingly natural. This ubiquity is due to most of light's applications fitting in telecommunications sciences where the current architectures of fibre optical networks and free-space mobile technologies — both using the wave-like and particle-like behaviours of light — are extensively developed. As such, quantum enhanced applications are well suited to such optical systems [36]. These include quantum communications [37] by means of quantum states of light and atomic ensembles [38] in order to achieve cohesive quantum networks leading to a quantum internet [39]; quantum cryptography where quantum random number generators (QRNGs) [40] generate ultrafast randomness entirely unpredictable by any eavesdropper [41], quantum key distribution (QKD) [42, 43] for which the exchange of cryptographic keys in a purely unhackable way is enabled and which has already been successfully implemented for satellite communications [44] and fibre optical networks [45] over state-of-the-art distances of 1200 km and 421 km, respectively; and optical atomic clocks taking advantage of entanglement to reach unprecedented levels of accuracy [46, 47].

Building upon this intrinsic interplay between fundamentals and applications, most of the work carried out today in quantum optics is designed to improve its current results in the above-mentioned applications. Overall, this is done by engineering entangled and superposition states of light encompassing increasingly more photons [48], overcoming the inevitable losses present in transmission channels [49, 50], improving detection efficiencies [51] and coming up with contrivances to leverage the quantum effects at hand in the most efficient manner. It is precisely along this line of thought that the work presented and detailed in this thesis has been done, hence its title *"Towards Practical Applications of Quantum Optics"*.

1.1 Thesis Outline

The outline of this thesis is as follows. Chapter 1, *"Introduction"*, contains the above introduction to this thesis. Then, as an introduction to the field, Part I entitled *"Fundamentals of Quantum Optics"*, describes the theoretical formalism of quantum optics. Chapter 2, *"The Quantum Theory of Light"*, covers the quantisation of the electromagnetic field by means of the quantum harmonic oscillator model, the various quantum states of light used in the works carried in the thesis, the Wigner function representation in phase space, the different modal transformations as well as the main measurements available in quantum optics.

In part II, *"Quantum Interface between Single- and Dual-Rail Optical Qubits"*, the first research project of this thesis is extensively detailed. It consists of a complex experiment used to demonstrate the first-ever interconversion between the single-rail and dual-rail encodings of a discrete variable optical qubit. This was achieved with the help of a hybrid entangled state between the two encodings from which remote state preparation, quantum teleportation as well as entanglement swapping were performed, all with state-of-the-art results. The first two chapters, Chapter 3, *"Background and Generalities"*, and Chapter 4, *"Theory"*, give a motivation for the research undertaken and the theoretical framework for what is sought, respectively. In Chapter 5, *"Experimental Details"*, a full detailed description of the complex setup utilised for the experiment is provided. Moreover, few intermediate results required for the full experiment are shown and discussed. The hope is that after carefully reading Chapter 5, the Reader will fully grasp the experiment's complexity as well as the origin of each key result presented in the next chapter. As announced, Chapter 6, *"Results"*, covers the state-of-the-art results obtained for remote state preparation, quantum teleportation and entanglement swapping. Additionally, sources of errors explaining the imperfections are discussed and these match the observations with high precision. A conclusion to part II and an associated outlook are then proposed in Chapter 7, *"Discussion and Outlook"*.

Part III, *"Certified Quantum Randomness from Untrusted Light"*, presents the second research project of this thesis. It comprises a novel idea — and its experimental implementation — for a source-device-independent (SDI) quantum random number generator (QRNG) achieving a state-of-the-art ultrafast randomness generation speed coupled with a rigorous randomness certification scheme. Similar to Part II, Part III starts with Chapter 8, *"Introduction and Background"*, wherein an intuitive motivation as to why quantum randomness is crucially required is provided as well as an extensive review of its current implementation in quantum optics. Then, in Chapter 9, *"Theory Overview"*, an overview of the theory developed for this research is proposed where the main result — in the form of a Theorem — is supplied. Chapter 10, *"Theory"*, comprises a full and detailed explanation of the theory exposed in Chapter 9. This chapter follows a Spinozan approach in which each important claim regarding the modelling presented is reinforced by a mathematical proof and where the complexity of the end model is built upon previously accepted and proved concepts. The next chapter, Chapter 11, *"Experiment"*, contains a characterisation of the experimental setup used as well as the preliminary results required and leading to the main results. In Chapter 12, *"Results"*, the main results and their signification are examined. To conclude part III, Chapter 13, *"Discussion and Conclusion"*, provides an extensive discussion aimed at comparing the state-of-the-art results obtained with respect to other current implementations as well as concluding remarks.

Ultimately, Chapter 14, *"Conclusion"*, proposes a conclusion to this thesis where a summary of the key results is given. Taken together, the novel and competitive results presented in this thesis contribute to the development of quantum optics and its application in quantum communications and quantum cryptography.

Part I

Fundamentals of Quantum Optics

Part I Abstract

This part of the thesis consists of a sole chapter providing an overview of the formalism of quantum optics wherein the key concepts later used in this thesis are presented and detailed. It should be noted that the goal of this thesis part is not to thoroughly derive the various formulas exposed in it; but rather inform the reader of the material and jargon that are familiar to the researcher in quantum optics.

Chapter 2

The Quantum Theory of Light

'Heil sei euch Geweihten!
Ihr dränget durch Nacht!
Dank! sei dir Osiris!
Dank! dir Isis gebracht!
Es siegte die Stärke
und krönet zum Lohn
die Schönheit und Weisheit
mit ewiger Kron'!'
Mozart's "Die Zauberflöte"

2.1 Quantum Harmonic Oscillator

One of the quintessential models in physics is that of the harmonic oscillator. In its unidimensional formulation, a mass m is attached to a spring with spring constant k. When the mass is displaced from its equilibrium position, it experiences a force $F = -kx$ proportional to the displacement x of the mass along the direction under consideration. The dynamics of this system is fully described in phase space where the canonical coordinates are the mass' position x and its momentum $p = mv = m\frac{dx}{dt}$. When one switches to the picture of quantum mechanics, the position and

momentum variables are replaced by operators $\hat{x}$ and $\hat{p}$, respectively. The energy of the system is then governed by the Hamiltonian

$$\hat{H} = \frac{\hat{p}^2}{2m} + \frac{1}{2}m\omega^2\hat{x}^2 \,, \tag{2.1}$$

where $\omega = \sqrt{\frac{k}{m}}$ is the angular frequency at which the mass oscillates.

Commencing with the general formulation of Schrödinger's equation

$$i\hbar\frac{\partial}{\partial t}\left|\psi_n(t)\right\rangle = \hat{H}\left|\psi_n(t)\right\rangle \,, \tag{2.2}$$

the time-independent Schrödinger equation reads

$$\hat{H}\left|\psi_n\right\rangle = E_n\left|\psi_n\right\rangle \,, \tag{2.3}$$

and it can then be solved analytically by means of the ladder operator

$$\hat{a} = \sqrt{\frac{m\omega}{2\hbar}}\left(\hat{x} + \frac{i}{m\omega}\hat{p}\right) \,, \tag{2.4}$$

and its transpose conjugate

$$\hat{a}^\dagger = \sqrt{\frac{m\omega}{2\hbar}}\left(\hat{x} - \frac{i}{m\omega}\hat{p}\right) \,. \tag{2.5}$$

As a result, one obtains the following quantised energies

$$E_n = \hbar\omega\left(n + \frac{1}{2}\right) \,, \tag{2.6}$$

for the Hamiltonian of the quantum harmonic oscillator expressed in Eq. (2.1) and where $n \in \mathbb{N}$ and $\hbar = \dfrac{h}{2\pi}$ is Planck's reduced constant. Note that the time-independent eigenvectors $\left|\psi_n\right\rangle$ in Eq. (2.3) have wavefunctions expressed by the Hermite polynomials $H_n(x)$ as will be seen below in Sec. 2.3.2.

2.2 Field Quantisation

The starting point in quantising the electromagnetic field $(\boldsymbol{E}, \boldsymbol{B})$ is the famous Maxwell's equations in vacuum

$$\begin{aligned} \boldsymbol{\nabla} \times \boldsymbol{B} &= \frac{\partial \boldsymbol{E}}{\partial t} && \text{Faraday's Law} \\ \boldsymbol{\nabla} \times \boldsymbol{E} &= -\frac{\partial \boldsymbol{B}}{\partial t} && \text{Ampere's Law} \\ \boldsymbol{\nabla} \cdot \boldsymbol{B} &= 0 && \text{Gauss' Law} \\ \boldsymbol{\nabla} \cdot \boldsymbol{E} &= 0 && \text{Coulomb's Law} \end{aligned} \quad . \tag{2.7}$$

The magnetic field $\boldsymbol{B}$ is derived from a vector potential $\boldsymbol{A}$ defined as

$$\boldsymbol{B} = \nabla \times \boldsymbol{A} \, . \tag{2.8}$$

Using the vector identity $\nabla \times \nabla \times \boldsymbol{A} = \nabla(\nabla \cdot \boldsymbol{A}) - \nabla^2 \boldsymbol{A}$ and working in the Coulomb gauge for which $\nabla \cdot \boldsymbol{A} = 0$, the vector potential $\boldsymbol{A}$ can be inserted into Maxwell's equations such that the following wave equation must be satisfied [14]

$$\nabla^2 \boldsymbol{A}(\boldsymbol{r}, t) = \frac{1}{c^2} \frac{\partial^2 \boldsymbol{A}(\boldsymbol{r}, t)}{\partial t^2} \, . \tag{2.9}$$

The solution to Eq. (2.9) is given by a set of k normal modes with corresponding frequencies ω_k. These modes are separable in time and space and are written as

$$\boldsymbol{A}(\boldsymbol{r}, t) = \sum_k \sqrt{\frac{\hbar}{2\omega_k \epsilon_0}} \left(a_k \boldsymbol{u}_k(\boldsymbol{r}) e^{-i\omega_k t} + a_k^* \boldsymbol{u}_k^*(\boldsymbol{r}) e^{i\omega_k t} \right) \, . \tag{2.10}$$

The solution in Eq. (2.10) is purely classical. The spatiotemporal distribution of each normal mode k is given by $\boldsymbol{u}_k(\boldsymbol{r}) e^{-i\omega_k t}$, with $\boldsymbol{u}_k$ satisfying Helmhotz' equation [52], while a_k is the mode's associated amplitude.

To quantise the electromagnetic field, one simply replaces the classical amplitude a_k with an operator $\hat{a}_k$ (and a_k^* with $\hat{a}_k^\dagger$). In fact, this operator is precisely the ladder operator introduced in Eq. (2.4) and it satisfies the bosonic commutation relations $[\hat{a}_i, \hat{a}_j] = 0$ and $[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}\mathbb{1}$, with δ_{ij} being Kroenecker's delta and $\mathbb{1}$ the identity matrix. This leads to the solution in Eq. (2.10) now being an operator $\hat{\boldsymbol{A}}$ given by

$$\hat{\boldsymbol{A}}(\boldsymbol{r}, t) = \sum_k \sqrt{\frac{\hbar}{2\omega_k \epsilon_0}} \left(\hat{a}_k \boldsymbol{u}_k(\boldsymbol{r}) e^{-i\omega_k t} + \hat{a}_k^* \boldsymbol{u}_k^*(\boldsymbol{r}) e^{i\omega_k t} \right) . \tag{2.11}$$

The expression in Eq. (2.11) is quantum and its quantum aspect arises from the mode's amplitude now being an operator $\hat{a}_k$, while each normal mode's spatiotemporal distribution is unaltered and thus remains classical.

As such, the only feature that will be considered quantum, and hence will be treated appropriately in the latter stages of this chapter when we shall go over the various quantum states of light, is the amplitude of the light mode under consideration in some given light field. To approach the stage where a quantum description of the states of light — through the mode's amplitude and thus its associated energy — is available, one naturally begins with the Hamiltonian of the electromagnetic field which is expressed as [14]

$$\hat{H} = \frac{1}{2}\epsilon_0 \int_V \left(|\hat{\boldsymbol{E}}(\boldsymbol{r}, t)|^2 + c^2 |\hat{\boldsymbol{B}}(\boldsymbol{r}, t)|^2 \right) d^3\boldsymbol{r} \, . \tag{2.12}$$

Now, using the solution in Eq. (2.11) as well as Maxwell's equations, one can rearrange the Hamiltonian to obtain

$$\hat{H} = \sum_k \hbar\omega_k \left(\hat{a}_k^\dagger \hat{a}_k + \frac{\mathbb{1}}{2} \right) , \tag{2.13}$$

where $\hat{a}_k$ are the ladder operators previously introduced in Eq. (2.4).

The Hamiltonian in Eq. (2.13) is that of an ensemble of k quantum harmonic oscillators with frequencies ω_k. Consequently, solving the time-independent Schrödinger

equation, one obtains — similarly to Eq. (2.6) — the following energy eigenstates for the k-th frequency

$$E_{n_k} = \hbar\omega_k \left(n_k + \frac{1}{2} \right) . \tag{2.14}$$

This means that light in quantum optics is a field whose spatiotemporal distribution is treated classically, while its energy is given by an ensemble of k quantum harmonic oscillators with frequencies ω_k. The resulting quanta of energy in light are called *photons* and they each carry an energy $\hbar\omega_k$. Additionally, from Eq. (2.6), there can be n_k such photons per quantum harmonic oscillator of frequency ω_k. Importantly, even when no such photon is present in one of the constituent quantum harmonic oscillator, a light field in quantum optics will still exhibit an energy $E_0 = \dfrac{\hbar\omega_k}{2}$ corresponding to the vacuum fluctuations.

Utilising further concepts of the quantum harmonic oscillator introduced in Sec. 2.1, the Hamiltonian of the quantum electromagnetic field can be expressed as a function of the conjugate rescaled quadrature operators $\hat{X}_k$ and $\hat{P}_k$ defined as follows

$$\hat{X}_k \equiv \sqrt{\frac{m\omega_k}{\hbar}}\, \hat{x}_k = \frac{1}{\sqrt{2}}(\hat{a}_k^\dagger + \hat{a}_k) \quad ; \quad \hat{P}_k \equiv \frac{1}{\sqrt{m\omega_k\hbar}}\, \hat{p}_k = \frac{i}{\sqrt{2}}(\hat{a}_k^\dagger - \hat{a}_k) . \tag{2.15}$$

These operators are Hermitian and they satisfy the canonical commutation relations

$$[\hat{X}_k, \hat{X}_l] = 0 \quad ; \quad [\hat{P}_k, \hat{P}_l] = 0 \quad ; \quad [\hat{X}_k, \hat{P}_l] = i\delta_{kl}\mathbb{1} . \tag{2.16}$$

The Hamiltonian of the quantum electromagnetic field in Eq. (2.13) is then expressed using the quadrature operators in Eq. (2.15) in the following manner

$$\hat{H} = \sum_k \hbar\omega_k \left(\frac{\hat{X}_k^2}{2} + \frac{\hat{P}_k^2}{2} \right) . \tag{2.17}$$

The signification of the quadrature operators defined in Eq. (2.15) is analogous to the position and momentum of the electromagnetic field's quantum harmonic

oscillator. However, in reality, they correspond to the *"in-phase and out-of-phase components of the electric field amplitude of the spatial-temporal mode"* [52] under consideration. Indeed, the electric field operator $\hat{\boldsymbol{E}}(\boldsymbol{r},t)$ associated with the vector potential of Eq. (2.11) is given by

$$\begin{aligned}\hat{\boldsymbol{E}}(\boldsymbol{r},t) &= \frac{i}{\sqrt{2}}\sum_k \sqrt{\frac{\hbar\omega_k}{\epsilon_0}}\boldsymbol{u}_k(\boldsymbol{r})\left(\hat{a}_k e^{-i\omega_k t} - \hat{a}_k^\dagger e^{i\omega_k t}\right) \\ &= \sum_k \sqrt{\frac{\hbar\omega_k}{\epsilon_0}}\boldsymbol{u}_k(\boldsymbol{r})\left(\hat{X}_k \sin(\omega_k t) - \hat{P}_k \cos(\omega_k t)\right),\end{aligned} \tag{2.18}$$

where $\boldsymbol{u}_k(\boldsymbol{r})$ have been assumed to be real. If they were complex, the expression in Eq. (2.18) would simply feature an additional term with a phase.

As a consequence, while the quadrature operators of light can be thought of as the position and momentum of an oscillator, this implication is not a strict equality. Moreover, a position and momentum associated with an electromagnetic oscillator would be rather ill-defined quantities when considering the context.

2.3 The Quantum States of Light

Given the formalism exposed for the quantisation of the electromagnetic field, one can now work towards expressing the various quantum states of light as well as inspect their particular properties. Once again, it should be reminded that these states *solely* comprise a description of the amplitude of the light field under consideration. A state of light retains its well-defined mode and classically well-understood characteristics such as wavelength, spatiotemportal distribution or polarisation.

2.3.1 Quadrature States

The first states we shall inspect are the eigenstates of the quadrature operators $\hat{X}$ and $\hat{P}$ introduced in Eq. (2.15). They are written as $|X\rangle$ and $|P\rangle$, where $|X\rangle$ is

called the position state, while $|P\rangle$ is the momentum state, and hence satisfy the following eigenvector equations

$$\hat{X}\,|X\rangle = X\,|X\rangle \quad ; \quad \hat{P}\,|P\rangle = P\,|P\rangle \ . \tag{2.19}$$

As was mentioned earlier, the quadrature operators are conjugate canonical observables such that the quadrature states — i.e. their eigenstates — have continuous and unbounded spectra. Furthermore, since the quadrature states form a basis, they are orthogonal

$$\langle X|X'\rangle = \delta(X - X') \quad ; \quad \langle P|P'\rangle = \delta(P - P')\,, \tag{2.20}$$

with $\delta(x)$ being the Dirac delta distribution, and complete

$$\int_{-\infty}^{+\infty} |X\rangle\,\langle X|\ dX = \int_{-\infty}^{+\infty} |P\rangle\,\langle P|\ dP = \mathbb{1}\,. \tag{2.21}$$

One important property is that the position and momentum states are mutually related to one another by Fourier transformation

$$\begin{aligned} |X\rangle &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{-iXP}\,|P\rangle\ dP \\ |P\rangle &= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{+iXP}\,|X\rangle\ dX\,. \end{aligned} \tag{2.22}$$

These states are however not normalisable. This lack of physicality implies that one cannot generate them experimentally. Nevertheless, the quadrature states are required to introduce the following quadrature wave functions

$$\psi(X) = \langle X|\psi\rangle \quad ; \quad \tilde{\psi}(P) = \langle P|\psi\rangle\ , \tag{2.23}$$

for the corresponding pure state $|\psi\rangle$.

In contrast to the intangibility of the quadrature states in Eq. (2.19), the quadrature wave functions defined in Eq. (2.23) have a clear physical meaning. Indeed, their moduli squared $|\psi(X)|^2$ and $|\tilde{\psi}(P)|^2$ correspond to the quadrature probability distributions of the pure state $|\psi\rangle$, which can be obtained by projecting it onto the quadrature eingenstates. As will be seen in Sec. 2.6.2, this can be precisely measured by means of homodyne detection.

Lastly, a well-known fact in quantum mechanics [53] is that for any pair of non-commuting Hermitian operators $\hat{A}$ and $\hat{B}$ (i.e. $[\hat{A}, \hat{B}] \neq 0$), there exists an uncertainty relation between the corresponding variances $(\Delta\hat{A})^2$ and $(\Delta\hat{B})^2$ expressed as

$$(\Delta\hat{A})^2(\Delta\hat{B})^2 \geq \frac{1}{4}\left|[\hat{A}, \hat{B}]\right|^2 , \tag{2.24}$$

for which the variance associated with the measurement of a general observable $\hat{O}$ in any basis $\{|\varphi\rangle\}$ is calculated as

$$(\Delta\hat{O}_{|\varphi\rangle})^2 = \langle\hat{O}^2\rangle_{|\varphi\rangle} - \langle\hat{O}\rangle^2_{|\varphi\rangle} , \tag{2.25}$$

and where $\langle\hat{O}\rangle_{|\varphi\rangle} = \langle\varphi|\hat{O}|\varphi\rangle$ denotes the expectation value of the observable $\hat{O}$.

From the commutator between the quadrature operators given in Eq. (2.16), one then concludes that

$$\Delta\hat{X}\Delta\hat{P} \geq \frac{1}{2} . \tag{2.26}$$

This important feature indicates that the two quadratures of a state — which define it in the optical phase space — cannot have well-defined values simultaneously. Therefore, one cannot measure both with arbitrary accuracy.

2.3.2 Fock States

Amongst the most important states in quantum optics are the Fock states $|n\rangle$, named after the Soviet physicist Vladimir Fock. These are defined as the eigenstates of the photon number operator $\hat{n} = \hat{a}^\dagger \hat{a}$, thereby yielding

$$\hat{n} \, |n\rangle = n \, |n\rangle \ . \tag{2.27}$$

Inspecting Eq. (2.13), one notes that the Fock states are also the eigenstates of the Hamiltonian associated with the electromagnetic field. A Fock state $|n\rangle$ thus contains precisely $n \in \mathbb{N}$ excitations — or *photons* — of the mode of the light field under consideration and one usually refers to $|n\rangle$ as being the n-photon state. Moreover, vacuum — for which the associated energy is non-zero — is a special case of the Fock state. It is written as $|0\rangle$ and hence corresponds to the state wherein no photon is present, i.e. $n = 0$. By virtue of Eq. (2.14), an n-photon state $|n\rangle$ features a corresponding energy of $E_n = \hbar\omega \left(n + \frac{1}{2} \right)$.

The Fock states are orthonormal

$$\langle n | n' \rangle = \delta_{nn'} \, , \tag{2.28}$$

and complete

$$\sum_{n=0}^{\infty} |n\rangle \, \langle n| = \mathbb{1} \, . \tag{2.29}$$

As such, the Fock states form a complete basis — the Fock basis — for the space of the allowable quantum states of light such that any such state can be written in the Fock state basis. Moreover, given the intuitive interpretation of Fock states given above, most quantum states of light will be defined as their expansions in the Fock basis, as will be seen below.

Using the eigenvector relation in Eq. (2.27), one can derive the following funda-

mentally important relations

$$\begin{aligned} \hat{a}\,|n\rangle &= \sqrt{n}\,|n-1\rangle \\ \hat{a}^\dagger\,|n\rangle &= \sqrt{n+1}\,|n+1\rangle\ , \end{aligned} \tag{2.30}$$

and $\hat{a}\,|0\rangle = 0$, linking the Fock states to the ladder operator $\hat{a}$ and its transpose conjugate $\hat{a}^\dagger$.

Because of the structure of Eq. (2.30), $\hat{a}$ is often called the annihilation operator and $\hat{a}^\dagger$ the creation operator. Indeed, upon applying the creation operator $\hat{a}^\dagger$ (annihilation operator $\hat{a}$) onto a Fock state $|n\rangle$, precisely one photon is added to (removed from) that state. This leads to the fairly useful relation

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}\,|0\rangle\ , \tag{2.31}$$

linking an excited state with n photons to the vacuum state $|0\rangle$.

An interesting feature of Fock states is their quadrature wave functions as introduced in Eq. (2.23). Starting with the vacuum state $|\psi\rangle = |0\rangle$, one can derive a differential equation for its position quadrature wave function $\psi_0(X) = \langle X|\psi\rangle = \langle X|0\rangle$. Indeed, from Eq. (2.4) one gets

$$\hat{a}\psi_0(X) = \frac{1}{\sqrt{2}}\left(X + \frac{\partial}{\partial X}\right)\psi_0(X) = 0\,. \tag{2.32}$$

The solution to this equation is

$$\psi_0(X) = \pi^{-1/4} e^{-X^2/2}\,, \tag{2.33}$$

i.e. a Gaussian distribution.

Alternatively, one obtains the same

$$\tilde{\psi}_0(P) = \pi^{-1/4} e^{-P^2/2}\,, \tag{2.34}$$

for the momentum wave function derived using Eq. (2.22).

Strikingly, even though the vacuum state of the electromagnetic field has an empty spatiotemporal mode as per Eq. (2.18), this *emptiness* still induces vacuum to exhibit a quadrature variance of 1/2. Indeed, a direct calculation from Eq. (2.25) and Eq. (2.30) shows that the normalised variance of the quadrature operators for an arbitrary Fock state $|n\rangle$ is

$$(\Delta\hat{X}_{|n\rangle})^2 = \langle n|\hat{X}^2|n\rangle = (\Delta\hat{P}_{|n\rangle})^2 = \langle n|\hat{P}^2|n\rangle = n + \frac{1}{2}\,. \tag{2.35}$$

This non-zero variance is a direct consequence of the uncertainty principle found in Eq. (2.26).

Finally, the quadrature wave function $\psi_n(X)$ of any Fock state $|n\rangle$ can be calculated from Eq. (2.30), for which one gets the following recursion

$$\hat{a}^\dagger\psi_{n-1}(X) = \frac{1}{\sqrt{2}}\left(X - \frac{\partial}{\partial X}\right)\psi_{n-1}(X) = \sqrt{n}\psi_n(X)\,. \tag{2.36}$$

This formula is then satisfied by

$$\psi_n(X) = \frac{H_n(X)}{\sqrt{2^n n!\sqrt{\pi}}}e^{-X^2/2}\,, \tag{2.37}$$

where $H_n(x)$ is the n-th order Hermite polynomial.

2.3.3 Coherent States

Another key quantum state of light is the coherent state. The coherent state $|\alpha\rangle$ (also known as a *Glauber state*) is defined as the eigenstate of the annihilation operator

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\ , \tag{2.38}$$

with eigenvalue α.

Since the annihilation operator $\hat{a}$ is not Hermitian, the coherent state's eigenvalue α can be a complex number. As such, using Euler's formalism, one writes

$$\alpha = |\alpha| e^{i\mathrm{Arg}(\alpha)} , \tag{2.39}$$

for which $|\alpha|$ is commonly referred to as being the coherent state's *amplitude*, while $\mathrm{Arg}(\alpha)$ is its *coherent phase*.

Coherent states are the closest quantum states of light to the classical picture of light as a harmonic oscillator, for which an amplitude and a phase are supplied. As a consequence of this feature, coherent states best model the light field in a coherent laser, a device ubiquitous in quantum optics and many more domains in physics.

From the definition in Eq. (2.38), it is possible to calculate the expectation values of the quadrature operators for the coherent states. One obtains

$$\begin{aligned} \langle \hat{X} \rangle_{|\alpha\rangle} \equiv X_\alpha &= \langle \alpha | \hat{X} | \alpha \rangle = \sqrt{2}\,\mathrm{Re}\{\alpha\} \\ \langle \hat{P} \rangle_{|\alpha\rangle} \equiv P_\alpha &= \langle \alpha | \hat{P} | \alpha \rangle = \sqrt{2}\,\mathrm{Im}\{\alpha\} . \end{aligned} \tag{2.40}$$

This allows one to write $\alpha = \dfrac{1}{\sqrt{2}}(X_\alpha + iP_\alpha)$, for which one then expresses the position and momentum quadrature wave functions as follows

$$\begin{aligned} \psi_\alpha(X) &= \pi^{-1/4} e^{-i\frac{X_\alpha P_\alpha}{2}} e^{iP_\alpha X} e^{-\frac{(X-X_\alpha)^2}{2}} \\ \tilde{\psi}_\alpha(P) &= \pi^{-1/4} e^{+i\frac{X_\alpha P_\alpha}{2}} e^{iX_\alpha P} e^{-\frac{(P-P_\alpha)^2}{2}} . \end{aligned} \tag{2.41}$$

By comparing Eq. (2.41) with Eq. (2.33) and Eq. (2.34), one notices that the coherent state's quadrature wave functions very much resemble that of the vacuum. In fact, the vacuum $|0\rangle$ is the particular case of a coherent state $|\alpha\rangle$ when $\alpha = 0$. Consequently, coherent states are states of minimal uncertainty as they saturate the uncertainty principle. This can be easily verified by calculating the variance of the

quadrature operators for a coherent state

$$(\Delta\hat{X}_{|\alpha\rangle})^2 = (\Delta\hat{P}_{|\alpha\rangle})^2 = \frac{1}{2}\,, \tag{2.42}$$

thereby indicating that it is equally divided between the two quadratures X and P and thus implying that $\Delta\hat{X}_{|\alpha\rangle}\Delta\hat{P}_{|\alpha\rangle} = \frac{1}{2}$, hence the saturation of Eq. (2.26).

An extremely useful expression is that of the coherent state expansion in the Fock basis. This eminent formula was derived by Glauber and it reads

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \ . \tag{2.43}$$

The first important observation possible from Eq. (2.43) is that the photon number statistics of a coherent state is a Poisson distribution. Indeed, from Born's rule, one gets the following photon number distribution

$$P(n) = |\,\langle n|\alpha\rangle\,|^2 = e^{-|\alpha|^2}\frac{|\alpha|^{2n}}{n!}\,. \tag{2.44}$$

As such, from the properties of Poisson's distribution, the mean and the variance of the photon number in a given coherent state $|\alpha\rangle$ are equal and they read

$$\langle\hat{n}\rangle_{|\alpha\rangle} = (\Delta\hat{n}_{|\alpha\rangle})^2 = |\alpha|^2\,. \tag{2.45}$$

This means that a coherent state is a coherent superposition of randomly distributed and uncorrelated photons, with an average photon number $\langle n\rangle \equiv |\alpha|^2$. Moreover, the photon number variance is equal to the average photon number and it is thus said to be *linear* in $\langle n\rangle$.

The second important observation is that, unlike the states previously introduced, coherent states are not orthogonal to one another. Instead, it is said that they are *approximately* orthogonal as long as their amplitudes differ sufficiently. Indeed, from

Eq. (2.43), one notes that

$$\langle\alpha|\alpha'\rangle = e^{-\frac{|\alpha'|^2}{2}-\frac{|\alpha|^2}{2}+\alpha^*\alpha'}\,, \tag{2.46}$$

such that one can derive

$$|\,\langle\alpha|\alpha'\rangle\,|^2 = e^{-|\alpha'-\alpha|^2}\,, \tag{2.47}$$

where the orthogonality constraint is now obvious.

Furthermore, coherent states are complete

$$\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} |\alpha\rangle\,\langle\alpha|\,\frac{dX_\alpha dP_\alpha}{2\pi} = \mathbb{1}\,. \tag{2.48}$$

Eq. (2.47) and Eq. (2.48) thus imply that one can express any quantum state of light in a coherent state basis. This is the famous *optical equivalence theorem*, wherein the density operator $\hat{\rho}$ of any quantum optical state is written as

$$\hat{\rho} = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} P(X_\alpha, P_\alpha)\,|\alpha\rangle\,\langle\alpha|\,dX_\alpha dP_\alpha\,, \tag{2.49}$$

where $P(X_\alpha, P_\alpha)$ is the so-called P function [54] for that particular state.

In general, the P function can be ill-defined and if it is regular (i.e. analytic and single-valued) then the state under consideration is said to be *classical*, otherwise it is *nonclassical*.

A final interesting remark about coherent states is that while it is generally straightforward to experimentally generate one of them with a large amplitude α (a mere laser pulse will do), large superpositions of coherent states or entanglement amongst them are extremely difficult to prepare in the lab. This difficultly originates from coherent states simultaneously behaving as classical waves in the quadrature picture and ensembles of uncorrelated particles in the photon number. As such, the study of this explicit wave-particle duality for superpositions of, or

entanglement amongst, large amplitude coherent states would push the boundaries of quantum mechanics' understanding even further. A famous class of such states are *Schrödinger cat states* [55, 56, 57, 58], defined as the quantum superposition of coherent states with equal and diametrically opposite amplitudes.

2.3.4 Thermal States

The final quantum state of light reviewed here is the thermal state. It is associated with states whose radiation is governed by Planck's law [4]. In its most common form, the thermal state's density operator $\hat{\rho}_{\text{th}}$ is expressed in the Fock basis

$$\hat{\rho}_{\text{th}} = \sum_{n=0}^{\infty} \frac{1}{\langle n \rangle + 1} \left(\frac{\langle n \rangle}{\langle n \rangle + 1} \right)^n |n\rangle \langle n| \,, \tag{2.50}$$

where $\langle n \rangle \equiv \langle \hat{n} \rangle_{\hat{\rho}_{\text{th}}}$ is the average photon number within the state.

From Eq. (2.50), the thermal state's photon number distribution is evident

$$P(n) = \langle n|\hat{\rho}_{\text{th}}|n\rangle = \frac{1}{\langle n \rangle + 1} \left(\frac{\langle n \rangle}{\langle n \rangle + 1} \right)^n . \tag{2.51}$$

The probability distribution in Eq. (2.51) is a geometric distribution. From it, one can calculate the variance of the photon number operator $\hat{n}$ for the thermal state and obtain

$$(\Delta \hat{n}_{\hat{\rho}_{\text{th}}})^2 = \langle n \rangle + \langle n \rangle^2 . \tag{2.52}$$

As can be seen from Eq. (2.52), the thermal state's photon number variance is *quadratic* in the average photon number $\langle n \rangle$. This key feature leads to thermal states being referred to as having *super-Poissonian* photon number statistics. This designation means that $\Delta n^2 > \langle n \rangle$, i.e. the photon number's variance is larger than that for a coherent state $|\alpha\rangle$, for which it equates the average photon number and one has Poissonian statistics defined by $\Delta n^2 = \langle n \rangle$.

2.4 Wigner Function Representation

In classical optics, the state of an electromagnetic oscillator at a given frequency is entirely described by its amplitude $|\alpha|$ and phase $\mathrm{Arg}(\alpha)$. This allows one to construct a two-dimensional complex phase space in which every point is assigned to a particular oscillator. Additionally, the evolution of that oscillator is governed by the statistics of $\alpha = |\alpha|e^{i\mathrm{Arg}(\alpha)}$. In practice, the field quadratures X and P are chosen to span this two-dimensional space. Given this construction, any probabilistic mixture of electromagnetic oscillators can thus be described by a probability distribution $W(X, P)$ over this space. This phase space distribution indicates the probability of retrieving a pair of field quadratures (X, P) in their simultaneous measurement. As such, any statistical quantity associated with the electromagnetic oscillator can be calculated as long as $W(X, P)$ is known.

Within the formalism of quantum optics, a similar concept can be introduced. However, owing to the inherent subtleties of quantum mechanics where one cannot measure simultaneously and precisely the position quadrature X and the momentum quadrature P and where quantum states are not directly observable, the concept of phase space in quantum optics leads to the probability distribution $W(X, P)$ being ill-behaved or negative [52]. As a result, such phase space probability distribution is labelled a *quasiprobability distribution* and its simplest and most widely used expression is the Wigner function. The Wigner function $W(X, P)$ for a single mode quantum state described by the density operator $\hat{\rho}$ is defined in phase space as follows [59]

$$W(X,P) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} e^{ixP}\left\langle X - \frac{x}{2}\middle|\hat{\rho}\middle|X + \frac{x}{2}\right\rangle dx\,. \tag{2.53}$$

Note that generalisations of this formula can be contrived in order to incorporate multimode quantum states of light. Moreover, the Wigner function is also easily expressed for pure states $\hat{\rho} = |\psi\rangle\langle\psi|$, for which the inner product term $\left\langle X - \frac{x}{2}\middle|\hat{\rho}\middle|X + \frac{x}{2}\right\rangle$ in Eq. (2.53) simply becomes $\psi(X - \frac{x}{2})\psi^*(X + \frac{x}{2})$, i.e. the product

of two position quadrature wave functions defined as per Eq. (2.23).

The Wigner function exhibits a few mathematical properties, allowing one to interpret it as an extension of a probability distribution. Let us enumerate them in a non-exhaustive fashion. First, the Wigner function is a real value function and its integral over the entire phase space is normalised. Indeed, one has

$$\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} W(X,P)\,dXdP = \mathrm{tr}\{\hat{\rho}\} \equiv 1\,. \tag{2.54}$$

Furthermore, the probability distributions associated with the X and P quadratures are retrieved from the Wigner function's following marginal distributions

$$\begin{aligned}\int_{-\infty}^{+\infty} W(X,P)\,dP &= \langle X|\hat{\rho}|X\rangle \\ \int_{-\infty}^{+\infty} W(X,P)\,dX &= \langle P|\hat{\rho}|P\rangle\ .\end{aligned} \tag{2.55}$$

If the system can be described by a pure state, one gets

$$\begin{aligned}\int_{-\infty}^{+\infty} W(X,P)\,dP &= |\psi(X)|^2 \\ \int_{-\infty}^{+\infty} W(X,P)\,dX &= |\tilde{\psi}(P)|^2\,,\end{aligned} \tag{2.56}$$

and owing to the Cauchy-Schwartz inequality, the Wigner function is constrained to be bounded as follows

$$-\frac{1}{\pi} \leq W(X,P) \leq \frac{1}{\pi}\,. \tag{2.57}$$

Interestingly, the bound in Eq. (2.57) disappears in the classical limit where $\hbar \to 0$.

Another particularly useful property of the Wigner function is the *overlap formula*

$$\mathrm{tr}\{\hat{F}_1\hat{F}_2\} = 2\pi\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} W_1(X,P)W_2(X,P)\,dXdP\,, \tag{2.58}$$

for any two operators $\hat{F}_1$ and $\hat{F}_2$ with Wigner functions $W_1(X,P)$ and $W_2(X,P)$.

This identity enables one to calculate a variety of expectation values, a key aspect of quantum mechanics. In fact, by performing a simple substitution, one obtains

$$\langle \hat{F} \rangle_{\hat{\rho}} \equiv \mathrm{tr}\{\hat{\rho}\hat{F}\} = 2\pi \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} W_{\hat{\rho}}(X,P) W_{\hat{F}}(X,P)\, dX dP\,, \tag{2.59}$$

as desired.

Overall, even given the properties listed above, the Wigner function is radically different from a probability distribution in the classical sense. Indeed, while its marginal distributions in Eq. (2.55) correspond to physical quantities that one can measure, the Wigner function itself does not have a clear physical meaning. Moreover, even though $W(X,P)$ takes well-defined values, it is known that the two field quadratures X and P do have simultaneously well-defined values by virtue of the uncertainty principle in Eq. (2.26). This leads to the Wigner function being negative for a large variety of states — such as Fock states with a strictly positive photon number — as will be seen below.

To start with, the Wigner function of a coherent state $|\alpha\rangle$ is expressed as

$$W_{|\alpha\rangle}(X,P) = \frac{1}{\pi}\, e^{-(X-X_\alpha)^2} e^{-(P-P_\alpha)^2}\,, \tag{2.60}$$

where α is, once again, retrieved from Eq. (2.40), thus yielding $\alpha = \dfrac{1}{\sqrt{2}}(X_\alpha + iP_\alpha)$.

The Wigner function of the coherent state in Eq. (2.60) is a Gaussian distribution centered at (X_α, P_α) — the coordinates corresponding to a single electromagnetic oscillator — but with a variance of $1/2$, arising from the quantum mechanical uncertainty on the field quadratures.

Alternatively, the Wigner function of a general Fock state matrix entry $\hat{\rho}_{mn} = |m\rangle\langle n|$ is given by the following expression

$$W_{\hat{\rho}_{mn}}(X,P) = \frac{(-1)^m}{\pi} \left(\frac{n!}{m!}\right)^{1/2} e^{-(X^2+P^2)} \left(-\sqrt{2}(X-iP)\right)^{m-n} L_n^{m-n}\left(2(X^2+P^2)\right)\,, \tag{2.61}$$

for $m \geq n$ and where L_n^{m-n} are the Laguerre polynomials.

Finally, owing to the linearity of the integral in Eq. (2.53), the Wigner function of any superposition of pure states can be explicitly derived by calculating the corresponding sum of individual Wigner functions.

As such, the Wigner functions for the following four Fock states: vacuum $|0\rangle$, single-photon Fock state $|1\rangle$, Fock state superposition $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and Fock state superposition $|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ are shown in Fig. 2.1.

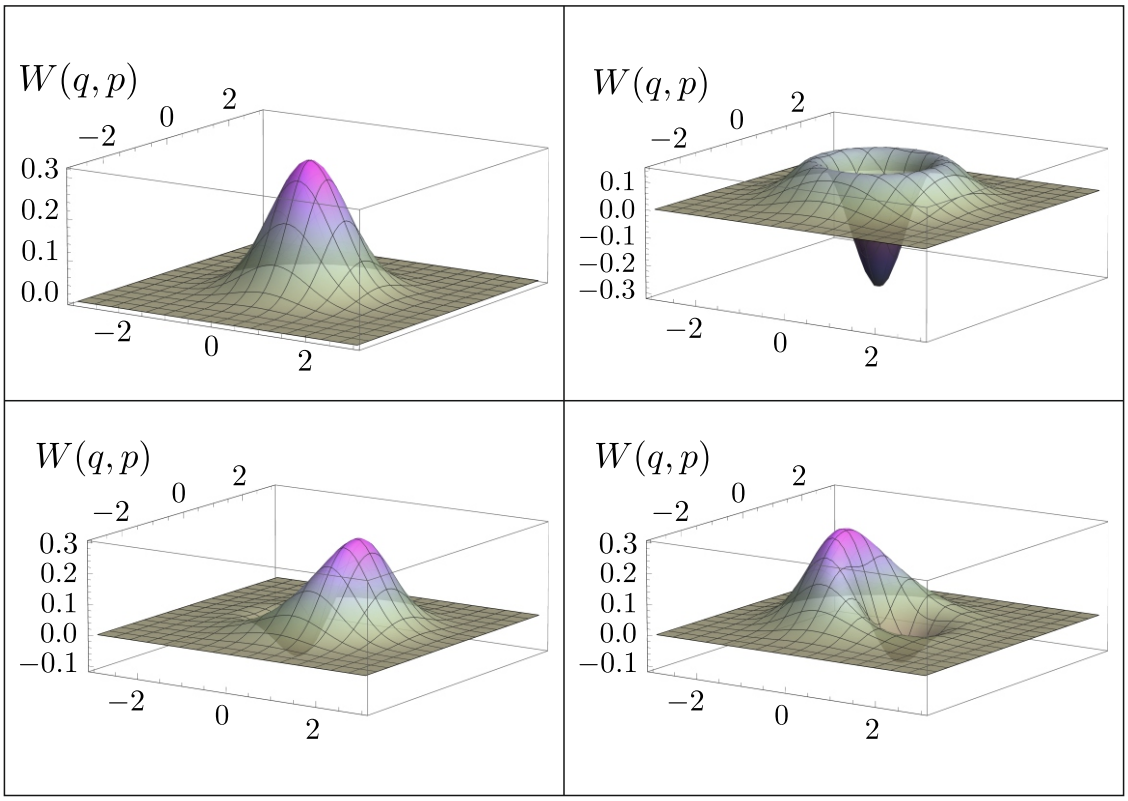


Figure 2.1: Wigner functions $W(q,p)$ of some Fock states. Top left: vacuum $|0\rangle$; top right: single-photon Fock state $|1\rangle$; bottom left: Fock state superposition $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$; bottom right: Fock state superposition: $|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Note that the field quadratures X and P are sometimes written as q and p instead.

In reality, the vacuum $|0\rangle$ and single Fock state $|1\rangle$ make the basis for the *single-rail qubit* in quatum optics which will be the subject of interest in part II of this thesis, entitled *"Quantum Interface between Single- and Dual-Rail Optics Qubits"*. Note that the difference between $|+\rangle$ and $|-\rangle$ shown in Fig. 2.1 is a phase shift of π. Indeed, any superposition of the vacuum and single Fock state can be written

as $|\varphi\rangle = a|0\rangle + be^{i\phi}|1\rangle$, yielding $\phi = 0$ for $|+\rangle$ and $\phi = \pi$ for $|-\rangle$, as can be seen in Fig. 2.1 for which the orthogonality of the states is evident. Moreover, it can be noticed that the Wigner function presents some negativity for the states $|\pm\rangle$ and most importantly $|1\rangle$. This is a clear sign that the states under consideration are quantum and hence the search for negativity in some given state is usually a criteria for quantumness in experimental works within quantum optics.

Lastly, the Wigner function of a state in phase space can be experimentally reconstructed statistically from measurements of that state's field quadratures using balanced homodyne detection. This will be covered below in Sec. 2.6.2 and further detailed in part II of this thesis.

2.5 Modal Transformations

After having described the various quantum states of light and their possible representations in phase space, now is the time to discuss the numerous mode transformations in quantum optics. These are not only useful from a conceptual point of view, but also for the experimentalist that wishes to fully understand his or her setup and its subsequent behaviour. As will be seen, some transformations even introduce states which are of ultimate importance in the field of quantum optics.

2.5.1 Displacement

The first transformation to be considered is the displacement operator $\hat{D}(\alpha)$ which is written as

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}, \tag{2.62}$$

where α is a complex number.

Because $\alpha\hat{a}^\dagger - \alpha^*\hat{a}$ is a Hermitian operator, the displacement operator $\hat{D}(\alpha)$ must be unitary. As intended from its denomination, the action of the displacement

operator upon the annihilation operator $\hat{a}$ is to effectively *displace* it by the complex number α as follows

$$\hat{D}^{\dagger}(\alpha)\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha\mathbb{1}\,. \tag{2.63}$$

From the relation in Eq. (2.63), one can derive the following expression [52]

$$\hat{a}\hat{D}(-\alpha)\,|\alpha\rangle = \hat{D}(-\alpha)(\hat{a} - \alpha\mathbb{1})\,|\alpha\rangle = 0\,, \tag{2.64}$$

as per Eq. (2.38), thereby implying that $\hat{D}(-\alpha)\,|\alpha\rangle$ is the vacuum state $|0\rangle$.

This is more commonly written as

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle\ , \tag{2.65}$$

from which it is said that coherent states are *displaced vacuums*.

The expression in Eq. (2.65) can be intuitively understood from the Wigner function of a coherent state in Eq. (2.60). Indeed, vacuum exhibits null mean quadratures $X_\alpha = P_\alpha = 0$ and hence, a coherent state with phase space coordinates (X_α, P_α) is a vacuum precisely displaced by $|\alpha| = \frac{1}{2}\sqrt{X_\alpha^2 + P_\alpha^2}$.

In practice, one can implement the displacement of a quantum optical state of light by an amount α by interfering it with a large coherent state $|\alpha/t\rangle$ on a beam splitter with reflectivity r — in the limit of a small reflectivity — and tracing over the reflected mode. Note that $t = (1-r)^{1/2}$ is the beam splitter's transmissivity. The resulting transmitted mode would have undergone displacement as desired.

2.5.2 Phase Shift

The next important operation is the one obtained from the phase shift operator $\hat{U}(\phi)$ defined as

$$\hat{U}(\phi) = e^{-i\phi\hat{n}}\,, \tag{2.66}$$

where ϕ is a real number.

Once again, as is implied from its name, $\hat{U}(\phi)$ introduces a phase shift of $-\phi$ to the annihilation operator $\hat{a}$, which is expressed in the following manner

$$\hat{U}^\dagger(\phi)\hat{a}\hat{U}(\phi) = e^{-i\phi}\hat{a}\,. \tag{2.67}$$

Its physical action is to change the phase of the electric field in Eq. (2.18). Moreover, its explicit action onto Fock states and coherent states yields

$$\hat{U}(\phi)\,|n\rangle = e^{-i\phi n}\,|n\rangle\ , \tag{2.68}$$

using the Taylor expansion of the exponential in Eq. (2.66), and

$$\hat{U}(\phi)\,|\alpha\rangle = \left|\alpha e^{-i\phi}\right\rangle\ , \tag{2.69}$$

respectively and where Eq. (2.69) is obtained using the Fock state expansion of a coherent state given in Eq. (2.43).

In the lab, the phase of an optical mode is defined with respect to a time reference mode from which measurements are taken. The phase then grows linearly — from 0 to 2π — in the path length undertaken by this mode under consideration.

2.5.3 Squeezing

An experimentally crucial modal transformation is the one referred to as squeezing, whose operator $\hat{S}(r)$ is expressed as

$$\hat{S}(r) = e^{\frac{r}{2}\left(\hat{a}^2-(\hat{a}^\dagger)^2\right)}\,, \tag{2.70}$$

with r a real number commonly dubbed the *squeezing parameter*.

This time, the apparent meaning of the name *squeezing* does not arise from its effect on the annihilation operator $\hat{a}$. Indeed, one has

$$\hat{S}^\dagger(r)\hat{a}\hat{S}(r) = \hat{a}\cosh r - \hat{a}^\dagger \sinh r\,. \tag{2.71}$$

Instead, it is particularly informative to observe the transformation of the field quadrature operators $\hat{X}$ and $\hat{P}$ under squeezing, for which one obtains

$$\begin{aligned} \hat{X} &\to \hat{S}^\dagger(r)\hat{X}\hat{S}(r) = \hat{X}e^{-r} \\ \hat{P} &\to \hat{S}^\dagger(r)\hat{P}\hat{S}(r) = \hat{P}e^{+r}\,, \end{aligned} \tag{2.72}$$

implying the following new quadrature variances

$$\begin{aligned} (\Delta\hat{X})^2 &\to (\Delta\hat{X})^2 e^{-2r} \\ (\Delta\hat{P})^2 &\to (\Delta\hat{P})^2 e^{+2r}\,. \end{aligned} \tag{2.73}$$

Judging from Eq. (2.72) and Eq. (2.73), the action of the squeezing operator is to *squeeze* the position quadrature while stretching the momentum quadrature such that the product of the two quadrature variances is unchanged and thus abides by the uncertainty principle in Eq. (2.26).

An immensely important state for experimentalist is the one obtained by literally *squeezing the vacuum*. Indeed, the resulting state $\hat{S}(r)\,|0\rangle$ is called the single-mode squeezed vacuum (SMSV) and it saturates the uncertainty principle in Eq. (2.26) as per the action of squeezing described by Eq. (2.73). This purely quantum state is often expressed in the Fock basis for which one has [60]

$$|\text{SMSV}\rangle = \hat{S}(r)\,|0\rangle = \frac{1}{\sqrt{\cosh r}} \sum_{n=0}^{\infty} (-\tanh r)^n \frac{\sqrt{(2n)!}}{2^n n!}\,|2n\rangle\,, \tag{2.74}$$

where one commonly defines the probability amplitude $\gamma \equiv -\tanh r$.

As can be seen from Eq. (2.74), a key property of the SMSV is that it consists solely

of even-photon Fock state superpositions. Physically, squeezing is implemented by means of a non-linear process governed by a Hamiltonian of the form

$$\hat{H} \propto r\left((\hat{a}^\dagger)^2 - \hat{a}^2\right) . \tag{2.75}$$

This Hamiltonian can be readily implemented using non-linear crystals such as potassium titanyl phosphate ($KTiOPO_4$ or simply written as KTP) onto which a strong pump field is impinging. In practice, phase matching conditions (i.e. satisfying the conservation of momentum between the input and output to the crystal) in the non-linear medium have to be met and the crystal is thus periodically poled, leading to the commonly used PPKTP crystal. In the photon number picture, each photon from the pump is probabilistically converted into pairs of photons with half the energy, as a consequence of energy conservation. This specific type of non-linear process is called *spontaneous parametric down conversion* (SPDC) and it explains the absence of odd-photon Fock states in the resulting SMSV state defined in Eq. (2.74).

Finally, the squeezing operator can be extended to incorporate two distinct modes — let us call them s and i — described by annihilation operators $\hat{a}$ and $\hat{b}$, respectively. Within this framework, the two-mode squeezing operator $\hat{S}_2(r)$ is written as

$$\hat{S}_2(r) = e^{\frac{r}{2}\left(\hat{a}\hat{b} - \hat{a}^\dagger\hat{b}^\dagger\right)} , \tag{2.76}$$

with r being the same as in Eq. (2.70).

Similar to the SMSV, a new state called the two-mode squeezed vacuum (TMSV) emanates from applying the two-mode squeezing operator $\hat{S}_2(r)$ onto the vacuum state. In the Fock basis, it is expressed as

$$|\text{TMSV}\rangle = \hat{S}_2(r)\,|0\rangle = \frac{1}{\cosh r}\sum_{n=0}^{\infty}(-\tanh r)^n\,|n\rangle_s\,|n\rangle_i \equiv \sqrt{1-\gamma^2}\sum_{n=0}^{\infty}\gamma^n\,|n\rangle_s\,|n\rangle_i , \tag{2.77}$$

where the subscripts s and i refer to the commonly-labelled *signal* and *idler* modes of the TMSV.

By observing Eq. (2.77), one notices that the TMSV is an entangled state exhibiting perfectly correlated photon numbers between the signal and idler modes. This implies that any measurement of n photons in the idler mode projects the signal mode onto an n-photon Fock state (and vice versa). Moreover, this state features quadrature correlations wherein the difference $\hat{X}_s - \hat{X}_i$ of the position quadratures associated with the signal and idler mode is squeezed, while the sum $\hat{P}_s + \hat{P}_i$ of the momentum quadratures is stretched [60]. Note that the average photon number contained in the TMSV is calculated as

$$\langle \hat{n} \rangle_{|\mathrm{TMSV}\rangle} = \sinh^2(r) \,. \tag{2.78}$$

The TMSV is experimentally generated from the same SPDC process as that for the SMSV. The only difference arises in the type of phase matching engineered in the crystal. Type I (e−o−o polarisations for the pump, signal and idler photons, respectively) is utilised for the SMSV, while the TMSV requires a type II (e−o−e) phase matching. Finally, in the presence of a TMSV, the signal and idler modes are usually spatially separated by means of a polarising beam splitter if the generated TMSV is collinear (i.e. both signal and idler photons have equal wave vectors $\boldsymbol{k}_s = \boldsymbol{k}_i = \boldsymbol{k}$), or they are already separated directly at the output of the crystal when the SPDC process is non-collinear.

2.5.4 Rotation

The rotation operator is a multimode generalisation of the phase shift operator introduced in Sec. 2.5.2. Let $\{\hat{a}_k\}_k$ be a collection of annihilation operators describing their corresponding optical modes. The rotation operator $\hat{R}$ coherently mixes

these modes together in the following manner

$$\hat{R} = e^{i \sum_{k,l} J_{kl} \hat{a}_k^\dagger \hat{a}_l} , \tag{2.79}$$

where $\boldsymbol{J}$ is a Hermitian matrix accounting for the couplings between the modes.

The effect of the rotation operator upon the annihilation operators — put in a vector $\hat{\boldsymbol{a}}$ for conveniency — is as follows

$$\hat{\boldsymbol{a}} \to \hat{R}^\dagger \hat{\boldsymbol{a}} \hat{R} = \boldsymbol{U} \hat{\boldsymbol{a}} \equiv e^{i\boldsymbol{J}} \hat{\boldsymbol{a}} , \tag{2.80}$$

where $\boldsymbol{U} = e^{i\boldsymbol{J}}$ is a unitary matrix.

From a physical point of view, this rotation can be viewed as an optical interference between the modes. A fundamental example of this is found in the optical beam splitter $\hat{B}$ which is described by the following 2×2 modal transformation [52]

$$\hat{\boldsymbol{a}} \to \hat{B} \hat{\boldsymbol{a}} = \begin{pmatrix} \cos(\theta/2) & \sin(\theta/2) \\ -\sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} , \tag{2.81}$$

where the beam splitter's reflectivity r and transmissivity t are set by $r = \sin(\theta/2)$ and $t = \cos(\theta/2)$, respectively .

2.5.5 Optical Loss

As the final transformation reviewed here, the optical loss stands out for being the most annoying to experimentalists as it often limits the applicability of quantum optical schemes. This is due to it introducing mixedness in states that would be otherwise pure, or reducing the amount of squeezing present in a state, or simply limiting the detection rates in some experiment.

To understand the transformation associated with optical loss, one has to first introduce a widely used formula that is the above-mentioned beam splitter trans-

formation, but expressed in the Fock basis instead. Given a Fock state $|n_1\rangle_1 |n_2\rangle_2$ at the input modes 1 and 2 of a beam splitter described by Eq. (2.81), the output state between output modes 3 and 4 thus reads [52]

$$\hat{B}\,|n_1\rangle_1 |n_2\rangle_2 = \frac{1}{\sqrt{n_1!n_2!}} \sum_{k_1=0}^{n_1} \sum_{k_2=0}^{n_2} \binom{n_1}{k_1} \binom{n_2}{k_2} (-1)^{k_2} r^{n_1-k_1+k_2} t^{n_2-k_2+k_1} \times ((k_1+k_2)!(n_1+n_2-k_1-k_2)!)^{1/2} |k_1+k_2\rangle_3 |n_1+n_2-k_1-k_2\rangle_4 \,. \tag{2.82}$$

An optical loss is thought of as the situation in which each photon in an optical mode has a probability η to be removed from such mode. This process is modelled by interfering the lossy mode with a vacuum state on a beam splitter with reflectivity $r = \eta^{1/2}$ and then tracing over the reflected channel, thus yielding a transmitted mode in which the effect of loss has been duly accounted for. Using Eq. (2.82), it is possible to apply such an optical loss transformation for a Fock state $|n\rangle$. Mixing it with vacuum $|0\rangle$ on a beam splitter with reflectivity η, one readily obtains

$$\hat{B}\,|n\rangle_1 |0\rangle_2 = \sum_{k=0}^{n} \binom{n}{k}^{1/2} (1-\eta)^{\frac{k}{2}} \eta^{\frac{n-k}{2}} |k\rangle_3 |n-k\rangle_4 \,, \tag{2.83}$$

with $t = (1-\eta)^{1/2}$.

As such, by tracing over mode 4 in Eq. (2.83), the effect of a lossy channel with loss η onto a Fock state $\hat{\rho} = |n\rangle\langle n|$ yields the state $\hat{\rho}'$ expressed as follows

$$\hat{\rho}' = \sum_{k=0}^{n} \binom{n}{k} (1-\eta)^k \eta^{n-k} |k\rangle\langle k| \,, \tag{2.84}$$

where the mode label 3 is omitted since, in reality, the physical mode containing $\hat{\rho}$ and undergoing loss is the same as the one describing $\hat{\rho}'$.

The physical interpretation of Eq. (2.84) is that, under loss, a pure Fock state $\hat{\rho}'$ has been transformed into an incoherent mixture of Fock states whose photon number distribution is given by a binomial distribution.

The effect of losses on a squeezed state is to reduce its squeezing. Indeed, given the position quadrature variance $(\Delta\hat{X})^2 e^{-2r}$ from Eq. (2.73) of a squeezed state with a squeezing parameter r, the new variance is obtained by adding the original variance — transmitted through the beam splitter with a factor $1-\eta$ — with that of the vacuum state (i.e. 1/2) reflected by η. This leads to

$$(\Delta\hat{X})^2 e^{-2r} \to (\Delta\hat{X})^2 e^{-2r}(1-\eta) + \frac{\eta}{2}\,, \tag{2.85}$$

where the loss of squeezing is apparent.

Finally, losses applied to a coherent state $|\alpha\rangle$ give the following state

$$|\alpha\rangle \to \left|\eta^{1/2}\alpha\right\rangle\,. \tag{2.86}$$

Note that the original coherent state $|\alpha\rangle$ can be recovered by amplification of the lossy coherent state expressed in Eq. (2.86) through an optical amplifier such as an Erbium Doped Fiber Amplifier (EDFA). This procedure, however, inevitably adds noise to the signal.

2.6 Measurements

To conclude this chapter dedicated to the quantum theory of light, one has to go over the various measurements available in quantum optics. Prior to doing that, let us recall that a general measurement in the formalism of quantum mechanics is described by a positive-operator valued measure (POVM) $\mathbb{M} = \{\hat{M}_i\}_{i=1}^k$ whose elements $\hat{M}_i$ are a set of Hermitian positive semidefinite operators on a Hilbert space $\mathcal{H}$ that sum to the identity operator

$$\sum_{i=1}^{k} \hat{M}_i = \mathbb{1}\,. \tag{2.87}$$

From this contrivance, given a state $\hat{\rho}$, the probability that the measurement of $\hat{\rho}$ results in the outcome i described by the POVM element $\hat{M}_i$ is given by

$$P(i) = \mathrm{tr}\{\hat{\rho}\hat{M}_i\}\,. \tag{2.88}$$

The two main measurements in quantum optics — namely photon number and homodyne measurements — are then described.

2.6.1 Photon Number Detection

As its name indicates, the goal of a photon number measurement is to detect the number of photons present in a certain state. Consequently, such measurement would easily be modelled by the POVM $\mathbb{M} = \{\hat{M}_n\}_{n=1}^{\infty}$ with corresponding POVM elements $\hat{M}_n = |n\rangle\langle n|$. However, such ideal detector does not exist[1] and one has to take into account detection efficiencies as well as noise such as dark counts, for which detection events are not a consequence of photons being present at the detector.

In reality, the presence of a photon in a particular mode is often detected by means of so-called *click detectors*. In most cases, these detectors react similarly to the presence of any number of incoming photon and are thus said to be non-resolving. The way they react is by *clicking* whenever photons impinge onto it. Conversely, when no such click is recorded — and assuming no dark counts — it can be inferred that no photon was present in the mode under consideration. These click detectors have an inherent quantum detection efficiency η such that the POVM elements associated with the *click* and *no click* detection events are

$$\begin{aligned} \hat{M}_{\text{no click}} &= \sum_{n=0}^{\infty}(1-\eta)^n\,|n\rangle\langle n| \\ \hat{M}_{\text{click}} &= \sum_{n=0}^{\infty}\left(1-(1-\eta)^n\right)|n\rangle\langle n|\,. \end{aligned} \tag{2.89}$$

[1] although it can be argued that they exist to some extent in Transition-Edge Sensors (TESs).

Tab. 2.1 shows the probabilities associated with the POVM elements in Eq. (2.89) for various input photon numbers n.

n	p(no click)	p(1 click)
0	$(1-\eta)^0$	0
1	$(1-\eta)^1$	η
2	$(1-\eta)^2$	$2\eta(1-\eta)$
3	$(1-\eta)^3$	$\eta((\eta-3)\eta+3)$

Table 2.1: Probabilities associated with the *no click* and *click* events described by POVM elements in Eq. (2.89) as a function of the photon number n present at the input of the click detector.

Finally, as opposed to homodyne detection, note that click detectors and measurements made in the Fock basis are not phase sensitive.

2.6.2 Homodyne Detection

The purpose of homodyne detection is to measure the field quadrature X or P of a given state in order to reconstruct its Wigner function in phase space. Therefore, the POVM elements of an ideal homodyne detector measuring the X quadrature — as is most common — are the projectors $|X\rangle\langle X|$ onto the eigenstates of $\hat{X}$. Note that a homodyne detection can be performed for any quadrature. However, due to the uncertainty principle in Eq. (2.26), one cannot make one homodyne detection for X and P simultaneously.

In practice, homodyne detection is implemented by interfering on a symmetric (i.e. $r = t = 2^{-1/2}$) beam splitter the quantum state of light $\hat{\rho}$ under consideration and a strong coherent state $|\alpha_{\mathrm{LO}}\rangle$ called the local oscillator (LO), and measuring the difference of the intensities recorded by two photodiodes placed in each output mode of the beam splitter. Let us assume that the modes containing $\hat{\rho}$ and $|\alpha_{\mathrm{LO}}\rangle$ are described by annihilation operators $\hat{a}_1$ and $\hat{a}_2$, respectively. In virtue of Eq. (2.81), the output modes 3 and 4 of the beam splitter thus have annihilation operators $\hat{a}_3$

and $\hat{a}_4$ given by the following

$$\begin{aligned} \hat{a}_3 &= \frac{1}{\sqrt{2}}(\hat{a}_1 + \hat{a}_2) \\ \hat{a}_4 &= \frac{1}{\sqrt{2}}(\hat{a}_2 - \hat{a}_1)\,. \end{aligned} \tag{2.90}$$

Given these, one can then calculate the number operators $\hat{n}_3 = \hat{a}_3^\dagger \hat{a}_3$ and $\hat{n}_4 = \hat{a}_4^\dagger \hat{a}_4$ associated with the number of photons present in modes 3 and 4 in order to obtain

$$\begin{aligned} \hat{n}_3 &= \frac{1}{2}(\hat{a}_1^\dagger \hat{a}_1 + \hat{a}_1^\dagger \hat{a}_2 + \hat{a}_2^\dagger \hat{a}_1 + \hat{a}_2^\dagger \hat{a}_2) \\ \hat{n}_4 &= \frac{1}{2}(\hat{a}_1^\dagger \hat{a}_1 - \hat{a}_1^\dagger \hat{a}_2 - \hat{a}_2^\dagger \hat{a}_1 + \hat{a}_2^\dagger \hat{a}_2)\,, \end{aligned} \tag{2.91}$$

such that their difference is expressed as

$$\hat{n}_- \equiv \hat{n}_3 - \hat{n}_4 = \hat{a}_1^\dagger \hat{a}_2 + \hat{a}_2^\dagger \hat{a}_1\,. \tag{2.92}$$

Then, by assuming a strong coherent state $|\alpha_{\mathrm{LO}}\rangle$ for the local oscillator, it allows one to replace the annihilation operator $\hat{a}_2$ by the classical amplitude $\alpha_{\mathrm{LO}} = |\alpha_{\mathrm{LO}}|e^{i\theta}$, since $\hat{a}_2 |\alpha_{\mathrm{LO}}\rangle = \alpha_{\mathrm{LO}} |\alpha_{\mathrm{LO}}\rangle$, and where θ is the phase of the local oscillator. Thus Eq. (2.92) becomes

$$\begin{aligned} \hat{n}_- &= \alpha_{\mathrm{LO}}^* \hat{a}_1^\dagger + \alpha_{\mathrm{LO}} \hat{a}_1 \\ &= |\alpha_{\mathrm{LO}}| \left(\hat{a}_1 e^{-i\theta} + \hat{a}_1^\dagger e^{i\theta} \right) \\ &= \sqrt{2} |\alpha_{\mathrm{LO}}| \hat{X}_\theta\,, \end{aligned} \tag{2.93}$$

where the generalised quadrature operator $\hat{X}_\theta$ is defined as

$$\begin{aligned} \hat{X}_\theta &= \frac{1}{\sqrt{2}} \left(\hat{a}_1 e^{-i\theta} + \hat{a}_1^\dagger e^{i\theta} \right) \\ &= \hat{X} \cos\theta + \hat{P} \sin\theta\,. \end{aligned} \tag{2.94}$$

As such, from Eq. (2.93) and Eq. (2.94), one concludes that by recording the

difference between the two intensities output by the photodiodes, the homodyne detector measures the position field quadrature X when $\theta = 0$ and the momentum field quadrature P when $\theta = \frac{\pi}{2}$.

Finally, the reconstruction of $\hat{\rho}$ (a task commonly referred to as *quantum state tomography*) is realised statistically by recording a set $S = \{X_j, \theta_j\}$ of j quadratures X_j and associated phases θ_j of $\hat{\rho}$ (these are defined with respect to the phase θ of the local oscillator that sets a global phase reference) and applying the maximum likelihood algorithm [61].

Part II

Quantum Interface between Single- and Dual-Rail Optical Qubits

Part II Abstract

Today's most widely used method of encoding quantum information in optical qubits is the dual-rail basis, often carried out through the polarisation of a single photon. On the other hand, many stationary carriers of quantum information — such as atoms — couple to light via the single-rail encoding in which the qubit is encoded in the number of photons. As such, interconversion between the two encodings is paramount in order to achieve cohesive quantum networks. In this part of the thesis, we demonstrate this by generating a hybrid entangled resource between the two encodings and using it to teleport a dual-rail qubit onto its single-rail counterpart. Our key results yield an average fidelity of $\mathcal{F} = (92.8 \pm 2.2)\%$ for the teleportation and $\mathcal{F} = (89.7 \pm 2.1)\%$ for entanglement swapping, thus confirming the applicability of this scheme towards a real-world implementation. This work completes the set of tools necessary for the interconversion between the three primary encodings of a qubit in the optical field: single-rail, dual-rail and continuous-variable.

The research presented here led to an article [62] written by the author of this thesis himself and his co-authors.

Chapter 3

Background and Generalities

'But we in it shall be remembered—
We few, we happy few, we band of brothers;
For he to-day that sheds his blood with me
Shall be my brother'
King Harry the Fifth in Shakespeare's "Henry V"

This chapter provides the reader with the critical arguments justifying the research undertaken. Furthermore, a conceptual description of some of the key elements used and investigated in this thesis part is given.

3.1 Background

Any physical system used for quantum information processing (QIP) can be broadly classified into two main categories:

1. Systems with a set of non-equidistant energy eigenstates. These include atoms, nitrogen-vacancy (NV) centers, quantum dots and superconducting qubits. In practice, the experimentalist chooses a precise inherent two-level system from that energy set which can then be utilised as a qubit for QIP. The resulting qubit is said to be discrete-variable (DV).

2. Harmonic oscillator-like systems in which the underlying energy structure is equidistant. The natural candidates are spin ensembles, optical resonators, mechanical membranes and optical modes. Here, the quantum information may be stored in continuous-variables akin to the position and momentum of the canonical harmonic oscillator and the obtained qubit is labelled as being continuous-variable (CV).

Moreover, with the development of quantum technology, it is becoming clear that different physical systems are optimal for various aspects of QIP. For example, superconducting circuits and trapped ions are well-suited for the implementation of quantum logic gates for computation and simulation; spin ensembles for quantum memories; natural and artificial atoms for precise sensing. A comprehensive quantum network should enable reliable exchange of quantum information among all these systems. The primary agent of such exchange is light, as it is the only physical system able to carry quantum information over large distances. Technologies of quantum coupling between light and stationary carriers of quantum information, such as superconducting cavity modes [63], spin ensembles in solids and atomic gases [64], optomechanical devices [65] and others are being developed.

However, these technologies must address an important challenge before their broadband deployment becomes possible. In many promising quantum settings — for example, excitons in quantum dots, single atoms and superconducting qubits — the natural basis for encoding the qubit consists of two energy eigenstates. When coupled to light, such a qubit is naturally converted into the so-called single-rail qubit: the encoding in which the vacuum $|0\rangle$ and single-photon $|1\rangle$ states correspond to the two logical states. Single-rail qubits are however notoriously inconvenient when it comes to QIP and communication by means of light. This is because single-qubit operations are difficult in this encoding [66]. Additionally, the information carried by a single-rail qubit can be easily distorted by optical loss, which results in $|1\rangle$ becoming $|0\rangle$.

A much more robust way of encoding the optical qubit is dual-rail, in which the logical states consist of the photon occupying one of the two orthogonal optical modes. In this way, the photon is present in any valid state of the qubit, thereby providing an easy way to identify when the qubit has been lost. In many applications, the two "rails" are the orthogonal polarisations, horizontal $|H\rangle$ and vertical $|V\rangle$. This allows easy realisation of single-qubit operations by means of polarisation rotators.

In principle, the dual-rail light qubit can be treated as a pair of single-rail qubits carried by each polarisation mode, as we can write $|H\rangle = |1_H\rangle\,|0_V\rangle$ and $|V\rangle = |0_H\rangle\,|1_V\rangle$. That is, a general dual-rail qubit can be split via a polarising beam splitter into two spatial modes, each of which would have to be individually coupled to a stationary system, as demonstrated in e.g. Ref. [67] and references therein. However, this approach necessarily demands a doubling of the number of components in the network. Further, it would still require a method for single-to-dual rail interconversion within the stationary system, which would need to be specific for each such system. It therefore appears more practical to develop a method for such interconversion only for light.

To date, there existed methods for preparing entangled states that connect single- and dual-rail qubits with continuous-variable qubits carried by coherent states of opposite phases [68, 69, 70] — generally labelled "Schrödinger cat states" [55, 56]. In principle, one could use these resources to convert between single-and dual-rail encodings through an intermediate step of continuous-variable encoding. However, this approach is quite cumbersome and susceptible to error. It would be much more desirable to develop a direct method for such interconversion.

This is precisely the goal of this thesis part. We propose and implement a technique to prepare an entangled resource of the form

$$|\aleph\rangle = a\,|H\rangle\,|1\rangle + b\,|V\rangle\,|0\rangle\ . \tag{3.1}$$

We show that this resource can be used for the interconversion between the two bases via quantum teleportation [71] from a qubit carried by a photon's polarisation onto the single-rail encoding. Specifically, we prepared all 6 primary basis states of a dual-rail discrete variable qubit $a|H\rangle + b|V\rangle$ and teleported them onto their single-rail counterparts $a|0\rangle + b|1\rangle$. In this aspect, our experiment achieves the goal pursued in theoretical proposals [72, 73], albeit with a different method which is more general, more experimentally accessible and less vulnerable to inefficiencies.

3.2 Generalities

3.2.1 Remote State Preparation

As mentioned in the abstract of Part II, the interconversion between the DV single-rail and DV dual-rail qubits is achieved by means of a hybrid entangled state with which a teleportation experiment is performed to convert and transfer information from one encoding to the other. Note that the adjective *hybrid* simply illustrates the fact that the entanglement consists of two qubits with different types of encodings.

Prior to realising the teleportation experiment, one needs to experimentally assess the entangled state. Consider such an entangled state $|\Omega\rangle_{12}$ between two spatially distinct modes. One way to assess the state is to perform remote state preparation [74]. The concept is shown in Fig. 3.1 and consists of projecting part of the entangled state $|\Omega\rangle_{12}$ in one mode — spatial mode 1 here — to remotely prepare the state $|\delta\rangle_2$ in another mode — mode 2. By carefully selecting the projection measurement in mode 1 and performing the quantum state tomography of the resulting state $|\delta\rangle_2$, one can thus verify the entanglement of $|\Omega\rangle_{12}$ as it strictly defines the dependence of $|\delta\rangle_2$ from the measurement. In the context of our experiment and as depicted in Fig. 3.1, the projection will be a general single-photon polarisation measurement of the form $|\pi\rangle = a|H\rangle + b|V\rangle$, where a and b are complex numbers, such that the

remote state preparation's result can readily be expressed as $|\delta\rangle_2 = \langle\pi|_1 |\Omega\rangle_{12}$.

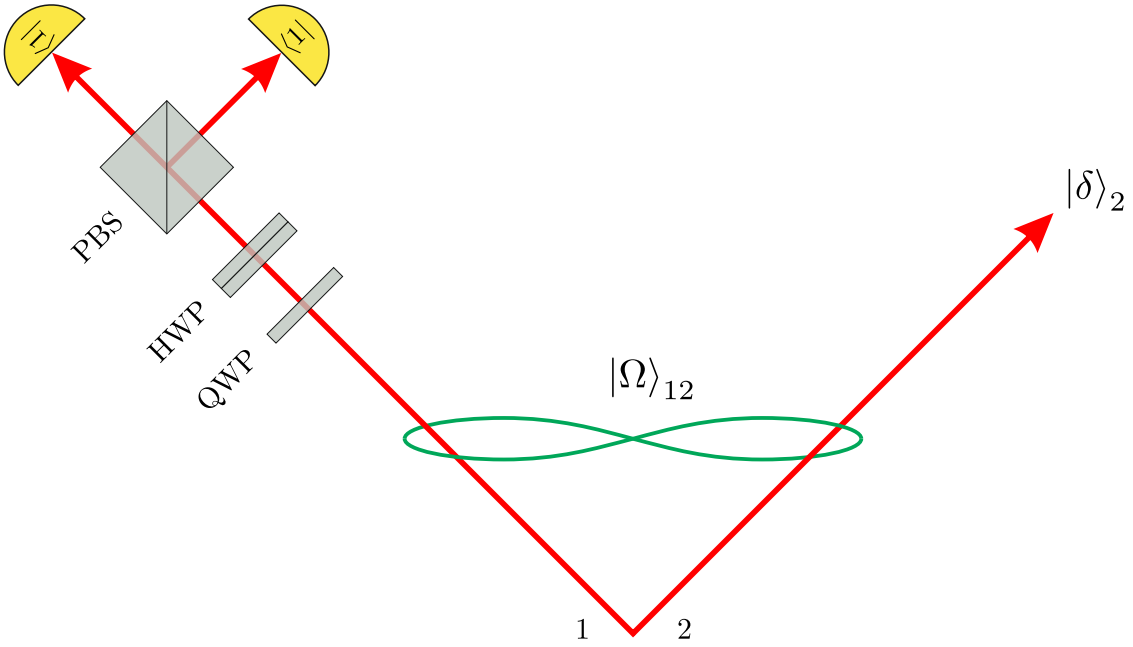


Figure 3.1: Remote State Preparation Concept. $|\Omega\rangle_{12}$ is an entangled state between spatial modes 1 and 2. A polarisation projection of $|\Omega\rangle_{12}$ is performed in mode 1 with the help of single-photon detectors, thus preparing the state $|\delta\rangle_2$ remotely. PBS: polarising beam splitter; HWP: half-wave plate; QWP: quarter-wave plate.

Note that this technique is frequently used in quantum optics where a two-mode squeezed vacuum state is generated from spontaneous parametric down conversion and utilised to heraldically prepare a single photon in one mode from a click measurement in the other mode [75, 76].

3.2.2 Bell State Measurement

One of the key aspects of a teleportation experiment is the ability to faithfully perform a projection onto one of the four Bell states [3], also commonly called *maximally entangled states*. In the polarisation encoding of a qubit, these are written

$$\begin{aligned} \left|\Phi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}} \left(|H\rangle |H\rangle \pm |V\rangle |V\rangle\right) \\ \left|\Psi^{\pm}\right\rangle &= \frac{1}{\sqrt{2}} \left(|H\rangle |V\rangle \pm |V\rangle |H\rangle\right) . \end{aligned} \tag{3.2}$$

As will be seen in the next subsection, a successful projection onto one of these states will signify that the teleportation has indeed occurred. One way to realise such a projective measurement in photonics is to use the setup shown in Fig. 3.2.

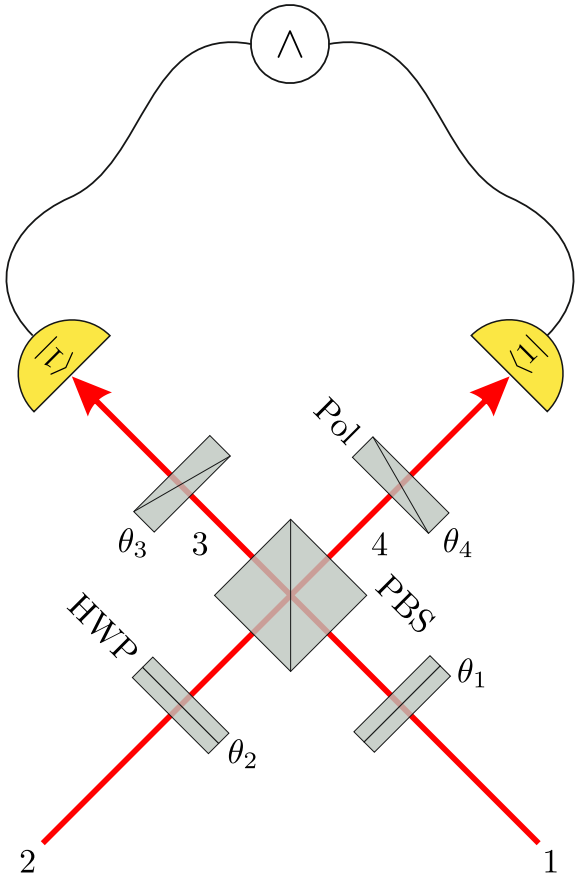


Figure 3.2: Photonic setup used for a polarisation Bell state projection in modes 1 and 2. HWP: half-wave plate; Pol: polarisers.

By carefully setting the angles θ_{1-4} of the half-wave plates (HWPs) and polarisers in modes 1-4 of Fig. 3.2, one can essentially discriminate one of the four Bell states in Eq. (3.2) from the three others when a coincidence click between the two single-photon detectors in modes 3 and 4 is recorded. This arises from the nature of the polarising beam splitter (PBS) which transmits (reflects) any incoming photon of horizontal (vertical) polarisation. Additional details along with an intuitive explanation of this projector are given in Sec. 5.1.2 and Sec. 5.2 where we carefully describe the experimental setup.

3.2.3 Quantum Teleportation

The concept of canonical quantum teleportation is presented in Fig. 3.3.

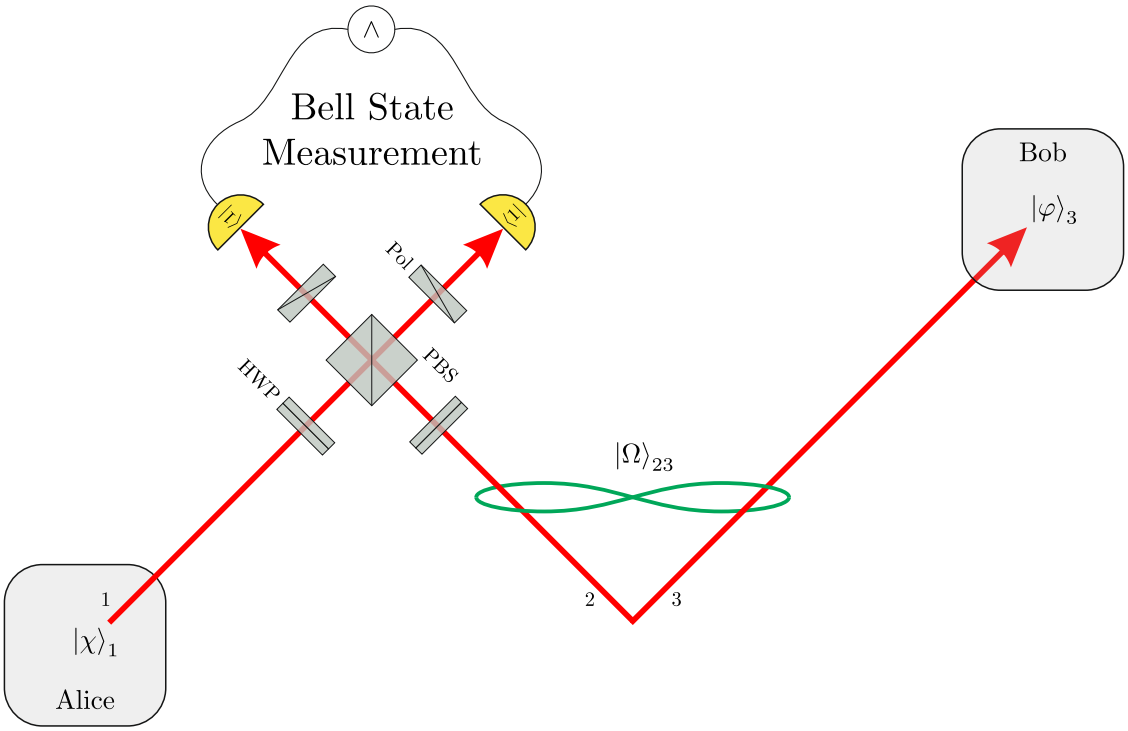


Figure 3.3: Concept of a canonical quantum teleportation experiment.

In this case, Alice wishes to teleport information to Bob. To do so, Alice sends her *source* state $|\chi\rangle_1$ in mode 1 onto the Bell state projector along with half of the state $|\Omega\rangle_{23}$ that is entangled between spatial modes 2 and 3. Upon successful Bell state projection onto one of the four Bell states in modes 1 and 2 (say $|\Psi^+\rangle_{12}$ as an example), Alice informs Bob of her measurement's outcome via classical communication, after which he receives his state $|\varphi\rangle_3$ in mode 3 which can be expressed as

$$|\varphi\rangle_3 = \langle\Psi^+|_{12} |\chi\rangle_1 |\Omega\rangle_{23} \ . \tag{3.3}$$

Note that in its traditional formulation and the first seminal experiments that followed thereafter [71, 77, 78], quantum teleportation assumes that Alice's source state $|\chi\rangle_1$ is unknown to the experimentalist and that she wishes to send Bob a strict copy of it. This necessity in the original formulation stems from the fact that the

no-cloning theorem [79] prevents anyone from cloning a quantum state. As such, quantum teleportation was proposed as a way to circumvent this purely quantum particularity in order to emulate classical signal amplification performed in today's modern communication's fibre optical networks. In our experiment, however, in order to fully characterise the quantum teleportation, we will know what Alice's source $|\chi\rangle_1$ will be — a dual-rail discrete variable qubit — and will wish to teleport it onto Bob in the form of a single-rail discrete variable qubit. It is only after the teleportation has been experimentally demonstrated to faithfully work for all 6 primary basis states that one can then use this scheme to perform teleportation with a purely arbitrary and unknown input source state.

3.2.4 Entanglement Swapping

Lastly, one of the most important results reported in this thesis part involves the concept of entanglement swapping [80, 81] which is illustrated in Fig. 3.4.

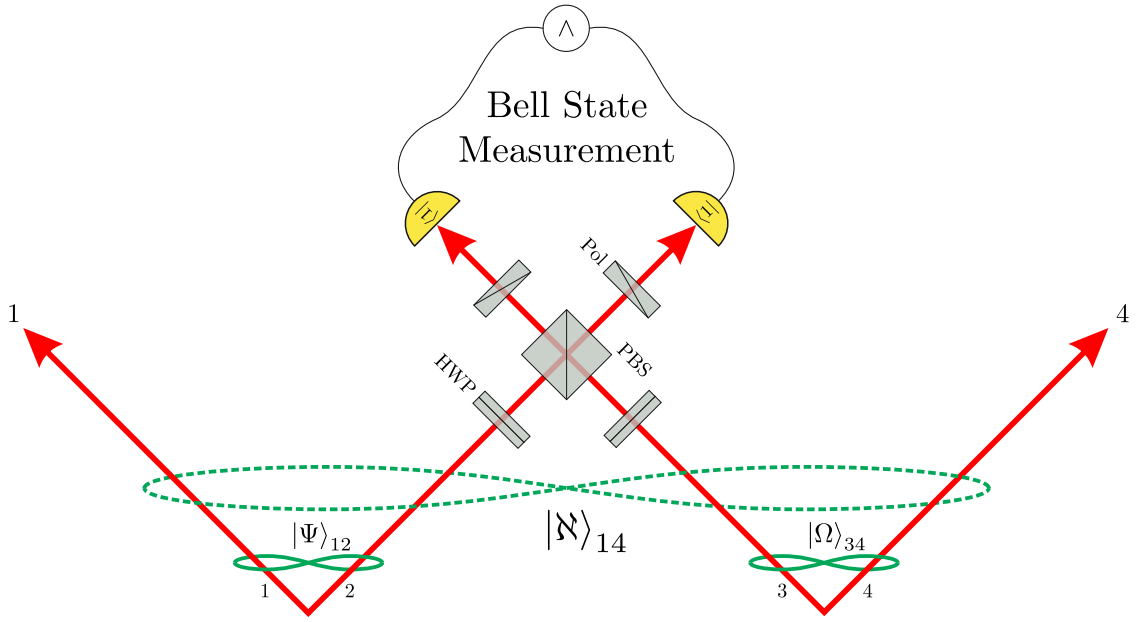


Figure 3.4: Entanglement swapping concept.

Let $|\Psi\rangle_{12}$ and $|\Omega\rangle_{34}$ be two independent entangled states between modes 1-2 and 2-3, respectively. By subjecting each subpart of $|\Psi\rangle_{12}$ and $|\Omega\rangle_{34}$ to a Bell state

measurement in modes 2 and 3, this procedure generates a newly entangled state $|\aleph\rangle_{14}$ between modes 1 and 4 that is expressed as

$$|\aleph\rangle_{14} = \langle\Psi^+|_{23} |\Psi\rangle_{12} |\Omega\rangle_{34} \ , \tag{3.4}$$

provided the Bell state projector did project onto e.g. $|\Psi^+\rangle_{23}$ in modes 2 and 3.

The key idea here is that while photons in modes 1 and 4 were freely propagating and never interacted with one another in any physical way, entanglement has been generated between them as a result of the Bell state measurement. Indeed, the destructive Bell state measurement effectively entangles modes 2 and 3 by projecting them onto $|\Psi^+\rangle_{23}$, leaving modes 1 and 4 in an entangled state. In that regard, entanglement has thus been *swapped* from modes 2 and 3 to modes 1 and 4.

Chapter 4

Theory

'(aside) Two truths are told,
As happy prologues to the swelling act
Of the imperial theme.
(to ROSS and ANGUS) I thank you, gentlemen.
(aside) This supernatural soliciting
Cannot be ill, cannot be good: if ill,
Why hath it given me earnest of success,
Commencing in a truth? I am thane of Cawdor:
If good, why do I yield to that suggestion
Whose horrid image doth unfix my hair
And make my seated heart knock at my ribs,
Against the use of nature? Present fears
Are less than horrible imaginings:
My thought, whose murder yet is but fantastical,
Shakes so my single state of man that function
Is smother'd in surmise, and nothing is
But what is not.'

Macbeth from Shakespeare's "Macbeth"

In this chapter, the theory of the research undertaken is exposed.

4.1 Hybrid Entangled State Generation

To produce the hybrid entangled resource state between the DV dual- and single-rail encodings of a photon, we begin from non-degenerate spontaneous parametric down conversion (SPDC) in crystal 1 as shown in Fig. 4.1. This produces the state $|\psi\rangle_{\mathrm{cr1},CB} = |0_H\rangle_C |0_V\rangle_B + \gamma_1 |1_H\rangle_C |1_V\rangle_B + \mathcal{O}(\gamma_1^2)$ in the vertical and horizontal polarisations of modes B and C, respectively, with γ_1 being the SPDC amplitude. We then use a polarising beam splitter (PBS) to inject a weak coherent state $|\alpha_V\rangle_C = |0_V\rangle_C + \alpha |1_V\rangle_C + \mathcal{O}(\alpha^2)$ into the vertical polarisation of mode C. The collective state $|\Omega\rangle_{CB}$ describing these two modes can be written as the tensor product

$$\begin{aligned} |\Omega\rangle_{CB} \equiv |\alpha_V\rangle_C \otimes |\psi\rangle_{\mathrm{cr1},CB} &\approx |0_H 0_V\rangle_C |0_V\rangle_B \\ &+ \gamma_1 |1_H 0_V\rangle_C |1_V\rangle_B + \alpha |0_H 1_V\rangle_C |0_V\rangle_B \\ &= |0\rangle_C |0\rangle_B + \gamma_1 |H\rangle_C |1\rangle_B + \alpha |V\rangle_C |0\rangle_B \ , \end{aligned} \tag{4.1}$$

up to the first order, where we chose the dual- and single-rail notations in mode C and the vertical polarisation of mode B, respectively, in the last line.

Although the state in Eq. (4.1) is separable, entanglement of the form given by Eq. (3.1) is present in its last two terms corresponding to a photon present in mode C. Intuitively, this reflects the ambiguous situation in which this photon could originate from either crystal 1 or the weak coherent state $|\alpha\rangle$. If such photon came from crystal 1 ($|\alpha\rangle$), then Bob receives a single photon $|1\rangle$ (vacuum $|0\rangle$) in the vertical polarisation of mode B.

Theoretically, this entanglement could be recovered by means of a non-demolition (for example parity [82]), polarisation-insensitive detector in mode C that would project that mode onto the single-photon state. Nevertheless, even without such a detector, the state $|\Omega\rangle_{CB}$ can be used post-selectively to perform the teleportation.

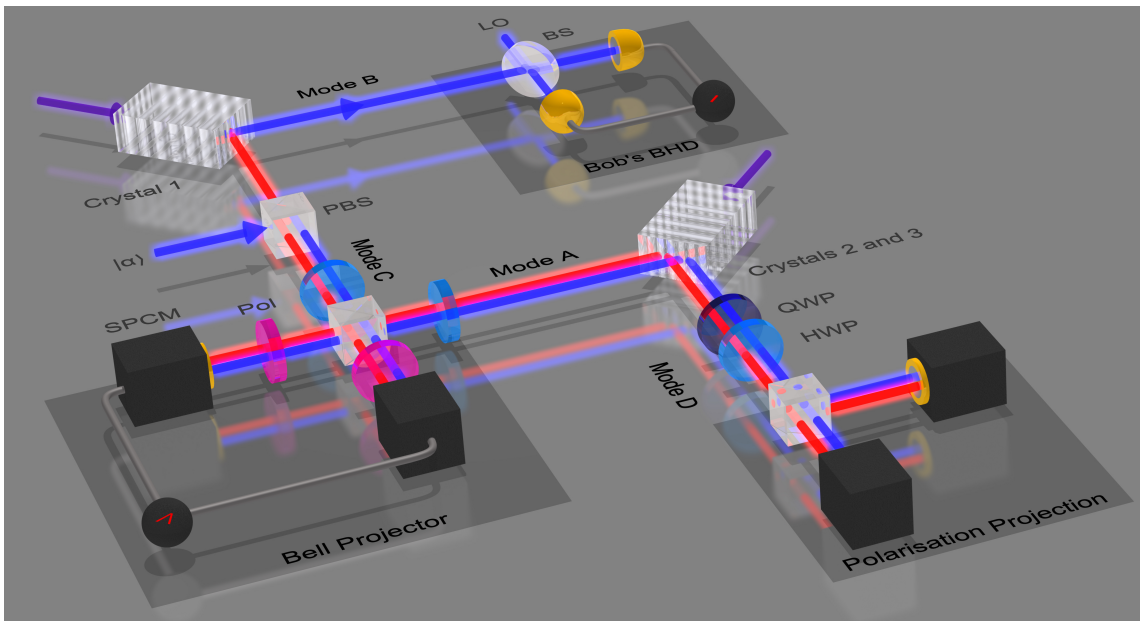


Figure 4.1: Setup for the experiment. To prepare the single-dual rail entangled resource of Eq. (4.1) in spatial modes C and B, one combines a photon from a pair generated in crystal 1 with a coherent state $|\alpha\rangle$ on a PBS. Alice's source state $|\chi\rangle_A$ is obtained by applying a polarisation projection in mode D to a Bell pair $|\Psi\rangle_{AD}$ produced by crystals 2 and 3 (represented in the figure as a single crystal). HWP: half-wave plates (blue); QWP: quarter-wave plates (dark blue); PBS: polarising beam splitters (grey cubes); SPCM: single-photon counting module (black boxes); BHD: balanced homodyne detector. The red (blue) lines correspond to horizontal (vertical) polarisation.

4.2 Remote State Preparation

For remote state preparation, we perform a polarisation projection of $|\Omega\rangle_{CB}$ in mode C onto $|\pi\rangle_C = a\,|H\rangle_C + b\,|V\rangle_C$ by means of a polarisation analyser and a pair of single-photon counting modules (SPCMs) as shown in Fig. 4.1. A click from the SPCM heralds the preparation in mode B of a DV single-rail qubit of the form

$$\begin{aligned} |\delta\rangle_B &= \langle\pi|_C\,|\Omega\rangle_{CB} \\ &= b\,\alpha\,|0\rangle_B + a\,\gamma_1\,|1\rangle_B\ . \end{aligned} \tag{4.2}$$

The procedure's result is analysed using a balanced homodyne detector (BHD) in mode B. Note that the coefficients a and b in Eq. (4.2) can be arbitrarily varied using a half-wave plate (HWP) and quarter-wave plate (QWP) prior to the PBS.

4.3 Quantum Teleportation

For the teleportation to occur, Alice starts by producing an entangled state $|\Psi\rangle_{AD} = |0\rangle_A |0\rangle_D + \gamma_{2,3} (|H\rangle_A |V\rangle_D + |V\rangle_A |H\rangle_D)$ between spatial modes A and D. This is achieved by means of SPDC crystals 2 and 3 (see Fig. 4.1) set in a Mach-Zehnder configuration. Then, a polarisation projection of $|\Psi\rangle_{AD}$ performed in mode D by one of the two SPCMs prepares a heralded dual-rail qubit of the form $|\chi\rangle_A = a |H\rangle_A + b |V\rangle_A$ in mode A which serves as the *source* state for quantum teleportation. Alice sends this state into a Bell state projector $\langle\Psi^+|_{AC} = \frac{1}{\sqrt{2}} (\langle H|_A \langle V|_C + \langle V|_A \langle H|_C)$, combining it with the part of the resource state $|\Omega\rangle_{CB}$ in mode C. Upon a successful application of the Bell state projector — characterised by a coincidence click from the two SPCMs in Fig. 4.1 — Bob finally obtains the following single-rail teleported state in his mode B

$$\begin{aligned} |\varphi\rangle_B &= \langle\Psi^+|_{AC} |\chi\rangle_A |\Omega\rangle_{CB} \\ &= \frac{1}{\sqrt{2}} (a\,\alpha\, |0\rangle_B + b\,\gamma_1 |1\rangle_B) \ . \end{aligned} \tag{4.3}$$

For faithful teleportation, we match the coherent state's amplitude to that of SPDC from crystal 1 so that $\alpha = \gamma_1$. Once again, quantum state tomography is performed in mode B with a balanced homodyne detector to assess the results.

4.4 Entanglement Swapping

The same scheme, but without a measurement in mode D, can in principle produce a freely-propagating single-dual entangled resource as in Eq. (3.1). This happens thanks to entanglement swapping when $|\Omega\rangle_{CB} |\Psi\rangle_{AD}$ is projected onto the Bell state

$|\Psi^+\rangle_{AC}$ in modes A and C. Indeed, this produces the state

$$\begin{aligned} |\aleph\rangle_{BD} &= \langle\Psi^+|_{AC} |\Omega\rangle_{CB} |\Psi\rangle_{AD} \\ &= \frac{\gamma_{2,3}}{\sqrt{2}} \left(\alpha |0\rangle_B |V\rangle_D + \gamma_1 |1\rangle_B |H\rangle_D\right) , \end{aligned} \tag{4.4}$$

which propagates freely in modes B and D and matches with Eq. (3.1).

This, however, would require a source of Bell states in modes A and D operating in a heralded [83, 84] or deterministic [85, 86] fashion. In the absence of such a source, we can still show the viability of this procedure by reconstructing the resulting state in modes B and D post-selectively [70] and assessing its *a posteriori* entanglement.

Chapter 5

Experimental Details

'Ho fermo il core in petto.

Non ho timor: verrò!'
Mozart's "Don Giovanni"

This chapter provides a full detailed description of the experimental setup, the data acquisition scheme and some key techniques utilised to perform the research present in this thesis part. Additionally, few intermediate experimental results required for the full experiment are shown and discussed.

5.1 Experimental Setup

5.1.1 Broad Overview

The experimental setup uses a master laser which is a pulsed Ti:Sapphire (Coherent Mira 900D) with a wavelength of $\lambda = 780\,\text{nm}$, mean output power of $1.3\,\text{W}$, repetition rate of $R_L = 76\,\text{MHz}$ and pulse width of $\tau_{\text{pulse}} = 1.6\,\text{ps}$. We perform frequency doubling in a lithium triborate (LBO) crystal with an efficiency of $\sim 30\%$ to generate the pump required for our SPDC crystals. After further spatial and spectral mode filtering, $50\,\text{mW}$ and $5\,\text{mW}$ of the frequency doubled wave pump crystal 1 and

both crystals 2 and 3, respectively. These are periodically poled potassium titanyl phosphate crystals (PPKTP) operating in a type II spectrally and spatially degenerate, but polarisation non-degenerate configuration, generating two-mode squeezed vacuum states of the form $|0_H\rangle |0_V\rangle + \gamma |1_H\rangle |1_V\rangle + \mathcal{O}(\gamma^2)$.

5.1.2 Detailed Overview

Here, we give a detailed description of the experimental setup which can be found in Fig. 5.1. There are three types of optical beams in the schematic of Fig. 5.1: the seed, the pump and the beams required during the experimental run, namely the local oscillator (LO), the coherent state and the auxiliary beam.

The primary function of the seed beam is to faithfully align the full optical setup. Indeed, as the laser operates at 780 nm and the single photons that will be used during the experiment will have the same wavelength, it thus appears much simpler to align the full experiment with the bright laser light using classical interferometry rather than weak single photons. As can be seen, there are three such seed beams: seed 1, seed 2 and seed 3; one for each nonlinear crystal used for the generation of single photons, i.e. crystals 1, 2 and 3.

The pump — as the name suggests — is the frequency doubled beam (i.e. with a wavelength of 390 nm) that will *pump* (or trigger) the SPDC process in crystals 1-3. It is generated in the LBO crystal labelled "$\mathrm{Cr_{SHG}}1$" in Fig. 5.1 with a $\sim 30\%$ efficiency. Once again, it is split and there are three pump beams; one for each SPDC crystal.

The local oscillator is used in conjunction with the balanced homodyne detector to perform quantum state tomography of the resulting state in mode B. It is a laser beam at 780 nm with an optical power of $10 - 11$ mW.

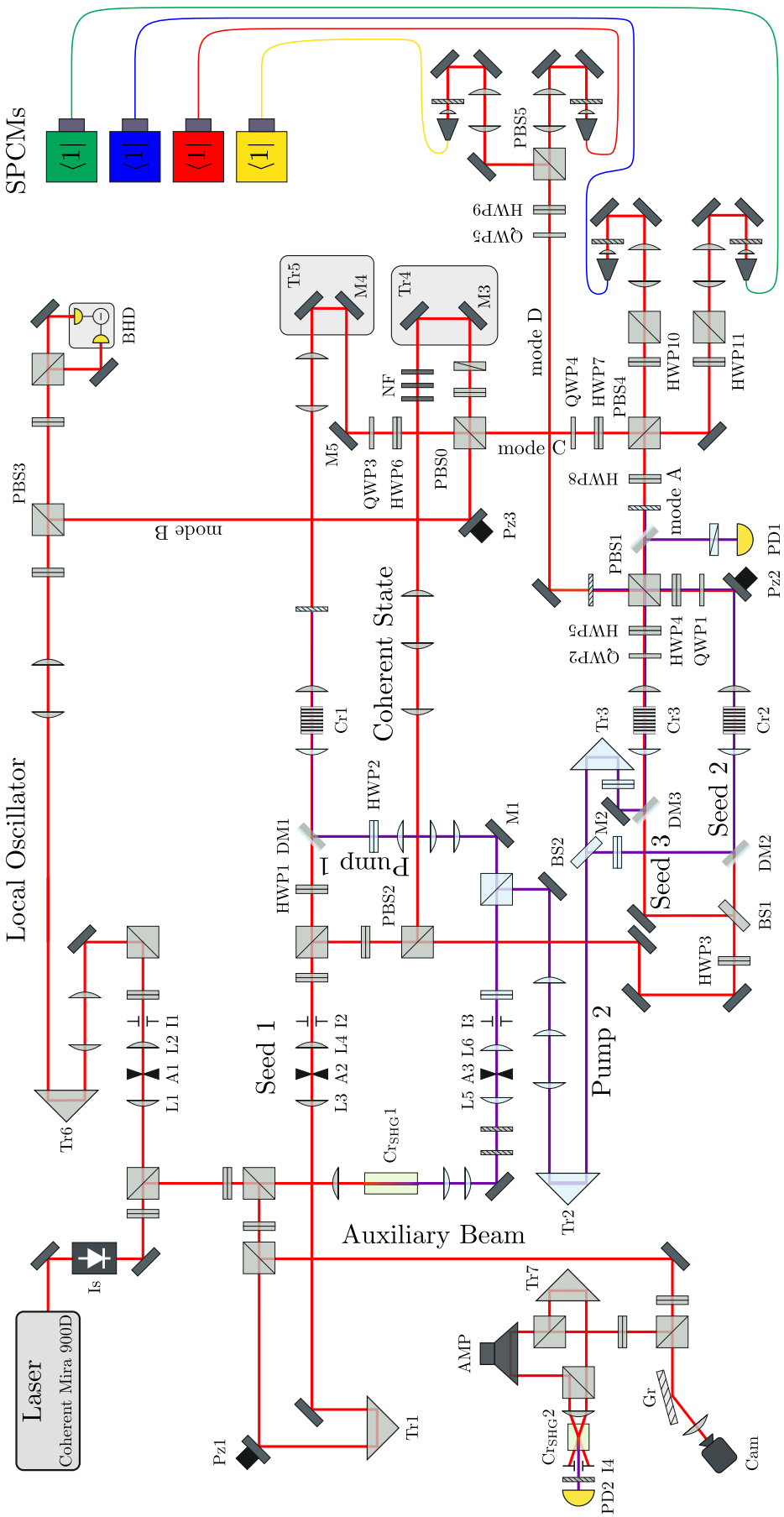


Figure 5.1: The complete optical setup used for the experiment. Is: optical isolator; L: lens; A: aperture; I: iris; Tr: time delay trombone; Pz: piezoelectric mirror; M: mirror; DM: dichroic mirror; Gr: diffraction grating; Cam: camera; PD: photodiode; AMP: acoustic amplifier; PBS: polarising beam splitter; BS: beam splitter; HWP: half-wave plate; QWP: quarter-wave plate; NF: neutral density filter; BHD: balanced homodyne detector; SPCM: single-photon counting module; Cr: nonlinear crystal. The red and blue beams indicate a wavelength of 780 nm and 390 nm, respectively.

The coherent state is the state $|\alpha\rangle$ that is used, along with the SPDC output of crystal 1, to generate the hybrid entangled state $|\Omega\rangle_{CB}$ of Eq. (4.1). In practice, it is obtained from the strong attenuation — via three successive neutral density filters — of a laser beam.

The auxiliary beam is utilised to determine, in real-time, the wavelength of the laser as well as its pulse duration. These two parameters are important since they can detrimentally impact the SPDC count rates and the resulting quality of single photons. To determine the laser wavelength, a diffraction grating along with a camera is used, while the pulse duration is measured by means of an optical autocorrelator. Details about these measurements are given in Sec. 5.1.4 and Sec. 5.1.5. Note that the Coherent Mira 900D laser allows for these parameters to be altered with the help of a monitor.

As can be seen in Fig. 5.1, all above-mentioned beams undergo prior spatial filtering by means of a combination of lenses, diffraction aperture and iris in order to give them a Gaussian-like spatial profile. Indeed, when the laser pulse goes through the circular aperture, the diffraction pattern — whose profile is an Airy disk described by the Bessel function J_1 — can be cut spatially with the help of an iris/diaphragm and the resulting spatial profile approximates that of a Gaussian beam very well.

The hybrid entangled state $|\Omega\rangle_{CB}$ between modes C and B is generated by mixing the weak coherent state $|\alpha\rangle$ and the output of crystal 1 onto the polarising beam splitter "PBS0" in Fig. 5.1.

Balanced homodyne detection is performed by combining the local oscillator and the quantum signal in mode B onto "PBS3".

The polarisation entangled photon pair $|\Psi\rangle_{AD}$ used by Alice to generate her dual-rail source state $|\chi\rangle_A$ is produced in a Mach-Zehnder architecture where the outputs of crystals 2 and 3 interfere on "PBS1". Since the optical path lengths leading

to crystals 2 and 3 are different, a phase difference is introduced in $|\Psi\rangle_{AD}$. This is compensated by the piezoelectric mirror "Pz2" in conjunction with a interferometric feedback loop (for which the signal is detected by the photodiode "PD1") acting as a phase lock. More details about this will be given in Sec. 5.3. Finally, Alice's source $|\chi\rangle_A$ is created by projecting $|\Psi\rangle_{AD}$ in mode D by means of the polarising beam splitter "PBS5" and the red and yellow SPCMs.

The Bell state projector can be found in Fig. 5.1 with the central polarising beam splitter being "PBS4". As can be seen, it takes as input the photons in modes A and C. A successful Bell state projection is obtained when the green and blue SPCMs simultaneously click.

Single photons are coupled into optical fibres by means of collimating lenses and a moveable 3-axis stage. The photons are then directed onto the SPCMs for click detection.

Lastly, it should be mentioned that the presence of piezoelectric mirrors as well as time delay trombones[1] in the setup of Fig. 5.1 is justified since the alignment procedure requires classical interferometry for which both spatial and temporal overlap between different laser pulses is needed.

5.1.3 Alignment

The experimental setup presented in Fig. 5.1 is complex and since the quantum effects needed in the experiment are sensitive to misalignments and fluctuations, the setup should be carefully aligned daily. As such, we propose here a detailed procedure for the alignment as it was performed in the lab.

The key idea is to align every beam with respect to one another. To do so, we always start with the seed beams as they have the wavelength of interest for the

[1]Note that time delay trombones, as their name suggests, introduce a time delay in the beam's path.

experiment when it will be run in the quantum regime, i.e. with single photons.

Golden Rule

All optical beams should be aligned to lie at a vertical distance of 12.1 cm above the level of the optical table. This ensures an overall horizontality for the beam path which makes it easier to insert new optical elements into the table since their mounts have the same height of 12.1 cm.

General Measurements

As a first step, one has to ensure that the second harmonic generation (SHG) process is optimal in the LBO crystal $\mathrm{Cr_{SHG}}1$. If it isn't, it indicates that the crystal's coating under focus might be damaged and consequently, move the crystal to maximise the output optical power. When doing so, it is key to ensure that the SHG beam still goes through the center of the lenses that will later be used for spatial filtering. Once this is done, measure the wavelength and pulse duration of the laser (processes described in Sec. 5.1.4 and Sec. 5.1.5, respectively) to make sure they are optimal.

Spatial Filtering of the Local Oscillator, Seed and Pump

The goal here is to generate a Gaussian-like transverse spatial distribution for the pulse. This procedure should be performed for the pump, the seed and the local oscillator and since it is the same for them all, we should solely describe it for the LO here. To start with, make sure that the LO goes through the center of lenses L1 and L2. Then, adjust the position of the circular aperture A1 in order to maximise the output power. By placing a piece of paper after the iris I1, one should see the result of the diffraction in the far-field, i.e. the Airy disk pattern whose spatial profile is given by the Bessel function J_1 [87]. Using the iris I1, cut all the high orders of

diffraction to leave only the center blob (the zero-th order). The obtained spatial distribution is very similar to a Gaussian pulse. For the seed (the pump), use lenses L3-L4 (L5-L6), circular aperture A2 (A3) and iris I2 (I3) for spatial filtering.

Tuning Crystal 1

SHG Optimisation. Send seed 1 onto crystal 1 and maximise the SHG generated by the crystal. This procedure ensures that the SPDC process used later will be optimal. To do so, first check the wavelength of the laser; if it drifted, readjust it using the Mira monitor. Then, ensure that HWP1 is set at an angle such that the polarisation of seed 1 is optimal for the SHG. The SHG process is sensitive to phase matching conditions and thus to the temperature in the crystal. To change the temperature, use the temperature monitors (i.e. voltage power supplies connected to Peltier units) that make use of the Peltier effect. Then, simply scan the temperature in order to reach a maximised SHG power. Once this is done, move crystal 1 in all three dimensions — it sits on moveable 3-axis stage — to maximise the SHG, thereby making sure that a good point in the crystal is under focus. As a final tip to faithfully optimise the SHG: look at the back reflection of the SHG and its overlap with the incoming red seed. For optimality, have the back reflected SHG beam slightly to the right or slightly to the left of the incoming red seed.

Interference between Pump 1 and the SHG Generated from Crystal 1 by Seed 1. This classical interference will align the pump and seed such that the pump will be optimal for the SPDC process. Similar to the myriad of interferences performed during the alignment, this one requires a piezoelectric mirror to introduce the interference, a time delay trombone to match the pulses in time and mirrors in order to realise spatial matching between the beams. In this case, the piezoelectric mirror is Pz1 which is used globally in the alignment; the time delay trombone is Tr1 and spatial alignment is performed by means of mirrors M1 and DM1 (a dichroic mirror that helps combine pump 1 and seed 1, thus directing them towards crystal 1). By

balancing on a photodiode the signals at 390 nm obtained from pump 1 and the SHG generated in crystal 1 by seed 1 and making sure blue filters are set in the beams' path, one should observe an interference pattern on the oscilloscope. To maximise the interference visibility, use Tr1 for time matching and mirrors M1 and DM1 for spatial overlap. Note that HWP2 must be set to have pump 1 match the SHG beam in polarisation. The classical interference visibility V is calculated as

$$V = \frac{V_{\max} - V_{\min}}{V_{\max} + V_{\min} - 2V_{\text{noise}}}, \tag{5.1}$$

where $V_{\max}$ ($V_{\min}$) is the maximum (minimum) voltage measured on the oscilloscope and V_{noise} is the background noise detected by the photodiode when no beam impinges upon it.

An optimal value for this classical interference should be $V \sim 92\%$. Note that this visibility, along with the other ones listed below, deviates from unity due to small mode and polarisation mismatches beyond experimental control. In this particular case involving a nonlinear signal generated at a crystal, the mode mismatch is aggravated due to the imperfections undergone by the beam throughout the crystal, hence explaining why the visibility does not attain $\sim 98\%$ or higher.

Tuning Crystals 2 and 3

Here, the required procedure is as follows and in the following order:

1. Maximise the SHG generation in crystal 2.
2. Maximise the interference between pump 2 and SHG from crystal 2.
3. Maximise the SHG generation in crystal 3.
4. Maximise the interference between pump 3 and SHG from crystal 3.
5. Maximise the interference between seed 2 and seed 3.

Note that in Fig. 5.1, "pump 2" is equally divided between a pump going to crystal 2 and another one to crystal 3 which we will label pump 2 and pump 3, respectively. This is achieved owing to the 50:50 beam splitter BS2 optimised for 390 nm.

1) Maximise SHG in Crystal 2. Similar procedure as for crystal 1. Make sure HWP3 sets the optimal polarisation of seed 2 and 3 for the SHG. Optimise the temperature and move crystal for the maximisation of the signal.

2) Interference between Pump 2 and the SHG Generated from Crystal 2 by Seed 2. Use Tr2 for time matching and BS2 along with DM2 to optimise the spatial matching between the beams. Note that the pump's polarisation has to be optimised too. The required visibility is $V \sim 92\%$.

3) Maximise SHG in Crystal 3. Same procedure as for crystals 1 and 2.

4) Interference between Pump 3 and the SHG Generated from Crystal 3 by Seed 3. For time matching, use Tr3 and mirrors M2 in conjunction with DM3 for spatial overlap. As before, the visibility should reach $V \sim 92\%$.

5) Interference between Seed 2 and Seed 3. This interference is key as it will grant a correct generation of the polarisation entangled state $|\Psi\rangle_{AD}$ that Alice uses to create her source $|\chi\rangle_A$ for quantum teleportation. Moreover, it is more complicated than the other interferences since its visibility has to be simultaneously optimised for both output modes of PBS1, i.e. modes A and D. The first step consists of making sure that PBS1 will properly transmit and reflect the horizontal and vertical polarisations of the single photons later generated by crystals 2 and 3. The idea will be to use the difference frequency generation (DFG) signals from both crystals and ensure a minimal interference between the seed and the DFG. In practice, one starts with crystal 2 and sets HWP3 such that the transmission of seed 2 through PBS1 into mode A is maximised. This can be achieved by introducing a photodiode in mode D and minimising its measured signal. Then, by inserting QWP1 and HWP4 at the output of crystal 2, one further maximises the transmission in mode A. To fine-tune

this maximisation, send pump 2 onto crystal and minimise the interference on the photodiode in mode A between the newly-generated DFG and seed 2. Then, repeat this whole procedure but with crystal 3 instead: with the same angle on HWP3, minimise the signal on the photodiode in mode A with QWP2 and HWP5, then introduce the DFG signal with pump 3 to further minimise the interference between seed 3 and the DFG in mode A. Once both crystals have thus been optimised, it is granted that PBS1 will correctly function to transmit (reflect) single photons of horizontal (vertical) polarisation. To optimise the interference between seed 2 and seed 3, set HWP3 at an angle $\frac{\pi}{8}$ such that seed 2 and seed 3 split evenly at PBS1. Then, place a photodiode in each output mode of PBS1, i.e. modes A and D, and proceed on with the spatial and temporal overlap. The spatial overlap is optimised by moving the piezoelectric mirror Pz2 and PBS1. Note that there is not any trombone here. Indeed, by moving PBS1 for spatial alignment, it already introduces a time delay between seeds 2 and 3. By carefully overlapping the beams in both output modes with the above-mentioned mirrors, a maximised interference visibility of $V \sim 98.5\%$ should be reached in both modes A and D. Finally, note that the use of QWPs in this procedure arises from the different birefringences generated by crystals 2 and 3.

Interference between Seed 2 and Coherent State $|\alpha\rangle$

For this interference, the spatial matching is granted by overlapping the beam using PBS2 and mirror M3. The time matching is maximised with the time delay trombone Tr4. Note that because the three neutral density (ND) filters NF highly attenuate $|\alpha\rangle$ (they have attenuation factor of 13 dB, 20 dB and 32 dB, respectively), one has to remove the 32 dB ND filter in order to detect $|\alpha\rangle$ on the photodiode in order to perform the interference with seed 2. By doing so, when the optimal spatial matching is reached, one has to insert the ND filter back and carefully readjust the time matching with Tr4 since the optical length for $|\alpha\rangle$ would have changed. The interference visibility should reach $V \sim 99\%$ here.

Interference between Seed 1 and Seed 2

Maximise the spatial overlap with mirrors M4 and M5 and the temporal matching with the time delay trombone Tr5. The interference visibility should reach $V \sim 99\%$. We have now ensured that all seed beams are aligned with respect to one another.

Interference between Seed 1 and LO

All quantum signals will be analysed by means of a balanced homodyne detector in mode B to perform quantum state tomography. As such, it is crucial to align the signal beam with respect to the BHD's LO. A first step towards this goal is taken with the help of this particular interference. Indeed, as will be seen in the next alignment paragraph, there is another classical way to better this alignment with the LO. The spatial overlap is maximised with the help of the piezoelectric mirror Pz3 and the polarising beam splitter PBS3, while the temporal matching can be optimised with the time delay trombone Tr6. The interference visibility here should reach $V \sim 98\%$.

Interference between DFG from Crystal 1 and LO

As we shall wish to detect single photons from SPDC in mode B via a BHD, the question as to which is the best classical technique to align these weak beams with the LO arises. In reality, it was shown [88] that it is the crystal's DFG signal that best resembles the spatiotemporal profile of photons originating from SPDC in that same crystal. Consequently, by maximising the classical interference between the LO and this DFG signal, one can ensure a sufficiently good preliminary alignment for quantum state tomography via balanced homodyne detection. To do so, start by minimising the SHG signal in crystal 1 using HWP1. Then, using QWP3 and HWP6, maximise the transmission of seed 1 through PBS0, i.e. in mode C. This can be done by placing a photodiode in mode B and seeking to minimise its measured

voltage. Once this is done, let pump 1 impinge onto crystal 1. This should generate the DFG that is supposed to propagate in mode B. Now, it is important to wait few minutes with a strong pump 1 onto crystal 1. This will "warm" the crystal up such that the DFG's spatial mode is optimal for the interference. After these few minutes, check that the interference between the DFG and seed 1 in mode C is minimal. If all the above-mentioned steps have duly been followed, the DFG signal from crystal 1 in mode B should be in good condition for the interference with the LO. Just like the previous interference, use the piezoelectric mirror Pz3 and the polarising beam splitter PBS3 in order to maximise the spatial overlap and move the time delay trombone Tr6 for time matching. The interference visibility should reach $V \sim 88\%$. Note that, since the LO and DFG signal from crystal 1 have a random phase difference that will fluctuate due to fluctuations in the air, one must switch on the piezoelectric mirror Pz3 to get rid of these fluctuations. Without this, the interference between the DFG signal from crystal 1 and the LO will randomly oscillate, thereby making it impossible to optimise faithfully.

Fibre Coupling

Fibre coupling was usually performed with seed 2 — note that it shouldn't matter since all the beams are aligned with respect to one another — and it consists of maximising the fibre coupling in the green, blue, red and yellow optical fibres leading up to the corresponding SPCMs. Each fibre coupling unit is mounted on a moveable 3-axis stage which has a circular lens attached to it used for the coupling. Prior to the stage, there is a collimating pair of lenses to ensure an optimised beam width. Lastly, a narrowband 0.2 nm interference filter is present in the path of each fibre coupler. These will make sure that the obtained single photons have the same wavelength and can thus interfere. In practice, one starts by orienting the interference filter such that the transmission of seed 2 through it is maximised. Then, using the pair of mirrors in front of the stage to direct the laser beam into the fibre, the coupling should be optimised by maximising the power measured at the fibre's output. Typical fibre

coupling efficiencies should be $\sim 87-92\%$. These are limited by the overlap between the laser's Gaussian pulses and the nearly Gaussian fundamental mode of the fibre. Note that it is quite important to check the laser's wavelength during this operation and make sure it is correctly set since the resulting interference filter's transmission will be lowered upon variation of the laser's wavelength.

Balanced Homodyne Detector

Send $10-11\,\mathrm{mW}$ of LO light onto the BHD. A proper alignment of the BHD will arise when the difference voltage output by the BHD no longer contains the laser's repetition rate frequency, thereby leaving a signal at twice that frequency. Recall that, in theory, mode-locking [89] from the laser gives a signal with all $\nu_n = n\nu$ integer times the laser repetition rate's frequency $\nu = \frac{c}{2L}$, where L is the laser's cavity length. However, in practice, the BHD doesn't erase all $n \geq 2$ frequencies when properly aligned and it is thus sufficient to consider that the detector is set when the $\nu_{n=1}$ laser repetition rate frequency has been erased. To do so, use the HWP in front of the PBS prior to the BHD in Fig. 5.1 to make the splitting at the PBS even — essentially acting as a 50:50 BS. Furthermore, the BHD being on a translational stage, move the stage along with the mirrors directing light onto the BHD to ensure a good suppression of the $\nu_{n=1}$ frequency.

Optimise the Single-Photon Efficiency

As an epilogue to the alignment procedure, one usually tests the alignment's quality upon the single-photon efficiency η. It is the single-photon efficiency arising from the single photons emitted by crystal 1. These are measured in mode B with the BHD when mode C has been projected with either the green or blue optical fibre (recall that crystal 1 prepares a two-mode squeezed vacuum and that remote state preparation is performed to obtained single photons from it). More details will be given about η and how to properly measure it in Sec. 5.4, however the

idea here is that the resulting single photon in mode B will be in a mixed state $(1-\eta)\left|0\right\rangle\left\langle 0\right|_B + \eta\left|1\right\rangle\left\langle 1\right|_B$ instead of a pure state $\left|1\right\rangle_B$ such that the larger the measured efficiency η, the better the alignment. Let us assume we can measure η without yet knowing how. In practice, a good value for it would be $\eta \sim 58-62\%$. To achieve and improve it, there are many routes available, some one which include:

1. Adjusting Pz3 to further improve spatial overlap between the single photons and the LO used in the balanced homodyne detector.

2. Moving crystal 1 along its three spatial axes. A better focus point within the crystal might be found and hence increase the efficiency.

3. Adjusting the position of the lenses in the LO path. This can help match the LO's beam width to that of the single photons.

4. Temporal overlap optimisation using Tr6.

5. Changing the laser's wavelength slightly for the SPDC process to be more efficient.

6. Slightly modifying the fibre coupling of the heralding mode — e.g. with the green fibre — to improve the resulting shape of the photons [88].

This completes the alignment procedure required for the setup in Fig. 5.1. In the next two subsections, we shall go over the auxiliary beam and its two associated measurements: that of the wavelength and the laser's pulse duration.

5.1.4 Laser Wavelength Measurement

The laser's wavelength measurement is implemented by means of a homemade calibrated spectrometer consisting of the optical grating Gr and the camera Cam in Fig. 5.1. In practice, one monitors the resulting signal on the camera with the help of the Mira wavelength monitor and ensures that it stays within a precise spatial

region calibrated to correspond to the laser's wavelength being optimal for the SPDC process.

The calibration is made off-line using a narrowband interference filter and Bragg's law. Indeed, when the transmission of the laser beam through the interference filter — whose orientation with respect to the beam is θ — is maximised, the distance x measured on a piece of paper — at a distance L from the interference filter — between the incoming beam and the minimised first order of diffraction from the crystal-like structure of the interference filter is dependent on the wavelength of the laser λ and the width d of the interference filter. Since the filter's width d is known, one can calculate the value of x such that the wavelength λ reaches its optimal experimental value. Thus, by adjusting λ with the Mira monitor in order to measure the optimal distance x, the laser's wavelength is optimised and its signature on the camera — obtained from the diffraction at the optical grating Gr — can then be used as a calibration for the real-time monitoring with the spectrometer.

Mathematically, this problem can be formalised using Bragg's law [90] for a destructive interference

$$2d \sin\theta = (2m+1)\frac{\lambda}{2}\,, \tag{5.2}$$

where $m \in \mathbb{N}$ is the order of diffraction, and noting that x and θ are linked geometrically by the principle of reflection for which one gets

$$\sin 2\theta = \frac{x}{\sqrt{x^2+L^2}}\,. \tag{5.3}$$

Then, using the trigonometric identity $\sin 2\theta = 2\sin\theta\cos\theta = 2\sin\theta\sqrt{1-\sin^2\theta}$, one can compare Eq. (5.2) and Eq. (5.3) to finally obtain

$$\lambda = 2\sqrt{2}\,d\sqrt{1+\frac{L}{\sqrt{x^2+L^2}}}\,, \tag{5.4}$$

for $m = 0$.

For fixed and known parameters d and L, Eq. (5.4) sets a direct relationship between λ and x, thereby enabling the experimentalist to calibrate the wavelength measurement as per the procedure described above.

5.1.5 Pulse Duration Measurement

As mentioned in Sec. 5.1.2, the laser pulse's duration measurement uses an optical autocorrelator. Its implementation can be found in Fig. 5.1 where the auxiliary beam is split between two arms of a Michelson interferometer [91]. The first beam — call it beam 1 — goes through the time delay trombone Tr7 that induces a spatial displacement Δ, while beam 2 experiences a periodic spatial displacement δ introduced by the acoustic amplifier AMP. Both beam 1 and beam 2 are then combined on a PBS, followed by the nonlinear crystal $\mathrm{Cr_{SHG}2}$ that will produce SHG whose amplitude [92] can be expressed as

$$E_{\mathrm{SHG}} \propto |E_1 + E_2|^2 = |E_1|^2 + |E_2|^2 + 2E_1E_2^*\,, \tag{5.5}$$

where $E_{1,2}$ are the electric fields corresponding to beams 1 and 2.

Intuitively, Eq. (5.5) indicates that the two photons required for SHG may originate from either the pulse E_1 or E_2, or that they may arise from one photon coming from each pulse. Given the orientation of beams 1 and 2 introduced by the lens prior to the SHG crystal, the phase matching condition $\boldsymbol{k}_{\mathrm{SHG}} = \boldsymbol{k}_1 + \boldsymbol{k}_2$ imposes the SHG pulse originating from beams 1 and 2 to be collinear. On the other hand, SHG pulses arising from solely beam 1 or beam 2 will keep travelling in the same non collinear direction as beam 1 and 2 (indeed, phase matching reads $\boldsymbol{k}_{\mathrm{SHG}} = \boldsymbol{k}_{1,2} + \boldsymbol{k}_{1,2} = 2\boldsymbol{k}_{1,2}$ here) such that one can easily block them using the iris I4 in Fig. 5.1. Consequently, the SHG signal impinging onto the photodiode PD2 is the following

$$E_{\mathrm{SHG}} \propto E_1(t, \Delta/c)E_2(t, \delta/c)\,, \tag{5.6}$$

with c the speed of light and where Δ/c and δ/c are the time delays introduced by the trombone Tr7 and the loudspeaker AMP, respectively. It should be noted that Eq. (5.6) almost resembles the mathematical definition of an autocorrelation function [93].

Assuming Gaussian laser pulses, one writes

$$E_1(t, \Delta/c) \propto e^{-\frac{(t-2\Delta/c)^2}{2\sigma^2}} \quad ; \quad E_2(t, \delta/c) \propto e^{-\frac{(t-2\delta/c)^2}{2\sigma^2}}, \tag{5.7}$$

where σ is the laser pulse's standard deviation in time.

The photodiode PD2 will integrate the intensity of the SHG signal in Eq. (5.6) over its electronic bandwidth BW_{PD}. Since the laser's pulse duration is such that $\frac{1}{\tau_{\text{pulse}}} \gg R_L \gg BW_{\text{PD}}$, the integration can be performed over infinity and the resulting detected SHG intensity I_{SHG} will be expressed as

$$I_{\text{SHG}}(\tau) \propto \int_{-\infty}^{+\infty} |E_1(t)E_2(t-\tau)|^2 \, dt \equiv \int_{-\infty}^{+\infty} |E(t)E(t-\tau)|^2 \, dt \,, \tag{5.8}$$

which is exactly the definition of the mathematical autocorrelation $A^{(2)}(\tau)$. As such, in an optical autocorrelator [94], the autocorrelation is directly linked to the measured intensity of a collinear SHG signal arising from two identical, time delayed and non collinear beams and one writes $A^{(2)} \propto I_{\text{SHG}}$.

Note that in our case, the time delay τ in the integral between pulse E_1 and E_2 (which were written as simply E in Eq. (5.8) given that they have the same temporal profile) is given by δ, while Δ will be used to determine τ_{pulse} as will be shown below.

Using the Gaussian beams of Eq. (5.7), one can derive the autocorrelation ex-

pressed in Eq. (5.8) to get

$$\begin{aligned} A^{(2)}(\delta,\Delta) &\propto \int_{-\infty}^{+\infty} |E_1(t,\Delta/c)E_2(t,\delta/c)|^2 \, dt \\ &\propto \int_{-\infty}^{+\infty} e^{-\frac{(t-2\Delta/c)^2}{\sigma^2}} e^{-\frac{(t-2\delta/c)^2}{\sigma^2}} \, dt \\ &= \sigma\sqrt{\frac{\pi}{2}} e^{-\frac{(\delta-\Delta)^2}{c^2\sigma^2/2}} \\ &\propto e^{-\frac{(\delta-\Delta)^2}{c^2\sigma^2/2}} , \end{aligned} \tag{5.9}$$

which is yet another Gaussian function.

Since the photodiode outputs the autocorrelation signal $A^{(2)}(\delta,\Delta)$ given by Eq. (5.9), the final step now is to measure the laser's pulse width τ_{pulse} from $A^{(2)}(\delta,\Delta)$.

Knowing that the full width at half maximum (FWHM) of a generic Gaussian pulse with standard deviation α is FWHM $= 2\alpha\sqrt{2\ln 2}$, the measured autocorrelation's FWHM is then

$$\text{FWHM}_{A^{(2)}} = c\sigma\sqrt{2\ln 2}\,. \tag{5.10}$$

Alternatively, the laser's pulse duration τ_{pulse} is defined as the FWHM of the laser beam's intensity pulse $I \propto E^2$. As such, given that the electric field is Gaussian, one can express the FWHM of the pulse's intensity as

$$\text{FWHM}_{\text{pulse}} \equiv \tau_{\text{pulse}} = 2\sigma\sqrt{\ln 2}\,. \tag{5.11}$$

To link τ_{pulse} to $\text{FWHM}_{A^{(2)}}$ from the autocorrelation's profile, it can be seen that $A^{(2)}(\delta^*,0)$ and $A^{(2)}(\delta^*,\Delta)$ intersect at half the maximum of the autocorrelation function $A^{(2)}(\delta,\Delta)$ for the particular value $\delta^* = \frac{\text{FWHM}_{A^{(2)}}}{2}$. This can be expressed mathematically as the following equations

$$A^{(2)}(\delta^*,0) = A^{(2)}(\delta^*,\Delta) = \frac{1}{2}\max A^{(2)} \equiv \frac{1}{2} \quad ; \quad \delta^* = \frac{\text{FWHM}_{A^{(2)}}}{2}\,. \tag{5.12}$$

Solving Eq. (5.12) for Δ gives the solution

$$\Delta = c\sigma\sqrt{2\ln 2}\,. \tag{5.13}$$

Finally, this enables one to measure τ_{pulse} from Δ by combining Eq. (5.13) and Eq. (5.11), thereby yielding

$$\tau_{\text{pulse}} = \frac{\sqrt{2}\Delta}{c}\,. \tag{5.14}$$

In practice, the photodiode PD2's output is read on an oscilloscope. The obtained autocorrelation is scanned horizontally by means of the acoustic amplifier AMP and the pulse width can be directly measured on the oscilloscope. Indeed, it has been calibrated such that one time division corresponds to a pulse duration of $\sim 1.6\,\text{ps}$ as per Eq. (5.14) with a spatial displacement of $\Delta = 0.35\,\text{mm}$.

5.2 Bell State Projector

Similar to the schematic in Fig. 3.2, the Bell state projector used in the experiment and shown in Fig. 5.1 is made of two input HWPs (HWP7 in mode C and HWP8 in mode A), a polarising beam splitter (PBS4) and two output polarisers which are implemented using a combination of HWP and PBS (HWP10 and HWP11 and their corresponding PBSs).

The central element in the projection apparatus is the PBS, which directs the input photons of different polarisations into the same output spatial mode, thereby preventing coincidence clicks from the input Bell states $|\Psi^{\pm}\rangle_{AC}$. The photons in the two PBS output modes are filtered by HWPs at an angle $\pm\frac{\pi}{8}$ in conjunction with PBSs (essentially acting as polarisers set at an angle $\pm\frac{\pi}{4}$) prior to detection, so that the state $|\Phi^{+}\rangle_{AC}$ is not transmitted. Therefore, a coincidence click projects the PBS's input onto $|\Phi^{-}\rangle_{AC}$ [95, 96, 97]. However, because both input modes of the Bell state projector are rotated by $\frac{\pi}{4}$ — using HWP7 and HWP8 set at an angle

$\frac{\pi}{8}$ — before entering the PBS, the state to which the Bell state projector responds is $|\Psi^+\rangle_{AC} = \frac{1}{\sqrt{2}}(|H\rangle_A |V\rangle_C + |V\rangle_A |H\rangle_C)$, as expected.

The benefits of our implementation of the Bell state projector are threefold with respect to the original version found in [98] that makes use of a sole 50:50 beam splitter. First, it reduces the rate of false positive Bell state detection events due to two photons present in the same input mode, being oblivious to events in which these two photons have orthogonal polarisations [95]. Second, given the polarisation sensitivity granted by the PBS, it allows us to perform remote state preparation by projecting $|\Omega\rangle_{CB}$ in mode C, thereby enabling the monitoring in real-time of the phase in channel B necessary for quantum state reconstruction of Bob's teleported state — this will be detailed in Sec. 5.5. Third, it obviates the need to align the regular beam splitter to an exact 50% reflectivity[2].

Prior to the full experiment, it is paramount to test that the Bell state projector is properly aligned, with the waveplate angles θ_{1-4} in Fig. 3.2 precisely set. To do so, we performed a Hong-Ou-Mandel (HOM) interference between the weak coherent state $|\alpha\rangle_C$ in mode C and Alice's source $|\chi\rangle_A$ in mode A. The weak coherent state is vertically polarised and can thus be written as $|\alpha\rangle_C = |0\rangle_C + \alpha |V\rangle_C$, while Alice's source was prepared from $|\Psi\rangle_{AD}$ such that we produced $|\chi\rangle_A = |V\rangle_C$ at the input of the projector in mode C. By recording the triple coincidence counts between the pair of SPCMs at the Bell state projector and the SPCM in mode D used for the heraldic preparation of $|\chi\rangle_A$, we obtained the Hong-Ou-Mandel dip signature in Fig. 5.2.

As can be seen in Fig. 5.2, the data fits the theoretical curve [99] well since a coefficient of determination $R^2 = 98.9\%$ was found. Additionally, the HOM dip visibility displays a $V = 97.67\%$ visibility (after subtraction of the noise background described below), thus confirming the proper alignment of the Bell state projector. Note that the black dashed noise floor in Fig. 5.2 represents the proportion of

[2]Indeed, by tilting the regular beam splitter and/or moving the detectors sideways, one can achieve a resulting 50:50 splitting ratio since all undesired reflections would have thus been eliminated.

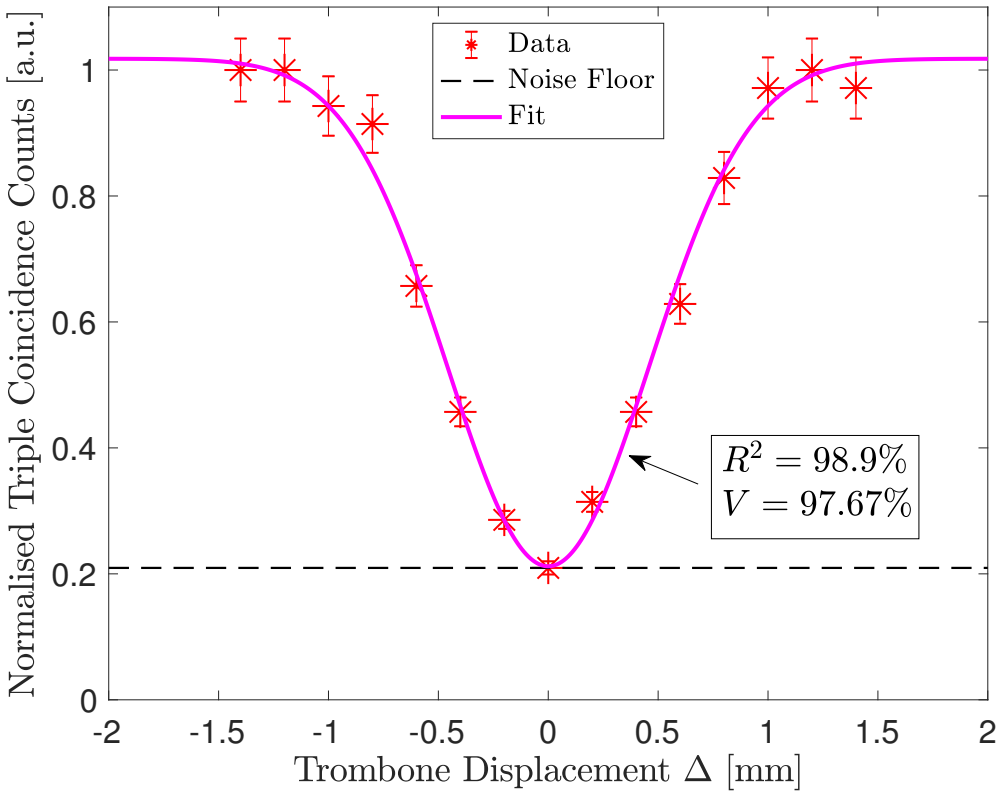


Figure 5.2: Hong-Ou-Mandel dip observed when mixing the weak coherent state $|\alpha\rangle_C$ in mode C and a single Fock state $|\chi\rangle_A$ in mode A at the input of the Bell state projector. The fit yields a coefficient of determination $R^2 = 98.9\%$ and the resulting calculated HOM dip has a $V = 97.67\%$ visibility.

unwanted triple coincidence clicks obtained from the weak coherent state $|\alpha\rangle_C$ in mode C and the projection of $|\Psi\rangle_{AD}$ in mode D while mode A was blocked. These triple clicks arose from spurious double coincidence clicks at the Bell state projector originating from $|\alpha\rangle_C$ and the usual click in mode D. Each data point was obtained from a 5 minutes waiting time and with a single-photon rate of $R_\alpha \sim 300\,\text{kHz}$ and $R_\chi \sim 2\,\text{kHz}$ measured by the green SPCM. Note that $R_\alpha \sim 300\,\text{kHz}$ was chosen to be large to speed up the acquisition of the data. The time delay required for the HOM interference was implemented using the displacement Δ of the trombone Tr4.

Finally, we found that adding the quarter-wave plate QWP4 in mode C prior to the projector's input half-wave plate HWP7 in Fig. 5.1 significantly increased the HOM dip visibility. This, in turn, drastically reduced the number of false positive Bell state projections measured. This can be intuitively understood since the QWP

corrects for the inevitable birefringence arising from the slanting of the Bell state projector's PBS (PBS 4) with respect to the PBSs used for the generation of $|\Omega\rangle_{CB}$ (PBS0) and $|\Psi\rangle_{AD}$ (PBS1), respectively.

5.3 Polarisation Entangled Photon Pair

One of the key aspects of the experiment is the polarisation entangled state $|\Psi\rangle_{AD}$ used by Alice to generate her source $|\chi\rangle_A$ for quantum teleportation. This section supplies details about the state's generation and the subsequent testing of its quality.

5.3.1 Generation

To generate Alice's entangled state $|\Psi\rangle_{AD}$, we used the Mach-Zehnder interferometer architecture introduced in [100], where the outputs of two SPDC crystals interfere on a PBS — PBS1 in the experimental setup of Fig. 5.1. Due to different optical path lengths in the Mach-Zehnder interferometer, photons from crystals 2 and 3 experience a phase difference $\Delta\phi_{\gamma_{2,3}}$ which is introduced in $|\Psi\rangle_{AD}$ — details will be provided in Sec. 5.5. We use the piezoelectric transducer Pz2 along with an interferometric feedback loop — monitored by the photodiode PD1 — to ensure $\Delta\phi_{\gamma_{2,3}} = 0$ at all times.

5.3.2 Assessment

The quality of the entangled state $|\Psi\rangle_{AD}$ has been tested by applying a polarisation projection in mode D and measuring the probability of a coincidence click between a pair of SPCMs in modes A and D as a function of the angle θ_A of a half-wave plate (HWP8) set in mode A. The polarisation projection in mode D is implemented using a half-wave plate (HWP9) at an angle θ_D and a polarising beam splitter (PBS5). As already mentioned, these two components act as polariser set

at an angle $2\theta_D$. One can thus readily obtain the normalised coincidence click probability between a pair of SPCMs in modes A and D as a function of θ_A and θ_D from Born's rule [101]

$$\begin{aligned} P_{\text{c.c}}(\theta_A;\theta_D) &= \mathcal{N}\left|\left(\cos 2\theta_A \langle H|_A + \sin 2\theta_A \langle V|_A\right)\left(\cos 2\theta_D \langle H|_D + \sin 2\theta_D \langle V|_D\right)|\Psi\rangle_{AD}\right|^2 \\ &= \mathcal{N}\frac{\gamma_{2,3}^2}{2}\left|\cos 2\theta_A \sin 2\theta_D + \sin 2\theta_A \cos 2\theta_D\right|^2 \\ &= \sin^2\left(2(\theta_A+\theta_D)\right) , \end{aligned} \tag{5.15}$$

where $\mathcal{N}$ is a normalising factor and for which the phase difference $\Delta\phi_{\gamma_{2,3}}$ in $|\Psi\rangle_{AD}$ was assumed to be zero. The measurement of $P_{\text{c.c}}(\theta_A;\theta_D)$ is plotted in Fig. 5.3.

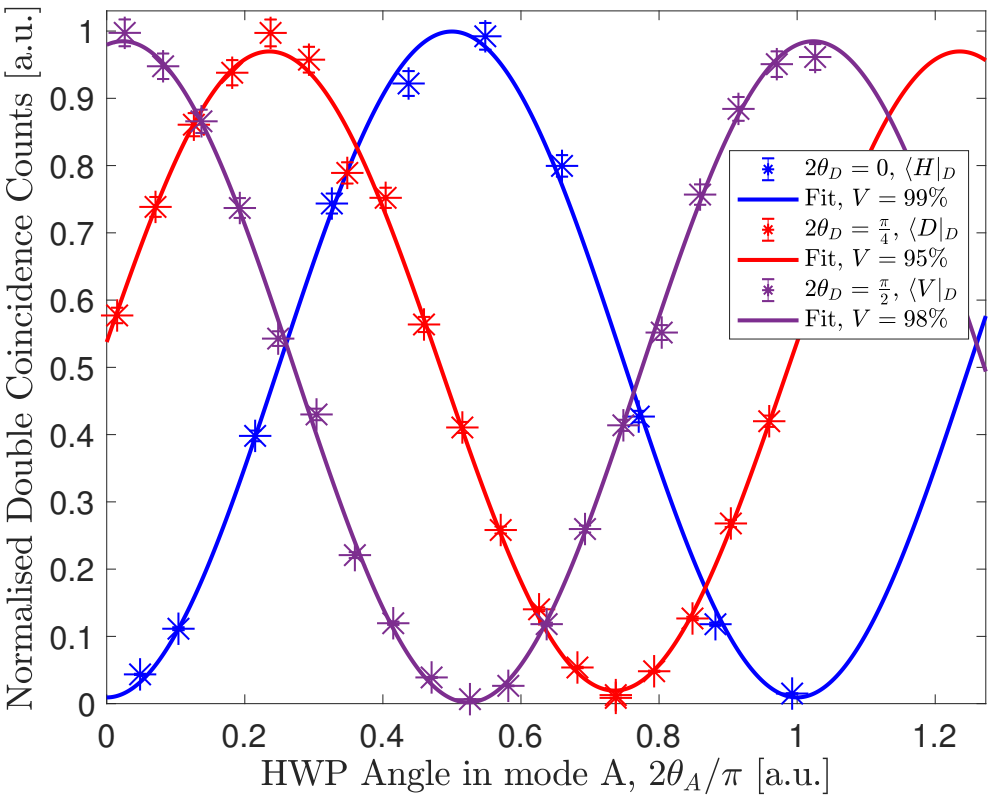


Figure 5.3: Assessment of the entanglement of $|\Psi\rangle_{AD}$ by plotting $P_{\text{c.c}}(\theta_A;\theta_D)$ as a function of θ_A in mode A and for three distinct polarisation projections in mode D; namely $\langle H|_D$, $\langle D|_D$ and $\langle V|_D$ in blue, red and purple, respectively. The corresponding visibilities calculated from theoretical fits are shown in the legend.

From Fig. 5.3, one can visualise the sinusoidal dependence of $P_{\text{c.c}}(\theta_A;\theta_D)$ in Eq. (5.15) as a function of θ_A — the angle of HWP8 — for three different po-

larisation projections performed in mode D: $\langle H|_D$, $\langle D|_D \equiv \frac{1}{\sqrt{2}}(\langle H|_D + \langle V|_D)$ and $\langle V|_D$. The data has been fitted by the theoretical curve in Eq. (5.15) and yields visibilities of 99%, 95% and 98% for the three above-mentioned projections, thereby confirming the entanglement of $|\Psi\rangle_{AD}$. The reason why the visibilities are not unity is because the interference between seed 2 and seed 3 is not perfect, leading to the preparation of an imperfect $|\Psi\rangle_{AD}$, and hence the non-unity visibilities in Fig. 5.3.

5.3.3 Generation of Alice's Source State $|\chi\rangle_A$

The generation of Alice's source state $|\chi\rangle_A$ is done by measuring the polarisation entangled state $|\Psi\rangle_{AD}$ in mode D. In practice, the combination of QWP5, HWP9 and PBS5 in Fig. 5.1 is used to perform this polarisation projection and thus prepare the six primary basis states of the dual-rail qubit in mode A; namely $\{|H\rangle_A, |V\rangle_A\}$ for the canonical basis, $\{|D\rangle_A \equiv \frac{1}{2}(|H\rangle_A + |V\rangle_A), |A\rangle_A \equiv \frac{1}{2}(|H\rangle_A - |V\rangle_A)\}$ for the diagonal basis and $\{|R\rangle_A \equiv \frac{1}{2}(|H\rangle_A + i|V\rangle_A), |L\rangle_A \equiv \frac{1}{2}(|H\rangle_A - i|V\rangle_A)\}$ for the circular basis.

For each basis, one of the two orthogonal states is prepared when a click is recorded by either the red or yellow SPCM. Indeed, this is ensured since, by definition, the two output modes of PBS5 leading to the red and yellow SPCMs are orthogonal in polarisation. As such, when one performs the full quantum teleportation experiment, depending on whether the red or yellow SPCM clicked, a different state $|\chi\rangle_A$ is produced as Alice's source in mode A and hence, Bob receives a different single rail qubit upon the successful realisation of the Bell state projection. Finally, since the probabilities that the red and yellow detectors click are equal, one simply needs to perform the teleportation experiment N times in order to obtain, on average, $\frac{N}{2}$ teleported states for either orthogonal source states $|\chi\rangle_A$ in the polarisation basis priorly chosen.

5.4 Single-Photon Efficiency Estimation

The single-photon efficiency η is used to benchmark the quality of the setup's alignment. Moreover, it will be assigned to the efficiency used in the efficiency correction required when the maximum likelihood algorithm [61] is utilised for quantum state tomography based on balanced homodyne detection.

In practice, η is measured by generating a single Fock state [76] in mode B from crystal 1 and performing quantum state tomography upon it with the BHD. Indeed, when such single Fock state $|1\rangle_B$ is generated heraldically via remote state preparation from the two-mode squeezed vacuum state of crystal 1 (assuming no dark counts from the heralding SPCM and no multiphoton generation from crystal 1), the resulting state ends up being mixed as it lost its purity due to losses and noise. Using Eq. (2.84), its density matrix is thus written as

$$\hat{\rho}_{|1\rangle} = (1-\eta)\,|0\rangle\langle 0|_B + \eta\,|1\rangle\langle 1|_B\,, \tag{5.16}$$

signifying that, with probability η, a single photon $|1\rangle\langle 1|_B$ is prepared in mode B whereas, with probability $1-\eta$, it is lost and the vacuum $|0\rangle\langle 0|_B$ is obtained instead.

Based on the definition of the quadrature observable $\hat{X} = \frac{\hat{a}+\hat{a}^\dagger}{\sqrt{2}}$, one can easily calculate the variance of $\hat{X}$ in the Fock state basis $\{|n\rangle\}$ to get

$$\mathrm{Var}_{|n\rangle}(\hat{X}) = \langle n|\hat{X}^2|n\rangle = n + \frac{1}{2}\,. \tag{5.17}$$

Using Eq. (5.17), one can directly derive the variance of the quadrature observable for the mixed state in Eq. (5.16) to obtain

$$\mathrm{Var}_{\hat{\rho}_{|1\rangle}}(\hat{X}) = (1-\eta)\,\mathrm{Var}_{|0\rangle}(\hat{X}) + \eta\,\mathrm{Var}_{|1\rangle}(\hat{X}) = (1-\eta)\,\frac{1}{2} + \eta\,\frac{3}{2}\,. \tag{5.18}$$

Therefore, by acquiring quadratures X for the mixed single-photon state $\hat{\rho}_{|1\rangle}$ in

Eq. (5.16) with the BHD, it is possible to measure η by calculating the variance of the obtained signal.

This principle is illustrated in Fig. 5.4 where the variance of the quadrature operator for the single-photon state $\mathrm{Var}_{\hat{\rho}_{|1\rangle}}(\hat{X})$ is shown at the bottom. It has been obtained from 8192 quadrature time traces acquired by the BHD and read on an oscilloscope. The three graphs shown in Fig. 5.4 are plotted against i, the data sample's time index on the oscilloscope. Furthermore, the oscilloscope is set to acquire 300 data samples with a sampling rate of $2\,GS/s$ and hence a total time trace of 150 ns. Given the laser's repetition rate $R_L = 76\,\mathrm{MHz}$, this means there are 11.4 laser pulses per time trace as can be verified by looking at the bottom graph of Fig. 5.4 where 12 such pulses are present.

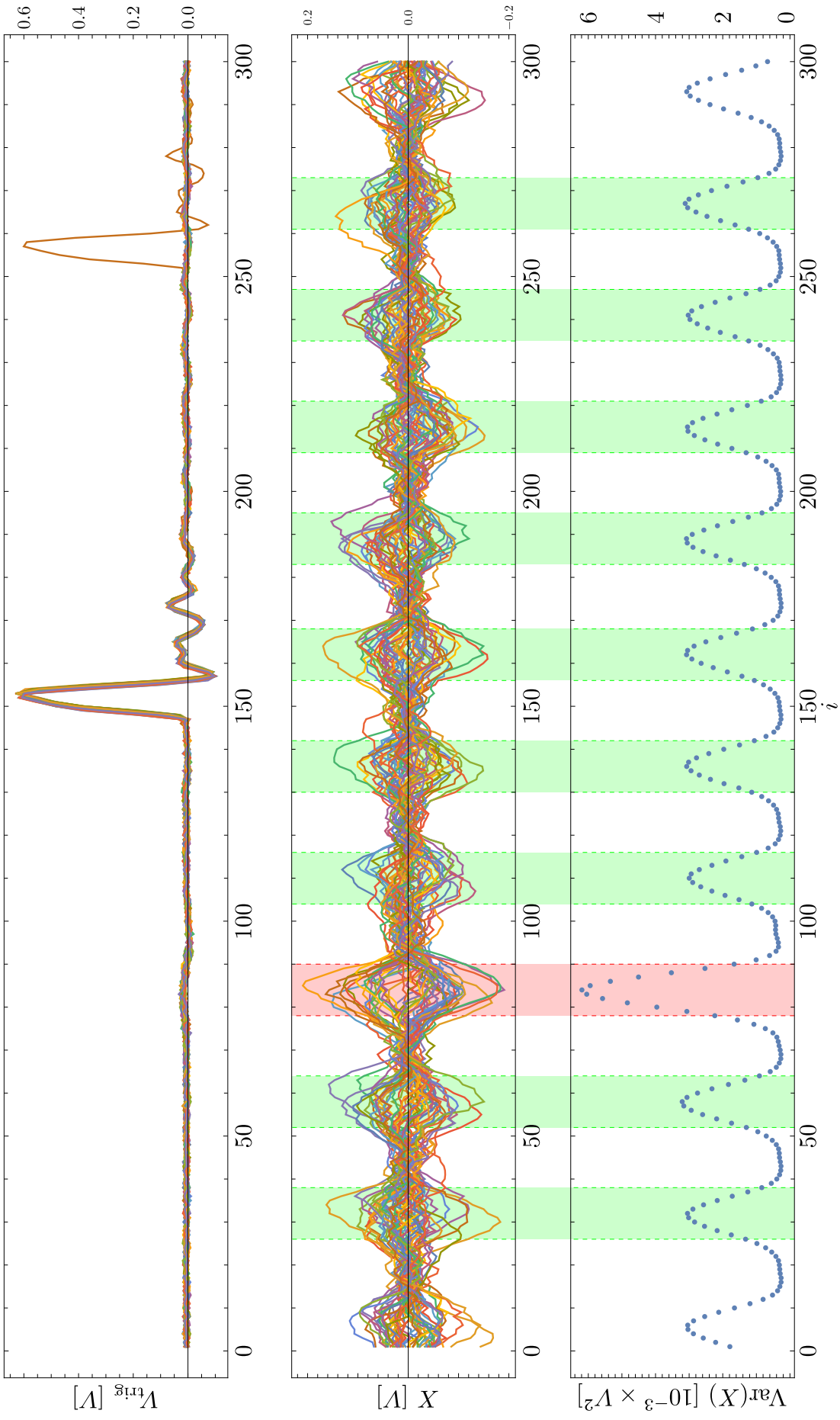


Figure 5.4: Determination of the single-photon efficiency η. On top: voltage pulses sent by the coincidence circuit and triggered by a single click from the green SPCM; middle: 50 quadrature time traces of $\hat{\rho}_{|1\rangle}$ recorded by the oscilloscope; bottom: resulting variance $\mathrm{Var}_{\hat{\rho}_{|1\rangle}}(\hat{X})$ calculated from 8192 quadrature time traces. All figures are plotted against i, the data sample's index on the oscilloscope. The green shaded regions correspond to pulses with vacuum $|0\rangle$ at the BHD, while the red shaded region indicates the presence of $\hat{\rho}_{|1\rangle}$ instead.

The top graph of Fig. 5.4 shows the voltage pulses measured on the oscilloscope and triggered by single clicks from the green SPCM. These are essentially the heralding clicks in mode C whereupon remote state preparation of the mixed single-photon state $\hat{\rho}_{|1\rangle}$ is achieved in mode B. These pulses were sent from a coincidence circuit connected to the four SPCMs. One can see on the top graph of Fig. 5.4 that the triggered pulses always reach the oscilloscope at the same time (around $i \sim 150$), apart from a spurious pulse in orange at $i \sim 255$ probably originating from a electrical back reflection in the BNC cable connecting the green SPCM to the coincidence circuit, thereby introducing a delay in the pulse's detection. When such a triggered pulse is recorded, the presence of $\hat{\rho}_{|1\rangle}$ is heralded in mode B, thus allowing its detection via balanced homodyne detection.

The middle graph of Fig. 5.4 presents 50 out of the 8192 measured quadrature time traces triggered by the coincidence circuit's pulses. Each time trace contains 300 data points which can be divided into time regions corresponding to a laser pulse having been fired. This is precisely the purpose of the shaded regions in this graph, for which the green regions correspond to pulses with no signal (hence $|0\rangle_B$) at the BHD and the red region indicates the presence of $\hat{\rho}_{|1\rangle}$ at the BHD. Note that it is possible to determine *a priori* which pulse contains $\hat{\rho}_{|1\rangle}$ since the arrival time of the triggered pulse from the coincidence circuit is finite and constant.

Finally, the bottom graph of Fig. 5.4 displays the variance of the quadrature operator for the single-photon state $\mathrm{Var}_{\hat{\rho}_{|1\rangle}}(\hat{X})$ obtained from 8192 quadrature time traces and plotted as a function of the sample time index i. As expected, there are 12 pulses and the one containing information about $\hat{\rho}_{|1\rangle}$ is shaded in red, while the other ones correspond to vacuum being present in mode B. Let b be the height of the vacuum fluctuations' variance observed for the green shaded pulses and a be the height of the pulse in the red shaded region, i.e. corresponding to $\hat{\rho}_{|1\rangle}$ present at the BHD in mode B. Given Eq. (5.18), one can calculate η from Fig. 5.4 as follows

$$\eta = \frac{\frac{a}{b} - 1}{2} \,. \tag{5.19}$$

From Fig. 5.4, we find $\eta = 47.3\%$ in this particular case. The deviation of η from unity arises from three main factors: losses, mode-matching between the signal and local oscillator at the BHD in mode B and the quantum efficiency of the homodyne detector's photodiodes at the laser's wavelength. Their estimated values are 80%, 81% and 86%, respectively. Note that when the setup is carefully aligned, typical values of the efficiency would reach $\eta \sim 62\%$. Furthermore, during the data acquisition runs — later called batches — for the teleportation experiment, the high pump power impinging onto crystal 1 systematically caused the SPDC mode's quality to degrade over time. By averaging over the duration of an acquisition batch (about an hour), we found $\eta = 50\%$ as will be mentioned and used for the final results in Chapter 6. It should be added that for the sake of clarity, we have chosen to reconstruct the results' final density matrices for the quantum teleportation and entanglement swapping experiments with both $\eta = 50\%$ and $\eta = 1$ so as to reflect the effect of efficiency correction on the resulting fidelities between the reconstructed states and their expected pure states.

5.5 Phase Reconstruction

5.5.1 Effect of the Phase on the States

To derive the effect of optical phases on the states used in the experiment, one should apply the phase shift operator $\hat{U}(\phi)$ introduced in Sec. 2.5.2 onto them.

Each SPDC crystal — i.e. crystals 1, 2 and 3 — produces a two-mode squeezed vacuum state of the form $|\psi\rangle_{\text{cr } j} = |0\rangle + \gamma_j |H\rangle |V\rangle$ up to the first order in γ_j and for $j = 1, 2, 3$. By applying the phase shift operator $\hat{U}(\phi_{\gamma_j}) = e^{-i\phi_{\gamma_j}\hat{a}^\dagger\hat{a}}$ upon the state, one obtains

$$\begin{aligned} |\psi\rangle_{\text{cr } j} &\to \hat{U}(\phi_{\gamma_j}) |\psi\rangle_{\text{cr } j} \\ &= |0\rangle + \gamma_j e^{-i\phi_{\gamma_j}} |H\rangle |V\rangle \ . \end{aligned} \tag{5.20}$$

For crystals 2 and 3, Eq. (5.20) implies that the state input to PBS1 of the Mach-Zehnder interferometer is

$$\begin{aligned} |\psi\rangle_{\text{in, cr2,3}} &= |\psi\rangle_{\text{cr2}} \otimes |\psi\rangle_{\text{cr3}} \\ &= |0\rangle\,|0\rangle + \gamma_{2,3}(|HV\rangle\,|0\rangle + e^{-i(\phi_{\gamma_3}-\phi_{\gamma_2})}\,|0\rangle\,|HV\rangle)\,, \end{aligned} \tag{5.21}$$

such that after PBS1, Alice's polarisation entangled state between modes A and D becomes the following

$$|\Psi\rangle_{AD} = |0\rangle_A\,|0\rangle_D + \gamma_{2,3}\left(|H\rangle_A\,|V\rangle_D + e^{-i\Delta\phi_{\gamma_{2,3}}}\,|V\rangle_A\,|H\rangle_D\right)\,, \tag{5.22}$$

where $\Delta\phi_{\gamma_{2,3}} \equiv \phi_{\gamma_3} - \phi_{\gamma_2}$ is the phase difference between the single photons generated by crystal 3 and crystal 2.

Regarding the resource state used for the quantum teleportation, acting the phase shift operator onto the input weak coherent states yields

$$\begin{aligned} |\alpha_V\rangle_C &\rightarrow \hat{U}(\phi_\alpha)\,|\alpha_V\rangle_C \\ &= \left|\alpha e^{-i\phi_\alpha}\right\rangle_C \\ &= |0_V\rangle_C + \alpha e^{-i\phi_\alpha}\,|1_V\rangle_C + \mathcal{O}(\alpha^2)\,, \end{aligned} \tag{5.23}$$

thus leading to the resource state

$$|\Omega\rangle_{CB} = |0\rangle_C\,|0\rangle_B + \gamma_1 e^{-i\phi_{\gamma_1}}\,|H\rangle_C\,|1\rangle_B + \alpha e^{-i\phi_\alpha}\,|V\rangle_C\,|0\rangle_B\,, \tag{5.24}$$

where ϕ_{γ_1} is the phase of the photons output by crystal 1 as per Eq. (5.20).

Using these results, it is now possible to derive the states for remote state preparation, quantum teleportation and entanglement swapping where the effect of the phase shift operator is taken into account. One finds

$$|\delta\rangle_B = b\,\alpha\,|0\rangle_B + a\,\gamma_1 e^{-i\left(\phi_{\gamma_1}-\phi_\alpha\right)}\,|1\rangle_B\,, \tag{5.25}$$

for remote state preparation,

$$|\varphi\rangle_B = \frac{1}{\sqrt{2}}\left(a\,\alpha\,|0\rangle_B + b\,\gamma_1 e^{-i\left(\phi_{\gamma_1}-\phi_\alpha-\Delta\phi_{\gamma_{2,3}}\right)}\,|1\rangle_B\right)\,, \tag{5.26}$$

for quantum teleportation and

$$|\aleph\rangle_{BD} = \frac{\gamma_{2,3}}{\sqrt{2}}\left(\alpha\,|0\rangle_B\,|V\rangle_D + \gamma_1 e^{-i\left(\phi_{\gamma_1}-\phi_\alpha-\Delta\phi_{\gamma_{2,3}}\right)}\,|1\rangle_B\,|H\rangle_D\right)\,, \tag{5.27}$$

for entanglement swapping.

5.5.2 Motivation for Phase Reconstruction

Precise determination of the teleported state's phase $\theta \equiv \phi_{\gamma_1} - \phi_\alpha - \Delta\phi_{\gamma_{2,3}}$ in Eq. (5.26) with respect to the local oscillator is essential for its reconstruction via homodyne tomography. Indeed, if one were to neglect the determination of the state's phase, fluctuations due to random turbulences in the air surrounding the optical table would yield the phase averaged state

$$\begin{aligned}
\left\langle\ |\varphi\rangle\,\langle\varphi|_B\ \right\rangle_\theta &= \frac{1}{2\pi}\int_0^{2\pi} |\varphi\rangle\,\langle\varphi|_B\ d\theta \\
&\equiv \frac{1}{2\pi}\int_0^{2\pi} \frac{1}{2}\left(|a\,\alpha|^2\,|0\rangle\,\langle 0|_B + a\,\alpha\,b^*\,\gamma_1^* e^{i\theta}\,|0\rangle\,\langle 1|_B\right. \\
&\qquad\qquad \left. + a^*\,\alpha^*\,b\,\gamma_1 e^{-i\theta}\,|1\rangle\,\langle 0|_B + |b\,\gamma_1|^2\,|1\rangle\,\langle 1|_B\right)\,d\theta \\
&= \frac{1}{2}\left(|a\,\alpha|^2\,|0\rangle\,\langle 0|_B + |b\,\gamma_1|^2\,|1\rangle\,\langle 1|_B\right)\,,
\end{aligned} \tag{5.28}$$

whose coherence is completely lost.

As such, it is imperative to lock all the state's phases with respect to the local oscillator used for quantum homodyne tomography.

5.5.3 Determination of the Teleported State's Phase

To evaluate the phase present in the teleported state $|\varphi\rangle_B$ of Eq. (5.26), note that the state $|\delta\rangle_B$ resulting from remote state preparation in Eq. (5.25) has a similar phase. Actually, conditioned on $\Delta\phi_{\gamma_{2,3}} = 0$ being satisfied at all times, $|\varphi\rangle_B$ and $|\delta\rangle_B$ exhibit exactly the same phase. This is precisely the purpose of the phase lock in the Mach-Zehnder interferometer mentioned in Sec. 5.3 and implemented using the piezoelectric mirror Pz2 and an interferometric feedback loop monitored by the photodiode PD1.

In practice, during the teleportation experiment, the angle of HWP7 in mode C is set at an angle of $\frac{\pi}{4}$ — to ensure a Bell state projection as per Sec. 5.2 — such that a single click on the green SPCM $\frac{\pi}{4}$ yields

$$\begin{aligned} |\delta\rangle_B &= \left(\frac{\langle H|_C + \langle V|_C}{\sqrt{2}}\right)|\Omega\rangle_{CB} \\ &= \frac{1}{\sqrt{2}}\left(\alpha\,|0\rangle_B + \gamma_1 e^{-i\left(\phi_{\gamma_1}-\phi_\alpha\right)}|1\rangle_B\right). \end{aligned} \tag{5.29}$$

To measure the phase of the state in Eq. (5.29) — and hence that of the teleported state in Eq. (5.26) given that the phase lock works — one continuously monitors the mean value of the quadrature observable $\hat{X}$ in Bob's channel with the help of the BHD. Indeed, a direct calculation shows that

$$\langle\hat{X}\rangle_{|\delta\rangle_B} = \frac{1}{\sqrt{2}}\,|\alpha\gamma_1|\cos\left(\phi_{\gamma_1} - \phi_\alpha\right). \tag{5.30}$$

Consequently, by fitting the mean quadrature signal with the function in Eq. (5.30), one can extract the argument of the cosine, thereby obtaining the phase of the teleported state. It has to be noted that the phase $\phi_{\gamma_1} - \phi_\alpha$ is none but the phase difference between the weak coherent state and the photon generated by crystal 1. In the lab, this phase difference is driven by the piezoelectric mirror Pz3 whose oscillating frequency is ω_p, thus giving $\phi_{\gamma_1} - \phi_\alpha = \pm\omega_p t$. As such, precise determi-

nation of Pz3's signal and its synchronisation with the measured mean quadrature expressed in Eq. (5.30) will be key. This, along with the other technical challenges arising in the state's phase reconstruction task, will be exposed in the next section.

Finally, it should also be added that since the experimental rate of remote state preparation's single clicks is five orders of magnitude higher than the successful triple coincidence clicks required for quantum teleportation, one can thus fit the phase of $|\delta\rangle_B$ in real-time. This allows for the determination of the teleported state's $|\varphi\rangle_B$ phase at any time as will be seen later.

5.6 Data Acquisition Scheme

5.6.1 Overall Goal

We finally reached the stage in which all the informations required to understand the data acquisition scheme for the quantum teleportation experiment have been formally introduced, defined and explained. Note that the data acquisition scheme for remote state preparation is relatively simple and won't be detailed since it can be easily understood from the much more complex scheme presented here.

In essence, the goal of the data acquisition scheme for the quantum teleportation experiment is rather simple: one wants to acquire a set $S = \{X_j, \theta_j\}$ of j quadratures X_j measured by the BHD and calculate their associated phases θ_j for the teleported state $|\varphi\rangle_B$ in order to faithfully reconstruct it by means of the maximum likelihood algorithm. The algorithm will statistically recreate the state present in mode B from a collection of $j = 2000$ data points.

5.6.2 Details and Time Synchronisation

A schematic detailing the data acquisition scheme for the quantum teleportation experiment can be found in Fig. 5.5.

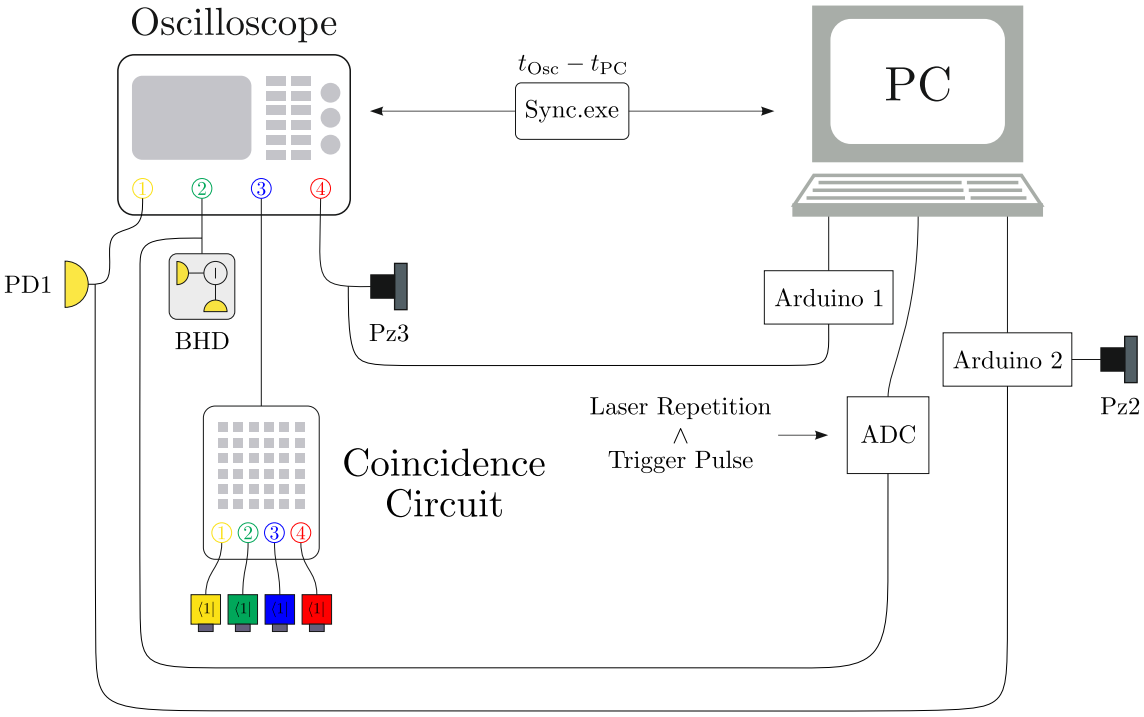


Figure 5.5: Data acquisition scheme for the quantum teleportation experiment.

From Fig. 5.5, one can discern the scheme's two key terminals: the oscilloscope and the PC. The oscilloscope is used to acquire the quadratures X_j, while the PC's goal is to determine the associated phases θ_j. Since both acquisition processes are performed over time, the internal clocks of the terminals are written as t_{Osc} and t_{PC} for the oscilloscope and the PC, respectively. The software "Sync.exe" then takes those internal clocks and calculates the difference $t_{\mathrm{Osc}} - t_{\mathrm{PC}}$ in order to match the measurements in time. However, due to network latencies in the coaxial cables' architecture linking the terminals, the "Sync.exe" software doesn't suffice and a new corresponding time variable τ has to be introduced such that the exact time difference Δt between the oscilloscope's and PC's internal clocks is given by

$$\Delta t = t_{\mathrm{Osc}} - t_{\mathrm{PC}} + \tau \,. \tag{5.31}$$

Assuming faithful measurements in time from each terminal taken independently, the exact determination of Δt is the major challenge in the experimental data acquisition and its solution will be given below. But prior to doing that, let us further examine Fig. 5.5 and understand what each terminal does.

The oscilloscope comprises 4 acquisition channels that output a voltage measurement every time a triple coincidence click — i.e. a teleportation event occurred — from the SPCMs has been registered. In particular, one has:

- Channel 1 which measures the photodiode PD1's signal used in the phase lock to set the phase $\Delta\phi_{\gamma_{2,3}} = 0$ in the polarisation entangled state $|\Psi\rangle_{AD}$ that Alice uses to generate her source $|\chi\rangle_A$ for quantum teleportation. In practice, for every quadrature data point X_j obtained, we use the measurement from channel 1 to check whether the photodiode's signal is within a pre-calibrated region corresponding to $\Delta\phi_{\gamma_{2,3}}$ being close to 0. If it isn't, we then throw away this quadrature point since we won't have a correct estimate of the associated phase as per our protocol introduced in Sec. 5.5.3.

- Channel 2 which is connected to the BHD's output and measures a voltage time trace triggered by a teleportation event. The quadrature X_j for that event j is calculated by averaging over the signal pulse corresponding to the event and details will be provided below.

- Channel 3: it is linked to the coincidence circuit's output. The coincidence circuit has four input channels — one for each SPCM (yellow, green, blue and red) — and sends a trigger pulse to the oscilloscope whenever a triple coincidence from the SPCMs has been recorded. In reality, there are two possible types of trigger pulses corresponding to a triple coincidence click from the SPCMs that indicate a quantum teleportation event: $G \wedge B \wedge Y$ and $G \wedge B \wedge R$, where G, B, Y and R correspond to a single click from the green, blue, yellow and red SPCMs, respectively. As was mentioned in Sec. 5.3.3, depending on whether the yellow or the red SPCM clicked, a different source

state $|\chi\rangle_A$ is produced and hence one of the two teleported states in the chosen single-rail basis can be obtained. To differentiate between the two types of events, the coincidence circuit outputs a *short* pulse when the event $G \wedge B \wedge Y$ is recorded and a *long* pulse for $G \wedge B \wedge R$. The *long* pulse ($\approx 10\,\text{ns}$) has a temporal width about thrice that of the *short* ($\approx 3.3\,\text{ns}$), thereby making it simple to check which event occurred — a visual example will be provided below. Lastly, it should be noted that the oscilloscope's acquisition is triggered by the very channel 3 since it is the one responsible for signal events triggering.

- Channel 4: it measures the voltage signal of the piezoelectric mirror Pz3 at the time of a signal event. Since Pz3 drives the phase difference between photons from the weak coherent state and crystal 1, we use channel 4's measurement in conjunction with the real-time fitted phase $\phi_{\gamma_1} - \phi_\alpha$ from remote state preparation to determine the phase θ_j of the teleported state $|\varphi\rangle_B$ associated with the quadrature X_j measured in channel 2. The remote state preparation's phase will be obtained using the PC for which explanations are given below.

Overall, depending on the rate of triple coincidence clicks, we acquired batches of $200 - 400$ signal points on the oscilloscope for each basis state of the teleportation experiment. Each data batch usually lasted $20 - 60$ minutes, after which the setup was locally realigned to re-optimise the quantum efficiency η affected by the large pump impinging onto crystal 1 as mentioned in Sec. 5.4. A typical example of the data acquired by the oscilloscope is found in Fig. 5.6.

The measurements from the oscilloscope's four channels are shown in Fig. 5.6 where channels 1-4 are displayed from top to bottom. Moreover, Fig. 5.6 contains the measurements for two signal events of the quantum teleportation experiment. Indeed, one can find in channel 3 a purple signal event corresponding to a *short* triggered triple coincidence pulse, while orange indicates that of a *long* pulse. As can be seen, both pulses are centered around the same index i of the oscilloscope and the *long* pulse has a width three times larger than the *short* pulse, as expected.

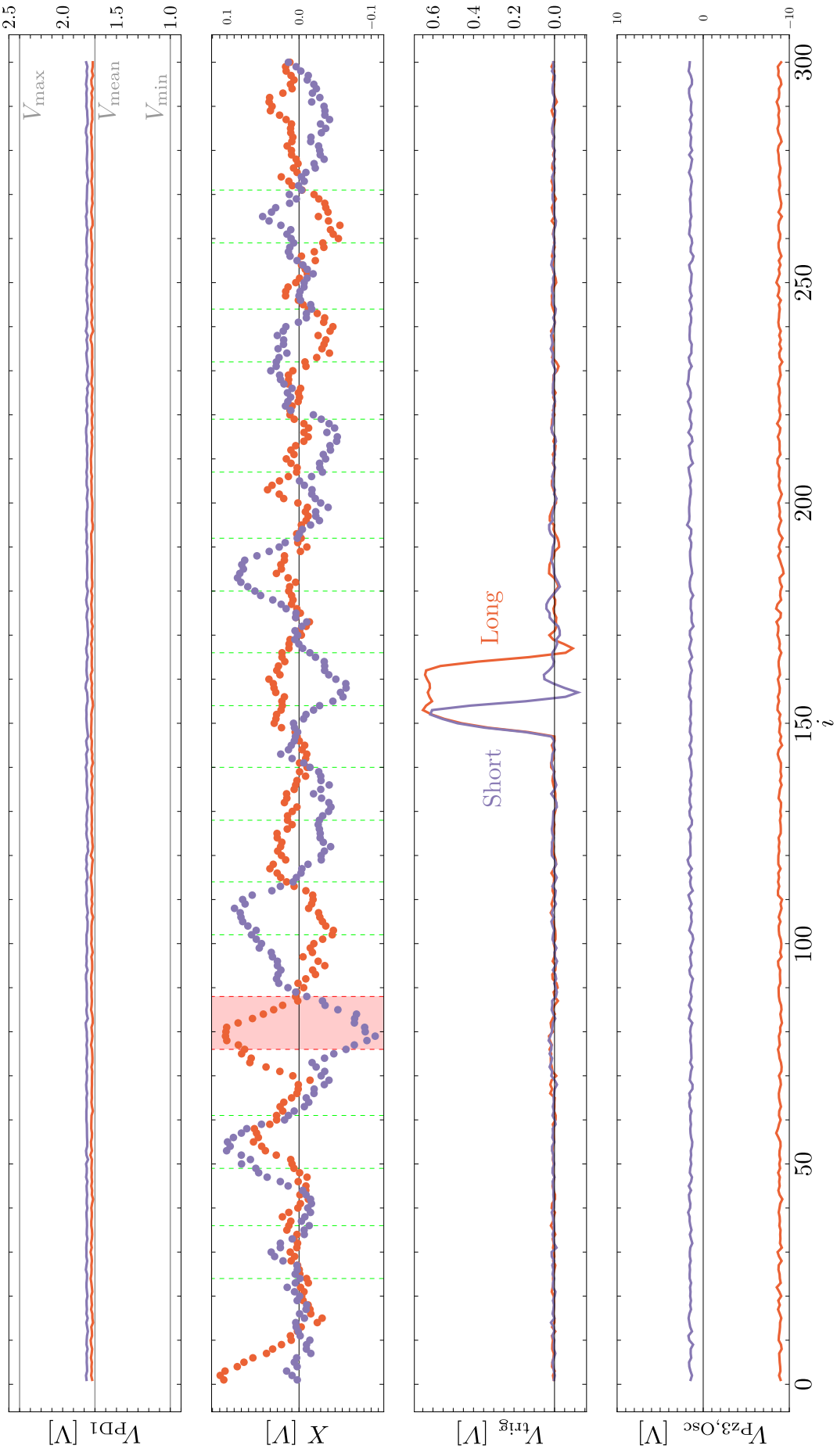


Figure 5.6: Data acquisition with the resulting measurements for the four channels of the oscilloscope for the quantum teleportation experiment. Channels 1-4 are depicted from top to bottom and each graph is plotted against i, the data sample's index on the oscilloscope.

In channel 1, the signal V_{PD1} of photodiode PD1 is constant for both events and lies near the mark $V_{\mathrm{mean}} = \frac{V_{\mathrm{min}}+V_{\mathrm{max}}}{2}$ which is the measured average voltage value where the signal should sit if one wants to grant $\Delta\phi_{\gamma_{2,3}} = 0$ and for which V_{min} and V_{max} are the corresponding voltage extrema of the interference observed when the phase lock is not switched on. Any acquired event for which V_{PD1} deviated from V_{mean} by $\sim 15\%$ has been disregarded. Channel 4 plots the voltage $V_{\mathrm{Pz3,Osc}}$ of the piezoelectric mirror Pz3 and one can see that it takes here two different average values for the events associated with the *short* and *long* pulses. This simply signifies that both data points will exhibit different phases θ_j when one will determine them with the PC. Finally, channel 2 plots the voltage measured from the BHD which is used to calculate the quadrature X_j for this quantum teleportation event. Note that, akin to Fig. 5.4, the horizontal axis is segmented by the green time delimitations of each laser pulse. In this graph, the 300 points contained in the time trace are explicitly shown such that one can visualise the 13 points present in the red shaded area that corresponds to the temporal presence of the signal pulse from the laser. From these 13 samples, we calculate the quadrature X_j by taking the average and normalising it by a pre-calibrated measurement of the vacuum noise fluctuations.

Now that the oscilloscope and its outputs have been explained, let us draw our attention to the PC in Fig. 5.5. It contains three main elements:

- Arduino 1 which is an Arduino — i.e. an analogue-to-digital converter (ADC) with a control board — that's labelled 1 and whose function is to sample in real-time the piezoeletric mirror Pz3's voltage signal. This sampled signal will then be used to reconstruct a smoothed fit $V^{\mathrm{fit}}_{\mathrm{Pz3,PC}}$ of the signal in order to determine τ and match in time the oscilloscope's and the PC's internal clocks as per Eq. (5.31) and with the help of the "Sync.exe" software.

- An ADC that records the signal from the BHD and hence calculates the mean quadrature $\langle \hat{X} \rangle_{|\delta\rangle_B}$ when a single click from the green SPCM heralding the remote state preparation of $|\delta\rangle_B$ in mode B is sent from the coincidence circuit.

In reality, the triggering mechanism of this ADC is more elaborated. Indeed, the ADC samples the BHD's voltage at a sampling rate equal to the laser's repetition rate $R_L = 76\,\text{MHz}$ and for every triggered pulse obtained from the green SPCM, it acquires an additional 4999 pulses. Note that this is what is meant by the indication "Laser Repetition $\wedge$ Trigger Pulse" drawn as an input to the ADC in Fig. 5.5. Furthermore, these 4999 pulses recorded at the laser's repetition rate correspond to vacuum being present in mode B and are therefore used for the vacuum normalisation of the signal's quadrature obtained for remote state characterisation heralded by the green SPCM. Once those 5000 pulses are recorded, the PC calculates one value of the quadrature $X_{|\delta\rangle_B}$ for $|\delta\rangle_B$ — the state obtained from remote state preparation. Then, by measuring 200 of these single quadratures $X_{|\delta\rangle_B}$, each obtained from 5000 pulses at the ADC, the computer calculates one value of the mean quadrature $\langle\hat{X}\rangle_{|\delta\rangle_B}$. By repeating this process in time, it is possible to plot the mean quadrature $\langle\hat{X}\rangle_{|\delta\rangle_B}$ obtained from remote state preparation as a function of t_{PC}, the internal clock of the PC . Finally, the phase θ_j of the teleported state is determined by fitting $\langle\hat{X}\rangle_{|\delta\rangle_B}$ with Eq. (5.30) and retrieving the argument of the cosine. Note that for this procedure to work, one requires to precisely match the oscilloscope's and PC's internal clocks as will be detailed below.

- A second Arduino — Arduino 2 — which is connected to the photodiode PD1 and controls in real-time the voltage sent onto the piezoelectric mirror Pz2 in order to lock the phase in the Mach-Zehnder interferometer. A program is written to implement a feedback loop based on the photodiode's voltage and hence ensure $\Delta\phi_{\gamma_{2,3}} = 0$ by constantly adjusting the position of the piezoelectric mirror Pz2.

Now that the PC's function has been explained, let us show how the key task of synchronising the oscilloscope and the PC is implemented. It consists of two parts. Consider the first part detailed in the graphs displayed in Fig. 5.7.

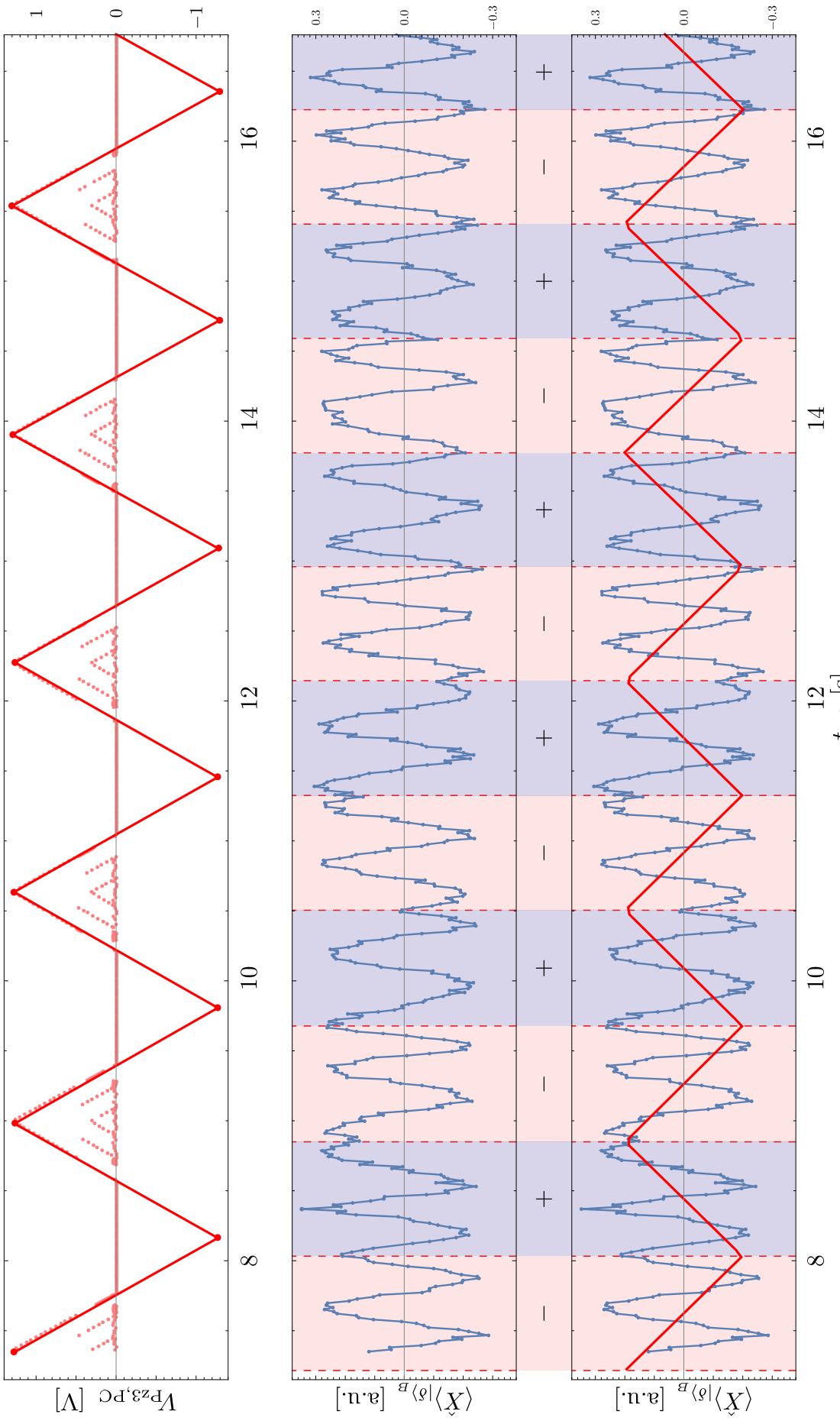


Figure 5.7: Part 1 of the scheme for the time synchronisation between the oscilloscope and the PC. On top: voltage data samples $V_{\mathrm{Pz3,PC}}$ of the piezoelectric mirror Pz3 acquired by Arduino 1 and its corresponding smoothed fit $V^{\mathrm{fit}}_{\mathrm{Pz3,PC}}$ in solid red; middle: mean quadrature $\langle \hat{X} \rangle_{|\delta\rangle_B}$ for remote state preparation; bottom: synchronisation of top and middle graph. All graphs are plotted against t_{PC}, the PC's internal clock. The alternating shaded regions in red and purple indicate the piezoelectric mirror Pz3's direction of oscillation (+ or −).

The first step is shown in the top graph of Fig. 5.7. The voltage data samples $V_{\text{Pz3,PC}}$ of the piezoelectric mirror Pz3 acquired by Arduino 1 are plotted against the PC's internal clock t_{PC}. The goal here is to find a smooth fit $V^{\text{fit}}_{\text{Pz3,PC}}$ for these data samples over the entire duration of the corresponding data acquisition batch, and then repeat this for every quantum teleportation data acquisition batch. As each batch lasted $20-60$ minutes and given the apparent high sampling rate of Arduino 1, it simply isn't feasible for one to manually construct the fit and check that it matches the data over the whole acquisition time — as well as repeat this particular process for the plethora of quantum teleportation data acquisition batches recorded. Moreover, since Arduino 1 cannot detect negative voltages, one can see that the data samples stop at a zero voltage instead of decreasing towards negative values as the voltage signal of Pz3 would normally do, thereby making the fitting of the signal with an appropriate triangular function more complicated. To solve this task, an algorithm based on background signal estimation from noisy data was conceived in order to faithfully filter and select the peaks of $V_{\text{Pz3,PC}}$, the voltage data samples measured by Arduino 1. Furthermore, given each positive data peak, the successive negative peak was reconstructed geometrically such that the resulting smooth curve $V^{\text{fit}}_{\text{Pz3,PC}}$ in red at the top of Fig. 5.7 is a perfect fit of the entire piezoelectric mirror Pz3's voltage signal over time.

The second step is illustrated in the middle graph of Fig. 5.7 where the mean quadrature $\langle \hat{X} \rangle_{|\delta\rangle_B}$ for remote state preparation is measured by the ADC — given the mechanism involving the 5000 pulses described above — and plotted against t_{PC}. As expected from Eq. (5.30), the resulting signal resembles that of a cosine. Additionally, one can notice that every ~ 2 periods of oscillation of $\langle \hat{X} \rangle_{|\delta\rangle_B}$, the signal undergoes a discontinuity. This originates from the piezoelectric mirror Pz3 changing its direction of oscillation. During this step of the process, one wants to precisely determine the time positions at which these breaks occur and the result is shown by the dashed red delimitations. Consequently, alternating shaded regions in red and purple are drawn to indicate the direction of oscillation of Pz3, whereby the

red (purple) colour designates a decreasing (increasing) piezoelectric voltage — and thus position — and hence is represented by a negative − (positive +) sign below.

Once the fitted curve $V^{\text{fit}}_{\text{Pz3,PC}}$ for $V_{\text{Pz3,PC}}$ and the various oscillation regions of $\langle \hat{X} \rangle_{|\delta\rangle_B}$ have been found, one superimposes them on the bottom graph of Fig. 5.7. Consequently, one gets the mean quadrature $\langle \hat{X} \rangle_{|\delta\rangle_B}$ for remote state preparation on top of the fitted signal $V^{\text{fit}}_{\text{Pz3,PC}}$ for the piezoelectric voltage signal of Pz3 along with its corresponding signs.

The second part of the synchronisation process is exhibited in Fig. 5.8.

In the top graph of Fig. 5.8, the voltage signal $V_{\text{Pz3,Osc}}$ of the piezoelectric mirror Pz3 as measured by the oscilloscope is plotted against the oscilloscope's internal clock t_{Osc}. Note that each orange data point corresponds to a triple coincidence click sent from the coincidence circuit, therefore heralding a quantum teleportation event. In essence, this graph simply displays the average voltage output by channel 4 of the oscilloscope — as depicted at the bottom of Fig. 5.6 — as a function of the event's time of occurrence and over the entire quantum teleportation data acquisition batch under consideration. Given all these orange data points forming a full acquisition batch, one then uses a scaled version of the fit $V^{\text{fit}}_{\text{Pz3,PC}}$ obtained in Fig. 5.7 to obtain the best fit of $V_{\text{Pz3,Osc}}$, resulting in the solid orange line — call it $V^{\text{fit}}_{\text{Pz3,Osc}}$. Note that while $V^{\text{fit}}_{\text{Pz3,Osc}}$ is a scaled version of $V^{\text{fit}}_{\text{Pz3,PC}}$, it has strictly the same period as $V^{\text{fit}}_{\text{Pz3,PC}}$ and can thus be seen as a "shifted" version of it in time.

The final step of the synchronisation process is illustrated in the middle graph of Fig. 5.8 where one superimposes the two previously determined fits $V^{\text{fit}}_{\text{Pz3,PC}}$ and $V^{\text{fit}}_{\text{Pz3,Osc}}$ on top of the mean quadrature $\langle \hat{X} \rangle_{|\delta\rangle_B}$ for remote state preparation plotted now against the oscilloscope's internal clock t_{Osc}. By definition, $V^{\text{fit}}_{\text{Pz3,PC}}$ (in red) matches perfectly with $\langle \hat{X} \rangle_{|\delta\rangle_B}$. However, now that both $V^{\text{fit}}_{\text{Pz3,PC}}$ (in red) and $V^{\text{fit}}_{\text{Pz3,Osc}}$ (in orange) are plotted against t_{Osc}, one can clearly see that they are relatively shifted in time. This is the essence of the newly introduced time variable τ in Eq. (5.31) that accounts for the latency in the coaxial cable architecture.

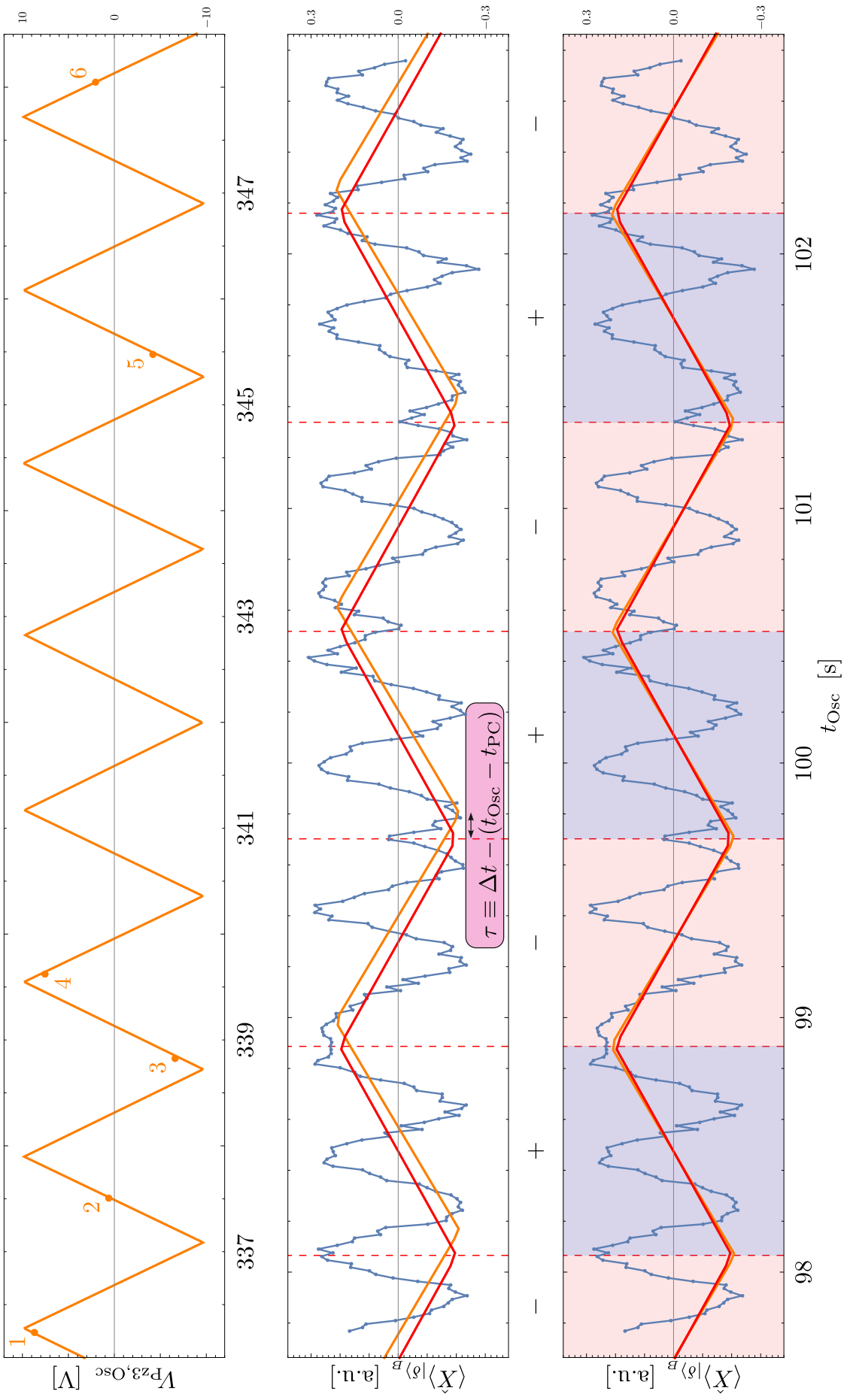


Figure 5.8: Part 2 of the scheme for the time synchronisation between the oscilloscope and the PC. On top: numbered $(1-6)$ data points for the voltage signal $V_{\mathrm{Pz3,Osc}}$ of the piezoelectric mirror Pz3 measured by the oscilloscope for each triple coincidence triggered signal event along with a corresponding fit in solid orange; middle: same orange fit as well as mean quadrature $\langle \hat{X} \rangle_{|\delta\rangle_B}$ for remote state preparation acquired by the ADC and fit of $V_{\mathrm{Pz3,PC}}$; bottom: same graph as middle but with the orange and red fit now synchronised. All graphs are plotted against the internal clock t_{Osc} of the oscilloscope. The shaded regions with corresponding signs (+ or −) are similar to Fig. 5.7.

Indeed, in Fig. 5.8, data from both the oscilloscope and the PC have already been subject to the removal of the time difference $t_{\text{Osc}} - t_{\text{PC}}$ between their inherent internal clocks by means of the "Sync.exe" software. Yet, as one can clearly notice in the middle graph of Fig. 5.8, $V^{\text{fit}}_{\text{Pz3,PC}}$ (in red) and $V^{\text{fit}}_{\text{Pz3,Osc}}$ (in orange) exhibit an additional time difference τ which has been highlighted in a pink box. Note that, empirically, τ is different for each quantum teleportation data acquisition batch such that one must reproduce this procedure for all batches. Therefore, by measuring τ, one can displace $V^{\text{fit}}_{\text{Pz3,Osc}}$ with respect to $V^{\text{fit}}_{\text{Pz3,PC}}$ and thus achieve full time synchronisation of the data measured by the oscilloscope and the PC — for each quantum teleportation data acquisition batch.

The bottom graph of Fig. 5.8 simply shows the mean quadrature $\langle \hat{X} \rangle_{|\delta\rangle_B}$ for remote state preparation along with the now time-matched fits $V^{\text{fit}}_{\text{Pz3,PC}}$ (in red) and $V^{\text{fit}}_{\text{Pz3,Osc}}$ (in orange). The shaded regions correspond to the piezoelectric mirror Pz3's direction of oscillation, which can either be positive (+) or negative (−).

5.6.3 Determination of the Phase θ_j

Now that most of the data acquisition scheme is explained and the key task of time synchronisation duly covered, one can finally obtain the phase θ_j for each quantum teleportation event within one single batch of data acquisition. The principle is shown in Fig. 5.9.

As can be seen, Fig. 5.9 is made of two similar graphs: one labelled *good* and one *bad*. As will be explained below, they correspond to the situations in which the phase θ_j is either faithfully reconstructed or not, respectively. Focusing on one of the two situations, say the top one with the *good* label, one can note that the top graph corresponds to the mean quadrature $\langle \hat{X} \rangle_{|\delta\rangle_B}$ for remote state preparation plotted as data points against the oscilloscope's internal clock t_{Osc}. Moreover, a fit of $\langle \hat{X} \rangle_{|\delta\rangle_B}$ as per Eq. (5.30) is drawn in a solid blue line.

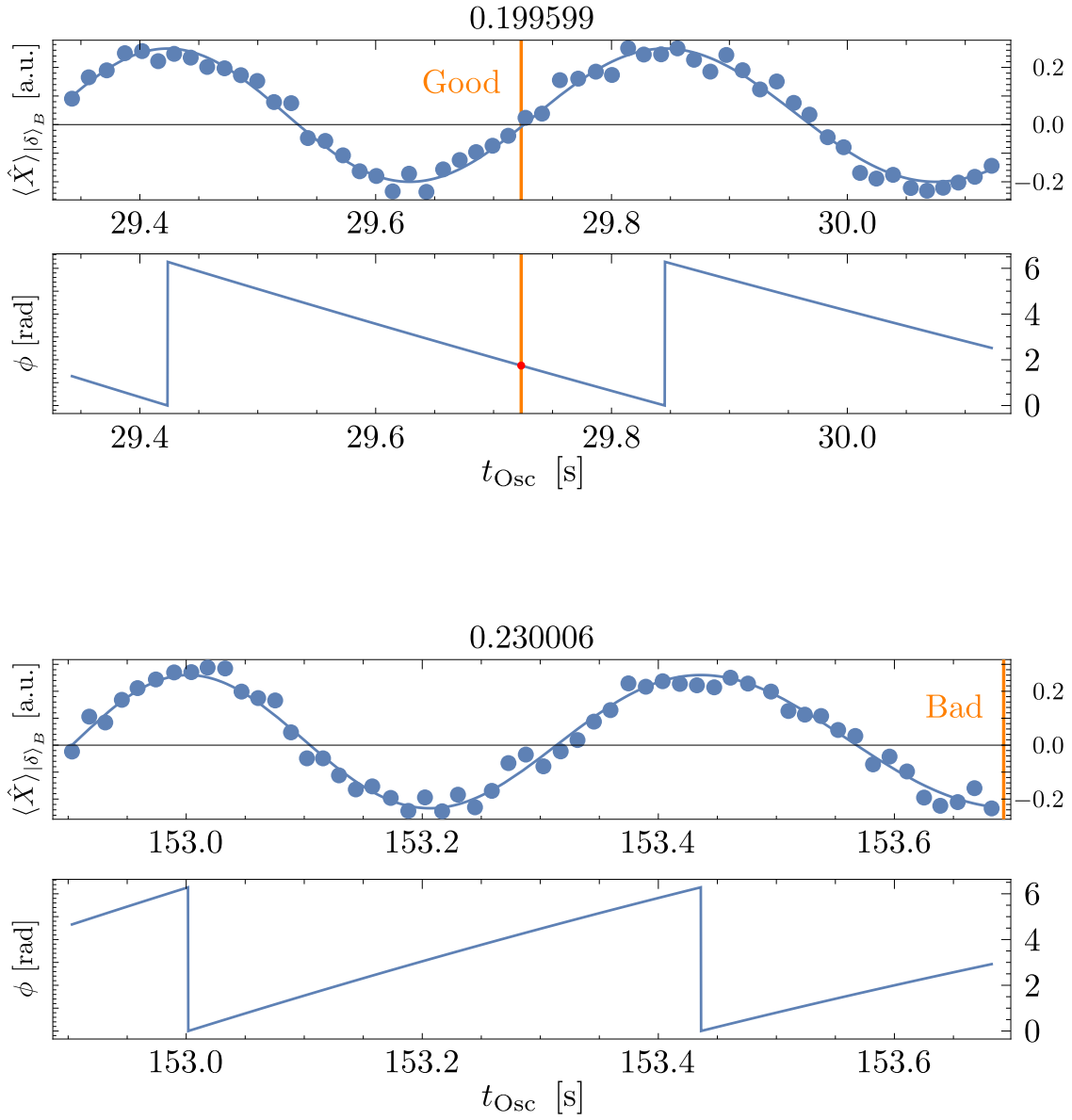


Figure 5.9: Determination of the phase θ_j of a quantum teleportation event and later used for the maximum likelihood algorithm. The figure features two graphs wherein a *good* and *bad* situation for the reconstruction of θ_j is shown. For each graph — on top: mean quadrature $\langle \hat{X} \rangle_{|\delta\rangle_B}$ for remote state preparation drawn as blue data points and associated fit as per Eq. (5.30) in the solid blue curve and whose quality is quantified by the mean squared error expressed above; bottom: corresponding phase ϕ (mod 2π) in solid blue obtained from the above-mentioned fit. The vertical orange line indicates the occurrence time of the triple coincidence signal event. All the graphs are plotted against the oscilloscope's internal clock t_{Osc} and over a sole time period of oscillation from Pz3.

The quality of the fit is expressed by calculating the mean squared error with respect to the data points and displaying it on top of the graph. Moreover, the vertical orange line corresponds to the time at which the triple coincidence click

heralding the quantum teleportation event occurred. Note that both $\langle \hat{X} \rangle_{|\delta\rangle_B}$ and the corresponding fit are plotted within a time region associated with a sole oscillation of the piezoelectric mirror Pz3. Indeed, this is a crucial constraint as we already observed that $\langle \hat{X} \rangle_{|\delta\rangle_B}$ undergoes a discontinuity whenever the oscillation direction of Pz3 flips sign, thereby rendering the fitting with Eq. (5.30) impossible and inconsistent. The bottom graph displays the phase $\phi \equiv \phi_{\gamma_1} - \phi_\alpha \pmod{2\pi}$ of the remote state preparation retrieved by taking the argument of the cosine in the above-mentioned fit. As expected, within the single oscillation period of Pz3, the phase ϕ monotonically decreases from $2\pi - 0$, thus corresponding to an oscillating period of Pz3 where the direction of oscillation is negative (-). Note that, as explained earlier, ϕ is equal to the phase θ_j of the teleported state $|\varphi\rangle_B$ present in mode B conditioned on $\Delta\phi_{\gamma_{2,3}} = 0$. To retrieve θ_j, one simply reads the value of ϕ at the time of occurrence of the teleportation event, indicated by the orange vertical line. This results in the red dot which will be used as the value for the phase θ_j along with the corresponding quadrature X_j obtained from the oscilloscope to perform quantum state tomography via the maximum likelihood algorithm.

In the case of the *bad* situation at the bottom of Fig. 5.9, one can observe from the orange vertical line that the triple coincidence click was obtained at the edge of the time window which now corresponds to a single positive (+) oscillation of the piezoelectric mirror Pz3. To be conservative, we assumed here that the phase wouldn't be precise since the mean quadrature $\langle \hat{X} \rangle_{|\delta\rangle_B}$ for remote state preparation would be too close to its discontinuity. As such, this event is labelled *bad* and the corresponding quadrature X_j is thrown away. Visually, an example of such a *bad* event would be the orange data point 1 in the top graph of Fig. 5.8 as it sits close to a sign flip of the piezoelectric mirror Pz3. On the other hand, the data point 2 in the top graph of Fig. 5.8 is a perfect candidate for a *good* event.

This now completes the data acquisition scheme's examination, after which we shall discuss the photon count rates observed in the experiment and further conclude this experimental chapter.

5.7 Photon Count Rates

Photons are measured by SPCMs from Excelitas. The typical count rates measured in both arms of the Bell state projector were $R_\alpha = R_{\gamma_1} = 22\,\text{kHz}$ for $|\alpha\rangle$ and crystal 1. For crystals 2 and 3, these rates were $R_{\gamma_{2,3}} = 1.7\,\text{kHz}$. These numbers reflect the loss factor of 4 introduced by the pairs of HWPs and polarisers in the Bell state projector. The average coincidence rate of the photons originating from crystals 2 and 3, measured between the yellow SPCM in mode D and the green SPCM of the Bell state projector, was $R^{\text{c.c}}_{\gamma_{2,3}} = 51\,\text{Hz}$. From these rates, we estimated a total photon detection efficiency[3] of $\eta_d = \frac{R^{\text{c.c}}_{\gamma_{2,3}}}{R_{\gamma_{2,3}}} \approx 3.0\%$. This value is rather small due to the presence of 0.2 nm narrowband filters in front of each SPCM, as well as the unavoidable optical losses present in the experiment. From here, we estimate $\gamma_1 = \left(\frac{R_{\gamma_1}}{R_L}\frac{1}{\eta_d}\right)^{1/2} \approx 0.20$ and $\gamma_{2,3} = \left(\frac{R_{\gamma_{2,3}}}{R_L}\frac{1}{\eta_d}\right)^{1/2} \approx 0.054$. Finally, we find for the "good" triple coincidence rate $R_{T,\text{good}} \approx \frac{1}{2}\eta_d^3 |\gamma_1|^2 |\gamma_{2,3}|^2 \approx 0.12\text{Hz}$. The corresponding experimentally observed rate was $R_T = (0.16 \pm 0.03)\,\text{Hz}$ as will be seen in the next chapter where the results are presented.

[3]Note that this efficiency takes into account the quantum efficiency of the detector as well as the losses incurred by the narrowband spectral filters in front of it, hence the small estimated value.

Chapter 6

Results

'This above all: to thine own self be true,

And it must follow, as the night the day,

Thou canst not then be false to any man.'

Polonius in Shakespeare's "Hamlet"

This chapter contains the results obtained for the various experiments described in Chapter 4; namely remote state preparation, quantum teleportation and entanglement swapping. Additionally, sources of errors are discussed.

6.1 Remote State Preparation Results

For remote state preparation, the resource state $|\Omega\rangle_{CB}$ in Eq. (4.1) was generated between modes C and B. Moreover, the polarisation projection was performed in mode C using the green SPCM and a total of 8192 quadratures associated with the resulting state $|\delta\rangle_B$ of Eq. (4.2) were collected on the oscilloscope. Since the single click's count rate was quite large — 22 kHz as expressed in Sec. 5.7 — the phase associated with the state was directly retrieved from the quadratures measured on the oscilloscope. Indeed, by plotting the mean quadrature over time, one can simply fit it with a cosine, akin to Eq. (5.30), and get the phase from its argument. The

states were reconstructed using the maximum likelihood algorithm with an efficiency correction of $\eta = 50\%$ and are shown in Fig. 6.1.

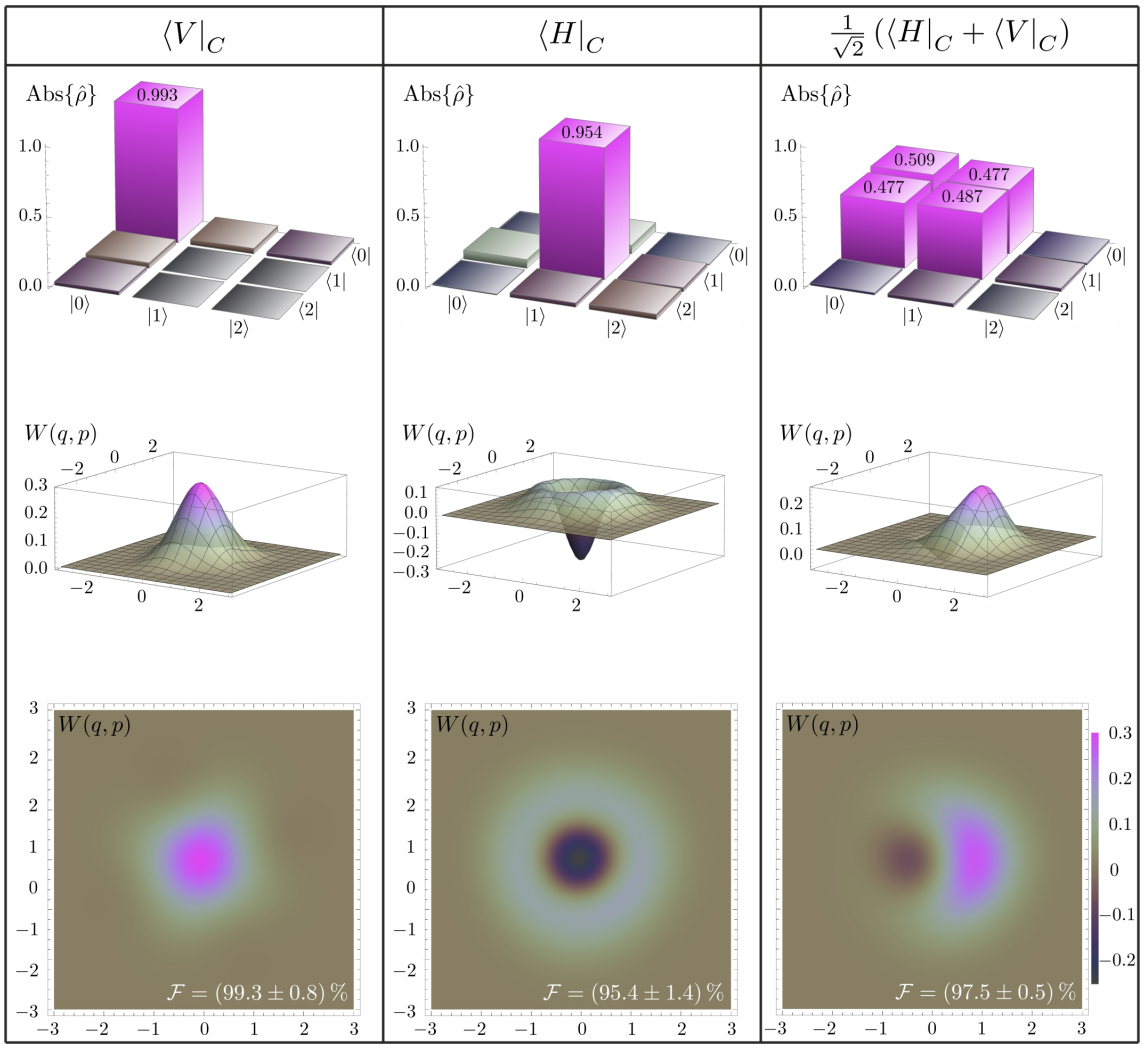


Figure 6.1: Remote state preparation results. The top line shows the polarisation projection $\langle \pi|_C$ performed in mode C using the green SPCM in the Bell state projector's arm. The resulting single-rail states are shown below. From top to bottom, we display the absolute value of the reconstructed density matrices Abs{$\hat{\rho}$} in the Fock basis, the Wigner functions $W(q,p)$ in phase space and their surface plots. Fidelities $\mathcal{F}$ calculated with respect to the expected pure states are given withal.

In Fig. 6.1, one can observe that three polarisation projections have been performed in mode C: $\langle V|_C$, $\langle H|_C$ and $\frac{1}{\sqrt{2}}(\langle H|_C + \langle V|_C)$. The expected single-rail qubits are successfully measured in mode B since large fidelities of $\mathcal{F} = (99.3 \pm 0.8)\%$, $\mathcal{F} = (95.4 \pm 1.4)\%$ and $\mathcal{F} = (97.5 \pm 0.5)\%$ with respect to the pure states in Eq. (4.2) are obtained. These results confirm the success of the remote state preparation experiment, thereby validating the usage of $|\Omega\rangle_{CB}$ for quantum teleportation. Lastly,

losses in the fidelities are attributed to an imperfect preparation of $|\Omega\rangle_{CB}$.

6.2 Quantum Teleportation Results

In this experiment, the down-conversion amplitudes were set, for the reason explained below, to unequal values of $\gamma_1 \approx 0.20$ and $\gamma_{2,3} \approx 0.054$. A *good* triple coincidence event arises when one photon is present in modes A and C — leading to a click of the Bell state projector — as well as one photon in mode D for the polarisation projetion. The probability of such a *good* triple coincidence event scales as $p_{\text{good}} \sim \eta_d^3 |\gamma_1|^2 |\gamma_{2,3}|^2$, where $\eta_d \approx 3\%$ is the total quantum efficiency associated with single-photon detection expressed in Sec. 5.7. The measured rate of the total triple coincidence events was $R_T \sim 0.16\,\text{Hz}$, in accordance with Sec. 5.7.

To reconstruct each teleported state in mode B, we acquired a total of 2000 quadratures and calculated their associated phases with the method described above. Quantum state tomography was then performed using the maximum likelihood algorithm with an efficiency correction of $\eta = 50\%$. The results are shown in Fig. 6.2.

As can be seen in Fig. 6.2, the teleportation has been implemented for the six primary basis states of a dual-rail discrete variable qubit: $|V\rangle$, $|H\rangle$, $\frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$ and $\frac{1}{\sqrt{2}}(|H\rangle \pm i\,|V\rangle)$. The corresponding output single-rail qubits show an average fidelity of $\mathcal{F} = (92.8 \pm 2.2)\%$ with respect to the expected pure states in Eq. (4.3). For clarity, we only show the density matrices up to 2 photons in Fig. 6.2, while the states used to compute the fidelity have been in fact reconstructed up to 4 photons. For the diagonal and circular inputs, the orthogonality between the resulting qubits, $|\pm\rangle_B = \frac{1}{\sqrt{2}}(|0\rangle_B \pm |1\rangle_B)$ and $|\pm i\rangle_B = \frac{1}{\sqrt{2}}(|0\rangle_B \pm i\,|1\rangle_B)$ clearly manifests itself since the Wigner functions are oriented in opposite directions, as expected from Fig. 2.1.

If the efficiency correction in the maximum likelihood algorithm is removed, the reconstructed states still yield an average fidelity of $\mathcal{F} = (77.7 \pm 1.5)\%$ with respect to the expected pure states in Eq. (4.3). Overall, these fidelities are state-of-the-art

compared to those achieved for traditional quantum teleportation experiments [102], despite a comparatively much higher complexity of our experiment.

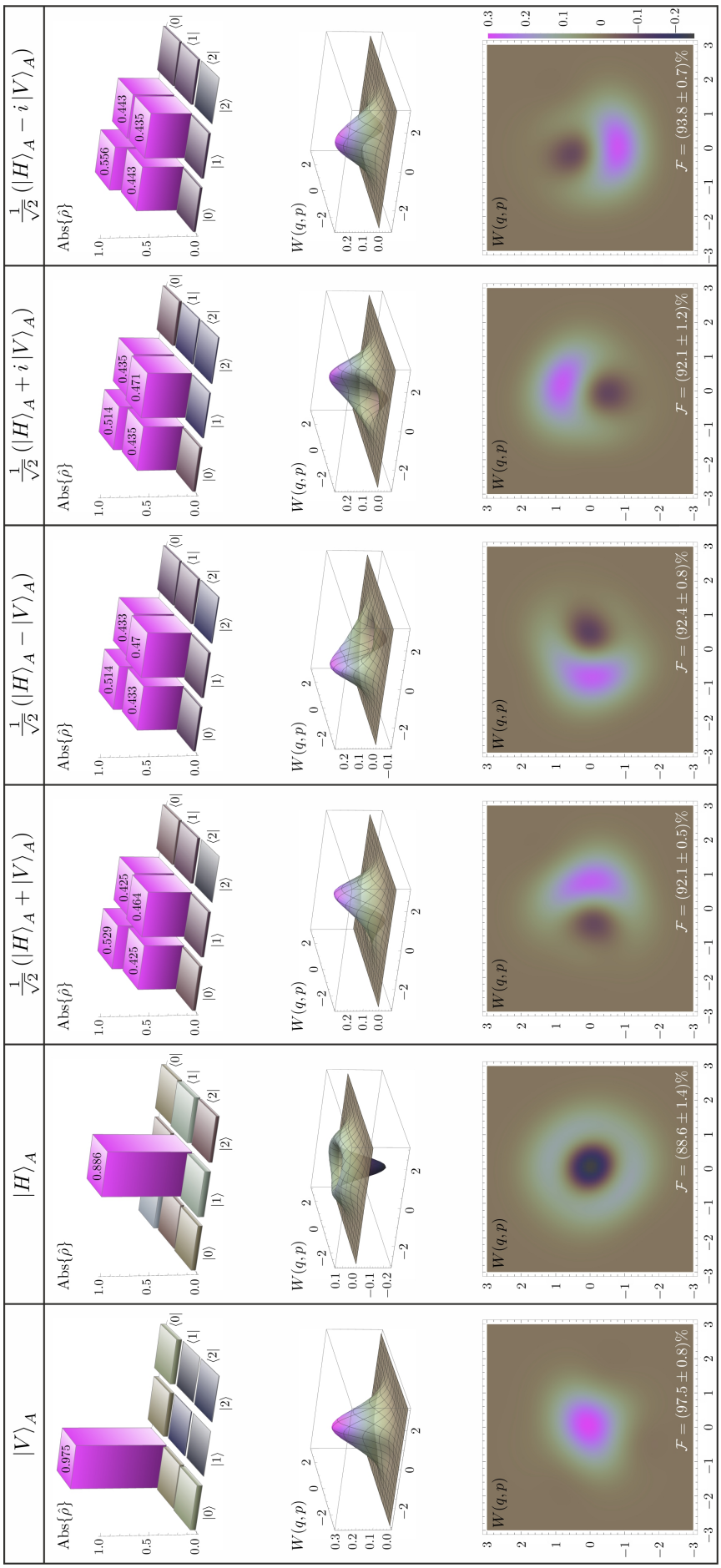


Figure 6.2: Teleportation experiment results. The top line shows the dual-rail source states $|\chi\rangle_A$ prepared by Alice. The resulting teleported single-rail qubits are shown below. From top to bottom, we display the absolute value of the reconstructed density matrices Abs{$\hat{\rho}$} in the Fock basis, the Wigner functions $W(q,p)$ in phase space and their surface plots. Fidelities $\mathcal{F}$ calculated with respect to the expected pure states are given withal.

The main source of error explaining the deviation of the experimentally observed teleported states from those predicted by Eq. (4.3) comes from the false positive Bell state projections [103, 104]: a coincidence click can be caused by both photons arriving from the same input mode, A or C, rather than one from each mode. We shall refer to these spurious events as those that are *bad*, in contrast with the *good* ones described above.

The probability of such events for the two photons coming from mode A and none being present in mode C scales as $p_{\text{bad,A}} \sim 2\eta_d^3 \left|\gamma_{2,3}\right|^4$. On the other hand, the probability for the two photons originating from mode C while one photon is present in mode A scales as $p_{\text{bad,C}} \sim 2\eta_d^3 \left|\gamma_1\right|^4 \left|\gamma_{2,3}\right|^2$. These values are different because one of the photons arriving from mode A is always heralded by a click in mode D in order to get a triple coincidence click. To minimise the ratio of these *bad* events with respect to the *good* ones while keeping the latter at a reasonable rate, we set $|\gamma_{2,3}| \sim |\gamma_1|^2$. This results in the false positives contributing $\sim 16\%$ to all triple coincidences. Since most of these noisy events lead to the admixture of the vacuum state to Bob's channel in mode B and because the theoretically expected output state — given the six input states in Fig. 6.2 — should contain, on average, one-half of the vacuum state, the effect of this admixture on the fidelity is $\sim 8\%$. This is consistent with our observations and the obtained average fidelity of $\mathcal{F} = (92.8 \pm 2.2)\%$ for the quantum teleportation experiment, thereby confirming the results' validity.

6.3 Entanglement Swapping Results

The teleportation outputs for the six inputs allow us to post-selectively reconstruct the bipartite state $\hat{\rho}_{BD}$ that is produced in modes B and D due to entanglement swapping after the Bell state measurement in modes A and C. To achieve this, we use technique detailed in [70] for which one can retrieve $\hat{\rho}_{BD}$ from its various projections. The result of the entanglement swapping is displayed in Fig. 6.3.

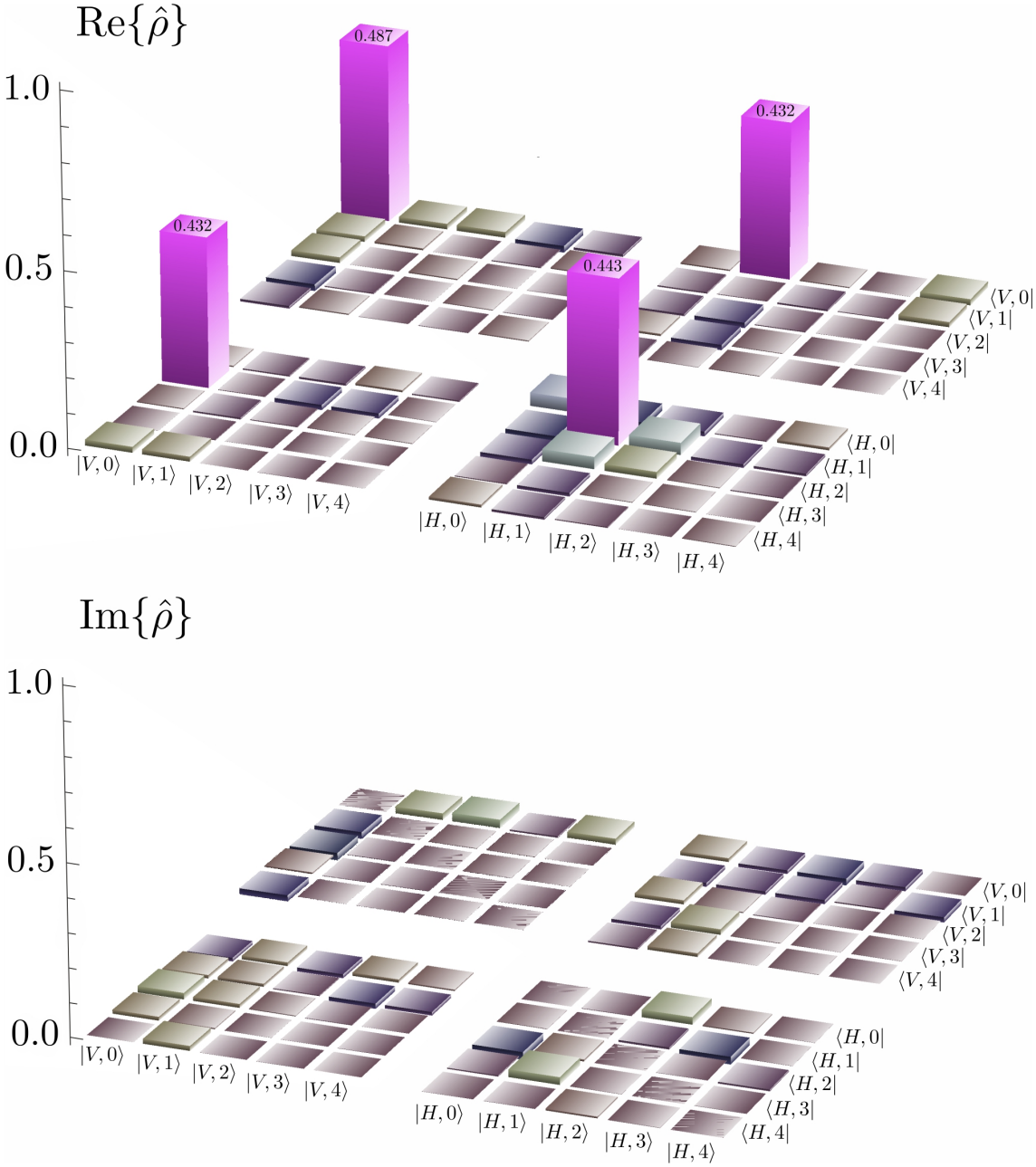


Figure 6.3: Entanglement swapping result. Density matrix $\hat{\rho}_{BD}$ of the post-selectively reconstructed state obtained through entanglement swapping in modes B and D after the Bell state measurement in modes A and C. The matrix' real and imaginary parts are presented in the basis $\{|H,n\rangle, |V,n\rangle\}$, where the polarisation and Fock states label the dual-rail mode D and single-rail mode B, respectively.

Comparing the result displayed in Fig. 6.3 with the expected maximally entangled state $|\aleph\rangle_{BD}$ of Eq. (4.4), we find a large fidelity of $\mathcal{F} = (89.7 \pm 2.1)\%$. If the efficiency correction in the maximum likelihood algorithm is removed, a fidelity of $\mathcal{F} = (66.8 \pm 1.3)\%$ is found nevertheless, thereby certifying the *a posteriori* entanglement of this state since the classical limit of 1/2 [105] is beaten.

Chapter 7

Discussion and Outlook

> *'I turn my body from the sun. What ho, Tashtego! let me hear thy hammer. Oh! ye three unsurrendered spires of mine; thou uncracked keel; and only god-bullied hull; thou firm deck, and haughty helm, and Pole-pointed prow,—death-glorious ship! must ye then perish, and without me? Am I cut off from the last fond pride of meanest shipwrecked captains? Oh, lonely death on lonely life! Oh, now I feel my topmost greatness lies in my topmost grief. Ho, ho! from all your furthest bounds, pour ye now in, ye bold billows of my whole foregone life, and top this one piled comber of my death! Towards thee I roll, thou all-destroying but unconquering whale; to the last I grapple with thee; from hell's heart I stab at thee; for hate's sake I spit my last breath at thee. Sink all coffins and all hearses to one common pool! and since neither can be mine, let me then tow to pieces, while still chasing thee, though tied to thee, thou damned whale! THUS, I give up the spear!'*
>
> *Captain Ahab's last words in Herman Melville's "Moby Dick"*

In summary, we have proposed and experimentally demonstrated a scheme to interconvert between the dual- and single-rail encodings of an optical qubit with state-of-the-art fidelities and large success probabilities. This scheme enables ef-

ficient exchange of quantum information between stationary carriers of different nature by means of light.

The quality of the results could be improved by having number-discriminating photon detectors in order to efficiently discriminate and remove events with false positive Bell state projections. Additionally, heralded or deterministic sources of entangled photons would make the single-dual rail entangled resource readily available through entanglement swapping.

There are three primary ways to encode a qubit in the optical field: single-rail, dual-rail and continuous-variable. While previous research [68, 69, 70] established techniques to connect the two discrete-variable encodings with the continuous-variable one, the present work completes the triad to enable interconversion among all three encodings, thus bringing us one step closer to real-world applications of quantum information by means of light.

Part III

Certified Quantum Randomness from Untrusted Light

Part III Abstract

A remarkable aspect of quantum theory is that certain measurement outcomes are entirely unpredictable to all possible observers. Such quantum events can be harnessed to generate numbers whose randomness is asserted based upon the underlying physical processes. We formally introduce and experimentally demonstrate an ultrafast optical quantum randomness generator that uses a totally untrusted photonic source. While considering completely general quantum attacks, we certify randomness at a rate of 1.1 Gbps with a rigorous security parameter of 10^{-20}. Our security proof is entirely composable, thereby allowing the generated randomness to be utilised for arbitrary applications in cryptography and beyond.

The research presented here led to an article [41] written by the author of this thesis himself and his co-authors. Additionally, a patent for this idea [106] was filed and the author of this thesis is one of its inventors along with the other listed co-inventors. Note that most of the content of this thesis part is directly taken from the article mentioned above.

The experiment was conceived and performed by the author of this thesis. The theoretical framework and the associated thorough security proof was done by Nathan Walk, assisted by the author of this thesis, Matty J Hoban and Jonathan Barrett. W Steven Kolthammer and Joshua Nunn proposed the early simple source-device-independent protocol detailed in the two paragraphs preceding and following Eq. (9.3) and Eq. (9.4). The final source-device-independent quantum randomness generation protocol was designed by the author of this thesis.

Chapter 8

Introduction and Background

> *'Lolita, light of my life, fire of my loins. My sin, my soul. Lo-lee-ta: the tip of the tongue taking a trip of three steps down the palate to tap, at three, on the teeth. Lo. Lee. Ta. She was Lo, plain Lo, in the morning, standing four feet ten in one sock. She was Lola in slacks. She was Dolly at school. She was Dolores on the dotted line. But in my arms she was always Lolita. Did she have a precursor? She did, indeed she did. In point of fact, there might have been no Lolita at all had I not loved, one summer, an initial girl-child. In a princedom by the sea. Oh when? About as many years before Lolita was born as my age was that summer. You can always count on a murderer for a fancy prose style. Ladies and gentlemen of the jury, exhibit number one is what the seraphs, the misinformed, simple, noble-winged seraphs, envied. Look at this tangle of thorns.'*
>
> *Humbert Humbert in Vladimir Nabokov's "Lolita"*

This chapter provides the reader with a general background motivating the research undertaken. In particular, it consists of a motivation to the field under consideration, its overview and a summary of the key findings obtained in this work.

8.1 Motivation

Historically, the concept of randomness has been defined as the lack of predictability in some given event. While this semantic definition arises from the illustrious *Oxford English Dictionary*, one might wonder what the mathematical equivalent is. To answer this question, one must consider the mathematical theory of probability and the concept of a distribution. Within this framework, randomness is a notion associated with numbers that follow a uniform distribution, i.e. the distribution wherein the occurrence of any particular event is equally likely. Once this definition was accepted, sequences of statistical tests [107] were contrived in order to assess the randomness of an arbitrary string of numbers. Examples of these tests range from rudimentarily counting the number of occurrences for each number to infer an underlying uniformity to more complex tests for which the spacing between *randomly* chosen points within the string should be asymptotically exponentially distributed, hence basing this analysis on the birthday paradox.

Acknowledging the above definitions, let us now consider Galton's board [108] shown on the left-hand side of Fig. 8.1.

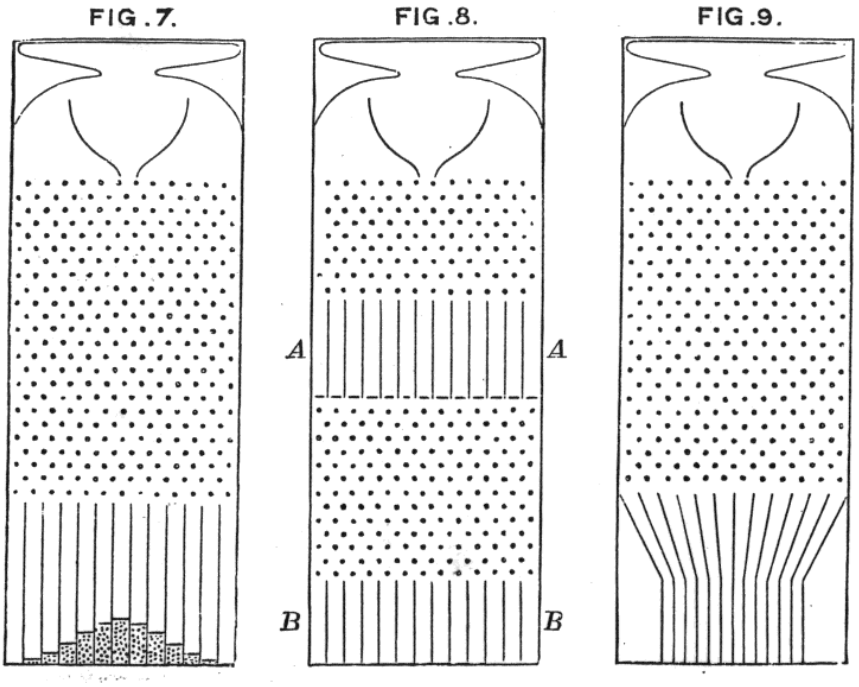


Figure 8.1: Galton's board on the left. Original drawing taken from [108].

Galton's board — also known as the bean machine — is an archetypical device used to test the central limit theorem and its functioning is described as follows. A leaden ball is fed into a structured network of metallic pins. Upon each collision at a pin, the ball has a probability $p = \frac{1}{2}$ to fall either to the left or right of the pin. After transmitting through the array of pins, the ball is finally registered in one of the bins at the bottom left of Fig. 8.1. The nature of the collision process at each pin is described by a Bernoulli random variable and as such, the repetition of these collisions for a single leaden ball naturally leads to a binomial distribution for the leaden ball's resulting position measured in the bins. By repeating this process and assuming a large number of leaden balls, the binomial distribution tends to a Gaussian distribution as per the central limit theorem and one can indeed observe its signature at the bottom left of Fig. 8.1. Now, if one were to assign a number to each collection bin and write it down every time a leaden ball is registered, one might ask oneself whether this device can be used for the generation of truly random numbers. Indeed, the leaden balls behave independently from one another and they follow a distribution not too dissimilar from a uniform distribution such that some randomness must arise from it as a consequence.

In reality, even though the statistical tests mentioned above would claim some randomness, random numbers based on Galton's board would be totally predictable. This comes from the fact that the seemingly random collisions involved in Galton's board are based on classical mechanics and consequently, the ball's resulting position in the bins is entirely predictable if one is provided sufficient computing power as well as the knowledge of the system's initial conditions. Such random number generators (RNGs) based on classical mechanics or deterministic theories are labelled Pseudo RNGs (PRNGs) and examples include thermal noise [109] across an electronic resistor, avalanche noise from an avalanche diode [110] or random numbers generated from deterministic computer algorithms [111]. One might argue that classical noise such as thermal noise is unpredictable, however this can only be the case if it is assumed that the system's microscopic details are not accessible to any

adversary. Moreover, noise such as the avalanche noise can be shown to have memory effects [40, 112] making it possible for an adversary to predict or — even worse — influence the outcome of such process.

This surprising paradox between the conformity of Galton's board with the mathematical definition of randomness provided above and the resulting numbers being purely predictable leads to the following definition of true randomness:

Definition 1. *To assert the randomness of some given numbers/events, the physical process generating the numbers/events has to be considered over their statistics. Such process is said truly random if uniform and uncorrelated to pre-existing information.*

That is why quantum mechanics — due to its inherent randomness — prevails as a means to generate such genuinely random numbers. No matter the computing power in possession or the knowledge of the system's initial conditions, one simply cannot determine in advance e.g. where each successive electron will land in a Stern-Gerlach apparatus [113], even though the electrons' statistical behavior is well characterised by the theory of quantum mechanics.

8.2 Introduction

The inherent randomness of quantum theory, embodied by Born's rule, creates fundamentally unpredictable events. The concept of a quantum random number generator (QRNG) is to leverage this principle to produce a random, unpredictable output with an unparalleled level of confidence. The central challenge faced by practical QRNGs is to rigorously quantify how much of the entropy generated by a real-world device is indeed intrinsically unpredictable.

To sketch the basic idea, let's consider a device completely described by parameters s which could be quantum or classical. These are used to generate a classical

outcome X that should appear unpredictable from the perspective of an agent external to the device. Consider such an agent E with access to a system which includes all the parameters s as well as any other side information (classical or quantum). For any given value of s, the joint system is described by a classical-quantum state $\hat{\rho}_{XE}$ and the outcome's predictability is simply the probability of the best guess

$$P_{\text{ideal},s}(X|E) = \sup_{\{\hat{E}_x\}} \sum_x p_x \text{tr}\left(\hat{E}_x \hat{\rho}_E^x\right) , \tag{8.1}$$

where the supremum is taken over all measurements $\{\hat{E}_x\}$ made by E on the system and $\hat{\rho}_E^x$ is the state of E conditioned on $X = x$. For a real device, however, s is never known exactly. In this case, a conservative estimate of the predictability is given by $P = \max_s P_{\text{ideal},s}(X|E)$, where the maximisation is taken over all plausible parameters s. Confidence in the randomness is thus linked to claims about trusted workings of the device and subsequent constraints on the knowledge of the external agent.

Approaches to QRNGs differ by the detail with which the devices need to be characterised in order to constrain s [40, 114]. Perhaps the simplest conceptually is a so-called device-independent QRNG, which can take the form of a Bell test [115, 116, 117, 118]. In this case, the device must be composed of two isolated measurements that employ independently selected bases — a requirement that can be verified with high confidence. With this condition, $P < 1$ as long as the measurement outcomes violate a Bell inequality [10, 11], which in turn constrain the plausible s [119]. In reality, however, even state-of-the-art implementations [120] are extremely complex and yield impractical bitrates of the order $\sim 100\,\text{bps}$. An alternate approach is to build a QRNG in which the entire device, from quantum source to measurement, is faithfully characterised and modelled [121]. Here, the detailed characterisation, which might use both off-line and in-line measurements, crucially constrains s (and thus E) sufficiently to assert a non-unit P. As such, this seemingly exhaustive type of characterisation of the setup, and hence trust in its proper inner

workings, opens up a myriad of potential attacks and malfunctions which might compromise the randomness output. A series of intermediate approaches have appeared, commonly referred to as having partial device-independence, which yield a QRNG that permits abstraction from part of the device while needing a detailed characterisation of the remainder. These can be broadly classified as those that are independent of the measurement devices [122, 123, 124] or the sources [125]. A third class, known as semi-device-independent makes no assumptions on either the source or measurements except to assert a global constraint on the relevant dimension [126, 127], energy [128] or orthogonality of the relevant states [129]. Finally, other works have combined assumptions, such as the semi-source independent protocols that invoke a dimension assumption in conjunction with a calibrated detection [130, 131, 132].

Successful design of a practical QRNG must balance confidence with ease of implementation, achievable bitrate, durability and cost. For example, QRNGs based on radioactive decay have limited bitrates, whereas those utilising electronic noise require careful distinction of quantum and thermal fluctuations [40]. In contrast, optical QRNGs promise well isolated quantum systems along with speed and technical ease. Implementations have been based on photon *welcher weg* [133, 134, 135], photon arrival time [136, 137], photon number statistics [138], vacuum fluctuations [139, 140, 141], phase noise [142, 143, 144] and Raman scattering [145, 146].

In this thesis part, we develop a certification of quantum randomness generated by an optical beam splitter for which one input field is the vacuum and the other is completely unknown. The certification was carried out in real-time using an additional vacuum mode to tap off part of the unknown light source prior to the randomness generation. This method probabilistically infers a lower bound on the photon number of the remaining untrusted source impinging onto the randomness generation measurement. We show that signals from carefully characterised photodetectors, which needn't resolve photon number, are sufficient to both generate and certify genuine quantum randomness. Our approach results in a composably secure proto-

col[1] and we provide an explicit security proof for high-speed quantum randomness expansion. Such a proof is necessary for all applications that wish to claim provable quantum-based security. Indeed, a key or random string only becomes useful in composition with other protocols (e.g. one-time pad or hashing) such that in order to retain provable quantum security, a composable proof is mandatory. To date, most randomness generation protocols fail to provide outputs that are useable in a composable framework, with, to our knowledge, only a handful shown to be composably secure in a device-dependent scenario [121, 148, 149] and only one partially device-independent result [125]. To experimentally demonstrate our scheme, we used off-the-shelf components — a laser source, high bandwidth photodiodes and basic linear optical elements — and generated ≈ 1.1 Gbps of quantum entropy with composable security parameter $\epsilon_{\text{fail}} = 10^{-20}$. Moreover, we implemented hashing on this data, thereby creating a string of random numbers that passed the NIST tests [107]. Overall, our framework is compatible with a wide range of optical detectors and avoids the need to trust or precisely characterise the source of light [121, 130].

[1]Let P_1 and P_2 be two general protocols that have associated failure probabilities ϵ_1 and ϵ_2. A protocol P that includes P_1 and P_2 is said to be *composably secure* [147] if and only if its failure probability ϵ is upper bounded by the sum of its constituent failure probabilities, i.e. $\epsilon_1+\epsilon_2$. In the case of P, we have $\epsilon = \underbrace{\epsilon_1\epsilon_2}_{\text{both fail}} + \underbrace{\epsilon_1(1-\epsilon_2)}_{P_1 \text{ fails and } P_2 \text{ passes}} + \underbrace{\epsilon_2(1-\epsilon_1)}_{P_2 \text{ fails and } P_1 \text{ passes}} = \epsilon_1+\epsilon_2-\epsilon_1\epsilon_2 \leq \epsilon_1+\epsilon_2$.

Chapter 9

Theory Overview

'Que je voudrais bien tenir un de ces puissants de quatre jours, si légers sur le mal qu'ils ordonnent, quand une bonne disgrâce a cuvé son orgueil ! Je lui dirais... que les sottises imprimées n'ont d'importance qu'aux lieux où l'on en gêne le cours ; que, sans la liberté de blâmer, il n'est point d'éloge flatteur ; et qu'il n'y a que les petits hommes qui redoutent les petits écrits.'

Figaro in Beaumarchais' "Le Mariage de Figaro"

This chapter provides an overview of the theory developed for this research. The complete theory along with its details are presented in the next chapter.

9.1 Generating Randomness from Untrusted Light

In Eq. (8.1), we quantified the randomness of an outcome X for an external agent E. As is common in quantum cryptography, we will refer to this agent as Eve the eavesdropper. An equivalent, but more convenient, way of quantifying this randomness is to compute the quantum conditional min-entropy of the quantum

state $\hat{\rho}_{XE}$ for the joint system XE [150]

$$H_{\min}(X|E)_{\hat{\rho}_{XE}} = -\log_2 \left(\sup_{\{\hat{E}_x\}} \sum_x p_x \mathrm{tr}\left(\hat{E}_x \hat{\rho}_E^x\right) \right) , \tag{9.1}$$

where the argument of the logarithm is the guessing probability for Eve to guess X, as in Eq. (8.1). This quantity has been shown to quantify the number of bits — almost perfectly random with respect to Eve — that can be *extracted* via post-processing [151]. Notice the distinction between a quantum randomness generator (QRG) which simply generates outputs with a certain conditional min-entropy and a QRNG that also includes the post-processing (hashing) necessary to produce almost perfect random numbers.

A certified randomness generation protocol allows for some, or all, devices to deviate arbitrarily from their purported specifications. A test $\mathcal{P}$ is applied to the experimental data and only upon that test passing is the output certified as having a certain amount of randomness except with some small failure probability. Furthermore, a useful generator will be robust, i.e. it will pass the test with high probability. Formally, we can define such a protocol as follows.

Definition 2. *An $(m, \kappa, \epsilon_{\text{fail,m}}, \epsilon_c)$-certified randomness generation protocol produces an output X of length m such that*

- ***Security:*** *If the certification test $\mathcal{P}$ is passed, then*

$$H_{\min}(X|E) \geq \kappa \, ,$$

  except with probability $\epsilon_{\text{fail,m}}$.

- ***Completeness:*** *There exists an honest implementation such that the test will be passed with probability $1 - \epsilon_c$.*

We define our source-device-independent (SDI) photonic QRG as a protocol in which detectors and passive optical devices (e.g. beam splitters) are taken to be

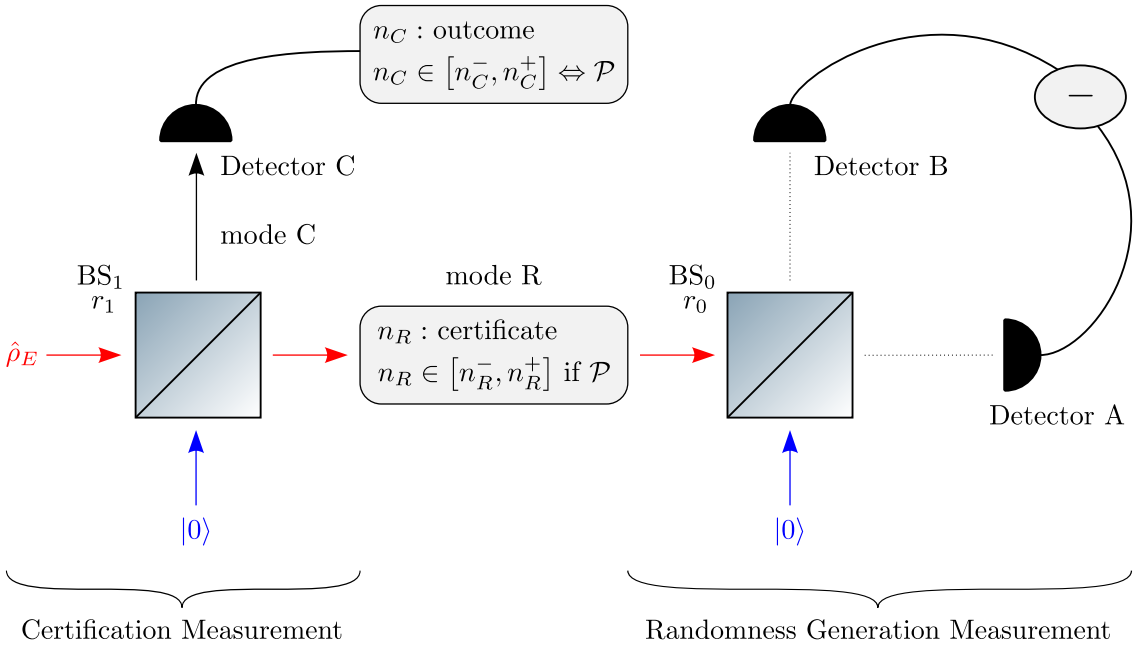


Figure 9.1: Scheme for our SDI protocol. An unknown light source $\hat{\rho}_E$ is mixed with a trusted vacuum on a beam splitter (BS) with reflectivity r_1 to perform a certification measurement. The measured outcome at detector C is subject to a test $\mathcal{P}$ that passes if the outcome lies within a certain range $[n_C^-, n_C^+]$. Upon passing the test, we certify a photon number n_R in mode R that impinges onto the randomness generation measurement except with probability ϵ_{fail}.

trusted. Photonic states are generated via a laser as input to the experiment (essentially preparing a large amplitude coherent state), however in the analysis, we will not assume anything about the state of these photons and in that sense we claim that randomness is generated in a SDI manner. Crucially, however, we also assume that it is possible to exploit a trusted vacuum mode. One might point out that this is in fact assuming at least one trusted source, namely the vacuum. Nevertheless, we argue that vacuum is a rather privileged source in the sense that it does not really require a "device" to be generated, merely the ability to block an input port to a beam splitter. Thus, it would seem highly preferable from a security perspective to trust a vacuum source rather than some photonic state created by a sophisticated device such as a laser or spontaneous parametric down conversion (SPDC) process.

To gain some intuition, let us start by considering the randomness generation measurement depicted in Fig. 9.1. It consists of a beam splitter BS$_0$ with reflectivity $r_0 = \frac{1}{2}$, an input mode R, a trusted vacuum fed into the other input mode and two

output photodetectors A and B performing a difference measurement. Assuming the photodetectors to be perfect, we can model them as performing a single measurement acting on the untrusted photonic randomness source in mode R. The outcomes of the measurement will be the photon numbers n_A and n_B detected by detectors A and B, respectively. Propagating this detection event back through the beam splitter and using our knowledge about the trusted vacuum mode, this measurement is then associated with positive-operator valued measure (POVM) elements of the form

$$\hat{M}(n_A, n_B)_R = \frac{(n_A + n_B)!}{2^{n_A+n_B} n_A! n_B!} |n_A + n_B\rangle \langle n_A + n_B|_R \ , \tag{9.2}$$

living in the Hilbert space of the input mode R (see Sec. 10.1 for details).

Given this, we now propose a simple certifiable randomness generation protocol. It consists of recording the value of the photon number sum $N := n_A + n_B$ and then using the difference measurement $x := n_A - n_B$ as the source of randomness. Therefore, we have two measurements: one of N and one of x. The POVM $\mathbb{Z}$ has elements $\hat{Z}(N)$ for the measurement of N that can be readily recovered as

$$\begin{aligned} \hat{Z}(N) &= \sum_{n_A=0}^{N} \hat{M}(n_A, N - n_B)_R \\ &= |N\rangle \langle N|_R \ . \end{aligned} \tag{9.3}$$

On the other hand, as we show in Sec. 10.1, the POVM $\mathbb{X}$ for the value of x has elements given by

$$\begin{aligned} \hat{X}(x) \ &= \ \sum_{n_A=|x|}^{\infty} 2^{-(2n_A-|x|)} \binom{2n_A - |x|}{n_A} \\ &\times \ |2n_A - |x|\rangle \langle 2n_A - |x||_R \ . \end{aligned} \tag{9.4}$$

We already see the inherent randomness of this scheme since $\hat{X}(x)$ has support over the whole Fock space. Therefore, for any state in mode R with total photon number $N > 0$, there will be multiple possible values x which can occur. More-

over, there is a clear independence from the photonic input state. Because the measurements described by $\hat{Z}(N)$ and $\hat{X}(x)$ are by definition compatible, we can always think of the $\hat{Z}(N)$ measurement happening first and projecting onto the state $|N\rangle$, which will subsequently produce randomness when measured with $\mathbb{X}$. Thus, conditioned upon observing a sum value of N, one would certify with probability $\epsilon_{\text{fail,m}} = 0$ an amount of randomness that scales as $\log_2(N\pi/2)$ as per Definition 2 and shown in Sec. 10.1.

Now, consider the full setup shown in Fig. 9.1. We introduce the certification measurement in mode C which is done by tapping off a fraction of the completely unknown incoming light in mode E with a beam splitter BS_1 of reflectivity r_1. The input state $\hat{\rho}_E$ is mixed with a trusted vacuum on BS_1 and the reflected beam in mode C is measured at detector C while the transmitted beam in mode R is input to the randomness generation measurement. Our test $\mathcal{P}$ is applied to the output of detector C with the protocol aborting if the result lies outside a range $[n_C^-, n_C^+]$. Upon passing the test, we obtain a certificate that n_R, the photon number in mode R, lies within a range $[n_R^-, n_R^+]$ except with some failure probability ϵ_{fail}. Then, by minimising the min-entropy over all states within this range, we obtain a certified lower bound on the generated randomness. For this idealised scenario, we could allow n_R^+ to be unbounded and would simply look to certify the largest possible value of n_R^- given a specific ϵ_{fail}.

9.2 Certifying Randomness with Realistic Devices

In a real experiment, several further complications must be taken into account. Even in a scenario of completely trusted and calibrated devices, care must be taken to quantify the amount of randomness that can be credibly claimed to have been generated. Firstly, real detectors only possess a finite dynamic range over which their response is meaningful. Secondly, measurement outcomes are coarse grained

to a finite resolution which must be carefully accounted for when determining the output randomness. Finally, noisy devices will exhibit fluctuations due to processes not under complete experimental control. Information about these processes might be accessible to external observers and, even if not, could certainly be stemming from physical processes that are far from random. Nevertheless, this can be accounted for provided the device noise is calibrated and not controlled by Eve. This makes the noise essentially classical, in the sense that we may assume that it is described by variables λ which are distributed according to a characterised probability distribution. These variables are then given to Eve on a shot-by-shot basis.

Consequently, the first step for analysing our experiment is to carefully calibrate and model the realistic photodiodes, which output noisy voltage measurements rather than exact photon numbers. More formally, following the approach of [152], we model the POVM describing our noisy, characterised measurements as a projective measurement on a larger system. For the case of our detectors (see Fig. 10.1 in Sec. 10.2 for a cohesive summary), the measured voltages are modelled as follows. First, we consider an $L := n_{\max} - n_{\min} + 1$ outcome photon number resolving measurement with a finite range $[n_{\min}, n_{\max}]$ described by measurement operators that are number state projectors (i.e. $\hat{N}(n) = |n\rangle\langle n|$), except for the first and last operators which are given by $\hat{N}(n_{\min}) = \sum_{n=0}^{n_{\min}} |n\rangle\langle n|$ and $\hat{N}(n_{\max}) = \sum_{n=n_{\max}}^{\infty} |n\rangle\langle n|$. This photon number is converted to a voltage via a conversion factor α and is then smeared by an additional Gaussian noise term λ of known variance σ^2 and finally coarse grained by an analogue to digital converter (ADC) that itself has only finite range $[V_{\min}, V_{\max}]$ and finite resolution of $2^{\Delta_{\text{ADC}}}$ bins, inducing an effective voltage resolution of $\delta V = \frac{V_{\max} - V_{\min}}{2^{\Delta_{\text{ADC}}}}$. The output of such a realistic measurement is an index, say j, corresponding to a voltage bin of width δV centered at $j\delta V$. We can therefore associate minimum and maximum voltages $v_j^{\pm} = \delta V(j \pm \frac{1}{2})$ with this outcome j.

The certification measurement is made by mixing the unknown photonic input $\hat{\rho}_E$ in mode E with vacuum $|0\rangle$ on a beam splitter of reflectivity r_1. The reflected mode C is then detected with a noisy photodiode (characterised by noise standard

deviation σ_C and voltage conversion factor α_C) that is coarse grained by an ADC. The protocol aborts for sufficiently large or small observed voltages ($\mathcal{P}$ is now a test applied directly to the measured voltage index). Finally, the randomness is generated by mixing the transmitted state in mode R with another vacuum on a beam splitter with reflectivity $r_0 = \frac{1}{2}$ and making a coarse-grained, noisy difference measurement characterised by noise standard deviation σ_D and voltage conversion factor α_D. As with the ideal case, we can write the measurements as operators in the input Hilbert space. As shown in Sec. 10.2, the POVM element for a realistic voltage difference measurement whose outcome is the bin labelled j is

$$\hat{V}_D^{\sigma_D,\Delta_{\mathrm{ADC}}}(j) = \int_{I_j^D} \hat{V}_D^{\sigma_D}(v_D)\, dv_D\,, \tag{9.5}$$

with

$$\hat{V}_D^{\sigma_D}(v_D) = \sum_{x=-(L-1)}^{L-1} \frac{e^{-(v_D-\alpha_D x)^2/(2\sigma_D^2)}}{\sqrt{2\pi}\sigma_D} \hat{X}_{\mathrm{fin}}(x)\,, \tag{9.6}$$

where $\hat{X}_{\mathrm{fin}}(x)$ are the POVM elements of a difference measurement that is identical to Eq. (9.4) except that it is made with finite range photodetectors described above and is hence only operationally equivalent over an input photon number range $[n_{\mathrm{min}}^D, n_{\mathrm{max}}^D]$.

Similarly, the certification measurement element corresponding to the outcome bin labelled i is given by

$$\hat{V}_C^{\sigma_C,\Delta_{\mathrm{ADC}}}(i) = \int_{I_i^C} \hat{V}_C^{\sigma_C}(v_C)\, dv_C\,, \tag{9.7}$$

with

$$\hat{V}_C^{\sigma_C}(v_C) = \sum_{n=n_{\mathrm{min}}^C}^{n_{\mathrm{max}}^C} \frac{e^{-(v_C-\alpha_C n_C)^2/(2\sigma_C^2)}}{\sqrt{2\pi}\sigma_C} \hat{N}_C(n_C)\,. \tag{9.8}$$

With this model in hand, we state our main theorem.

Theorem 1. *An optical setup consisting of*

- *Two trusted vacuum modes*
- *Two beam splitters of reflectivity* $r_0 = \frac{1}{2}$ *and* r_1
- *Two noisy photodetectors used to make a difference measurement as described in Eq. (9.5)*
- *A third noisy photodetector used to make a certification measurement as described in Eq. (9.7) which passes the test* $\mathcal{P}$ *if* i *falls in a chosen range* $[i_-, i_+]$

can be used as a certified $(m,\kappa,\epsilon_{\text{fail,m}},\epsilon_c)$*-randomness generation protocol as per Definition 2 without making any assumptions about the photonic source with*

$$\kappa \geq -m \log_2 \left(\sum_{x \in \mathcal{X}} 2^{-n_R^-} \binom{n_R^-}{\lfloor \frac{n_R^- + x}{2} \rfloor} \right) , \tag{9.9}$$

where

$$\mathcal{X} \in \mathbb{N} \cap \left[- \left\lfloor \frac{\delta V}{2\alpha_D} \right\rfloor , \left\lfloor \frac{\delta V}{2\alpha_D} \right\rfloor \right] , \tag{9.10}$$

with $\delta V = \frac{V_{\max} - V_{\min}}{2^{\Delta_{\text{ADC}}}}$,

$$\epsilon_{\text{fail,m}} \leq m \epsilon_{\text{fail}} , \tag{9.11}$$

where

$$\epsilon_{\text{fail}} = \max\{\epsilon_-, \epsilon_+\} + \epsilon_{\lambda_C} , \tag{9.12}$$

with

$$\begin{aligned}
\epsilon_- &= \exp\left(-2\frac{\left(\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} - r_1\left(\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1\right)\right)^2}{\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1}\right), \\
\epsilon_+ &= \exp\left(-2\frac{\left(n_R^+ - (1-r_1)\left(\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1\right)\right)^2}{\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1}\right), \\
\epsilon_{\lambda_C} &= 1 - \mathrm{erf}\left(\frac{\tilde{\lambda}}{\sqrt{2}\sigma_C}\right), \qquad (9.13)
\end{aligned}$$

provided n_R^+ is set to the saturating photon number of the difference measurement.

Moreover,

$$\epsilon_c = 1 - \mathrm{tr}\left\{\sum_{i=i_-}^{i_+} |\alpha\rangle\langle\alpha| \hat{V}_C^{\sigma_C,\Delta_{\mathrm{ADC}}}(i)\right\}, \qquad (9.14)$$

using a coherent state $|\alpha\rangle$ as an input.

9.3 Proof Sketch of the Main Theorem

For a complete proof, see Sec. 10.3. One part of the proof is to show that, for any given round of the protocol, conditioned on passing the test $\mathcal{P}$, the state in mode R can only reside in an interval within the photon number basis that lies almost entirely in the range $[n_R^-, n_R^+]$. More concretely, we maximise over all possible input states to upper bound

$$\epsilon_{\mathrm{fail}} := \max_{\hat{\rho}_E} \Pr\left[i^- \leq i \leq i^+ \wedge n_R \notin [n_R^-, n_R^+]\right], \qquad (9.15)$$

the joint probability that the test would be passed in mode C whilst a photon number outside the range $[n_R^-, n_R^+]$ was present in mode R. This quantity can be inter-

preted as the probability that the conditional state in mode R can be operationally distinguished from any state solely residing within $[n_R^-, n_R^+]$ (see Sec. 10.4).

The second part of the proof is to optimise over all possible input states that reside only in $[n_R^-, n_R^+]$ to derive a lower bound on the conditional min-entropy. Note that *a priori*, Eve has the freedom to choose an input state that is potentially entangled across all m rounds, i.e. we are considering completely general, so-called coherent attacks. Together, these results mean that either the min-entropy for a single round will be lower bounded or the protocol will abort except with probability ϵ_{fail}. For m rounds, one can simply add these lower bounds together to bound the min-entropy of the output string except with a probability

$$\epsilon_{\text{fail,m}} := 1 - (1 - \epsilon_{\text{fail}})^m \leq m\epsilon_{\text{fail}} \,, \tag{9.16}$$

as claimed in Eq. (9.11).

Intuitively, one would expect that Eve's optimal strategy to predict the outcome of a difference measurement would be to input a pure Fock state and this is indeed the case. The key fact is that the realistic difference measurement is still diagonal in the photon number basis and that an m-round protocol can be described as a tensor product of such measurements. Note that for the purposes of calculating the min-entropy, we consider the difference measurement in Eq. (9.5) from the perspective of Eve who knows the noise variable λ_D on a shot-by-shot basis, for which $\hat{V}_D^{\Delta_{\text{ADC}}}(j) = \sum_{x\in\mathcal{X}} \hat{X}(x)$, where $\mathcal{X} = \{x : \alpha_D x + \lambda_D \in I_j^D\}$. The fact that this measurement commutes with a diagonalising map in the photon number basis makes it straightforward to show that Eve's optimal guessing probability is achieved by inputting a pure Fock state. Provided we choose n_R^+ less than $n_{\max}$, the saturation value for the detectors, then direct calculation shows that the guessing probability decreases monotonically in n_R. Thus, for states restricted to $[n_R^-, n_R^+]$, the smallest min-entropy is achieved by inputting $|n_R^-\rangle$. Finally, the fact that the coefficients in Eq. (9.4) are those of a binomial distribution can be used to show that Eve's

min-entropy is minimised whenever x is minimal (0 or 1 depending if an odd or even photon number is input) and $\lambda_D = 0$. Assuming that this is always the case, direct evaluation of $\mathrm{tr}\left\{\left|n_R^-\right\rangle\left\langle n_R^-\right| \hat{V}_D^{\Delta_{\mathrm{ADC}}}\left(n_R^- \mod 2\right)\right\}$ yields the expression in Eq. (9.9).

Turning to the failure probability, we first define a failure operator which corresponds to taking the failure condition (i.e. a passing voltage is observed at detector C along with $n_R \notin [n_R^-, n_R^+]$ in mode R) and write it as an operator in the Hilbert space of Eve's input mode

$$\begin{aligned}\hat{V}_F^{\Delta_{\mathrm{ADC}}}(i, n_R^-, n_R^+) &= \sum_{\substack{n_C \in \mathcal{C} \\ n_R \notin [n_R^-, n_R^+]}} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} \\ &\times \left|n_C + n_R\right\rangle\left\langle n_C + n_R\right|_E ,\end{aligned} \tag{9.17}$$

where $\mathcal{C} = \{n_C : \alpha_C n_C + \lambda_C \in [i^-, i^+]\}$.

Since this operator is also diagonal in the photon number basis, one can repeat the previous arguments to show that Eve's optimal strategy to maximise this failure probability is also achieved by a Fock state.

The failure probability for a single round of the protocol can then be written as

$$\epsilon_{\mathrm{fail}} = \max_{n_E} \sum_{i=i^-}^{i^+} \left\langle n_E\right| \hat{V}_F^{\sigma_C, \Delta_{\mathrm{ADC}}}(i, n_R^-, n_R^+) \left|n_E\right\rangle . \tag{9.18}$$

To bound this quantity, we first use our knowledge of the certification noise variable λ_C. Except with probability $\epsilon_{\lambda_C} = 1 - \mathrm{erf}\left(\frac{\tilde{\lambda}}{\sqrt{2}\sigma_C}\right)$, we know that $|\lambda_C| \leq \tilde{\lambda}$. Substituting Eq. (9.17) in Eq. (9.18) yields two terms as the sum over $n_R \notin [n_R^-, n_R^+]$ decomposes as a sum for $0 \leq n_R < n_R^-$ and $n_R^+ < n_R \leq \infty$. Provided we have $\lambda_C \leq v_{i^+}^+ - \alpha_C\left(n_R^+ - n_R^- + 1\right)$, then there is no value of n_E for which both terms will be simultaneously non-zero and we can write

$$\epsilon_{\mathrm{fail}} = \max\{\epsilon_-, \epsilon_+\} + \epsilon_{\lambda_C} , \tag{9.19}$$

where ϵ_- (ϵ_+) corresponds to the lower (upper) sum.

Both of these are essentially cumulative binomial distributions. For example, for a particular value of n_E

$$\epsilon_- \leq \sum_{\substack{n_C=\max\{n_C^-,\\ n_E-(n_R^--1)\}}}^{n_E} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C!n_R!}\,, \tag{9.20}$$

where n_C^- is the smallest photon number allowed at mode C consistent with passing the test.

For unbounded λ_C, it would be impossible to determine n_C^- or ϵ_-, but again using $\tilde{\lambda}$, we can do so except with probability ϵ_{λ_C}. If we define $v_i^{-(+)}$ as the minimum (maximum) voltage compatible with the passing range $[i^-, i^+]$, we can obtain a minimum (maximum) photon number $n_C^- = (v_i^- - \tilde{\lambda})/\alpha_C$ ($n_C^+ = (v_i^+ + \tilde{\lambda})/\alpha_C$) for mode C compatible with passing the test. The varying lower limit on the sum in Eq. (9.20) stems from the fact that for Eve to cheat, there are two constraints on n_C. First, it must be the case that a sufficiently large number of photons go to detector C such that the test is passed, but for sufficiently large n_E this condition is superseded by the requirement that less than n_R^- photons go to mode R. Arguments based upon the nature of the binomial coefficients allow us to show that to maximise ϵ_-, Eve should choose the input state $n_E^{\text{opt}} = n_C^- + n_R^- - 1$. This can be directly substituted into Eq. (9.20) and the application of Hoeffding's bound yields the term appearing in Eq. (9.13). Finally, an analogous argument can be applied to bound ϵ_+ as per Eq. (9.13). In combination with Eq. (9.16) and Eq. (9.19), this completes the security proof.

Chapter 10

Theory

'Flammende Gluth umglühe den Fels;
mit zehrenden Schrecken scheuch' es den Zagen;
der Feige fliehe Brünnhildes Fels!
Denn Einer nur freie die Braut,
der freier als ich, der Gott!'
Wotan's Leb' wohl in Wagner's "Die Walküre"

This chapter covers in detail the theory developed for the research undertaken and presented as an overview in the previous chapter.

10.1 Ideal Difference Measurement's Certifiable Randomness

To begin with, consider the randomness generation measurement of Fig. 9.1. It consists of a beam splitter BS_0 with reflectivity $r_0 = \frac{1}{2}$, an input mode R, a trusted vacuum fed into the other input mode and two output photodetectors A and B performing a difference measurement. It simplifies matters greatly if we can prove that the potential eavesdropper in charge of our photonic source is making definite

photon number states (i.e. Fock states) for each round of the protocol. In particular, we would like to rule out any sophisticated, collective strategy where Eve sends a complicated state that is entangled across all rounds of the protocol.

Intuitively, this should be the case because the randomness generation measurement for each round is a photon number difference and can be thought of as a coarse graining over an initial measurement that is diagonal in the Fock basis. Here, this is shown by writing out the POVM directly and the optimality of unentangled Fock state inputs from Eve's perspective becomes explicit.

For a single round, the entire process of mixing $\hat{\rho}_R$ with a vacuum ancilla $|0\rangle \in \mathcal{H}_V$ and then making Fock state projections upon both output ports can be seen as a POVM on $\mathcal{H}_R$, the Hilbert space of $\hat{\rho}_R$. Consider the probability for detecting n_A and n_B photons at detectors A and B. This is given by

$$\begin{aligned} p(n_A, n_B) &= \mathrm{tr}\left\{\hat{U}_{BS_0}(\hat{\rho}_R \otimes |0\rangle\langle 0|)\hat{U}^\dagger_{BS_0}(|n_A\rangle |n_B\rangle \langle n_A| \langle n_B|)\right\} \\ &= \mathrm{tr}_R\left\{\mathrm{tr}_V\left\{(\hat{\rho}_R \otimes |0\rangle\langle 0|)\hat{U}^\dagger_{BS_0}(|n_A\rangle |n_B\rangle \langle n_A| \langle n_B|)\hat{U}_{BS_0}\right\}\right\} \\ &= \mathrm{tr}_R\left\{\hat{\rho}_R \hat{M}(n_A, n_B)\right\}, \end{aligned} \tag{10.1}$$

where

$$\hat{M}(n_A, n_B) = \langle 0| \hat{U}^\dagger_{BS_0} |n_A\rangle |n_B\rangle \langle n_A| \langle n_B| \hat{U}_{BS_0} |0\rangle , \tag{10.2}$$

is the corresponding POVM element in the input state Hilbert space (with the subscript R suppressed for brevity). This expression is just the evolution of the Fock state projections back through the beam splitter BS_0 and projected onto the vacuum ancilla. To get an explicit expression, it is simpler to switch to the Heisenberg picture

for the reverse beam splitter transformation

$$\begin{aligned}
|n_A\rangle\,|n_B\rangle &= \frac{(\hat{a}_A^\dagger)^{n_A}}{\sqrt{n_A!}}\frac{(\hat{a}_B^\dagger)^{n_B}}{\sqrt{n_B!}}\,|0\rangle \\
&\overset{U_{BS_0}^\dagger}{\mapsto} \frac{\left(\frac{\hat{a}_E^\dagger+\hat{a}_V^\dagger}{\sqrt{2}}\right)^{n_A}}{\sqrt{n_A!}}\frac{\left(\frac{\hat{a}_E^\dagger-\hat{a}_V^\dagger}{\sqrt{2}}\right)^{n_B}}{\sqrt{n_B!}}\,|0\rangle \\
&= \frac{\sum_{k=0}^{n_A}\sum_{j=0}^{n_B}(\hat{a}_E^\dagger)^{n_A-k}(\hat{a}_V^\dagger)^k\binom{n_A}{k}(-1)^j(\hat{a}_E^\dagger)^{n_B-j}(\hat{a}_V^\dagger)^j\binom{n_B}{j}}{2^{(n_A+n_B)/2}\sqrt{n_A!n_B!}}\,|0\rangle \\
&= \frac{\sum_{k=0}^{n_A}\sum_{j=0}^{n_B}\sqrt{(n_A+n_B-j-k)!(j+k)!}\binom{n_A}{k}(-1)^j\binom{n_B}{j}}{2^{(n_A+n_B)/2}\sqrt{n_A!n_B!}} \\
&\quad\times|n_A+n_B-j-k\rangle_R\,|j+k\rangle_V\ . \qquad (10.3)
\end{aligned}$$

Acting on the left with $\langle 0|$ on the ancilla mode implies that we must have $j+k=j=k=0$, thus

$$\langle 0|\,\hat{U}_{BS_0}^\dagger\,|n_A\rangle\,|n_B\rangle = \frac{\sqrt{(n_A+n_B)!}}{2^{(n_A+n_B)/2}\sqrt{n_A!n_B!}}\,|n_A+n_B\rangle_R\ , \qquad (10.4)$$

and hence

$$\begin{aligned}
\hat{M}(n_A,n_B) &= \frac{(n_A+n_B)!}{2^{(n_A+n_B)}n_A!n_B!}\,|n_A+n_B\rangle\langle n_A+n_B|_R \\
&= 2^{-N}\frac{N!}{n_A!(N-n_A)!}\,|N\rangle\langle N|_R\ , \qquad (10.5)
\end{aligned}$$

where we have substituted in the total photon number $N := n_A + n_B$. As expected, each POVM element is proportional to a single Fock state of fixed photon number N and the coefficient can be understood intuitively. Indeed, each of the N photons can be thought of as individually randomising at the beam splitter. The probability for a specific sequence of paths taken by each photon is 2^{-N} and thus the probability of observing the POVM element $\hat{M}(n_A,n_B)$ is the number of paths such that n_A out of N photons could have been recorded at detector A, which is $\binom{N}{n_A}$ as above.

If we consider the sum measurement, it is just a coarse graining over the two outcome POVM, summing together all the elements such that $n_A + n_B = N$. The

POVM elements of the sum measurement $\mathbb{Z} = \{\hat{Z}(N)\}$ are

$$\hat{Z}(N) = \sum_{n_A=0}^{N} \hat{M}(n_A, N - n_A)\,. \tag{10.6}$$

Using the fact that $\sum_{k=0}^{n} \binom{n}{k} = 2^n$, we can see that $\hat{Z}(N) = |N\rangle\langle N|_R$ and it is thus just a photon number projector as expected.

The randomness generation measurement is another coarse graining. However, it will turn out to have larger rank and consequently some randomness for all possible input states other than the vacuum. Define $\mathbb{X} = \{\hat{X}(x)\}$ as the POVM elements of the randomness generation measurement corresponding to the cases where $n_A - n_B := x$. These are given by

$$\begin{aligned} \hat{X}(x) &= \sum_{n_A=x}^{\infty} \hat{M}(n_A, n_A - x) \\ &= \sum_{n_A=x}^{\infty} 2^{-(2n_A-x)} \binom{2n_A - x}{n_A} |2n_A - x\rangle\langle 2n_A - x|_R\,, \end{aligned} \tag{10.7}$$

if x is positive and

$$\begin{aligned} \hat{X}(x) &= \sum_{n_A=|x|}^{\infty} \hat{M}(n_A - |x|, n_A) \\ &= \sum_{n_A=|x|}^{\infty} 2^{-(2n_A-|x|)} \binom{2n_A - |x|}{n_A} |2n_A - |x|\rangle\langle 2n_A - |x||_R\,, \end{aligned} \tag{10.8}$$

if x is negative or

$$\hat{X}(x) = \sum_{n_A=|x|}^{\infty} 2^{-(2n_A-|x|)} \binom{2n_A - |x|}{n_A} |2n_A - |x|\rangle\langle 2n_A - |x||_R\,, \tag{10.9}$$

for all x.

Note that for x even (odd), then $\hat{X}(x)$ only has support over even (odd) number states. Clearly, if Eve inputs a vacuum state, then the difference outcome can be predicted with certainty as $x = 0$. However, as pointed out in Sec. 9.1, if

Alice observes a value N for her sum measurement, then regardless of the original input, she performs a projection onto the state $|N\rangle$ and can immediately calculate the guessing probability of the $\mathbb{X}$ measurement $p_{\text{guess}} = \max_x \langle N| \hat{X}(x) |N\rangle$ from Eq. (10.9) and hence the associated min-entropy. For perfect measurements, this would guarantee the min-entropy with certainty and in a SDI manner.

Now, consider the full setup shown in Fig. 9.1. We introduce the certification measurement in mode C which is done by tapping off a fraction of the completely unknown incoming light in mode E with a beam splitter BS_1 of reflectivity r_1. The input state $\hat{\rho}_E$ is mixed with vacuum on BS_1 and the reflected beam in mode C is measured at detector C while the transmitted beam in mode R is input to the randomness generation measurement. For simplicity, we will imagine that the outcome at detector C is also always given to Eve. Writing the photon number projections as operators on the input Hilbert space $\mathcal{H}_E$ is the same calculation as Eq. (10.5), except now with a beam splitter of reflectivity r_1 instead of $\frac{1}{2}$. This gives

$$\hat{M}(n_C, n_R) = \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle \langle n_C+n_R|_E , \quad (10.10)$$

and hence the certification measurement has elements

$$\hat{N}_C(n_C) = \sum_{n_R=0}^{\infty} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle \langle n_C+n_R|_E . \quad (10.11)$$

Given this measurement, one cannot exactly determine the number of photons in mode R incident onto the randomising beam splitter BS_0, but one can obtain a lower bound on the min-entropy of m such measurements except with some failure probability $\epsilon_{\text{fail,m}}$. Specifically, we impose a test $\mathcal{P}$ at detector C which is passed if the measured photon number is greater than a lower threshold n_C^-. Upon passing the test $\mathcal{P}$, we certify a lower bound n_R^- on the photon number in mode R impinging onto the randomness generation measurement. We formally state and prove this result below.

Theorem 2. *An optical setup consisting of*

- *Two trusted vacuum modes*
- *Two beam splitters of reflectivity* $r_0 = \frac{1}{2}$ *and* r_1
- *Three ideal photon counting detectors A, B and C*

utilised to perform a certification measurement modelled by Eq. (10.11) with lower threshold n_C^- *and a randomness generation measurement modelled by Eq. (10.9) can be used as a certified* $(m,\kappa,\epsilon_{\text{fail,m}},\epsilon_c)$*-randomness generation protocol as per Definition 2 without making any assumptions about the photonic source with*

$$\begin{aligned} \kappa &\geq -m \log_2 \left(2^{-n_R^-} \binom{n_R^-}{\left\lfloor \frac{n_R^-}{2} \right\rfloor} \right) \\ &\geq m \left(\log_2 \left(\frac{1}{2} \pi n_R^- \right) - \mathcal{O}\left(\frac{1}{n_R^-} \right) \right) , \end{aligned} \tag{10.12}$$

$$\epsilon_{\text{fail,m}} \leq m \exp \left(- \frac{2(r_1(n_R^- + n_C^- - 1) - n_C^-)^2}{n_R^- + n_C^- - 1} \right) , \tag{10.13}$$

and

$$\epsilon_c = 1 - e^{-|\alpha|^2} \sum_{n=0}^{\infty} \sum_{n_C=n_C^-}^{\infty} \frac{|\alpha|^{2n}}{n!} \frac{r_1^{n_C} (1-r_1)^{n-n_C} n!}{n_C!(n-n_C)!} , \tag{10.14}$$

using a coherent state $|\alpha\rangle$ *as an input.*

Proof. **Security:** The key feature here is the diagonal nature in the photon number basis of all measurements performed in the protocol. We first prove a Lemma regarding such measurements.

Lemma 1. *For an m-round, SDI protocol involving a measurement $\mathbb{Q}$ in each round that is diagonal in the number basis with elements*

$$\hat{Q}(q) = \sum_n c_n(q) \left|n\right\rangle \left\langle n\right|, \quad \sum_q \hat{Q}(q) = \mathbb{I}, \tag{10.15}$$

Eve's optimal strategy to maximise the probability of a desired outcome q^* is to input a pure Fock state $|n^*\rangle$ for each round. Moreover, this remains true for inputs with restricted support in the Fock basis.

Proof. One way to see this is to consider a diagonalising map in the Fock basis applied to the input of the i^{th} round

$$\hat{\mathcal{D}}_i(\hat{\rho}) = \sum_n \left\langle n\right| \hat{\rho} \left|n\right\rangle \left|n\right\rangle \left\langle n\right| . \tag{10.16}$$

This operator commutes with the $\mathbb{Q}$ measurement and there is no operational way for Eve (or anyone else) to distinguish between directly measuring $\mathbb{Q}$ or measuring $\mathbb{Q}$ after first applying $\hat{\mathcal{D}}$. As such, we could imagine that we are in fact always applying $\hat{\mathcal{D}}$ to each run of the protocol[1]. To start with, since $\hat{\mathcal{D}}$ satisfies the definition of an entanglement breaking map [153], we may safely conclude that Eve's optimal strategy will not include any entanglement as there is no way for such entanglement to be noticeable. Moreover, if we consider any individual round of the protocol, we can write its purification as a mode E' held by Eve (including potentially all the other rounds of the protocol) in the Schmidt form $|\Psi_{E'E}\rangle = \sum_j \lambda_j \left|j\right\rangle_{E'} \left|j\right\rangle_E$ (with $|j\rangle$ not necessarily the Fock basis) and act $\hat{\mathcal{D}}$ upon it. This yields

$$\begin{aligned} (\mathbb{I} \otimes \hat{\mathcal{D}}) \left|\Psi_{E'E}\right\rangle \left\langle \Psi_{E'E}\right| &= \sum_{j,k} \lambda_j \lambda_k^* \left|j\right\rangle \left\langle k\right| \hat{\mathcal{D}}(\left|j\right\rangle \left\langle k\right|) \\ &= \sum_n \hat{\sigma}_{E'_n} \otimes \left|n\right\rangle \left\langle n\right| , \end{aligned} \tag{10.17}$$

[1]That is, the probabilities for any string of measurement outcomes $X^m = [x_1, x_2, .., x_m]$ satisfy $p(X^m) = \mathrm{tr}\{\hat{\rho}^m_{AE} \otimes_{\nu=1}^m \hat{X}(x_\nu)\} = \mathrm{tr}\{\hat{\sigma}^m_{AE} \otimes_{\nu=1}^m \hat{X}(x_\nu)\}$ where $\hat{\sigma}^m_{AE} = \otimes_{\nu=1}^m \hat{\sigma}_\nu$ with $\hat{\sigma}_\nu = \hat{\mathcal{D}}(\mathrm{tr}_{\bar{\nu}}\{\hat{\rho}^m_{AE}\})$. Note that $\mathrm{tr}_{\bar{\nu}}$ denotes the trace over all modes except the ν^{th} mode.

where $\hat{\sigma}_{E'_n} = \sum_{j,l,n} \lambda_l \lambda_j^* \langle n|l\rangle \langle j|n\rangle |l\rangle \langle j|$. This means that the most general state Eve can effectively prepare for the input mode E is of the form

$$\hat{\rho}_E = \sum_n p(n) |n\rangle \langle n| \ , \tag{10.18}$$

where $p(n) = \sum_j |\lambda_j \langle n|j\rangle|^2$. In other words, the input state for each run of the protocol is effectively just a mixture of Fock states (potentially classically correlated between rounds). Intuitively, one would imagine that the best strategy for Eve would be to choose a state such that $\{|j\rangle\}$ is indeed the Fock basis and, moreover, to make $p(n)$ simply a delta function at some fixed n.

We can show this as follows. Let $p^*(n)$ be the distribution of the optimal input state that maximises the probability of q^* and $\{c_n(q^*)\}$ be the Fock state coefficients for that element as given in Eq. (10.15). Then, Eve's optimal probability is given by

$$\begin{aligned} p_{\text{guess}} &= \text{tr}\{\hat{\rho}_{E'E}(\mathbb{I} \otimes \hat{Q}(q^*))\} \\ &= \sum_n p^*(n) c_n \leq \max_n c_n \times \sum_n p^*(n) = c_{n^*} \ , \end{aligned} \tag{10.19}$$

where we have defined n^* as the value that achieves the maximum. This optimal guessing probability would be saturated by choosing an input state $|n^*\rangle$, therefore the optimal input state is indeed a pure Fock state.

Note that the result extends straightforwardly to the case where the input state is restricted to have support only over a finite range of number states $[n_R^-, n_R^+]$. Let $p^*(n)$ be a probability distribution over $[n_R^-, n_R^+]$, x^* be the value of the most likely POVM element of the difference measurement given that input state and c_n be the

Fock state coefficients for that element as given in Eq. (10.9). Then

$$\begin{aligned} p_{\text{guess}} &= \text{tr}\{\hat{\rho}_{E'E}(\mathbb{I} \otimes \hat{X}(x^*))\} \\ &= \sum_{n_R^-}^{n_R^+} p^*(n) c_n \leq \max_{n \in [n_R^-, n_R^+]} c_n \times \sum_n p^*(n) = c_{n^*} \,. \end{aligned} \tag{10.20}$$

Therefore, the optimal input state is $|n\rangle$ with $n \in [n_R^-, n_R^+]$. This result can be independently applied to each run of the protocol (by including the other rounds in the purification, Eve has already been granted the option to utilise a sophisticated collective encoding), hence we can conclude that Eve's optimal probability to obtain a string of outcomes for all m rounds is to choose a single Fock state for each round.

□

Given Lemma 1, we now lower bound the min-entropy under the assumption that Eve's input state only has support over number states in the range $[n_R^-, \infty[$. Eve's guess for the difference measurement outcome will always be just the outcome of the most likely element of the difference element defined in Eq. (10.9). Thus, if we choose x^* to be the most probable outcome of the difference measurement (whatever that might be), then we can immediately conclude that for input states restricted to have support only over the range $[n_R^-, \infty[$, Eve's optimal strategy to maximise the occurrence of x^* (and hence her guessing probability) will be to input a number state $|n\rangle \in [n_R^-, \infty[$. In fact, it will be optimal to input the smallest number state $\left|n_R^-\right\rangle$. We have

$$\begin{aligned} p_{\text{guess}} &= \max_n \langle n| \hat{X}(x^*) |n\rangle \\ &\leq \max_{n \in [n_R^-, \infty[} 2^{-n} \binom{n}{\left\lfloor \frac{n+|x^*|}{2} \right\rfloor} \\ &= \max_{n \in [n_R^-, \infty[} 2^{-n} \binom{n}{\left\lfloor \frac{n}{2} \right\rfloor} \\ &= 2^{-n_R^-} \binom{n_R^-}{\left\lfloor \frac{n_R^-}{2} \right\rfloor}, \end{aligned} \tag{10.21}$$

where in the penultimate line, we used the fact that $\binom{n}{k}$ is maximal for $k = \lfloor \frac{n}{2} \rfloor$ and monotonically decreases for greater and smaller values of k, which means that the smallest allowed x will be optimal. In the final line, we used that $2^{-n}\binom{n}{\lfloor \frac{n+x}{2} \rfloor}$ decreases monotonically in n. To see this, first note that for n even $\lfloor \frac{n+1}{2} \rfloor = \lfloor \frac{n}{2} \rfloor$ and for n odd $\lfloor \frac{n+1}{2} \rfloor = \lfloor \frac{n}{2} \rfloor + 1$. Thus the ratio of successive terms is

$$\begin{aligned} \frac{2^{-(n+1)}\binom{n+1}{\lfloor \frac{n+1}{2} \rfloor}}{2^{-n}\binom{n}{\lfloor \frac{n}{2} \rfloor}} &= \frac{1}{2}(n+1)\frac{\lfloor \frac{n}{2} \rfloor!}{\lfloor \frac{n+1}{2} \rfloor!}\frac{\left(n - \lfloor \frac{n}{2} \rfloor\right)!}{\left(n+1-\lfloor \frac{n+1}{2} \rfloor\right)!} \\ &= \begin{cases} \frac{1}{2}(n+1)\frac{\left(n-\frac{n}{2}\right)!}{\left(n+1-\frac{n}{2}\right)!} = \frac{1}{2}\frac{(n+1)}{n+1-\frac{n}{2}} = \frac{n+1}{n+2} < 1\,, & n \text{ even} \\ \frac{1}{2}(n+1)\frac{\lfloor \frac{n}{2} \rfloor!}{(\lfloor \frac{n}{2} \rfloor+1)!} = \frac{1}{2}\frac{n+1}{\lfloor \frac{n}{2} \rfloor+1} = 1\,, & n \text{ odd} \end{cases} . \end{aligned} \tag{10.22}$$

Substituting this optimal guessing probability into the definition of the conditional min-entropy gives the expression in Eq. (10.12).

Now, we show that provided that in each round the certification measurement outcome is above a certain threshold n_C^-, the input to the randomness generation measurement is $\epsilon_{\text{fail,m}}$-indistinguishable from a state with support only over $[n_R^-, \infty[$. The worst case scenario would be that whenever Eve can distinguish the real state from one with restricted support, she learns the full measurement record. We can thus interpret this distinguishing probability as a lower bound to the failure probability for the whole protocol.

Specifically, we are interested in the probability where the certification measurement takes a value which passes our test $\mathcal{P}$ whilst simultaneously a smaller than desired number of photons goes to the randomness generation measurement, thereby representing a failure of the protocol. As such, we introduce a failure operator corresponding to there being n_R^- or fewer photons in mode R given n_C photons in mode C expressed as

$$\hat{F}(n_C, n_R^-) = \sum_{n_R=0}^{n_R^-} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle \langle n_C+n_R|_E \,. \tag{10.23}$$

The failure probability for Eve successfully cheating the test in a single round is then given by

$$\epsilon_{\text{fail}} = \max_{\hat{\rho}_E} \text{tr} \left\{ \hat{\rho}_E \sum_{n_C=n_C^-}^{\infty} \hat{F}(n_C, n_R^-) \right\} . \tag{10.24}$$

It is straightforward to see (and we show it in Sec. 10.4) that this probability is also explicitly the probability of passing the test, multiplied by the distinguishing probability between the real input to the randomness measurement, $\hat{\rho}_R$, and the closest state with support solely in the range $[n_R^-, \infty[$ as one would expect in a composably secure framework. Since $\hat{F}$ is once more diagonal in the photon number basis, we can again apply Lemma 1 to conclude that Eve's optimal strategy is achieved by a single number state $|n_E\rangle$. Substitution via Eq. (10.23) gives

$$\epsilon_{\text{fail}} \leq \max_{n_E} \sum_{\substack{n_C=\max\{n_C^-, \\ n_E-(n_R^--1)\}}}^{n_E} \frac{r_1^{n_C}(1-r_1)^{n_E-n_C} n_E!}{n_C!(n_E-n_C)!} . \tag{10.25}$$

The lower limit on n_C in the sum comes from the fact that for $n_E > n_C^- + n_R^- - 1$, the requirement for at least n_C^- photons at detector C is superseded by the requirement that there be less than n_R^- photons in mode R which implies $n_C > n_E - n_R^-$. In fact, we show that Eve's optimal input is to send precisely $n_E^{\text{opt}} = n_C^- + n_R^- - 1$ photons. The summand is a generic binomial distribution

$$\mathcal{B}(r_1, n_E, k) = \frac{r_1^k (1-r_1)^{n_E-k} n_E!}{k!(n_E-k)!} , \tag{10.26}$$

such that the failure probability in Eq. (10.25) can be seen as the complement of the binomial cumulative distribution function (CDF). For a fixed lower limit in the sum, the failure probability increases monotonically with n_E. However, once $n_E > n_C^- + n_R^- - 1$, the situation is more complicated because the limits of the sum change as well as the summand. Indeed, instead of running from n_C^- to n_E, it

will run from $n_C^- + 1$ to $n_E + 1$ as argued above. We now show that the difference between successive terms of the sum for all values n_E larger than this threshold is negative and thus the function is monotonically decreasing in n_E. Hence, it reaches its maximum for $n_E^{\text{opt}} = n_C^- + n_R^- - 1$.

For $n_E = n_C^- + n_R^- - 1$, we can write ϵ_{fail} for the corresponding successive input Fock states, $\Delta\epsilon_{\text{fail}}(n_E) \equiv \epsilon_{\text{fail}}(n_E + 1) - \epsilon_{\text{fail}}(n_E)$, as

$$\begin{aligned}
\Delta\epsilon_{\text{fail}}(n_E) &= \sum_{n_C=n_C^-+1}^{n_E+1} r_1^{n_C}(1-r_1)^{n_E+1-n_C}\binom{n_E+1}{n_C} - \sum_{n_C=n_C^-}^{n_E} r_1^{n_C}(1-r_1)^{n_E-n_C}\binom{n_E}{n_C} \\
&= \sum_{n_C=n_C^-+1}^{n_E} r_1^{n_C}(1-r_1)^{n_E-n_C}\left((1-r_1)\binom{n_E+1}{n_C} - \binom{n_E}{n_C}\right) \\
&+ r_1^{n_E+1} - r_1^{n_C^-}(1-r_1)^{n_E-n_C^-}\binom{n_E}{n_C^-} \\
&= \sum_{n_C=n_C^-+1}^{n_E} r_1^{n_C}(1-r_1)^{n_E-n_C}\left(-r_1 + \frac{n_C}{n_E-n_C+1}(1-r_1)\right)\binom{n_E}{n_C} \\
&+ r_1^{n_E+1} - r_1^{n_C^-}(1-r_1)^{n_E-n_C^-}\binom{n_E}{n_C^-}, \qquad (10.27)
\end{aligned}$$

where we used Pascal's identity $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$ and $\binom{n}{k-1} = \frac{k}{n+1-k}\binom{n}{k}$ in the last line.

Using the following result

$$\sum_{n_C=n_C^-}^{n_E}\binom{n_E}{n_C} = \binom{n_E}{n_C^-}\,{}_2F_1(1, n_C^- - n_E; n_C^- + 1; -1)\,, \qquad (10.28)$$

where ${}_2F_1$ is the hypergeometric function, it can be shown after some algebra that Eq. (10.27) simply reduces to

$$\epsilon_{\text{fail}}(n_E + 1) - \epsilon_{\text{fail}}(n_E) \;\leq\; -(1-r_1)^{n_E-n_C^-+1} r_1^{n_C^-}\binom{n_E}{n_C^-}\,, \qquad (10.29)$$

which is always negative for any n_C^-. Moreover, Eve adding extra photons will always result in deleting the lowest term in the summation in Eq. (10.25) so that the failure

probability monotonically decreases for all $n_E \geq n_C^- + n_R^- - 1$. Thus, the optimal value for Eve to maximise the failure probability is the single Fock state with photon number $n_E^{\text{opt}} = n_C^- + n_R^- - 1$. Substitution into Eq. (10.25) then gives

$$\begin{aligned} \epsilon_{\text{fail}} &\leq \sum_{n_C=n_C^-}^{n_E^{\text{opt}}} r_1^{n_C}(1-r_1)^{n_E^{\text{opt}}-n_C}\binom{n_E^{\text{opt}}}{n_C} \\ &\leq \exp\left(-2\frac{(n_C^- - r_1 n_E^{\text{opt}})^2}{n_E^{\text{opt}}}\right), \end{aligned} \tag{10.30}$$

where the last line is given by Hoeffding's inequality which states that for a binomial distribution $\mathcal{B}(r_1, n_E, k)$ with $n_C^- \geq n_E r_1$, one gets

$$\sum_{k=n_C^-}^{n_E} \mathcal{B}(r_1, n_E, k) \leq \exp\left(-2\frac{(n_C^- - r_1 n_E)^2}{n_E}\right). \tag{10.31}$$

Finally, the probability that any one of the m rounds fails is the complement that all of them pass thus

$$\epsilon_{\text{fail,m}} = 1 - (1-\epsilon_{\text{fail}})^m \leq 1 - (1 - m\epsilon_{\text{fail}}) = m\epsilon_{\text{fail}}, \tag{10.32}$$

which is precisely the result stated Eq. (10.13), thereby completing the proof.

Completeness: Substituting in the number state expansion for a coherent state $|\alpha\rangle$ and calculating the probability for the certification test to pass via Eq. (10.23) gives the desired result expressed in Eq. (10.14).

□

10.2 Modelling Detectors

Here, we remove the idealised assumptions from the previous section and present a detailed detector model.

10.2.1 Finite Range of Photodetectors

As a first idealisation, we shall remove the assumption of infinite dynamic range for the photodiodes. In fact, the detectors only respond linearly above and below certain photon numbers thresholds, namely $n_{\min}$ and $n_{\max}$. In reality, as the detectors enter this nonlinear regime, there will still be quantum randomness in their outcome statistics, but we take the worst case view and assume that all states with overly large or small photon numbers will be mapped with certainty to "end bins", thereby yielding no such randomness. Thus, instead of a sum over all photon number states, we model a photodetection with $L := n_{\max} - n_{\min} + 1$ measurement operators given by

$$\begin{aligned} \hat{N}(n_{\min}) &= \sum_{n=0}^{n_{\min}} |n\rangle\langle n| \,, \\ \hat{N}(n) &= |n\rangle\langle n| \,, \ \forall \ n_{\min} < n < n_{\max} \,, \\ \hat{N}(n_{\max}) &= \sum_{n=n_{\max}}^{\infty} |n\rangle\langle n| \,. \end{aligned} \tag{10.33}$$

This can make quite a difference to the output randomness since if Eve either inputs a sufficiently small or large number of photons, she can be sure that the lower or upper outcome will occur on detectors A and B, leading to a difference outcome of 0 with certainty. This can be seen directly by calculating the difference measurement POVM elements using finite range photodetectors as an operator in Eve's input Hilbert space as before to find

$$\hat{X}_{\text{fin}}(x) = \begin{cases} \sum_{n_A=n_{\min}+|x|}^{n_{\max}} \hat{M}(n_A, n_A - |x|) \,, & x \geq 0 \\ \sum_{n_A=n_{\min}+|x|}^{n_{\max}} \hat{M}(n_A - |x|, n_A) \,, & x < 0 \end{cases} \,, \tag{10.34}$$

where

$$\hat{M}(n_A, n_B) = \langle 0| \hat{U}_{BS_0}^{\dagger} \hat{N}(n_A) \otimes \hat{N}(n_B) \hat{U}_{BS_0} |0\rangle \,. \tag{10.35}$$

For states with an appropriate photon number support, a difference measurement made using finite range photodetectors will be virtually indistinguishable from the ideal difference measurement in Eq. (10.9). Specifically, if a number state $|n\rangle$ is input to a difference measurement with two detectors A and B that have linearity ranges $[n_{\min}, n_{\max}]$ such that $n_{\min} \ll n/2 \ll n_{\max}$, then the probability that either detector will register a number of photons outside its linear range will be given by the tails of a binomial distribution. It can then be checked whether this probability is smaller than the other failure probabilities in the protocol (typical realistic values will render it far smaller, i.e. $\propto 1 \times 10^{-30000}$). Alternatively, one can also directly empirically verify the linear response range $[n^D_{\min}, n^D_{\max}]$ of a difference measurement by inputting a known photonic laser source and observing that the difference variance indeed grows linearly when the laser's optical power is increased, as shown in Sec. 11.2.

This finite range of the photodetection also applies to the certification measurement in mode C using a finite range detector with linear range $[n^C_{\min}, n^C_{\max}]$ and $L_C = n^C_{\max} - n^C_{\min} + 1$ possible outcomes. We have

$$\begin{aligned} \hat{N}_{C,\text{fin}}(n^C_{\min}) &= \sum_{n_C=0}^{n^C_{\min}} \hat{N}_C(n_C)\,, \\ \hat{N}_{C,\text{fin}}(n_C) &= \hat{N}_C(n_C)\,, \ \forall\ n^C_{\min} < n_C < n^C_{\max}\,, \\ \hat{N}_{C,\text{fin}}(n^C_{\max}) &= \sum_{n_C=n^C_{\max}}^{\infty} \hat{N}_C(n_C)\,, \end{aligned} \tag{10.36}$$

where $\hat{N}_C(n_C)$ is given in Eq. (10.11).

Finally, we can also write the failure operator associated with this certification measurement. It will be similar to the ideal case in Eq. (10.23) except for the end bins. The failure of the protocol occurs when the test is passed and there are either too many (more than n^+_R) or too few (less than n^-_R) photons incident onto the

difference measurement. We obtain the following failure operator

$$\begin{aligned}
\hat{F}(n^C_{\min}, n^-_R, n^+_R) &= \sum_{n_C=0}^{n^C_{\min}} \left(\sum_{n_R=0}^{n^-_R} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle \langle n_C+n_R|_E \right. \\
&+ \left. \sum_{n_R=n^+_R+1}^{\infty} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle \langle n_C+n_R|_E \right) , \\
\hat{F}(n^C_{\max}, n^-_R, n^+_R) &= \sum_{n_C=n^C_{\max}}^{\infty} \left(\sum_{n_R=0}^{n^-_R} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle \langle n_C+n_R|_E \right. \\
&+ \left. \sum_{n_R=n^+_R+1}^{\infty} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle \langle n_C+n_R|_E \right) , \\
\hat{F}(n_C, n^-_R, n^+_R) &= \sum_{n_R=0}^{n^-_R} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle \langle n_C+n_R|_E \\
&+ \sum_{n_R=n^+_R+1}^{\infty} \frac{r_1^{n_C}(1-r_1)^{n_R}(n_C+n_R)!}{n_C! n_R!} |n_C+n_R\rangle \langle n_C+n_R|_E , \\
&\forall \quad n^C_{\min} < n_C < n^C_{\max} . \qquad (10.37)
\end{aligned}$$

10.2.2 Voltage Response and Temporal Behaviour

The next step in our modelling is to take into account the fact that the detector response is not completely flat over the time window that makes up one round of the protocol. Instead, the voltage response decays exponentially in time. However, using careful spectral filtering, one can enforce an effectively flat temporal distribution for incoming photons. Considering this, we show that we can model the voltage response with a single average conversion factor α.

In general, the detector response of a photodiode can be regarded as analogous to a RC circuit where the voltage at time T is given by

$$V(T) = \frac{1}{C} \int_0^{\infty} e^{-\tau/RC} I(T-\tau)\, d\tau , \qquad (10.38)$$

where $I(T-\tau)$ is the current generated by the absorbed photons. However, one

cannot take the above equation too literally since a genuinely continuous time dependence would correspond to a detector with infinite temporal resolution. Instead, we model a voltage detector as having K finite time intervals $\delta_t = T/K$ over which the response is flat (i.e. the detector cannot resolve temporal differences smaller than δ_t). The entire detection over the time window T can then be regarded as post-processing of the K outcomes arising from each of the detection intervals δ_t. This resulting POVM has elements of the form

$$\hat{M}(\mathbf{n}) = \hat{N}(n_1) \otimes \hat{N}(n_2)... \otimes \hat{N}(n_K)\,, \tag{10.39}$$

where $\mathbf{n} = [n_1, n_2, ...n_K]$. The voltage response to a photon arriving at the k^{th} interval is given by a conversion factor

$$\alpha_k := \beta e^{-(K-k)BW\delta_t}\,, \tag{10.40}$$

where β is a constant. The voltage POVM is thus expressed as

$$\hat{V}(v) = \sum_{\mathbf{n}} c_{n,k}(v)\hat{M}(\boldsymbol{n})\,, \tag{10.41}$$

with

$$c_{n,k}(v) \;\; = \;\; \delta(v - \mathbf{n}\boldsymbol{\alpha}^T)\,, \tag{10.42}$$

where $\boldsymbol{\alpha}^T = [\alpha_1, .., \alpha_k]^T$ and the sum is over all L^K possible values for $\mathbf{n}$.

In principle, this temporal detector response could open loopholes for Eve to exploit. For example, if she were able to generate extremely short time pulses, Eve could saturate individual detectors which would then be heavily damped in time (due to the exponential term in Eq. (10.40)), resulting in a certification voltage that would appear acceptable even though there would be no randomness in this case. However, these temporal attacks can be circumvented via an appropriate choice of

spectral filtering in the detection process. For transform-limited pulses, a sufficiently narrow spectral filter *enforces* an effectively flat temporal distribution for the detected photons. Since the source in our experiment is extremely narrowband (single frequency CW laser), we can afford to use a correspondingly narrow filter without altering the detection rates in our actual implementation. Note that a pulsed system which cannot afford to be similarly filtered without reducing the resulting count rates would require a careful analysis of the effects of Eve's temporal modulation of the source on the output statistics. This highlights the importance of considering *all* relevant physical degrees of freedom in certified randomness generation.

Considering our implementation, the voltage response of a detector to a photon arrival is given by a time averaged conversion factor

$$\alpha := \frac{hcBW\eta G}{\lambda}\,, \tag{10.43}$$

where h is Planck's constant, c is the speed of light, BW is the detector's bandwidth, η is its responsitivity (in $\mathrm{A\,W^{-1}}$) at the wavelength λ considered and G is the transimpedence gain.

10.2.3 Electronic Noise

So far, all measurements have been described without the presence of detector noise. As outlined in Sec. 9.2, our detector's noise λ is well modelled as being Gaussian with variance σ^2. We want to write down the POVM describing a voltage measurement over an appropriate basis as parameterised by its outcome. Given that the noisy measurement is still phase insensitive, the POVM elements can be written diagonally in the Fock basis as

$$\hat{V}^{\sigma}(v) = \sum_{n=n_{\min}}^{n_{\max}} \frac{e^{-(v-\alpha n)^2/(2\sigma^2)}}{\sqrt{2\pi}\sigma}\hat{N}(n)\,. \tag{10.44}$$

Consider the randomness generation measurement. Since the detector noise terms are taken to be independent from one another, we can equivalently combine them into a single overall noise variable λ_D with variance $\sigma_D^2 = \sigma_A^2 + \sigma_B^2$ (this joint variable is what was determined in practice during device calibration) that acts to smear out the ideal difference measurement to obtain[2]

$$\hat{V}_D^{\sigma_D}(v_D) = \sum_{x=-(L-1)}^{L-1} \frac{e^{-(v_D-\alpha_D x)^2/(2\sigma_D^2)}}{\sqrt{2\pi}\sigma_D} \hat{X}_{\text{fin}}(x)\,, \tag{10.45}$$

with $\hat{X}_{\text{fin}}(x)$ given by Eq. (10.34) but effectively by Eq. (10.9) for the photon ranges we will certify.

In addition, the certification measurement's POVM accounting for the Gaussian noise characterised by variance σ_C^2 is given by

$$\hat{V}_C^{\sigma_C}(v_C) = \sum_{n=n_{\min}^C}^{n_{\max}^C} \frac{e^{-(v_C-\alpha_C n_C)^2/(2\sigma_C^2)}}{\sqrt{2\pi}\sigma_C} \hat{N}_{C,\text{fin}}(n_C)\,. \tag{10.46}$$

Finally, for the failure operator associated with the certification measurement with Gaussian electronic noise, we have the following

$$\hat{V}_F^{\sigma_C}(v_C, n_R^-, n_R^+) = \sum_{n_C=n_{\min}^C}^{n_{\max}^C} \frac{e^{-(v_C-\alpha_C n_C)^2/(2\sigma_C^2)}}{\sqrt{2\pi}\sigma_C} \hat{F}(n_C, n_R^-, n_R^+)\,, \tag{10.47}$$

where α_C is the voltage conversion factor for the photodetector C and σ_C is the standard deviation of its associated electronic noise.

For the security analysis later, we will often be interested in the measurement operators from Eve's perspective who always knows the relevant value of λ. This

[2]For detectors with the same conversion factor α, a particular outcome at the detectors A and B would lead to a difference value $d = n_A - n_B + \lambda_A - \lambda_B = x + \lambda_D$ where we have combined the independent noise variables.

leads to a voltage POVM given by

$$\hat{V}(v) = \hat{N}\left(\frac{v-\lambda}{\alpha}\right), \tag{10.48}$$

a difference measurement

$$\hat{V}_D(v_D) = \hat{X}_{\text{fin}}\left(\frac{v_D-\lambda_D}{\alpha_D}\right), \tag{10.49}$$

a certification measurement

$$\hat{V}_C(v_C) = \hat{N}_{C,\text{fin}}\left(\frac{n_C-\lambda_C}{\alpha_C}\right), \tag{10.50}$$

and a failure operator associated with certification voltage measurement

$$\hat{V}_F(v_C, n_R^-, n_R^+) = \hat{F}\left(\frac{v_C-\lambda_C}{\alpha_C}, n_R^-, n_R^+\right). \tag{10.51}$$

10.2.4 Finite Resolution and Range of Oscilloscope and Analogue-to-Digital Converter

In the previous section, we modelled the detectors as having a finite range but otherwise being perfectly photon-number resolving and convolved with a classical noise variable subsequently given to the eavesdropper. In fact, the randomness generation measurement has a finite resolution which corresponds to an extra coarse graining. Specifically, the analogue-to-digital converter (ADC) which processes the voltage signal can only record a certain set range of voltages $[V_{\text{min}}, V_{\text{max}}]$, with all voltages greater or smaller than this amount registered as results in the "end bin". Furthermore, within the range $[V_{\text{min}}, V_{\text{max}}]$, voltages are only recorded with a finite resolution. Therefore, whilst an ideal voltage measurement might have unbounded and continuous values, a real detector in combination with an ADC with finite bits of resolution Δ_{ADC} outputs $J = 2^{\Delta_{\text{ADC}}}$ outcomes with corresponding POVM elements

$\{\hat{V}^{\sigma,\Delta_{\rm ADC}}(j)\}_j$ for the measured $j^{\rm th}$ bin expressed as

$$\hat{V}^{\sigma,\Delta_{\rm ADC}}(j) = \int_{I_j} \hat{V}^{\sigma}(v)\, dv\,, \tag{10.52}$$

where the integration regions are given by

$$\begin{aligned} &I_{\lfloor -(J-1)/2\rfloor} = [-\infty, V_{\rm min} + \delta V[, \quad I_{\lfloor -(J-1)/2+1\rfloor} = [V_{\rm min} + \delta V, V_{\rm min} + 2\delta V[, \ldots, \\ &I_0 = [-\delta V/2, \delta V/2[, \ldots, \quad I_{\lceil (J-1)/2\rceil} = [V_{\rm min} + (J-1)\delta V, \infty[\,, \end{aligned} \tag{10.53}$$

and $\delta V = \frac{V_{\rm max}-V_{\rm min}}{2^{\Delta_{\rm ADC}}}$ is the effective voltage resolution induced by $\Delta_{\rm ADC}$.

As a result, the coarse grained noisy difference measurement operators are given by $\{\hat{V}_D^{\sigma_D,\Delta_{\rm ADC}}(j)\}_j$ for which

$$\hat{V}_D^{\sigma_D,\Delta_{\rm ADC}}(j) = \int_{I_j^D} \hat{V}_D^{\sigma_D}(v_D)\, dv_D\,. \tag{10.54}$$

The corresponding difference measurement from Eve's perspective (i.e. given the relevant λ) would be

$$\begin{aligned} \hat{V}_D^{\Delta_{\rm ADC}}(j) &= \int_{I_j^D - \lambda_D} \hat{V}_D(v_D)\, dv_D \\ &= \sum_{x\in\mathcal{X}} \hat{X}_{\rm fin}(x)\,, \end{aligned} \tag{10.55}$$

where

$$\mathcal{X} = \{x : \alpha_D x + \lambda_D \in I_j^D\}\,. \tag{10.56}$$

The certification voltage measurement is recorded by an ADC with the same resolution and consequently it is still a J-outcome measurement but over an ADC range $[V_{\rm min}^C, V_{\rm max}^C]$ and a corresponding voltage resolution $\delta V_C = \frac{V_{\rm max}^C - V_{\rm min}^C}{2^{\Delta_{\rm ADC}}}$. This leads to intervals I_i^C which are defined as per Eq. (10.53) and coarse-grained certification

measurements elements

$$\hat{V}_C^{\sigma_C,\Delta_{\text{ADC}}}(i) = \int_{I_i^C} \hat{V}_C^{\sigma_C}(v_C)\, dv_C\,. \tag{10.57}$$

Moreover, the associated failure operator is

$$\hat{V}_F^{\sigma_C,\Delta_{\text{ADC}}}(i, n_R^-, n_R^+) = \int_{I_i^C} \hat{V}_F^{\sigma_C}(v_C, n_R^-, n_R^+)\, dv_C\,. \tag{10.58}$$

For a fixed value of the noise variable λ_C, we have the following failure operator from Eve's perspective

$$\begin{aligned} \hat{V}_F^{\Delta_{\text{ADC}}}(i, n_R^-, n_R^+) &= \int_{I_i^C - \lambda_C} \hat{V}_F(v_C, n_R^-, n_R^+)\, dv_C \\ &= \sum_{n_C \in \mathcal{C}} \hat{F}(n_C, n_R^-, n_R^+)\,, \end{aligned} \tag{10.59}$$

where

$$\mathcal{C} = \{n_C : \alpha_C n_C + \lambda_C \in I_i^C\}\,. \tag{10.60}$$

In general, one must be mindful of the interplay between the conversion from photon number to voltage and the final voltage resolution. Indeed, if the signal were to experience strong attenuation (very small α), then the voltage distribution would start to become small with respect to the fixed voltage resolution and the entropy would decrease. In our implementation, we carefully kept track of the coarse graining, thus avoiding such issue.

Before we proceed further, we show in Fig. 10.1 a schematic drawing summarising our detector's model. The POVMs present in the figure are those specified in this section.

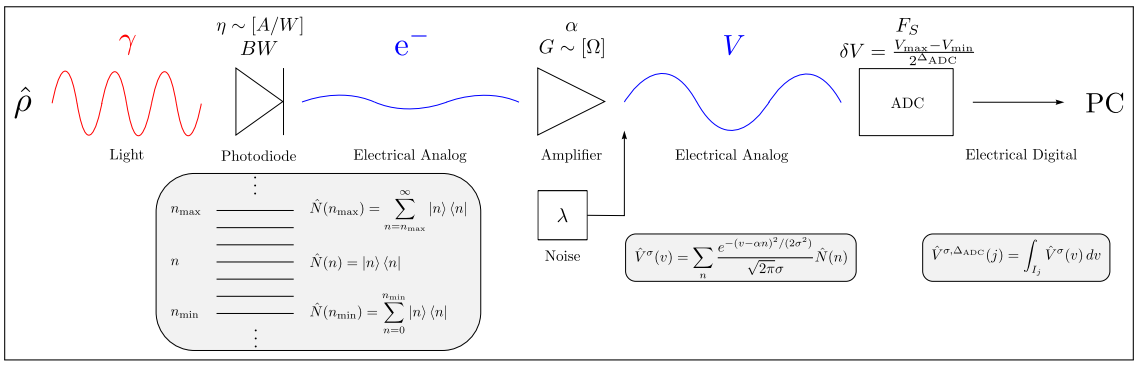


Figure 10.1: Detector model. Photons from a photonic state $\hat{\rho}$ impinge onto a photodiode whose linear range and equivalent L photon projectors are given in Eq. (10.33). The photodiode's voltage response is given by the conversion factor α expressed in Eq. (10.40) in general and Eq. (10.43) in our case. This factor incorporates the photodiode's bandwidth BW, its responsitivity η (in $\mathrm{A\,W^{-1}}$) and the transimpedence gain G. Noise characterised by a Gaussian random variable λ is then added onto the voltage, leading to the voltage POVM in Eq. (10.44). Finally, the voltage is discretised by an ADC with resolution δV and at a sampling rate F_S, yielding the POVM associated with the measurement of the j^{th} voltage bin expressed in Eq. (10.52). Light has been effectively converted from photons to a digital electrical signal which one can subsequently read on a PC or oscilloscope.

10.3 Proof of the Main Theorem

In this section, we provide the full security proof for the more realistic QRG protocol carried out in the experiment. As per the idealised protocol, the proof proceeds in two steps. First, we calculate the worst-case min-entropy for a certain class of states, namely those with a limited support over Fock states. Secondly, we calculate the failure probability of the protocol which is the maximum probability that a state not in that class could have passed the certification test. We rewrite theorem 1 given in Sec. 9.2 and proceed with our proof.

Theorem 3. *An optical setup consisting of*

- *Two trusted vacuum modes*
- *Two beam splitters of reflectivity* $r_0 = \frac{1}{2}$ *and* r_1
- *Two noisy photodetectors used to make a difference measurement as described in Eq. (10.54)*

- *A third noisy photodetector used to make a certification measurement as described in Eq. (10.57) which passes the test $\mathcal{P}$ if i falls in a chosen range $[i_-, i_+]$*

can be used as a certified (m,κ,$\epsilon_{\text{fail,m}}$,ϵ_c)-randomness generation protocol as per Definition 2 without making any assumptions about the photonic source with

$$\kappa \geq -m \log_2 \left(\sum_{x \in \mathcal{X}} 2^{-n_R^-} \binom{n_R^-}{\lfloor \frac{n_R^- + x}{2} \rfloor} \right) , \tag{10.61}$$

where

$$\mathcal{X} \in \mathbb{N} \cap \left[-\left\lfloor \frac{\delta V}{2\alpha_D} \right\rfloor , \left\lfloor \frac{\delta V}{2\alpha_D} \right\rfloor \right] , \tag{10.62}$$

with $\delta V = \frac{V_{\max} - V_{\min}}{2^{\Delta_{\text{ADC}}}}$,

$$\epsilon_{\text{fail,m}} \leq m \epsilon_{\text{fail}} , \tag{10.63}$$

where

$$\epsilon_{\text{fail}} = \max\{\epsilon_-, \epsilon_+\} + \epsilon_{\lambda_C} , \tag{10.64}$$

with

$$\begin{aligned}
\epsilon_- &= \exp\left(-2 \frac{\left(\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} - r_1 \left(\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1 \right) \right)^2}{\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1} \right) , \\
\epsilon_+ &= \exp\left(-2 \frac{\left(n_R^+ - (1 - r_1) \left(\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1 \right) \right)^2}{\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1} \right) , \\
\epsilon_{\lambda_C} &= 1 - \text{erf}\left(\frac{\tilde{\lambda}}{\sqrt{2}\sigma_C} \right) ,
\end{aligned} \tag{10.65}$$

provided n_R^+ is set to the saturating photon number of the difference measurement.

Moreover,

$$\epsilon_c = 1 - \mathrm{tr}\left\{ \sum_{i=i_-}^{i_+} |\alpha\rangle \langle\alpha| \hat{V}_C^{\sigma_C, \Delta_{\mathrm{ADC}}}(i) \right\} , \tag{10.66}$$

using a coherent state $|\alpha\rangle$ as an input.

Proof. **Security:** Consider the task of guessing the difference measurement from the perspective of Eve who knows λ_D on a shot-by-shot basis, which is given by Eq. (10.55). First, this measurement satisfies the conditions of Lemma 1 and so Eve's optimal state is a number state. Her strategy will be to add λ_D to the most likely value of the noiseless difference measurement which, as shown in Sec. 10.1, is 0 or 1 depending upon whether Eve inputs an odd or even number of photons. Therefore, Eve's best guess will be the voltage bin I_j^D with $j = \left[\frac{\lambda_D}{\delta V}\right]$ or $j = \left[\frac{(1+\lambda_D)}{\delta V}\right]$, where [.] is the nearest integer rounding function. The guessing probability is given by the sum of all the probabilities associated with the outcomes $\hat{X}(x)$ for which Eve's guess would remain true. This can be expressed as the following set

$$\mathcal{X} \;=\; \{x \in [-(L-1), L-1] : \;\; \alpha_D x + \lambda_D \in I_j^D\} . \tag{10.67}$$

For states restricted to the range $[n_R^-, n_R^+]$, the guessing probability corresponds to

$$p_{\mathrm{guess}} \;=\; \max_{n \in [n_R^-, n_R^+]} \langle n| \sum_{x \in \mathcal{X}} \hat{X}(x) |n\rangle , \tag{10.68}$$

where again the sum only includes even (odd) values of x when n is even (odd).

From the expressions above, the interplay between the voltage conversion factor α_D and the voltage resolution δV becomes clear. The number of difference measurement elements that will be mapped to a given voltage bin is given by $\left\lceil \frac{\delta V}{\alpha_D} \right\rceil$,

such that as α_D becomes smaller, this number grows and Eve's guessing probability will increase. Since we will only consider number states within the linear regime of the difference measurement (i.e. $n_R^+ = n_{\max}$), we can safely assert that $\langle n| \hat{X}(x) |n\rangle = 2^{-n}\binom{n}{\lfloor \frac{n+x}{2} \rfloor}$ is a binomial distribution. Thus, the largest guessing probability for a given n will occur when λ_D is such that the $\left\lceil \frac{\delta V}{\alpha_D} \right\rceil$ bins are centered evenly around the origin, i.e. the middle portion of the binomial distribution. Moreover, we know from Sec. 10.1 that the guessing probability will decrease monotonically with the photon number. This yields

$$p_{\text{guess}} \leq \sum_{x \in \mathcal{X}} 2^{-n_R^-} \binom{n_R^-}{\lfloor \frac{n_R^- + x}{2} \rfloor}, \tag{10.69}$$

which is exactly Eq. (10.61). While this expression can be directly evaluated numerically, for large n_R^- (recall here that $n_R^- > 10^5$), one can use the Gaussian distribution as an excellent approximation for the binomial distribution and evaluate the sum as an integral to get the following compact expression

$$p_{\text{guess}} \leq \frac{1}{2}\left(\operatorname{erf}\left(\frac{\frac{\delta V}{2\alpha_D}}{\sqrt{\frac{n_R^-}{4}}}\right) - \operatorname{erf}\left(\frac{-\frac{\delta V}{2\alpha_D} - 1}{\sqrt{\frac{n_R^-}{4}}}\right)\right). \tag{10.70}$$

The failure probability for the protocol is given by the probability of passing the test even though a state with too few, or too many, photons is incident onto the difference measurement in mode R. We can express the probability of Eve successfully cheating in a single round as

$$\begin{aligned} \epsilon_{\text{fail}} &= \max_{\hat{\rho}_E} \Pr\left[i^- \leq i \leq i^+ \wedge n_R \notin [n_R^-, n_R^+]\right] \\ &= \max_{\hat{\rho}_E} \operatorname{tr}\left\{\hat{\rho}_E \sum_{i=i^-}^{i^+} \hat{V}_F^{\sigma_C, \Delta_{\text{ADC}}}(i, n_R^-, n_R^+)\right\} \\ &= \max_{n_E} \operatorname{tr}\left\{|n_E\rangle\langle n_E| \sum_{i=i^-}^{i^+} \hat{V}_F^{\sigma_C, \Delta_{\text{ADC}}}(i, n_R^-, n_R^+)\right\}, \end{aligned} \tag{10.71}$$

where in the last we line we used the fact that $\hat{V}_F$ satisfies the conditions of Lemma

1, implying that Eve's optimal input state will be a number state.

To begin with, let us consider this probability given a particular value for λ_C, the detector's noise variable. Then, from Eve's perspective, this electronic noise λ_C is effectively removed as expressed in Eq. (10.59) and we have

$$\begin{aligned}
\epsilon_{\text{fail}} &= \max_{n_E} \operatorname{tr}\left\{ |n_E\rangle\langle n_E| \sum_{n_C=n_C^-}^{n_C^+} \hat{F}(n_C, n_R^-, n_R^+) \right\} \\
&= \max_{n_E} \operatorname{tr}\left\{ |n_E\rangle\langle n_E| \sum_{n_C=n_C^-}^{n_C^+} \left(\sum_{n_R=0}^{n_R^-} \mathcal{B}(r_1, n_C+n_R, n_C) \, |n_C+n_R\rangle\langle n_C+n_R|_E \right.\right. \\
&+ \left.\left. \sum_{n_R=n_R^++1}^{\infty} \mathcal{B}(r_1, n_C+n_R, n_C) \, |n_C+n_R\rangle\langle n_C+n_R|_E \right) \right\} \\
&= \max_{n_E} \left\{ \sum_{n_C=\max\{n_C^-, n_E-(n_R^--1)\}}^{\min\{n_C^+, n_E\}} \mathcal{B}(r_1, n_E, n_C) \right. \\
&+ \left. \sum_{n_R=\max\{n_R^+, n_E-(n_C^++1)\}}^{n_E} \mathcal{B}(1-r_1, n_E, n_R) \right\}, \qquad (10.72)
\end{aligned}$$

where $n_C^- = \min_{n_C}\{n_C : \alpha_C n_C + \lambda_C \in I^C_{[i^-,i^+]}\}$ and $n_C^+ = \max_{n_C}\{n_C : \alpha_C n_C + \lambda_C \in I^C_{[i^-,i^+]}\}$ with $I^C_{[i^-,i+]}$ being the entire voltage range for which the test $\mathcal{P}$ is passed.

Let $v_i^{\pm} = \delta V(i \pm \frac{1}{2})$ be the smallest and largest voltages corresponding to bin i. Therefore, the minimum (maximum) voltage consistent with passing the test is $v_{i_-}^-$ ($v_{i_+}^+$). The corresponding minimum and maximum photon numbers are

$$\begin{aligned}
n_C^- &= \frac{v_{i_-}^- - \lambda_C}{\alpha_C}, \\
n_C^+ &= \frac{v_{i_+}^+ - \lambda_C}{\alpha_C}. \qquad (10.73)
\end{aligned}$$

We can use our knowledge of the detector's noise distribution to turn these into worst case upper and lower bounds for n_C^+ and n_C^-, respectively. Recalling that λ_C

is Gaussian with variance σ_C^2, we can say that except with a probability

$$\epsilon_{\lambda_C} = 1 - \mathrm{erf}\left(\frac{\tilde{\lambda}}{\sqrt{2}\sigma_C}\right), \tag{10.74}$$

one has $|\lambda_C| < \tilde{\lambda}$. This gives

$$\begin{aligned} n_C^- &\geq \frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C}, \\ n_C^+ &\leq \frac{v_{i_+}^+ + \tilde{\lambda}}{\alpha_C}. \end{aligned} \tag{10.75}$$

Next, the varying limits in the sums of Eq. (10.72) can be explained as follows. For the first sum, an unconditional lower limit is given by n_C^-. However, for sufficiently large inputs n_E, this requirement is superseded by the constraint that $n_R < n_R^-$, which in turn necessitates that $n_C \geq n_E - (n_R^- - 1)$. The upper limit simply comes from the fact that if $n_E < n_C^+$, then the binomial distribution can only run up to n_E. For the second sum, we have an unconditional constraint $n_R > n_R^+$, however again for sufficiently large n_E, the requirement that $n_C < n_C^-$ implies that we must have $n_R > n_E - (n_C^+ + 1)$. Notice that depending upon the bounds for n_C^+ and n_C^-, there are certain values of n_E for which the first or second sums may vanish. This turns out to be the case here (i.e. for our values only one of the sums will be non-zero at a time).

The first sum in Eq. (10.72) will vanish whenever $n_E > n_C^+ + n_R^- - 1 \geq \frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^- - 1$ and the second when $n_E < n_R^+$. In summary, as long as

$$\begin{aligned} n_R^+ &> \frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^- - 1 \\ \Rightarrow \tilde{\lambda} &\leq v_{i^+}^+ - \alpha_C\left(n_R^+ - n_R^- + 1\right), \end{aligned} \tag{10.76}$$

it implies that there are no values of n_E for which both sums will be simultaneously

nonzero. In our case, this condition evaluates to

$$|\tilde{\lambda}| \leq 1.155\,. \tag{10.77}$$

We will always be making a much tighter probabilistic bound on $\tilde{\lambda}$ such that Eq. (10.76) is satisfied at all times. Substitution in Eq. (10.74) indicates that this will be true except with probability $10^{-3769921}$, which is far below the other failure probabilities that we certify.

Except with probability ϵ_{λ_C}, we can then write the single round failure probability as

$$\begin{aligned}\epsilon'_{\text{fail}} \;=\; \max\Bigg\{ &\max_{n_E} \sum_{n_C=\max\{n_C^-,n_E-(n_R^--1)\}}^{\min\{n_C^+,n_E\}} \mathcal{B}(r_1,n_E,n_C), \\ &\max_{n_E} \sum_{n_R=\max\{n_R^+,n_E-(n_C^++1)\}}^{n_E} \mathcal{B}(1-r_1,n_E,n_R)\Bigg\}\,. \end{aligned} \tag{10.78}$$

Considering the first term, we have

$$\max_{n_E} \sum_{n_C=\max\{n_C^-,n_E-(n_R^--1)\}}^{\min\{n_C^+,n_E\}} \mathcal{B}(r_1,n_E,n_C) \leq \max_{n_E} \sum_{n_C=\max\{n_C^-,n_E-(n_R^--1)\}}^{n_E} \mathcal{B}(r_1,n_E,n_C)\,. \tag{10.79}$$

This expression is exactly the same as Eq. (10.25) for which we already know that $n_E^{\text{opt}} = n_C^- + n_R^- - 1$. Therefore, we can apply Hoeffding's bound to the binomial cumulative distribution to obtain

$$\begin{aligned}\max_{n_E} \sum_{n_C=n_C^-}^{n_E} \mathcal{B}(r_1,n_E,n_C) \;&\leq\; \exp\left(-2\frac{(n_C^- - r_1(n_C^-+n_R^--1))^2}{n_C^-+n_R^--1}\right) \\ &\leq\; \exp\left(-2\frac{\left(\frac{v_{i\_}^- - \tilde{\lambda}}{\alpha_C} - r_1\left(\frac{v_{i\_}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1\right)\right)^2}{\frac{v_{i\_}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1}\right), \end{aligned} \tag{10.80}$$

provided there exists a n_R^- such that $n_R^- > \frac{1-r_1}{r_1}\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C}$.

The second term in the maximisation is again just the cumulative tail of a binomial distribution and via the same argument as in Eq. (10.25), we know that Eve should choose $n_E^{\text{opt}} = n_R^+ + n_C^+ + 1$ to maximise this term, giving

$$\begin{aligned}\sum_{n_R=n_R^+}^{n_E} \mathcal{B}(1-r_1, n_E, n_R) &\leq \exp\left(-2\frac{(n_R^+ - (1-r_1)(n_C^+ + n_R^+ + 1))^2}{n_C^+ + n_R^+ + 1}\right) \\ &\leq \exp\left(-2\frac{\left(n_R^+ - (1-r_1)\left(\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1\right)\right)^2}{\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1}\right), \quad (10.81)\end{aligned}$$

provided there exists $n_R^+ > \frac{1-r_1}{r_1}\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C}$.

Thus, the total failure probability for one round of the protocol is given by

$$\begin{aligned}\epsilon_{\text{fail}} &= \epsilon'_{\text{fail}} + \epsilon_{\lambda_C} \\ &= \max\left\{\exp\left(-2\frac{\left(\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} - r_1\left(\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1\right)\right)^2}{\frac{v_{i_-}^- - \tilde{\lambda}}{\alpha_C} + n_R^- - 1}\right),\right. \\ &\qquad \left.\exp\left(-2\frac{\left(n_R^+ - (1-r_1)\left(\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1\right)\right)^2}{\frac{v_{i_+}^+ - \tilde{\lambda}}{\alpha_C} + n_R^+ + 1}\right)\right\} \\ &+ 1 - \text{erf}\left(\frac{\tilde{\lambda}}{\sqrt{2}\sigma_C}\right). \quad (10.82)\end{aligned}$$

which is exactly Eq. (10.65), thereby completing the proof.

Completeness: Lastly, the argument for completeness is the same as that in Sec. 10.1.

□

10.4 Mathematical Details

Here, we are interested in the photon number distribution of $\hat{\rho}_R^{\text{pass}}$, the state input to the randomness generation measurement that passes the test $\mathcal{P}$ given that we observe $n_C > n_C^-$. We can precisely quantify the extent to which $\hat{\rho}_R^{\text{pass}}$ is operationally indistinguishable from a state $\hat{\sigma}_{n_R^-}$ with support over $[n_R^-, \infty[$ by calculating the trace distance to the closest such state. Since the trace distance determines the maximum probability that Eve can distinguish the two situations, as mentioned above, we can interpret this quantity as the upper bound on the probability that the protocol fails and the min-entropy is not lower bounded by Eq. (10.12). Thus, recalling that without loss of generality, we can take both states to be diagonal in the Fock basis such that the trace distance is effectively calculated between classical probability distributions. We obtain the following expression

$$\begin{aligned}
\frac{\epsilon_{\text{fail}}}{p_{\text{pass}}} &\leq \max_{\hat{\rho}_E} \frac{1}{2} ||\hat{\rho}_R^{\text{pass}} - \hat{\sigma}_{n_R^-}||_1 \\
&= \max_{\hat{\rho}_E} \sum_{n_R=0}^{n_R^-} \langle n_R | \hat{\rho}_R^{\text{pass}} | n_R \rangle \\
&= \max_{\hat{\rho}_E} \sum_{n_C=n_C^-}^{\infty} \sum_{n_R=0}^{n_R^-} \text{tr}\{\hat{\rho}_E \hat{M}(n_C, n_R)\} \\
&= \max_{\hat{\rho}_E} \text{tr} \left\{ \hat{\rho}_E \sum_{n_C=n_C^-}^{\infty} \hat{F}(n_C, n_R^-) \right\} ,
\end{aligned} \tag{10.83}$$

where the maximisation is taken over Eve's input to the certification measurement, $||\cdot||_1$ is the trace norm and p_{pass} is the probability to pass the certification test. This can also be simply understood as the joint probability for detecting n_C^- or more photons in mode C and less than n_R^- in mode R and it is the same as Eq. (10.24), as claimed in Sec. 10.1.

10.5 SDI Quantum Random Number Expansion

The certified QRG either aborts or, except with some failure probability $\epsilon_{\text{fail,m}}$, produces an output X with a min-entropy $H_{\min}(X|E) \geq \kappa > 0$ with respect to any third party, even one with complete control over the photonic source and access to all other environmental modes. However, the final goal of a randomness expansion protocol is to utilise an initial random seed in order to generate a much longer bit string that is "ϵ-close" (in some well chosen metric) to perfectly uniformly distributed and unpredictable with respect to any third party. This can be achieved via randomness extraction (also sometimes called privacy amplification), which is a judiciously chosen post-processing of the measurements. We would also like to be confident that a realistic implementation of the protocol will succeed with high probability. Without loss of generality, the output state S of this post-processing can be written as a classical-quantum state

$$\hat{\rho}_{SE} = \sum_s P_S(s) \left|s\right\rangle \left\langle s\right| \otimes \hat{\rho}_E^s \,, \tag{10.84}$$

for which we have the following definition.

Definition 3. *A protocol that outputs a state of the form in Eq. (10.84) is*

- ***Security:*** *ϵ_s-secure (or sound) if*

$$p_{\text{pass}} \frac{1}{2} ||\hat{\rho}_{SE} - \hat{\tau}_S \otimes \hat{\sigma}_E||_1 \leq \epsilon_s \,, \tag{10.85}$$

  where p_{pass} is the probability that the certification test is passed, $||\cdot||_1$ is the trace norm and $\hat{\tau}_S$ is the uniform (i.e. maximally mixed) state over S. This means that there is no device or procedure that can distinguish between the actual protocol and an ideal protocol with probability higher than ϵ_{s}.

- ***Completeness:*** *ϵ_c-complete (or robust) if there exists an honest implementation such that $1 - p_{\text{pass}} \leq \epsilon_c$.*

The properties of the trace norm ensure that randomness satisfying Definition 3 is composable, which is critical for cryptographic applications [154].

Particular care must be taken against quantum adversaries to choose an extractor that has provable security when considering potentially quantum side information. In general, quantum-secure randomness extraction can be seen as a function $\text{Ext} : \{0,1\}^{m\Delta_{\text{ADC}}} \times \{0,1\}^d \rightarrow \{0,1\}^l$ that involves processing the m-bit measurement outcomes along with a random d-bit seed to produce an l-bit output that is ϵ-close to being perfectly random.

A very attractive choice is two-universal hashing[3] (or leftover hashing) which is secure against quantum adversaries [150, 155] and can be implemented efficiently as it achieves an excellent trade-off between ϵ and l. It should be noted that this extractor still requires a perfectly random seed of length d and thus any protocol that makes use of leftover hashing can technically only be regarded as a randomness expansion protocol [156, 157]. Whilst the length of the seed must be chosen proportional to m, it only has to be generated once and can be safely reused to hash arbitrarily many blocks, meaning that the initial random seed can be used to generate an unbounded amount of randomness. This also means that the seed can be hard-coded into the hashing device (for a further discussion and an explicit implementation, see [152]). Other quantum-secure methods, such as the Trevisan extractor, are more efficient in the length of the required seed. However, this is a more computationally expensive process and cannot currently be performed at speeds at which our protocol can generate raw randomness. Thus, to achieve bit-generation rates of the same speed as the randomness generation rates reported here, it seems necessary to perform randomness extraction via leftover hashing.

We now have the tools to write down the following result for certified randomness expansion. Although this is essentially a repeat of standard techniques (see e.g.

[3]Let X, S be sets of finite cardinality $|S| \leq |X|$. A family of hash functions $\{\mathcal{F}\}$ is a set of functions $f : X \rightarrow S$ and is called *two-universal* if for f drawn uniformly at random from $\mathcal{F}$, it holds that $\forall, (x, x') \in X$, $x \neq x'$, $\Pr[(f(x) = f(x')] \leq \frac{1}{|S|}$. The purpose of the random seed d is to pick a function uniformly at random, hence $d = \log_2 |\mathcal{F}|$.

[155, 152]) adapted to our specific setup, we state it as a standalone theorem for completeness.

Theorem 4. *A certified SDI (m,κ,$\epsilon_{\text{fail,m}}$,ϵ_c)-randomness generation protocol as defined in Definition 2 can be processed with a randomness generation seed of length m via leftover hashing to produce a certified SDI random string of length*

$$l \;=\; \kappa + 2 - \log_2 \frac{1}{\epsilon_{\text{hash}}^2}\,, \tag{10.86}$$

that is ϵ_c-complete and $\epsilon_{\text{hash}} + \epsilon_{\text{fail,m}}$ secure.

Proof. **Security:** Let X be the variable describing the measurement outcomes. Recall that the output of the randomness generation protocol after the measurement including the potential side information can be written as a classical-quantum state

$$\hat{\rho}_{XE} = \sum_{x\in\mathcal{X}} P_X(x)\,|x\rangle\langle x| \otimes \hat{\rho}_E^x\,, \tag{10.87}$$

where $\mathcal{X}$ is the alphabet of possible measurement outcomes and $\hat{\rho}_E^x$ is the state of the eavesdropper given the outcome x. A randomly chosen leftover hashing function is then applied to distill a final random string denoted by the variable S. The joint state is now

$$\hat{\rho}_{SE} = \sum_{s} P_S(s)\,|s\rangle\langle s| \otimes \hat{\rho}_E^s\,. \tag{10.88}$$

We then apply the Leftover Hash Lemma with quantum side information [155] and its extension to infinite dimensional Hilbert spaces [158, 159] which is necessary for our purposes.

Lemma 2. *Let $\hat{\rho}_{XE}$ be a state of the form in Eq. (10.87) where X is defined over a discrete-valued and finite alphabet and E is a finite or infinite dimensional system. If one applies a hashing function drawn at random from a family of two-universal*

hash functions that maps X to S and generates a string of length l, then

$$\frac{1}{2}||\hat{\rho}_{SE} - \hat{\tau}_S \otimes \hat{\sigma}_E||_1 \leq \sqrt{2^{l - H_{\min}(X|E) - 2}}\,, \tag{10.89}$$

where $H_{\min}(X|E)$ is the conditional smooth min-entropy (with smoothing parameter $\epsilon = 0$) of the raw measurement data given Eve's quantum system.

Comparing the security definitions in Eq. (10.85) and Eq. (10.89), we note that with an appropriate choice of l, we can ensure the security condition is met. In particular, we see that the smooth min-entropy is a lower bound on the extractable key length. To get a more exact expression, first notice that if we choose

$$l \;=\; H_{\min}(X|E) + 2 - 2\log_2\left(\frac{p_{\text{pass}}}{\epsilon_{\text{hash}}}\right), \tag{10.90}$$

for some $\epsilon_{\text{hash}} > 0$, then the right hand side of Eq. (10.89) becomes $\epsilon_{\text{hash}}/p_{\text{pass}}$. Then, provided we have definitively bounded the smooth min-entropy, we will satisfy Eq. (10.85) for any $\epsilon_{\text{hash}} > 0$. Finally since $\log_2(p_{\text{pass}}) < 0$, we have

$$l \geq H_{\min}(X|E) + 2 - \log_2\left(\frac{1}{\epsilon_{\text{hash}}^2}\right). \tag{10.91}$$

Now, suppose that we are only able to bound the smooth min-entropy $H_{\min}(X|E) \geq \kappa$ with a certain probability $1 - \epsilon_{\text{fail,m}}$ as is the case here. Then, the convexity and boundedness of the trace distance implies that this string of length l will be ϵ_s-secure for any security parameter

$$\epsilon_s \geq \epsilon_{\text{hash}} + \epsilon_{\text{fail,m}}\,, \tag{10.92}$$

if the length is chosen as per Eq. (10.86).

Completeness: This follows immediately from the completeness of the certified randomness generation protocol. □

Chapter 11

Experiment

'Cowards die many times before their deaths;
The valiant never taste of death but once.
Of all the wonders that I yet have heard,
It seems to me most strange that men should fear;
Seeing that death, a necessary end,
Will come when it will come.'
Caesar in Shakespeare's "Julius Caesar"

In this chapter, the experimental setup used in the research undertaken is presented. Furthermore, preliminary results leading to the main results are shown.

11.1 Experimental Setup

The experimental setup is displayed in Fig. 11.1 and consists of a fully fibre-connected architecture with commercially available components.

The light source utilised is a continuous wavelength (CW) laser (Koheras Adjustik E15) at telecom wavelength $\lambda = 1550\,\text{nm}$. Note that the source's linewidth is less than 100 Hz, thereby ensuring it to be effectively single-frequency. The laser output is directed onto a fibre optical isolator (Thorlabs IO-H-1550APC) in order to

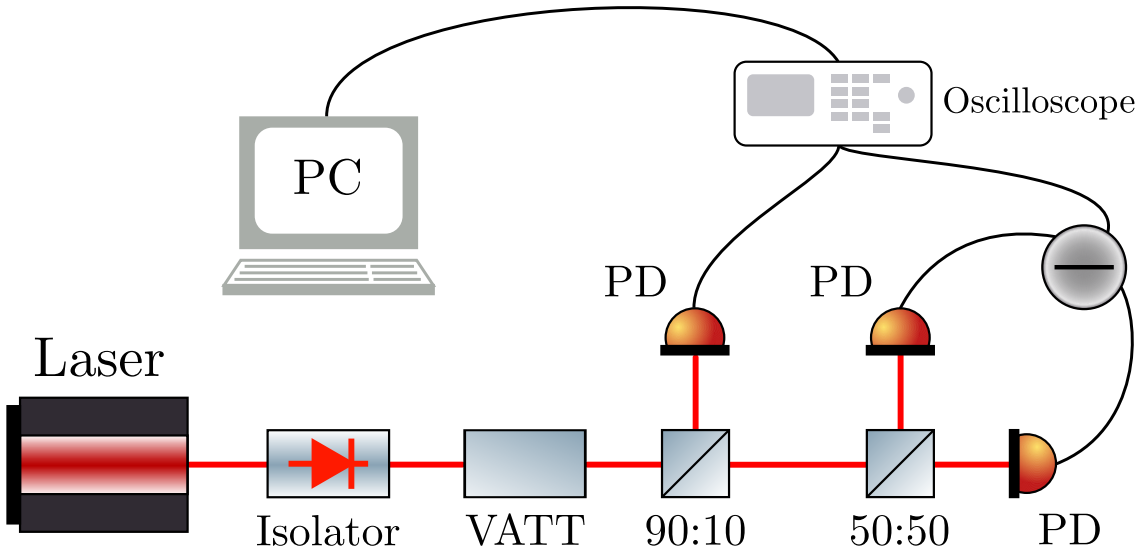


Figure 11.1: Schematic of the fibre-connected optical setup. VATT: (variable optical attenuator); PD: photodiode.

prevent unwanted back reflections into the laser. A fibre optical variable attenuator (model MAP-220CX-A from JDSU) is used to generate different photon numbers impinging onto the QRG by varying the laser's optical power. The certification and randomness generation measurements are implemented using standard fibre couplers (Thorlabs 10202A) with reflectivities $r_1 = 0.0965$ (i.e. $\approx$ 90:10) and $r_0 = \frac{1}{2}$ (i.e. 50:50), respectively. Detector C — used for the certification measurement — is a fibre-coupled InGaAs PIN photodiode (Thorlabs DET08CFC/M) with a large bandwidth $BW_C = 5\,\text{GHz}$, a responsitivity $\eta_C = 1.04\,\text{A}\,\text{W}^{-1}$ at $\lambda = 1550\,\text{nm}$, a transimpedance gain $G_C = 50\,\Omega$ and a measured electronic noise with standard deviation $\sigma_C \approx 0.33\,\text{mV}$. On the other hand, the randomness generation measurement made of detectors A and B is implemented by means of a fibre-coupled AC-coupled balanced detector (Thorlabs PDB-480C-AC) with the following corresponding specifications: $BW_D = 1.6\,\text{GHz}$, $\eta_D = 0.95\,\text{A}\,\text{W}^{-1}$ at $\lambda = 1550\,\text{nm}$, $G_D = 16000\,\Omega$ and $\sigma_D \approx 3.05\,\text{mV}$. Signals from the detectors are sampled by an oscilloscope (Lecroy WaveRunner 204MXi) with a 2 GHz bandwidth, a sampling rate of $F_S = 10\,GS/s$ and a voltage resolution of $V_{\text{max}} - V_{\text{min}} = 10\,\text{mV/div}$. The measurements are recorded by an ADC as an 8-bit output, but with a calibrated bit depth of $\Delta_{\text{ADC}} = 4.772$. This corresponds to the effective number of bits free of ADC internal noise.

11.2 Shot-Noise-Limited Detection

A key requirement for the measurement apparatus presented in Fig. 11.1 is its ability to faithfully detect photons. This implies that the characteristics of the light under consideration must dominate any signature arising from electronic noise when a measurement is performed. As such, we tested the so-called *shot-noise-limited* detection of the balanced detector used for the randomness generation measurement. This was realised by plotting the voltage variance of the balanced detector measured on the oscilloscope from two light sources — the laser mentioned above and a CW superluminescent light-emitting diode (SLED, Exalos EXS1550-045) at $\lambda = 1550\,\text{nm}$ — as a function of their optical power. The results are shown in Fig. 11.2.

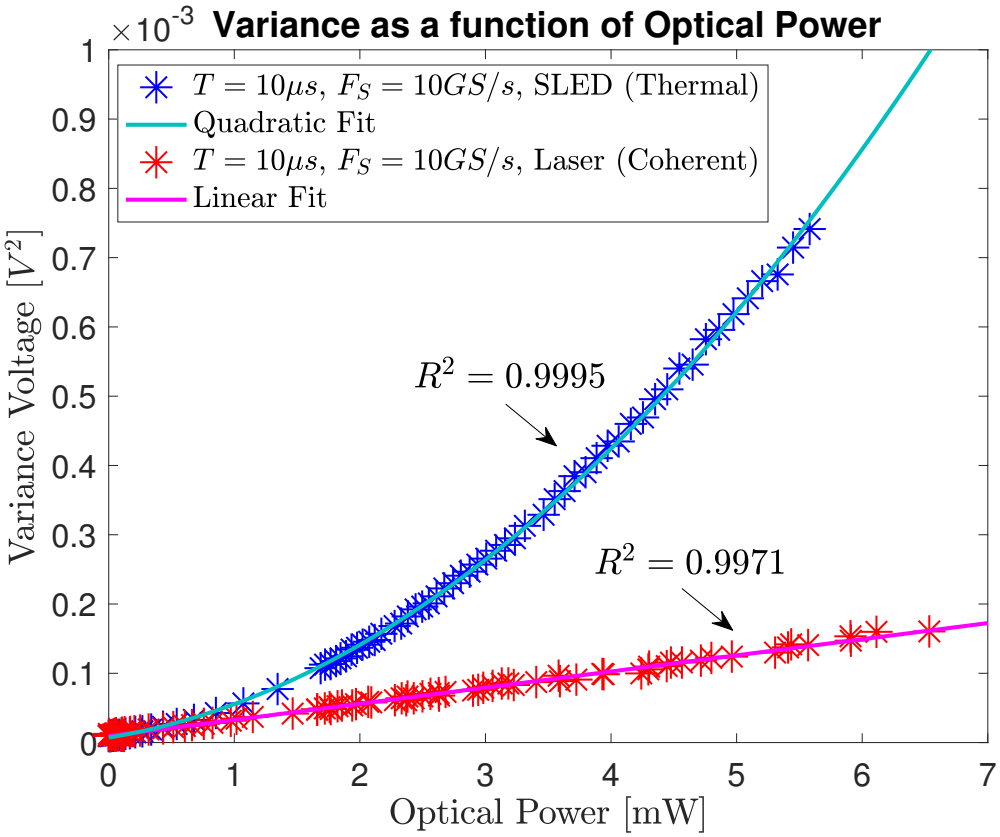


Figure 11.2: Voltage variance of the balanced detector for two light sources — a laser source and a SLED — and plotted against the source's optical power.

As can be observed in the legend of Fig. 11.2, each data point for the SLED (in blue) and the laser (in red) was obtained by measuring the output of the balanced detector from a time trace of $T = 10\,\mu\text{s}$ and a sampling rate of $F_S = 10\,GS/s$ on

the oscilloscope. The SLED is based on amplified spontaneous emission wherein light from spontaneous emission is amplified in a single pass through an optical waveguide. The resulting frequency spectrum is broadband and the SLED is thus considered to be a thermal light source. As a consequence, its variance should be quadratic in the Fock basis and this is exactly what is observed from the balanced detector and the quadratic fit in Fig. 11.2. On the other hand, the laser source is coherent such that its variance is linear in the Fock basis which is, one again, what can be seen from the linear fit in Fig. 11.2. The linear and quadratic fits feature large coefficients of determination $R^2 = 99.71\%$ and $R^2 = 99.95\%$, respectively.

In essence, the signatures of shot noise for the laser source and thermal noise for the SLED are readily visible from Fig. 11.2 and hence, they validate the desired performance of the balanced detector later used for the QRG's randomness generation measurement.

11.3 Retrieval of the Experimental Min-Entropy

Since the final results shown in the next chapter will compare the SDI model for the QRG hereby presented with various device-dependent models on the basis of their respective estimates of the min-entropy, the process used to experimentally retrieve the device-dependent min-entropy from the setup in Fig. 11.1 is detailed.

The goal is to get an experimental estimate of the device-dependent min-entropy, that is, the min-entropy associated with the measurement outcome from the randomness generation measurement — i.e. the balanced detector — given the laser source used. We show in Fig. 11.3 the voltage time traces for the difference measurement as well as the associated certification measurement obtained with the oscilloscope.

Both measurements in Fig. 11.3 are presented for 24 different values of P, the optical power of the laser beam prior to the balanced detector. These 24 data sets are the ones used in the main results examined in Sec. 12.2. As can be seen, and as one

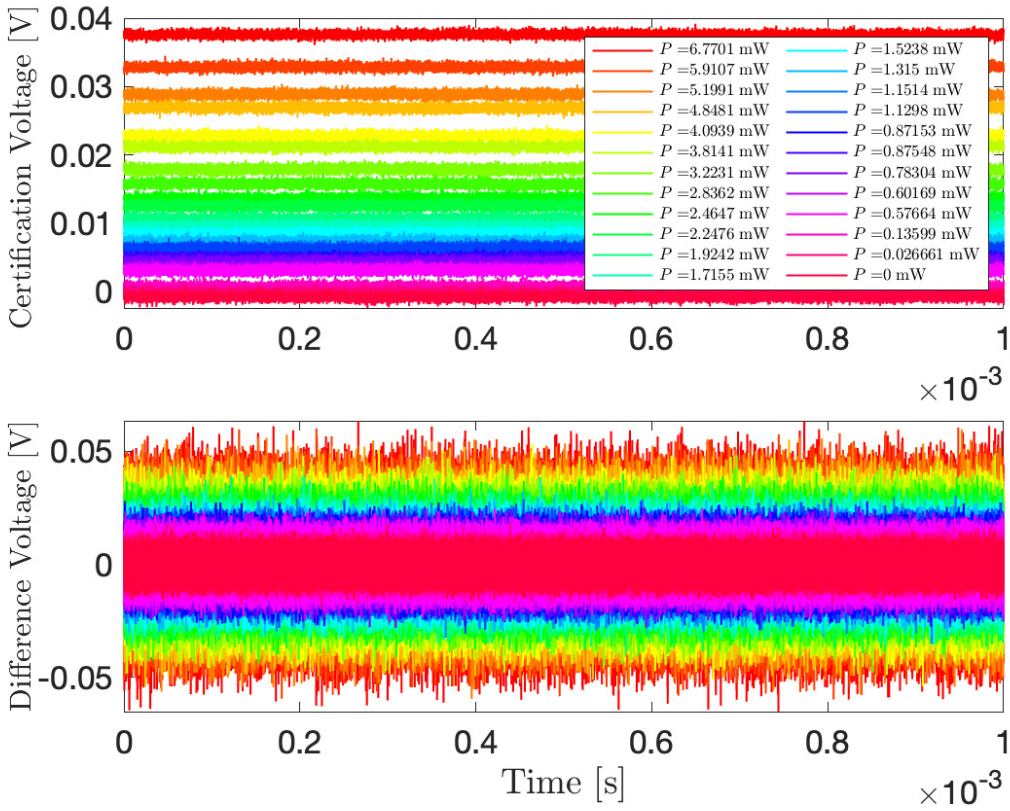


Figure 11.3: Time traces of the difference measurement and the certification measurement for 24 different optical powers P of the laser.

can expect from Fig. 11.2, the difference measurement exhibits more variance when the optical power P increases. Alternatively, the average voltage of the certification measurement also increases for higher values of P, thereby confirming intuition. Note that the last curve for which $P = 0\,\mathrm{mW}$ simply corresponds to electronic noise in the system as it was acquired when the laser was switched off.

The next step to determine the device-dependent min-entropy experimentally is to generate the voltage histograms of the difference measurement. The histograms corresponding to the difference measurements in Fig. 11.3 are displayed at the top of Fig. 11.4. Given these histograms, one then performs a Gaussian fit. Indeed, the distribution of the difference voltage measurement given by Eq. (9.5) is binomial and since the photon number incoming onto the symmetric beam splitter BS_0 prior to the difference measurement is large, the binomial distribution becomes a Gaussian distribution. The resulting fits are presented at the bottom of Fig. 11.4.

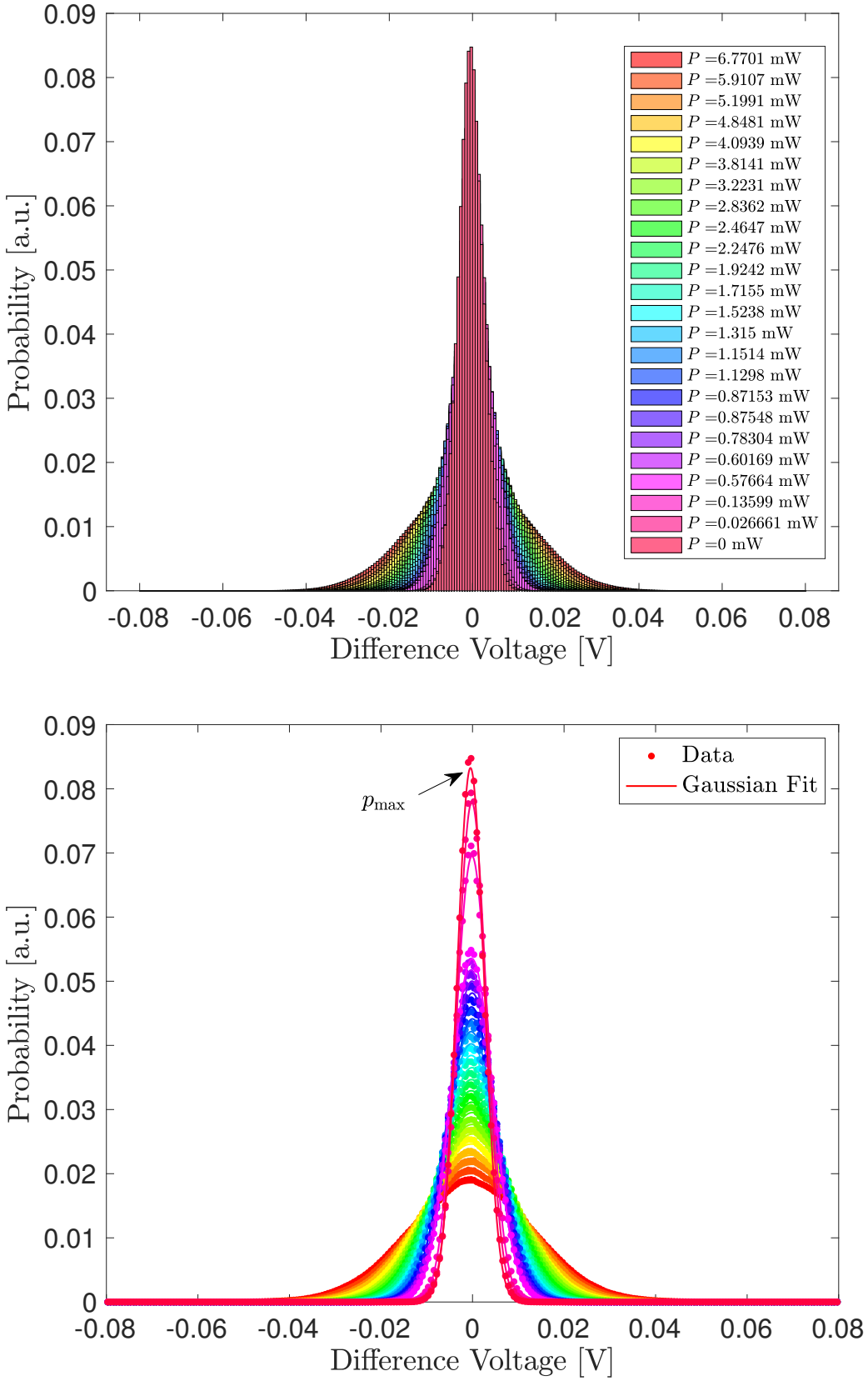


Figure 11.4: Top: histograms of the voltage difference measurement for 24 different optical powers P of the laser; bottom: associated Gaussian fits.

From Fig. 11.4, it can be concluded that the Gaussian fits are in excellent accordance with the histograms. Finally, the maximum probability $p_{\max}$ for each gaussian fit shown at the bottom of Fig. 11.4 is used to calculate the estimate of the experimental device-dependent min-entropy for various values P of the laser's optical power. Indeed, to do so, one simply uses the definition of the min-entropy $H_{\min} = -\log_2(p_{\max})$, thus yielding the desired result.

Chapter 12

Results

'What can we do? We must live out our lives. [A pause] Yes, we shall live, Uncle Vanya. We shall live all through the endless procession of days ahead of us, and through the long evenings. We shall bear patiently the burdens that fate imposes on us. We shall work without rest for others, both now and when we are old. And when our final hour comes, we shall meet it humbly, and there beyond the grave, we shall say that we have known suffering and tears, that our life was bitter. And God will pity us. Ah, then, dear, dear Uncle, we shall enter on a bright and beautiful life. We shall rejoice and look back upon our grief here. A tender smile — and — we shall rest. I have faith, Uncle, fervent, passionate faith. We shall rest. We shall rest. We shall hear the angels. We shall see heaven shining like a jewel. We shall see evil and all our pain disappear in the great pity that shall enfold the world. Our life will be as peaceful and gentle and sweet as a caress. I have faith; I have faith. [Wiping away her tears] My poor, poor Uncle Vanya, you are crying! [Weeping] You have never known what it is to be happy, but wait, Uncle Vanya, wait! We shall rest. We shall rest. We shall rest.'

Sonya in Anton Tchekhov's "Uncle Vanya" (translated in english)

This chapter presents and details the key results obtained in this research.

12.1 Proceedings

As already mentioned in Sec. 11.3, the results shown below were acquired from a total of 24 data sets — of the difference and certification measurements — that scan the optical power from 0 mW to 6.77 mW, thereby corresponding to the balanced detector's linearity response range. Each measurement was carried out with a time trace of $T = 1\,\text{ms}$, yielding 10 million samples per power setting data set.

To evaluate the certified randomness of this data for a desired failure probability ϵ_{fail}, we must first fix $\tilde{\lambda}$ such that $\epsilon_{\lambda_C} < \epsilon_{\text{fail}}$ (here we choose $\epsilon_{\lambda_C} = \epsilon_{\text{fail}}/2$). Then, given the difference measurement's saturation power, we set n_R^+ equal to the corresponding saturating photon number $n_{\text{max}}^D = 1.06 \times 10^7$ and choose an upper voltage threshold v_{i_+} in Eq. (9.13) such that $\epsilon_+ < \epsilon_{\text{fail}}/2$. Finally, for a given lower voltage threshold v_{i_-}, we solve Eq. (9.13) to find n_R^- such that $\epsilon_- = \epsilon_{\text{fail}}/2$. This ensures that the photon number input to the difference measurement lies within $[n_R^-, n_R^+]$ except with probability $\max\{\epsilon_-, \epsilon_+\} + \epsilon_{\lambda_C} = \epsilon_- + \epsilon_{\lambda_C} = \epsilon_{\text{fail}}$ and the certified randomness can then be determined by plugging n_R^- into Eq. (9.9) to retrieve the conditional min-entropy.

This establishes the protocol's SDI security as per Definition 2. However, to understand how much randomness we can expect to obtain in practice, we should also consider the protocol's completeness. Typically, we will have some claimed specifications for the source and can choose thresholds accordingly. We would normally only attempt to certify a quantity and quality of randomness such that the corresponding test $\mathcal{P}$ would be passed with high probability by a source satisfying the claimed specifications using Eq. (9.14). Here, for simplicity, for each input power, we will only allow ourselves to apply thresholds such that all 10^7 measured samples pass the test.

12.2 Results

In Fig. 12.1, the certified minimum photon number n_R^- in mode R is plotted against the input optical power for various security parameters ϵ_{fail}.

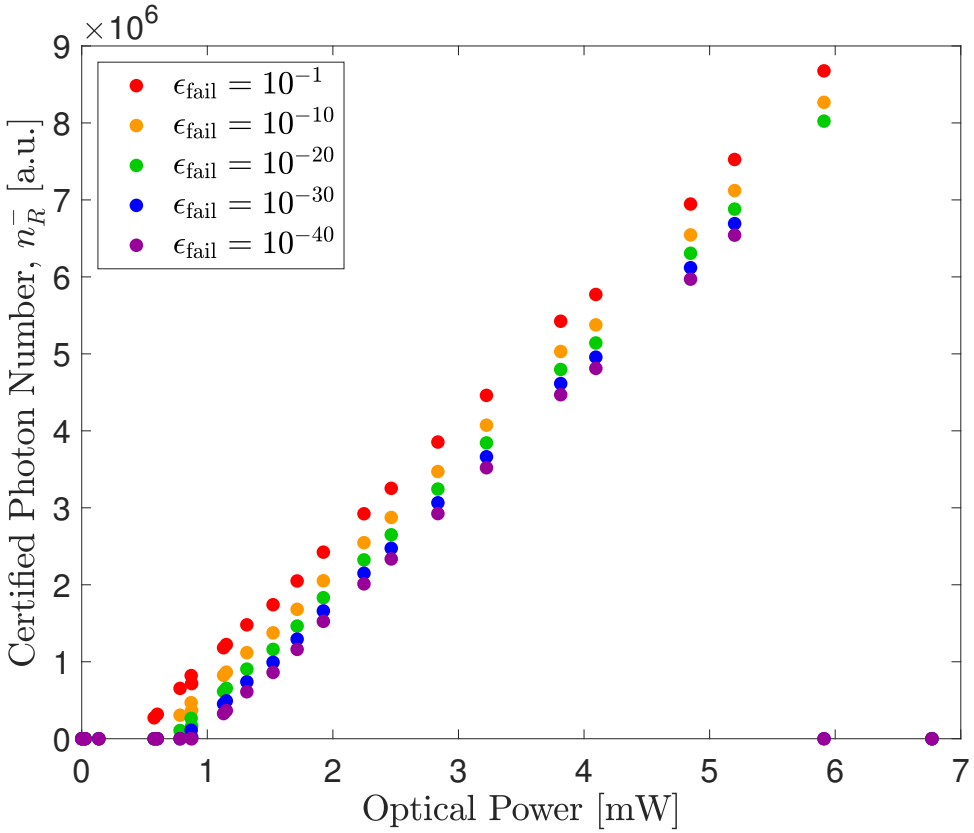


Figure 12.1: Certified minimum photon number n_R^- in mode R plotted against input optical power for various security parameters ϵ_{fail}. Voltage thresholds used in the test $\mathcal{P}$ are constrained such that all samples pass.

The input power was scanned across the linear range of the balanced detector, with the voltage thresholds $(v_{i_\pm}^\pm)$ at each power setting constrained such that all samples passed the test $\mathcal{P}$. Under these constraints, we chose a voltage threshold within the range 0 mV to 39.2 mV. As can be seen, the certified photon number scales linearly with the input power and vanishes for sufficiently small or large photonic inputs. For small powers, n_R^- goes to zero as no positive solution for Eq. (9.13) with the required ϵ_- can be found. This is as expected given that, when a low photon number impinges onto detector C, one cannot discern the produced voltage from the detector's inherent electronic noise. Alternatively, for large powers, one can easily

achieve a small value for ϵ_- but it now is not possible to obtain a value of ϵ_+ such that the total certification is valid for ϵ_{fail}. This feature arises as one approaches the balanced detector's saturating power. Finally, for increasing security (i.e. smaller ϵ_{fail}), n_R^- decreases for a given input power and remains positive over a smaller range of inputs. Indeed, the penultimate data point is non-zero only for $\epsilon_{\text{fail}} \geq 10^{-20}$ and no photon number can be certified with any security for the final point.

The main result of this thesis part is shown in Fig. 12.2.

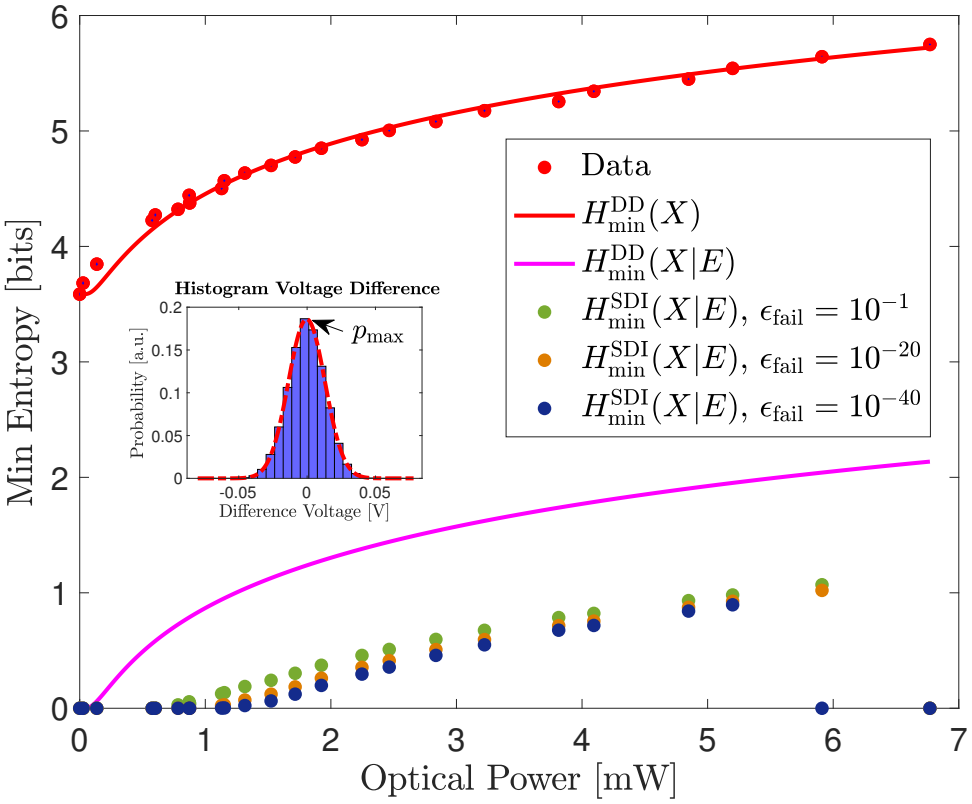


Figure 12.2: Comparison between different min-entropy models. The red data points are the experimentally estimated min-entropies for different optical powers. These are obtained from the difference measurement's voltage histograms shown in the inset (the voltage bins have been artificially thickened by a factor of 10 to make the figure comprehensible). Error bars for the data points have been included with the vertical component arising from the precision of the histogram's Gaussian fit and the horizontal error showing the electronic noise's contribution of detector C when measuring the optical power. $H_{\min}^{\text{DD}}(X)$ (red) and $H_{\min}^{\text{DD}}(X|E)$ (pink) are the device-dependent (DD) min-entropy models unconditioned and conditioned on Eve's knowledge of the noise. $H_{\min}^{\text{SDI}}(X|E)$ (green, orange and blue) are our SDI estimations of the conditional min-entropy plotted against the input optical powers and for various security parameters ϵ_{fail}.

It consists of a comparison between the experimentally estimated min-entropy, various device-dependent (DD) min-entropy models and our SDI approach. The red data points are experimental estimates of the unconditional min-entropy for different average input powers of the laser. These have been calculated using the method detailed in Sec. 11.3 whereby histograms of the difference measurement output by the balanced detector are determined — an example is shown as inset to Fig. 12.2. Given these histograms, a Gaussian fit was performed and the retrieved maximum probability $p_{\max}$ was used to estimate the unconditional min-entropy via $H_{\min} = -\log_2(p_{\max})$. This corresponds to a naive analysis where all observed fluctuations are assumed to be truly random. The red line is a device-dependent prediction for $H_{\min}^{\mathrm{DD}}(X)$, calculated using our detector model and assuming that the laser is well modelled by a coherent state $|\alpha\rangle$. The resulting curve fits the data well with a coefficient of determination $R^2 = 98.96\%$, thereby confirming the validity of our modelling. In pink, $H_{\min}^{\mathrm{DD}}(X|E)$ corresponds to the usual device-dependent conditional min-entropy, assuming a known source but accounting for Eve's knowledge of the electronic noise present in our measurement apparatus. As such, it is equal to $H_{\min}^{\mathrm{DD}}(X)$ but shifted down by the min-entropy associated with the electronic noise of the balanced detector. Finally, in green, orange and blue points, we show our SDI model for the certified conditional min-entropy $H_{\min}^{\mathrm{SDI}}(X|E)$ for different values of the security parameter ϵ_{fail}. These were calculated via Eq. (9.9) using the minimum certified photon numbers n_R^- displayed in Fig. 12.1 for each ϵ_{fail}.

When comparing the different min-entropies in Fig. 12.2, it is clear that the claimed level of randomness critically depends on what assumptions are made about the QRG. Indeed, if one were to naively take $H_{\min}^{\mathrm{DD}}(X)$ as a consistent min-entropy model, the QRG's output would consequently be predictable since the electronic noise can be accessible to Eve. On the other hand, whilst $H_{\min}^{\mathrm{DD}}(X|E)$ correctly removes such classical side information, it nevertheless is a device-dependent model for which the experimentalist must trust the proper working of the entire setup, having carefully modelled it and its possible deviations. This means that such

scheme must be secure against all sorts of complicated attacks from Eve. In the canonical setup of Fig. 11.1, a key origin of experimental complexity arises from the input light source. Our approach provides total independence from such complexity whilst still certifying a substantial amount of min-entropy per measurement as well as an explicit quantification of its confidence given by ϵ_{fail}. As can be seen in Fig. 12.2, we certify up to ≈ 1.1 bit of min-entropy with $\epsilon_{\text{fail}} = 10^{-20}$ for the penultimate data point. While this value is about half of what $H_{\min}^{\text{DD}}(X|E)$ predicts, we argue that such compromise is reasonable given that we can still achieve large randomness bitrates for the added SDI security. Indeed, the importance of our SDI protocol's security is starkly illustrated by the final and initial input powers for which no min-entropy is assigned as opposed to the device-dependent model $H_{\min}^{\text{DD}}(X|E)$.

Using a conservative random numbers' acquisition rate of 1 GHz (i.e. a detection window of 1 ns), we obtain a secure bit rate of 1.1 Gbps with a security parameter $\epsilon_{\text{fail}} = 10^{-20}$. This achieves an ultrafast and highly secure QRG based on commercially available components and entirely independent on the incoming light source $\hat{\rho}_E$ for which the randomness is characterised and certified in real-time by the certification measurement.

Test Name	p-value	prop	Assessment
Frequency	0.39532	993/1000	Passed
BlockFrequency	0.48113	991/1000	Passed
Runs	0.80822	992/1000	Passed
LongestRun	0.36734	993/1000	Passed
Rank	0.38645	991/1000	Passed
DFT	0.97803	991/1000	Passed
NonOverlappingTemplate	1.00003	992/1000	Passed
OverlappingTemplate	0.05557	989/1000	Passed
Universal	0.99805	993/1000	Passed
LinearComplexity	0.93639	992/1000	Passed
Serial	0.77269	991/1000	Passed
ApproximateEntropy	0.84102	992/1000	Passed
CumulativeSums	0.35073	989/1000	Passed
RandomExcursions	0.02874	861/868	Passed
RandomExcursionsVariant	0.09028	860/868	Passed

Table 12.1: NIST tests results. All the tests successfully passed.

Lastly, these bits have been converted into strings of random numbers using the Lefthover Hash Lemma (detailed in Sec. 10.5). A corresponding estimated min-entropy of 1 bits per measurement was used and the obtained random numbers have successfully passed all the NIST tests [107], as can be seen in Tab. 12.1. Indeed, for each test to pass, the obtained proportion of passing sequences (prop) has to be greater than the threshold value of 98%.

Chapter 13

Discussion and Conclusion

'I do the wrong, and first begin to brawl.
The secret mischiefs that I set abroach
I lay unto the grievous charge of others.
Clarence, whom I indeed have cast in darkness,
I do beweep to many simple gulls,
Namely, to Derby, Hastings, Buckingham,
And tell them 'tis the queen and her allies
That stir the king against the duke my brother.
Now they believe it and withal whet me
To be revenged on Rivers, Dorset, Grey;
But then I sigh and, with a piece of scripture,
Tell them that God bids us do good for evil;
And thus I clothe my naked villainy
With odd old ends stolen out of Holy Writ,
And seem a saint when most I play the devil.'
Richard III in Shakespeare's "Richard III"

This chapter provides a discussion to compare the results achieved with respect to the current state-of-the-start implementations. Additionally, a conclusion is given.

13.1 Discussion

We now return to the desiderata previously outlined for evaluating the usefulness of a QRG device, namely, level of security, performance (achievable bitrate) and practicality (ease of implementation, durability, and cost). Our protocol used cheap and robust off-the-shelf components that lend themselves to prolonged, high-speed usage and would be amenable to miniaturisation in an integrated photonic architecture (please consult and refer to our patent [106] if you wish to undertake this route). Whilst real-time post-processing was not implemented in this work, it has already been shown that field-programmable gate array (FPGA) technology is already sufficiently advanced to carry out the necessary hashing at speeds in the Gbps range [141, 160] and would therefore not lead to a reduction in the final rate of random numbers.

In terms of security and performance, our work considers completely general quantum attacks and achieves significantly higher bitrates for a given security parameter than the fastest known source- (5 Kbps in [125]), measurement- (5.7 Kbps in [124]), semi- (16.5 Mbps in [129]) or fully device-independent protocols (180 bps in [118]). Moreover, the only directly comparable work which offers a composable security proof is [125], whose randomness generation rate we improve upon by 6 orders of magnitude.

The experimental architectures most similar to ours are a recent series of papers that involve homodyning the vacuum [131], or squeezed state [161], or dual-homodyning the vacuum [162] and were claimed to be SDI. Indeed, these works also achieve impressive rates as high as 17 Gbps. To derive a SDI proof, these works apply entropic uncertainty relations that can, in principle, lead to devices for which randomness can be certified even if the source of quantum states is completely unknown, provided the measurements acting on these states are well-characterised. However, for realistic homodyne detectors with finite range, the corresponding uncertainty relation becomes trivial and no randomness can be certified [159]. This problem can

be ameliorated but only at the price of introducing an energy assumption (similar to the semi-device-independent approach) upon the source, thus jeopardising the claimed SDI.

Another key consideration when developing a protocol for certified randomness is whether such a protocol is composably secure [150, 154]. That is, whether the output of the protocol can then be used as an input to other cryptographic protocols without compromising the security. For example, it can be input to a randomness extractor along with a seed to achieve certified randomness expansion using well known techniques [152, 155]. It is still unknown whether fully device-independent protocols are composably secure without extra assumptions, e.g. devices are memoryless [163]. It is thus necessary to move beyond device-independence if one desires a composably secure protocol.

13.2 Conclusion

In summary, we presented and experimentally implemented a SDI protocol based on the quantum nature of untrusted light. Our scheme achieves state-of-the-art ultrafast randomness bitrates whilst providing a rigorous and specific security parameter for the certified conditional min-entropy totally independent of the light source. There are several avenues to further improve the performance of our scheme. A higher bandwidth balanced detector for the randomness generation speed as well as a larger bit-resolution of the ADC for the retrievable min-entropy per sample are primary examples among them.

Chapter 14

Conclusion to the Thesis

'Thus, gentle Reader, I have given thee a faithful History of my Travels for Sixteen Years, and above Seven Months; wherein I have not been so studious of Ornament as of Truth. I could perhaps like others have astonished thee with strange improbable Tales; but I rather chose to relate plain Matter of Fact in the simplest Manner and Style; because my principal Design was to inform, and not to amuse thee.'

The Honourable Captain Lemuel Gulliver from Jonathan Swift's "Gulliver's Travels"

In this thesis, two avenues towards practical applications of quantum optics have been suggested and successfully implemented.

In the first application, a scheme has been proposed and experimentally demonstrated to interconvert between the dual-rail and single-rail encodings of an optical qubit with state-of-the-art fidelities and large success probabilities, thereby enabling efficient exchange of quantum information between stationary carriers of different nature by means of light.

It should be pointed out that the approach undertaken for the experimental demonstration consists of four main shortcomings. While these are effectively present,

their nature is solely technical rather than conceptual. The first issue lies in the complexity of setting up an optical circuit containing three nonlinear crystals. Secondly, the installation is subject to a high sensitivity to air fluctuations since the quantum states in consideration propagate in free space within numerous different optical paths and over relatively large distances, thus leading to the need for a phase lock and a complex phase retrieval procedure. These two drawbacks can be simply eliminated by choosing fibre or integrated optical architectures instead [164]. The third disadvantage is the required states' low probability of successful preparation. This problem can be alleviated by using nonlinear crystals with large nonlinearity indices, or utilising either heralded or deterministic sources of polarisation entangled photon pairs as already specifically mentioned. Lastly, the lack of number-discriminating photon detectors leads to a decrease in the probability of success of the proposed teleportation protocol. Moreover, this introduces false positive Bell state projections which affect the fidelity of the resulting teleported states. This problem, however, is peculiar to most modern quantum optical protocols and it can partially be solved with the help of TESs.

Taking into account the mentioned limitations and the implementation of their proposed solutions, one can now envisage routes towards hybrid quantum networks wherein the quantum information would be stored in photons in the dual-rail encoding that would easily be steered with polarisation rotators, and could then be converted into their single-rail encoding with the help of the proposed scheme in order to coherently exchange information with stationary quantum gates made of trapped ions or cold atoms. In this regard, the scheme proposed in the first part of this thesis would shift the experimental focus onto improving quantum gates' fidelities and thus bring us closer to realisable quantum networks.

The second work has presented and experimentally implemented a composably secure SDI protocol based on the quantum nature of untrusted light. Within this work, competitive ultrafast randomness bitrates were achieved, whilst providing a rigorous and specific security parameter for the certified conditional min-entropy

totally independent of the light source used in the implementation of the scheme. Moreover, a patent has been filed for this idea, making it therefore possible for one to use these random numbers in real-world applications of cryptography.

The most sensible route to undertake for the continuation of this work would be to set the experimental implementation on a miniaturised chip that includes, or is coupled to, fast real-time post-processing for the data's hashing. Once again, both tasks are purely technical and their solutions broadly accessible. Indeed, the chip only requires careful electro-optical engineering [165], while the hashing can be implemented with FPGA circuitry [166].

Achieving these two technical goals associated with the work presented in the second part of this thesis would result in a convenient, ultrafast, highly secure and readily available QRNG. One can then imagine easily inserting this device into any desired application of quantum communication and quantum crystography, e.g. a particular QKD implementation, the violation of a Bell's inequality or simply the need for genuinely random numbers.

Bibliography

[1] Erwin Schrödinger. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften*, 23(49):823–828, 1935.

[2] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865, 2009.

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

[4] Max Planck. Über das Gesetz der Energieverteilung im Normalspektrum. In *Von Kirchhoff bis Planck*, pages 178–191. Springer, 1978.

[5] Albert Einstein. Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt. *Annalen der Physik*, 322(6):132–148, 1905.

[6] Niels Bohr. XXXVII. On the constitution of atoms and molecules. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 26(153):476–502, 1913.

[7] Louis De Broglie. *Recherches sur la théorie des quanta*. PhD thesis, Migration-université en cours d'affectation, 1924.

[8] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777, 1935.

[9] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental tests of realistic local theories via Bell's theorem. *Physical Review Letters*, 47(7):460, 1981.

[10] John S Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[11] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880, 1969.

[12] Philippe Grangier, Gerard Roger, and Alain Aspect. Experimental evidence for a photon anticorrelation effect on a beam splitter: a new light on single-photon interferences. *EPL (Europhysics Letters)*, 1(4):173, 1986.

[13] Leonard Mandel and Emil Wolf. *Optical coherence and quantum optics*. Cambridge university press, 1995.

[14] Rodney Loudon. *The quantum theory of light*. OUP Oxford, 2000.

[15] Chong-Ki Hong, Zhe-Yu Ou, and Leonard Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters*, 59(18):2044, 1987.

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

[17] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Advances in quantum metrology. *Nature Photonics*, 5(4):222, 2011.

[18] R_E Slusher, LW Hollberg, Bernard Yurke, JC Mertz, and JF Valley. Observation of squeezed states generated by four-wave mixing in an optical cavity. *Physical Review Letters*, 55(22):2409, 1985.

[19] Min Xiao, Ling-An Wu, and H Jeffrey Kimble. Precision measurement beyond the shot-noise limit. *Physical Review Letters*, 59(3):278, 1987.

[20] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum-enhanced measurements: beating the standard quantum limit. *Science*, 306(5700):1330–1336, 2004.

[21] J Abadie, BP Abbott, R Abbott, TD Abbott, M Abernathy, C Adams, R Adhikari, C Affeldt, B Allen, GS Allen, et al. A gravitational wave observatory operating beyond the quantum shot-noise limit. *Nature Physics*, 7(12):962, 2011.

[22] Junaid Aasi, J Abadie, BP Abbott, Richard Abbott, TD Abbott, MR Abernathy, Carl Adams, Thomas Adams, Paolo Addesso, RX Adhikari, et al. Enhanced sensitivity of the LIGO gravitational wave detector by using squeezed states of light. *Nature Photonics*, 7(8):613, 2013.

[23] Benjamin P Abbott, Richard Abbott, TD Abbott, MR Abernathy, Fausto Acernese, Kendall Ackley, Carl Adams, Thomas Adams, Paolo Addesso, RX Adhikari, et al. Observation of gravitational waves from a binary black hole merger. *Physical Review Letters*, 116(6):061102, 2016.

[24] A Einstein. Die Grundlage der allgemeinen Relativitätstheorie. *Annalen der Physik*, 354(7):769–822, 1916.

[25] Albert Einstein and Nathan Rosen. On gravitational waves. *Journal of the Franklin Institute*, 223(1):43–54, 1937.

[26] AI Lvovsky, R Ghobadi, A Chandra, AS Prasad, and C Simon. Observation of micro–macro entanglement of light. *Nature Physics*, 9(9):541, 2013.

[27] Natalia Bruno, Anthony Martin, Pavel Sekatski, Nicolas Sangouard, RT Thew, and Nicolas Gisin. Displacement of entanglement back and forth between the micro and macro domains. *Nature Physics*, 9(9):545, 2013.

[28] Richard P Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6):467–488, 1982.

[29] David Deutsch. Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[30] David P DiVincenzo. Quantum computation. *Science*, 270(5234):255–261, 1995.

[31] Andrew Steane. Quantum computing. *Reports on Progress in Physics*, 61(2):117, 1998.

[32] Charles H Bennett and David P DiVincenzo. Quantum information and computation. *Nature*, 404(6775):247, 2000.

[33] Emanuel Knill, Raymond Laflamme, and Gerald J Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46, 2001.

[34] Pieter Kok, William J Munro, Kae Nemoto, Timothy C Ralph, Jonathan P Dowling, and Gerard J Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79(1):135, 2007.

[35] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001.

[36] Jeremy L O'brien, Akira Furusawa, and Jelena Vučković. Photonic quantum technologies. *Nature Photonics*, 3(12):687, 2009.

[37] Timothy C Ralph and Ping K Lam. A bright future for quantum communications. *Nature photonics*, 3(12):671, 2009.

[38] L-M Duan, MD Lukin, J Ignacio Cirac, and Peter Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414(6862):413, 2001.

[39] H Jeff Kimble. The quantum internet. *Nature*, 453(7198):1023, 2008.

[40] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004, 2017.

[41] David Drahi, Nathan Walk, Matty J Hoban, W Steven Kolthammer, Joshua Nunn, Jonathan Barrett, and Ian A Walmsley. Certified quantum randomness from untrusted light. *arXiv preprint arXiv:1905.09665*, 2019.

[42] Charles H Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.*, 560(12):7–11, 2014.

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

[44] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43, 2017.

[45] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, et al. Secure quantum key distribution over 421 km of optical fiber. *Physical Review Letters*, 121(19):190502, 2018.

[46] David J Wineland. Nobel lecture: Superposition, entanglement, and raising Schrödinger's cat. *Reviews of Modern Physics*, 85(3):1103, 2013.

[47] Andrew D Ludlow, Martin M Boyd, Jun Ye, Ekkehard Peik, and Piet O Schmidt. Optical atomic clocks. *Reviews of Modern Physics*, 87(2):637, 2015.

[48] Xi-Lin Wang, Yi-Han Luo, He-Liang Huang, Ming-Cheng Chen, Zu-En Su, Chang Liu, Chao Chen, Wei Li, Yu-Qiang Fang, Xiao Jiang, et al. 18-qubit entanglement with six photons' three degrees of freedom. *Physical Review Letters*, 120(26):260502, 2018.

[49] Yoshiaki Tamura, Hirotaka Sakuma, Keisei Morita, Masato Suzuki, Yoshinori Yamamoto, Kensaku Shimada, Yuya Honma, Kazuyuki Sohma, Takashi Fujii,

and Takemi Hasegawa. The first 0.14-db/km loss optical fiber and its impact on submarine transmission. *Journal of Lightwave Technology*, 36(1):44–49, 2018.

[50] M Minder, M Pittaluga, GL Roberts, M Lucamarini, JF Dynes, ZL Yuan, and AJ Shields. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nature Photonics*, 13(5):334, 2019.

[51] F Marsili, Varun B Verma, Jeffrey A Stern, S Harrington, Adriana E Lita, Thomas Gerrits, Igor Vayshenker, Burm Baek, Matthew D Shaw, Richard P Mirin, et al. Detecting single infrared photons with 93% system efficiency. *Nature Photonics*, 7(3):210, 2013.

[52] Ulf Leonhardt. *Measuring the quantum state of light*, volume 22. Cambridge university press, 1997.

[53] W Heisenberg. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Z. Phys.*, 43:172–198, 1927.

[54] Roy J Glauber. Coherent and incoherent states of the radiation field. *Physical Review*, 131(6):2766, 1963.

[55] VV Dodonov, IA Malkin, and VI Man'Ko. Even and odd coherent states and excitations of a singular oscillator. *Physica*, 72(3):597–615, 1974.

[56] Alexei Ourjoumtsev, Rosa Tualle-Brouri, Julien Laurat, and Philippe Grangier. Generating optical Schrödinger kittens for quantum information processing. *Science*, 312(5770):83–86, 2006.

[57] Alexei Ourjoumtsev, Hyunseok Jeong, Rosa Tualle-Brouri, and Philippe Grangier. Generation of optical 'Schrödinger cats' from photon number states. *Nature*, 448(7155):784, 2007.

[58] Wei-Bo Gao, Chao-Yang Lu, Xing-Can Yao, Ping Xu, Otfried Gühne, Alexander Goebel, Yu-Ao Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei

Pan. Experimental demonstration of a hyper-entangled ten-qubit Schrödinger cat state. *Nature Physics*, 6(5):331, 2010.

[59] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.*, 40:749–759, June 1932.

[60] Alexander I Lvovsky. Squeezed light. *Photonics: Scientific Foundations, Technology and Applications*, 1:121–163, 2015.

[61] AI Lvovsky. Iterative maximum-likelihood reconstruction in quantum homodyne tomography. *Journal of Optics B: Quantum and Semiclassical Optics*, 6(6):S556, 2004.

[62] David Drahi, Demid V Sychev, Khurram K Pirov, Ekaterina A Sazhina, Valeriy A Novikov, Ian A Walmsley, and AI Lvovsky. Quantum interface between single-and dual-rail optical qubits. *arXiv preprint arXiv:1905.08562*, 2019.

[63] Reed W Andrews, Robert W Peterson, Tom P Purdy, Katarina Cicak, Raymond W Simmonds, Cindy A Regal, and Konrad W Lehnert. Bidirectional and efficient conversion between microwave and optical light. *Nature Physics*, 10(4):321, 2014.

[64] Alexander I Lvovsky, Barry C Sanders, and Wolfgang Tittel. Optical quantum memory. *Nature Photonics*, 3(12):706, 2009.

[65] Markus Aspelmeyer, Tobias J Kippenberg, and Florian Marquardt. Cavity optomechanics. *Reviews of Modern Physics*, 86(4):1391, 2014.

[66] Dominic W. Berry, A. I. Lvovsky, and Barry C. Sanders. Interconvertibility of single-rail optical qubits. *Opt. Lett.*, 31(1):107–109, Jan 2006.

[67] Pierre Vernaz-Gris, Kun Huang, Mingtao Cao, Alexandra S Sheremet, and Julien Laurat. Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble. *Nature Communications*, 9(1):363, 2018.

[68] Olivier Morin, Kun Huang, Jianli Liu, Hanna Le Jeannic, Claude Fabre, and Julien Laurat. Remote creation of hybrid entanglement between particle-like and wave-like optical qubits. *Nature Photonics*, 8(7):570, 2014.

[69] Hyunseok Jeong, Alessandro Zavatta, Minsu Kang, Seung-Woo Lee, Luca S Costanzo, Samuele Grandi, Timothy C Ralph, and Marco Bellini. Generation of hybrid entanglement of light. *Nature Photonics*, 8(7):564, 2014.

[70] Demid V Sychev, Alexander E Ulanov, Egor S Tiunov, Anastasia A Pushkina, A Kuzhamuratov, Valery Novikov, and AI Lvovsky. Entanglement and teleportation between polarization and wave-like encodings of an optical qubit. *Nature Communications*, 9(1):3672, 2018.

[71] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[72] TC Ralph, AP Lund, and HM Wiseman. Adaptive phase measurements in linear optical quantum computation. *Journal of Optics B: Quantum and Semiclassical Optics*, 7(10):S245, 2005.

[73] Jaromír Fiurášek. Interconversion between single-rail and dual-rail photonic qubits. *Phys. Rev. A*, 95:033802, Mar 2017.

[74] Charles H Bennett, David P DiVincenzo, Peter W Shor, John A Smolin, Barbara M Terhal, and William K Wootters. Remote state preparation. *Physical Review Letters*, 87(7):077902, 2001.

[75] CK Hong and Leonard Mandel. Experimental realization of a localized one-photon state. *Physical Review Letters*, 56(1):58, 1986.

[76] Alexander I Lvovsky, Hauke Hansen, T Aichele, O Benson, J Mlynek, and S Schiller. Quantum state reconstruction of the single-photon Fock state. *Physical Review Letters*, 87(5):050402, 2001.

[77] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575, 1997.

[78] Akira Furusawa, Jens Lykke Sørensen, Samuel L Braunstein, Christopher A Fuchs, H Jeff Kimble, and Eugene S Polzik. Unconditional quantum teleportation. *Science*, 282(5389):706–709, 1998.

[79] William K Wootters and Wojciech H Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802, 1982.

[80] Jian-Wei Pan, Dik Bouwmeester, Harald Weinfurter, and Anton Zeilinger. Experimental entanglement swapping: entangling photons that never interacted. *Physical Review Letters*, 80(18):3891, 1998.

[81] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[82] Christopher C Gerry, A Benmoussa, and RA Campos. Quantum nondemolition measurement of parity and generation of parity eigenstates in optical fields. *Physical Review A*, 72(5):053818, 2005.

[83] Stefanie Barz, Gunther Cronenberg, Anton Zeilinger, and Philip Walther. Heralded generation of entangled photon pairs. *Nature Photonics*, 4(8):553, 2010.

[84] Claudia Wagenknecht, Che-Ming Li, Andreas Reingruber, Xiao-Hui Bao, Alexander Goebel, Yu-Ao Chen, Qiang Zhang, Kai Chen, and Jian-Wei Pan. Experimental demonstration of a heralded entanglement source. *Nature Photonics*, 4(8):549, 2010.

[85] Markus Müller, Samir Bounouar, Klaus D Jöns, M Glässl, and P Michler. On-demand generation of indistinguishable polarization-entangled photon pairs. *Nature Photonics*, 8(3):224, 2014.

[86] Hui Wang, Hai Hu, T-H Chung, Jian Qin, Xiaoxia Yang, J-P Li, R-Z Liu, H-S Zhong, Y-M He, Xing Ding, et al. On-demand semiconductor source of entangled photons which simultaneously has high fidelity, efficiency, and indistinguishability. *Physical Review Letters*, 122(11):113602, 2019.

[87] Max Born and Emil Wolf. *Principles of optics: electromagnetic theory of propagation, interference and diffraction of light*. Elsevier, 2013.

[88] T Aichele, Alexander I Lvovsky, and S Schiller. Optical mode characterization of single photons prepared by means of conditional measurements on a biphoton state. *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, 18(2):237–245, 2002.

[89] Willis E Lamb Jr. Theory of an optical maser. *Physical Review*, 134(6A):A1429, 1964.

[90] William Henry Bragg and William Lawrence Bragg. The reflection of X-rays by crystals. *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, 88(605):428–438, 1913.

[91] Albert A Michelson and Edward W Morley. On the relative motion of the Earth and of the luminiferous ether. *Sidereal Messenger, vol. 6, pp. 306-310*, 6:306–310, 1887.

[92] Robert W Boyd. *Nonlinear optics*. Elsevier, 2003.

[93] John A Gubner. *Probability and random processes for electrical and computer engineers*. Cambridge university press, 2006.

[94] Jean-Claude Diels and Wolfgang Rudolph. *Ultrashort laser pulse phenomena*. Elsevier, 2006.

[95] Luo-Kan Chen, Hai-Lin Yong, Ping Xu, Xing-Can Yao, Tong Xiang, Zheng-Da Li, Chang Liu, He Lu, Nai-Le Liu, Li Li, et al. Experimental nested purification for a linear optical quantum repeater. *Nature Photonics*, 11(11):695, 2017.

[96] Yoon-Ho Kim, Sergei P. Kulik, Maria V. Chekhova, Warren P. Grice, and Yanhua Shih. Experimental entanglement concentration and universal Bell-state synthesizer. *Phys. Rev. A*, 67:010301, Jan 2003.

[97] Alexander Lvovsky. *Quantum physics: an introduction based on photons*. Springer-Verlag Berlin Heidelberg, 2018.

[98] Samuel L Braunstein and A Mann. Measurement of the Bell operator and quantum teleportation. *Physical Review A*, 51(3):R1727, 1995.

[99] David S Simon, Gregg Jaeger, and Alexander V Sergienko. *Quantum metrology, imaging, and communication*. Springer, 2017.

[100] Paul G Kwiat, Philippe H Eberhard, Aephraim M Steinberg, and Raymond Y Chiao. Proposal for a loophole-free Bell inequality experiment. *Physical Review A*, 49(5):3209, 1994.

[101] Max Born. Quantenmechanik der Stoßvorgänge. *Zeitschrift für Physik*, 38(11-12):803–827, 1926.

[102] Stefano Pirandola, Jens Eisert, Christian Weedbrook, Akira Furusawa, and Samuel L Braunstein. Advances in quantum teleportation. *Nature Photonics*, 9(10):641, 2015.

[103] Samuel L Braunstein and H Jeff Kimble. A posteriori teleportation. *Nature*, 394(6696):840, 1998.

[104] Jian-Wei Pan, Sara Gasparoni, Markus Aspelmeyer, Thomas Jennewein, and Anton Zeilinger. Experimental realization of freely propagating teleported qubits. *Nature*, 421(6924):721, 2003.

[105] Cass A Sackett, David Kielpinski, Brian E King, Christopher Langer, Volker Meyer, Christopher J Myatt, M Rowe, QA Turchette, Wayne M Itano, David J Wineland, et al. Experimental entanglement of four particles. *Nature*, 404(6775):256, 2000.

[106] Ian Walmsley, Joshua Nunn, Steve Kolthammer, Gil Triginer, and David Drahi. Random number generator, 2018.

[107] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-Allen and Hamilton Inc Mclean Va, 2001.

[108] Sir Francis Galton. *Natural inheritance*. Macmillan, 1894.

[109] Huang Zhun and Chen Hongyi. A truly random number generator based on thermal noise. In *ASICON 2001. 2001 4th International Conference on ASIC Proceedings (Cat. No. 01TH8549)*, pages 862–864. IEEE, 2001.

[110] Ben Lampert, Riad S Wahby, Shane Leonard, and Philip Levis. Robust, low-cost, auditable random number generation for embedded system security. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, pages 16–27. ACM, 2016.

[111] Richard M Karp. An introduction to randomized algorithms. *Discrete Applied Mathematics*, 34(1-3):165–201, 1991.

[112] Mario Stipčević. Quantum random number generators and their use in cryptography. In *2011 Proceedings of the 34th International Convention MIPRO*, pages 1474–1479. IEEE, 2011.

[113] Walther Gerlach and Otto Stern. Der experimentelle Nachweis der Richtungsquantelung im Magnetfeld. *Zeitschrift für Physik A Hadrons and Nuclei*, 9(1):349–352, 1922.

[114] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang. Quantum random number generation. *npj Quantum Information*, 2:16021, 2016.

[115] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry 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, 2010.

[116] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. *Nature*, 540(7632):213, 2016.

[117] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam, et al. Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature*, 556(7700):223, 2018.

[118] Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Weijun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan, et al. Device-independent quantum random-number generation. *Nature*, 562(7728):548, 2018.

[119] Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Physical Review Letters*, 108(10):100402, 2012.

[120] Yang Liu, Xiao Yuan, Ming-Han Li, Weijun Zhang, Qi Zhao, Jiaqiang Zhong, Yuan Cao, Yu-Huai Li, Luo-Kan Chen, Hao Li, et al. High-speed device-independent quantum random number generation without a detection loophole. *Physical Review Letters*, 120(1):010503, 2018.

[121] Morgan W Mitchell, Carlos Abellan, and Waldimar Amaya. Strong experimental guarantees in ultrafast quantum random number generation. *Physical Review A*, 91(1):012314, 2015.

[122] Zhu Cao, Hongyi Zhou, and Xiongfeng Ma. Loss-tolerant measurement-device-independent quantum random number generation. *New Journal of Physics*, 17(12):125011, 2015.

[123] Anubhav Chaturvedi and Manik Banik. Measurement-device–independent randomness from local entangled states. *EPL (Europhysics Letters)*, 112(3):30003, 2015.

[124] You-Qi Nie, Jian-Yu Guan, Hongyi Zhou, Qiang Zhang, Xiongfeng Ma, Jun Zhang, and Jian-Wei Pan. Experimental measurement-device-independent quantum random-number generation. *Physical Review A*, 94(6):060301, 2016.

[125] Zhu Cao, Hongyi Zhou, Xiao Yuan, and Xiongfeng Ma. Source-independent quantum random number generation. *Physical Review X*, 6(1):011020, 2016.

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

[127] 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.

[128] Thomas Van Himbeeck, Erik Woodhead, Nicolas J. Cerf, Raúl García-Patrón, and Stefano Pironio. Semi-device-independent framework based on natural physical assumptions. *Quantum*, 1:33, November 2017.

[129] Jonatan Bohr Brask, Anthony Martin, William Esposito, Raphael Houlmann, Joseph Bowles, Hugo Zbinden, and Nicolas Brunner. Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination. *Physical Review Applied*, 7(5):054018, 2017.

[130] Giuseppe Vallone, Davide G Marangon, Marco Tomasin, and Paolo Villoresi. Quantum randomness certified by the uncertainty principle. *Physical Review A*, 90(5):052327, 2014.

[131] Davide G Marangon, Giuseppe Vallone, and Paolo Villoresi. Source-device-independent ultrafast quantum random number generation. *Physical review letters*, 118(6):060503, 2017.

[132] A Máttar, P Skrzypczyk, GH Aguilar, RV Nery, PH Souto Ribeiro, SP Walborn, and D Cavalcanti. Experimental multipartite entanglement and random-

ness certification of the W state in the quantum steering scenario. *Quantum Science and Technology*, 2(1):015011, 2017.

[133] JG Rarity, PCM Owens, and PR Tapster. Quantum random-number generation and key sharing. *Journal of Modern Optics*, 41(12):2435–2444, 1994.

[134] 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.

[135] 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.

[136] Michael A Wayne, Evan R Jeffrey, Gleb M Akselrod, and Paul G Kwiat. Photon arrival time quantum random number generation. *Journal of Modern Optics*, 56(4):516–522, 2009.

[137] You-Qi Nie, Hong-Fei Zhang, Zhen Zhang, Jian Wang, Xiongfeng Ma, Jun Zhang, and Jian-Wei Pan. Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Applied Physics Letters*, 104(5):051110, 2014.

[138] 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.

[139] Christian Gabriel, Christoffer Wittmann, Denis Sych, Ruifang Dong, Wolfgang Mauerer, Ulrik L Andersen, Christoph Marquardt, and Gerd Leuchs. A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, 4(10):711, 2010.

[140] 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.

[141] Thomas Symul, SM Assad, and Ping K Lam. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Applied Physics Letters*, 98(23):231103, 2011.

[142] Hong Guo, Wenzhuo Tang, Yu Liu, and Wei Wei. Truly random number generation based on measurement of phase noise of a laser. *Physical Review E*, 81(5):051137, 2010.

[143] C Abellán, W Amaya, M Jofre, M Curty, A Acín, J Capmany, V Pruneri, and MW Mitchell. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. *Optics Express*, 22(2):1645–1654, 2014.

[144] You-Qi Nie, Leilei Huang, Yang Liu, Frank Payne, Jun Zhang, and Jian-Wei Pan. The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. *Review of Scientific Instruments*, 86(6):063105, 2015.

[145] Philip J Bustard, Duncan G England, Josh Nunn, Doug Moffatt, Michael Spanner, Rune Lausten, and Benjamin J Sussman. Quantum random bit generation using energy fluctuations in stimulated Raman scattering. *Optics Express*, 21(24):29350–29357, 2013.

[146] DG England, PJ Bustard, DJ Moffatt, J Nunn, R Lausten, and BJ Sussman. Efficient Raman generation in a waveguide: a route to ultrafast quantum random number generation. *Applied Physics Letters*, 104(5):051117, 2014.

[147] Ran Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *Proceedings 42nd IEEE Symposium on Foundations of Computer Science*, pages 136–145. IEEE, 2001.

[148] Jing-Yan Haw, SM Assad, AM Lance, NHY Ng, V Sharma, Ping Koy Lam, and Thomas Symul. Maximization of extractable randomness in a quantum random-number generator. *Physical Review Applied*, 3(5):054004, 2015.

[149] Tobias Gehring, Cosmo Lupo, Arne Kordts, Dino Solar Nikolic, Nitin Jain,

Thomas B Pedersen, Stefano Pirandola, and Ulrik L Andersen. 8 GBit/s real-time quantum random number generator with non-iid samples. *arXiv preprint arXiv:1812.05377*, 2018.

[150] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[151] Robert Konig, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9):4337–4347, 2009.

[152] Daniela Frauchiger, Renato Renner, and Matthias Troyer. True randomness from realistic quantum devices. *arXiv preprint arXiv:1311.4547*, 2013.

[153] Michael Horodecki, Peter W Shor, and Mary Beth Ruskai. Entanglement breaking channels. *Reviews in Mathematical Physics*, 15(06):629–641, 2003.

[154] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution. *arXiv preprint arXiv:1409.3525*, 2014.

[155] Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory*, 57(8):5524–5535, 2011.

[156] Stefano Pironio and Serge Massar. Security of practical private randomness generation. *Physical Review A*, 87(1):012336, 2013.

[157] Yun Zhi Law, Jean-Daniel Bancal, Valerio Scarani, et al. Quantum randomness extraction for various levels of characterization of the devices. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424028, 2014.

[158] Mario Berta, Fabian Furrer, and Volkher B Scholz. The smooth entropy formalism for von Neumann algebras. *Journal of Mathematical Physics*, 57(1):015213, 2016.

[159] Fabian Furrer, Mario Berta, Marco Tomamichel, Volkher B Scholz, and Matthias Christandl. Position-momentum uncertainty relations in the presence of quantum memory. *Journal of Mathematical Physics*, 55(12):122205, 2014.

[160] Xiao-Guang Zhang, You-Qi Nie, Hongyi Zhou, Hao Liang, Xiongfeng Ma, Jun Zhang, and Jian-Wei Pan. Note: Fully integrated 3.2 Gbps quantum random number generator with real-time extraction. *Review of Scientific Instruments*, 87(7):076102, 2016.

[161] Thibault Michel, Jing Yan Haw, Davide G Marangon, Oliver Thearle, Giuseppe Vallone, Paolo Villoresi, Ping Koy Lam, and Syed M Assad. Real-time source independent quantum random number generator with squeezed states. *arXiv preprint arXiv:1903.01071*, 2019.

[162] Marco Avesani, Davide G Marangon, Giuseppe Vallone, and Paolo Villoresi. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. *Nature Communications*, 9(1):5365, 2018.

[163] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Memory attacks on device-independent quantum cryptography. *Physical Review Letters*, 110(1):010503, 2013.

[164] Francesco Lenzini, Jiri Janousek, Oliver Thearle, Matteo Villa, Ben Haylock, Sachin Kasture, Liang Cui, Hoang-Phuong Phan, Dzung Viet Dao, Hidehiro Yonezawa, et al. Integrated photonic platform for quantum information with continuous variables. *Science Advances*, 4(12):eaat9331, 2018.

[165] Francesco Raffaelli, Giacomo Ferranti, Dylan H Mahler, Philip Sibson, Jake E Kennard, Alberto Santamato, Gary Sinclair, Damien Bonneau, Mark G Thompson, and Jonathan CF Matthews. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers. *Quantum Science and Technology*, 3(2):025003, 2018.

[166] Ziyong Zheng, Yichen Zhang, Weinan Huang, Song Yu, and Hong Guo. 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. *Review of Scientific Instruments*, 90(4):043105, 2019.