Practical protocols for quantum communication networks

Federico Centrone

Université de Paris
Institut de Recherche en Informatique Fondamental (IRIF)
Ecole doctorale ED 386

En affiliation avec:
Sorbonne Université
Laboratoire d'Informatique Paris 6 (LIP6)

Practical protocols for quantum communication networks

Presenté par Federico Centrone

Thèse de doctorat de Informatique

Présentée et soutenue publiquement le 25 Novembre 2021

Devant un jury composé de:

Anthony Leverrier	INRIA Paris	Rapporteur
Norbert Lütkenhaus	University of Waterloo	Rapporteur
Pérola Milman	CNRS, Université de Paris	Examinatrice
Yasser Omar	University of Lisbon	Examinateur
Iordanis Kerenidis	CNRS, Université de Paris and QC WARE	Directeur de thèse
Eleni Diamanti	CNRS, Sorbonne Université	Co-directrice de thèse

Short summary
In this thesis, we study networks of entangled quantum optical systems at different degrees of complexity, with a special regard to their application to quantum communication scenarios. In quantum communication, we want to allow two or more distant parties to exploit the properties of quantum systems to communicate in a certain way that would be unattainable with classical technology. The archetype of quantum communication is Quantum Key Distribution (QKD), that allows two agents to share a secret random key to perform secure communications, while preventing a third malicious agent from gaining knowledge about their key. In this manuscript, however, we will explore quantum communication scenarios that go beyond standard QKD in order to test the many possibilities offered by interconnected networks of quantum devices, also known as quantum internet. Specifically, we present three different types of quantum networks, that correspond to three levels of complexity of the quantum internet. In each of these levels, we describe the communication scenario, the physical requirements necessary to build the specific architecture and a novel quantum protocol that cannot be reproduced without quantum resources. In this work, we paid particular attention to the "practicality" of the protocols, namely the fact that it should be possible to implement them in realistic conditions with current technology, at least as a proof of principle.
The first concerns an interactive proof quantum protocol showing experimental evidence of computational quantum advantage in the interactive setting for the first time. In this scenario, we have a computationally unbounded quantum prover who wants to convince an honest verifier of the existence of a certain solution to a complex mathematical problem, by sending part of the proof in the form of quantum states. Our quantum scheme lets the verifier verify the prover's assertion without actually receiving the whole solution. We prove that if the agents were not allowed to use quantum resources, the verification protocol would require an exponential time in the size of the solution, leading to a quantum advantage in computational time that we could demonstrate in our laboratory.
The second copes with an electronic-voting protocol that exploits an untrusted multipartite entangled quantum source to carry on an election without relying on election authorities, whose result is publicly verifiable without compromising the robustness of the scheme and that can be readily implemented with state-of-the-art technology for a small number of voters. Unlike previous results, our scheme does not require simultaneous broadcasting and works also in noisy scenarios, where the security is bounded by the fidelity of the quantum state being used.
Last, we simulate many modes squeezed states as continuous variables Gaussian quantum networks with complex topologies, characterizing their correlations and estimating the scaling of their cost while the networks grow using a squeezing resource theory. We prove a result that allows us to enhance the entanglement between two nodes in the network by measuring the multiple paths linking them and we employ this effect to devise an entanglement routing protocol, whose performance is particularly effective on large complex networks.
Key-words: quantum networks, quantum optics, quantum information.

Court résumé
Dans cette thèse, nous étudions les réseaux des états optiques quantiques intriqués avec différents degrés de complexité, avec une attention particulière portée à leur application dans des scénarios de communication quantique. Le but de la communication quantique est de permettre à deux ou plusieurs parties de communiquer d'une façon qui serait impossible avec de la technologie classique. Spécifiquement, nous présentons trois types de réseaux quantiques, qui correspondent à trois niveaux de complexité d'internet quantique. Dans chaque niveau, nous décrivons le scénario de communication, les exigences physiques nécessaires pour construire l'architecture spécifique et un nouveau protocole qui ne peut pas être reproduit sans des ressources quantiques. Dans cette document, nous veillons particulièrement à la "praticité" des protocoles, notamment le fait que leur implémentation doit être possible dans des conditions réalistes avec technologie existante, au moins comme preuve du principe.
Le premier concerne un protocole quantique à preuves interactives qui montre pour la première fois une preuve expérimentale d'un avantage quantique dans un cadre interactif. Dans ce scénario, il y a un prouveur avec de la puissance calculatoire illimitée qui veut convaincre un vérifieur honnête de l'existence d'une certaine solution d'un problème mathématique complexe, en lui envoyant une partie de la preuve sous forme d'états quantiques. Notre construction permet au vérifieur de vérifier l'assertion du prouveur sans recevoir la solution entière. Nous prouvons que sans ressources quantiques, le protocole de vérification exigerait un temps exponentiel en la taille de la solution, menant à un avantage quantique en terme de temps de calcul, avantage que nous avons démontré dans notre laboratoire.
Le deuxième porte sur un protocole de vote électronique qui exploite un état quantique multipartite intriqué non fiable pour réaliser une élection sans s'appuyer sur des autorités électorales, dont le résultat peut être vérifié publiquement sans compromettre la robustesse de la construction et qui peut être implémenté aisément avec les technologies de pointe existantes pour un petit nombre de votant. À l'invers des résultats précédents, notre protocole n'exige pas une émission simultanée et marche aussi dans des scénarios bruyants, où la sécurité est limitée par la fidélité de l'état quantique utilisé.
Enfin, nous simulons des états comprimés de la lumière de nombreux modes comme des réseaux quantique Gaussien à variables continues avec des topologies complexes, nous caractérisons leur corrélations et nous estimons l'intensification de leur coût pendant que les réseaux grandissent avec une théorie de ressource de compression. Nous prouvons un résultat qui permet de renforcer l'intrication entre deux nœuds du réseau si on mesure les chemins multiples qui les connectent et nous utilisons cet effet pour concevoir un protocole de routage d'intrication dont les performance sont particulièrement efficace dans des réseaux complexes grands.
Mots-clés: réseaux quantique, optique quantique, information quantique.

Long résumé

La science est née d'une révolution, il n'est donc pas surprenant que les scientifiques soient quelque peu habitués à des changements spectaculaires dans leur façon d'observer la nature. La révolution scientifique, qui a eu lieu après la publication de *De revolutionibus orbium coelestium* par Copernic et a atteint son apogée avec *Principia* de Newton après être passée par la formulation de la méthode scientifique par Galilée, a profondément modifié la vision de la société sur la Nature. Après avoir accepté l'héliocentrisme, la gravité, l'optique, l'électricité et la chimie comme piliers du paradigme scientifique, les théories révolutionnaires suivantes telles que l'évolutionnisme, la génétique et la radioactivité sont passées presque comme un jeu d'enfant. Les gens ont été témoins du pouvoir de la science dans la description des phénomènes naturels et du formidable développement technologique qui a suivi, remodelant la société humaine de manière inconcevable.

Au tournant du 20e siècle, lorsque les fleurs vaporeuses de la révolution industrielle se sont transformées en fruits électriques juteux, l'idée positiviste selon laquelle l'Homo Sapiens avait apprivoisé la nature grâce à la science et à la technologie était largement ancrée dans l'esprit de nombreux universitaires. C'est ce qui ressort des propos d'un professeur de physique de Munich qui déconseillait à Max Planck, pionnier de la théorie quantique, de se lancer dans la physique, arguant que les choses les plus importantes avaient déjà été découvertes et qu'il ne restait que "quelques trous" à combler. À cette époque, la mécanique newtonienne régissait toutes les explications physiques, on croyait que la lumière se propageait dans l'éther et l'idée de l'existence des atomes et des molécules était en grande partie rejetée par la communauté scientifique. En conséquence, la théorie de la mécanique statistique de Ludwig Boltmann était probablement perçue de la même manière que nous considérons aujourd'hui la théorie des cordes.

Tout a soudainement changé en une année, "annus mirabilis" 1905, au cours de laquelle un employé du Bureau des brevets nommé Albert Einstein, avec l'aide tacite de sa femme Mileva Marić, a publié quatre articles qui ont jeté les bases de toute la physique moderne. Dix ans avant sa théorie la plus acclamée de la relativité générale, le génie emblématique avait déjà écrit l'ouvrage digne du prix Nobel pour sa description de l'effet photoélectrique. Dans cet article, Einstein a utilisé un concept mathématique précédemment développé par Planck pour décrire le rayonnement du corps noir, mais lui a donné une interprétation physique concrète : l'énergie d'un rayon de lumière n'est pas distribuée de manière continue, mais consiste en des paquets discrets qui ne peuvent être absorbés et générés que comme des entités entières localisées dans l'espace et le temps. La lumière est faite de *quanta d'énergie*!

Lorsque Einstein a baptisé le concept qui a donné son nom à la théorie la plus aboutie de la physique, la mécanique quantique était loin d'être formulée correctement. Il lui a fallu encore quelques décennies et les débats animés de dizaines de génies pour arriver à sa version mature. Depuis lors, la théorie s'est développée en une myriade de branches très distinctes, allant de la physique de l'état solide à la gravité quantique. Néanmoins, certaines des questions fondamentales qui ont enflammé les discussions acharnées des pre-

miers développements du domaine restent sans réponse. En particulier, la formulation de la mécanique quantique d'Heisenberg, qui est effectivement la première, a permis de prédire la probabilité d'observer une certaine quantité physique d'un système, sans tenir compte de l'état du système lui-même. Toutefois, elle n'explique pas comment la nature "sait" que nous observons un système. Aucune des reformulations et interprétations suivantes de la théorie n'a été en mesure d'aborder ce problème d'une manière qui soit universellement acceptée par la communauté scientifique et il s'agit toujours d'une question très risquée si vous souhaitez avoir une conversation pacifique avec des physiciens quantiques.

La mécanique quantique est difficile à digérer: Einstein n'a jamais accepté sa nature probabiliste, Schrödinger a formulé le fameux paradoxe du chat pour mettre en évidence les problèmes apportés par son interprétation standard, tandis que Feynman était plus direct: "Je pense pouvoir dire sans risque que personne ne comprend vraiment la mécanique quantique". Et ainsi de suite, après un siècle entier, malgré toutes ses controverses, les problèmes qui se posent à toutes les échelles, les polémiques qu'elle a suscitées et tous les efforts déployés pour trouver une nouvelle théorie ultime des particules et des interactions fondamentales, la théorie des quanta n'a pourtant jamais échoué et a contribué aux résultats et aux prédictions les plus remarquables de l'histoire de la science.

Outre l'enthousiasme qu'elle a suscité chez les physiciens et les chercheurs de toutes les sciences en général, l'influence de la mécanique quantique a très vite transcendé les murs de l'académie. Un groupe d'étudiants de vingt ans avait osé, de manière indépendante et irrévérencieuse, défier la plus haute autorité de la physique imposée par la mécanique newtonienne, qui était restée incontestée pendant des siècles. Ce changement sensationnel du paradigme de la conception des lois de la nature, provoqué dans tout le monde en 1900 par les nouvelles théories de la relativité et de la mécanique quantique, élégantes descriptions de deux mondes différents et inconciliables, a ébranlé de nombreux aspects de la société humaine, de l'art à la technologie, de la philosophie à la culture populaire.

De nos jours, il n'est pas rare de voir quelqu'un porter un t-shirt avec le chat de Schrödinger ou un tatouage avec l'équation de Dirac. Néanmoins, la renommée de la mécanique quantique reste liée au charme de ses sombres mystères et paradoxes, alors que nous avons tendance à oublier à quel point la société moderne a été façonnée par notre compréhension des mécanismes du monde atomique. Elle nous a permis de comprendre et de manipuler les propriétés des éléments chimiques, des métaux et des semi-conducteurs, permettant ainsi de produire de nouveaux médicaments et matériaux, de construire et de miniaturiser des transistors et de concevoir des supraconducteurs. Elle a libéré le pouvoir perturbateur des noyaux atomiques, fourni de nouveaux dispositifs d'imagerie médicale et nous a donné les lasers.

Notre société aurait un aspect très différent sans les technologies fournies par la physique non classique. Pourtant, ce n'est que la partie émergée de l'iceberg par rapport aux promesses offertes par la prochaine génération de technologies quantiques. Des dispositifs tels que les diodes électroluminescentes (LED), les transistors à effet de champ à effet tunnel (TFET),

les dispositifs d'interférence quantique supraconducteurs (SQUID), la résonance magnétique nucléaire (RMN) ou la tomographie par émission de positrons (TEP), nécessitent tous une compréhension approfondie des principes de la mécanique quantique pour être conçus, mais la description de leurs principes de fonctionnement et de leurs effets peut être semi-classique ou entièrement classique. Une véritable machine quantique serait capable de s'adresser à des systèmes quantiques individuels et d'exploiter largement la cohérence quantique afin d'obtenir une fonctionnalité ou une performance qui serait autrement inaccessible.

Les tout premiers dispositifs issus de cette deuxième révolution quantique sont les capteurs quantiques, qui sont également les premières machines quantiques à être largement utilisées à des fins pratiques. La détection quantique utilise des phénomènes quantiques pour effectuer des mesures de haute précision dépassant la sensibilité de tout dispositif classique. Les photodiodes à avalanche qui mesurent des photons uniques et la nouvelle génération de détecteurs d'ondes gravitationnelles en sont des exemples. Cependant, le Saint Graal des technologies quantiques est souvent considéré comme la simulation quantique ou, dans un sens plus large, l'informatique quantique. L'idée est que si nous pouvons contrôler une grande machine quantique, nous pouvons l'utiliser pour simuler des processus quantiques dynamiques complexes, tels que les réactions chimiques, le repliement des protéines et les systèmes à plusieurs corps. De plus, il a été prouvé, théoriquement et récemment dans des expériences, que certaines classes spécifiques de problèmes mathématiques peuvent être résolues efficacement sur une machine quantique, alors que le meilleur superordinateur existant prendrait un temps qui dépasse la durée de vie prévue de notre système solaire.

Le physicien théoricien Richard Feynman a été le premier à proposer l'idée d'utiliser une machine quantique pour simuler des systèmes quantiques complexes. Cependant, c'est l'informaticien Peter Shor qui a été le premier à fournir un algorithme quantique ayant des applications cruciales pour une tâche de calcul considérée comme irréalisable par un ordinateur standard. Le domaine de l'information quantique, qui étudie comment coder, manipuler et extraire des informations dans les états quantiques, est né du chevauchement de l'informatique et de la physique quantique. Cependant, le lien entre le concept d'information et la physique est en réalité beaucoup plus profond.

La théorie mathématique de la communication, écrite par l'ingénieur et mathématicien Claude Shannon, a fourni la première formulation mathématique de la théorie de l'information. Dans son livre, Shannon avait proposé une façon de quantifier l'information contenue dans un certain canal de communication et, sous la suggestion de Von Neumann, il l'a appelée entropie, d'abord parce qu'elle partageait la même formule et ensuite parce que "personne ne sait ce qu'est réellement l'entropie" [1]. Cette analogie mathématique avec une quantité physique a permis l'utilisation de techniques issues de la mécanique statistique et a contribué au développement de la théorie de l'information. Cependant, ce n'est qu'avec les résultats remarquables de Szilard, Landauer et Bennett que l'on s'est rendu compte que l'on pouvait interpréter l'information comme une ressource physique et l'utiliser pour extraire le travail thermodynamique. Pour reprendre les mots de Charles Bennett : "Les ordinateurs

peuvent être considérés comme des moteurs permettant de transformer l'énergie gratuite en chaleur résiduelle et en travail mathématique" [2]. L'information est physique et nous pouvons utiliser des outils de physique pour étudier la théorie de l'information et vice versa. C'est l'une des raisons pour lesquelles l'information quantique semble être un domaine si prometteur.

D'une part, le développement des techniques de la théorie de l'information a permis une manipulation et une transmission efficaces de grandes quantités de données avec une sécurité certifiable fournie par des protocoles cryptographiques. D'autre part, la mécanique quantique a permis la maîtrise des semi-conducteurs et des matériaux à l'état solide et donc la production en masse des puces électroniques et de toute l'électronique nécessaire à la construction des systèmes de télécommunication modernes. Les progrès parallèles et indépendants de ces deux domaines ont conduit l'humanité directement à l'ère de l'information actuelle et à la construction de l'une des plus grandes architectures de notre histoire : Internet.

Internet est le réseau mondial de télécommunication constitué d'ordinateurs interconnectés qui utilisent une suite spécifique de protocoles Internet pour permettre la communication entre les appareils. Internet a eu un impact radical sur notre monde, a permis des communications sécurisées à des distances arbitraires et joue un rôle crucial dans la plupart des activités humaines actuelles. L'information quantique promet d'améliorer les caractéristiques de l'internet et même de développer de nouvelles fonctionnalités qui sont tout simplement irréalisables avec les technologies classiques [3]. Un tel Internet quantique fonctionnerait parallèlement à l'Internet classique dont nous disposons aujourd'hui, permettant une communication quantique entre des dispositifs arbitraires partout dans le monde. Plusieurs applications fascinantes ont déjà été étudiées, notamment la cryptographie indépendante des dispositifs, l'authentification sécurisée, la synchronisation des horloges, les économies exponentielles en matière de communication, les réseaux de capteurs quantiques et le calcul quantique délégué à l'aveugle [4]. Cependant, comme pour toute nouvelle technologie révolutionnaire, les applications les plus importantes doivent encore être imaginées.

Nous sommes finalement arrivés au sujet principal de cette thèse. Les réseaux quantiques sont une technologie très prometteuse et leur étude interpelle entre la recherche fondamentale et les applications du monde réel [5]. De nombreux systèmes physiques, tels que les matériaux à l'état solide et les grandes molécules comme les protéines, peuvent en effet être modélisés comme des réseaux quantiques. La structure sous-jacente de certains systèmes quantiques peut profondément influencer leurs propriétés et l'étude théorique des réseaux quantiques peut aider à comprendre de nombreux phénomènes importants tels que la localisation d'excitations cohérentes [6], les transitions de phase [7], le condensat de Bose-Einstein [8] et le transport quantique [9]. De plus, la compréhension de la distribution de l'intrication dans des structures quantiques complexes peut aider au développement d'algorithmes quantiques efficaces pour le calcul distribué [10] et même jouer un rôle dans l'étude des sous-espaces sans décohérence [11] et de la gravité quantique [12]. Enfin, le sujet principal de ce manuscrit sera les réseaux de communication quantiques, dans lesquels

plusieurs dispositifs quantiques placés à différents endroits géographiques sont interconnectés par des canaux quantiques. Il va sans dire que pour développer des communications quantiques à grande échelle et construire un internet quantique, il est obligatoire de saisir les potentialités des réseaux quantiques et d'exploiter toutes leurs caractéristiques exceptionnelles.

La route est encore longue avant le développement complet d'un internet quantique et le scepticisme persiste quant à ses potentialités réelles, mais des réseaux quantiques à petite échelle ont déjà été mis en œuvre et toutes les étapes préliminaires de l'internet quantique semblent présenter des cas d'utilisation intéressants. En tout premier lieu, il devrait permettre la réalisation de la distribution de clés quantiques (QKD) entre ses nœuds. Alors que la cryptographie standard assure la sécurité des communications en se fondant sur des hypothèses mathématiques ou sur les limites technologiques présumées des adversaires, qui pourraient se révéler inexactes, la QKD repose sur des principes physiques testés expérimentalement. Stephen Wiesner a été le premier à proposer l'idée d'un protocole de cryptographie quantique qui pourrait être utilisé pour produire de la monnaie quantique infalsifiable ; son article a toutefois été rejeté par la revue IEEE Information Theory. Son approche a ensuite été formalisée par Bennett et Brassard qui ont conçu le premier protocole QKD nommé BB84 [13]. De nombreux développements ont suivi ces premières découvertes et la cryptographie quantique est devenue l'un des domaines les plus actifs de l'information quantique.

Le premier réseau de distribution de clés quantiques au monde était le DARPA Quantum Network [14], qui est devenu pleinement fonctionnel en 2003, fonctionnant parmi 10 nœuds optiques à travers Boston et Cambridge pendant trois ans. Depuis lors, plusieurs de ces formes naissantes d'internet quantique ont été mises en œuvre et de nouvelles sont en cours de déploiement, avec même quelques applications commerciales limitées. En 2017, le premier QKD satellite-sol a finalement été mis en place [15], ce qui pourrait fortement stimuler la mise à l'échelle de ces réseaux, qui est actuellement sévèrement limitée par l'absence de répéteurs quantiques efficaces. En outre, de nombreux laboratoires de recherche étudient et mettent en œuvre des réseaux quantiques avec de nouveaux attributs remarquables qui vont au-delà du simple QKD [16].

Dans ce manuscrit, nous nous intéresserons à trois niveaux différents d'internet quantique, avec des architectures distinctes et des stades de complexité croissants. Pour chacun de ces niveaux, nous proposerons un protocole quantique qui réalise une fonctionnalité qui serait impraticable ou impossible sur l'Internet classique actuel. Outre la rigueur mathématique, le critère sera celui de l'aspect pratique, nous analyserons donc les propriétés des protocoles dans des conditions réalistes et, pour le premier d'entre eux, nous présenterons une mise en œuvre expérimentale.

Nous ne savons pas encore quelle sera l'architecture réelle de l'internet quantique, mais nous savons que le substrat des porteurs d'informations quantiques sera constitué de photons ! Les ondes électromagnétiques ont en effet toujours été le support privilégié des

télécommunications. Les photons peuvent parcourir de longues distances à la vitesse maximale autorisée par les lois de la physique sans perdre leur cohérence, ils interagissent très peu avec les molécules de l'atmosphère, ils peuvent être transportés efficacement dans des guides d'ondes et ils peuvent être distribués et manipulés facilement avec notre technologie actuelle. De plus, la lumière a toujours eu une importance majeure en mécanique quantique depuis sa toute première conception et le langage des quanta est en grande partie emprunté à l'optique classique. Par conséquent, nous consacrerons une partie importante de l'attention à l'étude de l'optique quantique et des propriétés des états quantiques de la lumière.

Cette thèse est divisée en deux parties distinctes. La première partie est consacrée à l'examen des outils et techniques mathématiques nécessaires à la compréhension des sujets de nos travaux. Des sujets avancés de l'information quantique, de l'optique quantique, de l'informatique et de la théorie des réseaux seront abordés, cependant le lecteur familier avec l'un ou l'autre de ces arguments peut sauter les sections correspondantes sans aucune complication. Plus précisément, le chapitre 1 sera consacré aux concepts concernant la mécanique quantique et l'optique quantique, tandis que le chapitre 2 traite de l'informatique et des réseaux. Dans la deuxième partie, nous explorerons les propriétés des réseaux quantiques et expliquerons les protocoles que nous avons conçus. Notre voyage à travers les différentes étapes de l'Internet quantique commence au chapitre 3 avec l'architecture de communication la plus simple, un canal quantique de bout en bout entre deux agents. Nous montrerons un protocole qui permet à un simple client quantique de vérifier la solution d'un problème mathématique complexe fournie par un serveur non fiable sans avoir accès à la solution complète. Nous présenterons l'infaisabilité d'un tel schéma sans ressources quantiques et la première démonstration expérimentale d'un avantage quantique computationnel dans le cadre interactif. Le chapitre 4 présente notre deuxième étape de l'Internet quantique, qui se déroule sur un réseau quantique plus large dans lequel tous les agents sont connectés à un nœud central qui distribue un état quantique. Le protocole que nous avons développé met en œuvre un système de vote électronique qui exploite une source quantique multipartite intriquée non fiable pour effectuer une élection sans dépendre des autorités électorales, dont le résultat est vérifiable publiquement sans compromettre la robustesse du système. et qui peut être facilement mis en œuvre avec les technologies les plus récentes. Enfin, dans le chapitre 5, nous présentons la dernière étape de l'internet quantique, où nous examinerons des topologies complexes arbitraires de réseaux quantiques, en caractérisant leurs corrélations, en estimant la mise à l'échelle de leur coût pendant la croissance des réseaux et en évaluant les performances d'un protocole de routage.

Bien que cette thèse ait été consacrée au sujet principal du développement de protocoles de communication pour l'internet quantique, une partie des efforts de ce doctorat a été employée à un autre projet, présenté en annexe A. Dans ce travail, nous montrons comment nous pouvons utiliser les états quantiques de la lumière comme des batteries, en testant l'efficacité et la puissance de la procédure de charge lorsque la batterie est immergée dans un environnement bruyant.

Contents

Introduction **1**

I Background 7

1 Quantum Toolbox **9**
1.1 The principles of Quantum Mechanics . . . 10
1.1.1 First Postulate: physical states . . . 10
1.1.2 Second postulate: physical quantities . . . 11
1.1.3 Third postulate: measurement . . . 11
1.1.4 Fourth postulate: dynamics . . . 12
1.1.5 Fifth postulate: composite systems . . . 12
1.2 Quantum states of light . . . 13
1.2.1 From Maxwell to Dirac . . . 13
1.2.2 Fock states . . . 18
1.2.3 Coherent states . . . 19
1.2.4 Squeezed states . . . 20
1.2.5 Two modes squeezed light . . . 22
1.2.6 Multipartite entangled states . . . 25
1.2.7 Measuring light: discrete vs. continuous variables . . . 26
1.2.8 Gaussian States . . . 28

2 Computer Science Toolbox **33**
2.1 Algorithms . . . 34
2.1.1 Computational time . . . 35
2.1.2 NP complete problems . . . 36
2.1.3 Interactive proof systems . . . 40
2.2 Networks . . . 42
2.2.1 Complex networks . . . 43
2.2.2 Technological networks . . . 45
2.2.3 Information networks . . . 46
2.2.4 Social networks . . . 48
2.2.5 Biological networks . . . 49

II Protocols 51

3 Quantum verification of NP problems **53**
3.1 What is quantum advantage . . . 54
3.2 Coping with NP-completness . . . 57

3.2.1 2-out-of-4 Sat . . . 57
3.2.2 Previous work . . . 58
3.2.3 Sketch of the scheme . . . 60
3.3 The verification protocol . . . 61
3.3.1 Quantum proofs encoded in coherent states . . . 61
3.3.2 The verification test . . . 63
3.3.3 Classical complexity of verification . . . 66
3.3.4 Dealing with practical imperfections. . . . 67
3.3.5 Experimental results . . . 72
3.4 Discussion . . . 78

4 Quantum electronic voting **79**
4.1 Why electronic voting is still a bad idea . . . 81
4.2 Quantum e-voting protocol . . . 82
4.2.1 Notation . . . 82
4.2.2 High level protocol description . . . 83
4.2.3 Subroutines . . . 85
4.2.4 Quantum e-voting pseudo code . . . 90
4.3 E-voting protocol Analysis . . . 91
4.3.1 $(\sigma_H, \sigma_D, \gamma)$-Correctness . . . 93
4.3.2 ζ-Privacy . . . 94
4.3.3 Authentication . . . 96
4.3.4 Double voting . . . 96
4.3.5 Verifiability . . . 96
4.3.6 Receipt freeness . . . 97
4.3.7 Additional candidates . . . 97
4.3.8 Proof of Theorem 1 . . . 99
4.3.9 Proof of Theorem 2 . . . 100
4.3.10 Proof of Theorem 3 . . . 104
4.4 Discussion . . . 105

5 Quantum Complex Networks **107**
5.1 What is a CV network . . . 108
5.2 Arbitrary Gaussian Network . . . 110
5.2.1 Gaussian quantum states . . . 110
5.2.2 Graph states as quantum networks . . . 111
5.3 Interplay between squeezing and symplectic spectra . . . 113
5.4 A resource theory of Squeezing . . . 114
5.5 Squeezing cost for network generation . . . 115
5.5.1 Regular Networks . . . 115
5.5.2 Complex Networks . . . 118
5.6 Quantum teleportation Gaussian Networks . . . 122
5.7 Multi-path entanglement . . . 124

5.7.1 Graphical Calculus . . . 124
5.7.2 Parallel enhancement of entanglement . . . 125
5.8 Routing protocol . . . 129
5.9 Discussion . . . 134

Conclusions and Perspectives **139**

A Quantum batteries **143**
A.1 Why we need a quantum battery . . . 144
A.2 The system and charging cycle . . . 145
A.2.1 The open dynamics of the quantum battery . . . 147
A.2.2 Energetic considerations . . . 148
A.2.3 Efficient charging process . . . 150
A.2.4 Assessment of charging power and temporal considerations . . . 151
A.3 Closed-system dynamics . . . 154
A.3.1 Channel picture . . . 154
A.3.2 Continuous time evolution . . . 155
A.4 Multimode system . . . 157
A.5 Discussion . . . 157

Bibliography **172**

Acknowledgements **173**

Introduction

"*Aristotle said a bunch of stuff that was wrong. Galileo and Newton fixed things up. Then Einstein broke everything again. Now, we've basically got it all worked out, except for small stuff, big stuff, hot stuff, cold stuff, fast stuff, heavy stuff, dark stuff, turbulence, and the concept of time.*"
– Zach Weinersmith

Science was born from revolution, so it should not surprise us that scientists are somewhat used to dramatic changes in the way they observe Nature. The scientific revolution, that took place after the publication of *De revolutionibus orbium coelestium* by Copernicus and touched its climax with Newton's *Principia* after passing through the formulation of the scientific method by Galilei, profoundly altered the view of society on Nature. After accepting heliocentrism, gravity, optics, electricity and chemistry as pillars of the scientific paradigm, the succeeding groundbreaking theories such as evolutionism, genetics and radioactivity passed through almost like a piece of cake. People had witnessed the power of Science in describing natural phenomena and the tremendous technological development that followed, reshaping human society in inconceivable ways.

At the turn of 20th century, when the steamy flowers of Industrial Revolution turned into juicy electrical fruits, the positivist idea that Homo Sapiens had tamed Nature through Science and technology was largely rooted in the mind of many academics. This is apparent from the words of a Munich physics professor who advised Max Planck, pioneer of quantum theory, against going into physics, advocating that the most important things had already been discovered and there were only "a few holes" to fill. At that time, Newtonian mechanics ruled all physical explanations, light was believed to propagate in aether and the idea of the existence of atoms and molecules was in large part rejected by the scientific community.

That all suddenly changed in one year, "annus mirabilis" 1905, in which a Patent Office employee named Albert Einstein, with the tacit help of his wife Mileva Marić, published four papers that laid the foundation of all modern Physics. Ten years before his most acclaimed theory of general relativity, the iconic genius had already written the Nobel prize worthy work for his description of the photoelectric effect. In that paper, Einstein employed a mathematical concept previously developed by Planck to describe the black body radiation, but gave it a concrete physical interpretation: the energy of a ray of light is not continuously distributed but consists of discrete packets that can only be absorbed and generated as whole entities localized in space and time. Light is made of *energy quanta*!

When Einstein had baptized the concept that gave the name to the most successful theory of physics, quantum mechanics was quite far from being properly formulated. It needed a few more decades and the heated debate of dozens of geniuses to arrive to its mature version. Since then, the theory developed in a myriad of very distinct branches, ranging from solid state physics to quantum gravity. Nonetheless, some of the fundamental questions that

inflamed the fierce discussions of the early development of the field remain unanswered. In particular, Heisenberg's formulation of quantum mechanics, which is indeed the first, was able to predict the probability of observing some physical quantity of a system, disregarding the state of the system itself. However it did not explain how does Nature "know" that we are observing a system. None of the following reformulations and interpretations of the theory was able to tackle this problem in a way that is universally accepted by the scientific community and it is still a very risky matter if you want to have a pacific conversation with quantum physicists.

Quantum mechanics is hard to digest: Einstein never accepted its probabilistic nature, Schrödinger formulated the famous cat paradox to put in evidence the problems brought by its standard interpretation, while Feynman was more direct: "I think I can safely say that nobody really understands quantum mechanics". So on and so forth, after a whole century, despite all its controversies, the problems arising at all scales, the polemics it generated and all the efforts spent to find a new ultimate theory of fundamental particles and interactions, the theory of quanta has yet never failed and has contributed to the most outstanding results and predictions in the history of Science.

Alongside the enthusiasm it generated among physicists and scholars from all sciences in general, the influence of quantum mechanics very soon transcended the walls of Academia. A group of twenty years old students had independently and irreverently dared to challenge the highest authority of physics imposed by Newtonian Mechanics, that had been standing undisputed for centuries. This sensational change of the paradigm of conceiving how the laws of Nature act, brought throughout all of '900 by the new theories of Relativity and Quantum Mechanics, elegant descriptions of two different and irreconcilable worlds, shook the ground of many aspect of Human society, from art to technology, from philosophy to popular culture.

Nowadays it is not rare to see someone wearing a Schrödinger's cat t-shirt or a Dirac's equation tattoo. Nonetheless, the fame of quantum mechanics is still tied to the charm of its dark mysteries and paradoxes, while we tend to forget how much modern society was shaped by our comprehension of the mechanisms of the atomic world. It let us understand and manipulate the properties of the chemical elements, of metals and semiconductors, allowing to produce new medicines and materials, to build and miniaturize transistors and engineer superconductors. It unleashed the disruptive power of the atomic nuclei, provided new medical imaging devices and gave us lasers.

Our society would have a very different look without the technologies delivered by non-classical physics. Yet, this is only the tip of the iceberg compared to the promises offered by the forthcoming generation of quantum technologies. Devices like Light Emitting Diodes (LED), Tunnel field-effect transistors (TFET), Superconducting Quantum Interference Device (SQUID), Nuclear Magnetic Resonance (NMR) or Positron Emition Tomography (PET), in fact all require a thorough comprehension of the principles of quantum mechanics to be designed, however the description of their working principles and effects can be semi-

classical or fully classical. An actual quantum machine would be able to address individual quantum systems and extensively exploit quantum coherence in order to gain a functionality or performance which would otherwise be unattainable [17].

The very first devices arising from this second quantum revolution are quantum sensors, which are also the first quantum machines to be broadly employed for practical purposes. Quantum sensing employs quantum phenomena to perform high precision measurements beyond the sensitivity of any classical device. Examples include Avalanche Photo-Diodes that measures single photons and the new generation of Gravitational Wave Detectors. The Holy Grail of quantum technologies, however, is often considered to be quantum simulation, or in a broader sense quantum computing. The idea is that if we can control a large quantum machine, we can use it to simulate complex dynamical quantum processes, such as chemical reactions, protein folding and many-body systems. Moreover, it was proven, theoretically and only recently in experiments, that certain specific classes of mathematical problems can be efficiently solved on a quantum machine, whereas the best existing supercomputer would take a time that exceeds the expectation life of our Solar system.

The first to propose the idea of using a quantum machine to simulate complex quantum systems was again the theoretical physicist Richard Feynman. However, the first to actually provide a quantum algorithm with crucial applications for a computational task that is considered unfeasible for a standard computer was the computer scientist Peter Shor. The field of quantum information, that studies how to encode, manipulate and extract information in quantum states, bloomed from the overlap of computer science and quantum physics. The connection between the concept of information and physics, however, is actually much deeper.

The *Mathematical Theory of Communication* written by the engineer and mathematician Claude Shannon [18] , provided the first mathematical formulation for the Theory of Information. In his book, Shannon had proposed a way to quantify the information contained in some communication channel and, under suggestion of Von Neumann, he called it entropy, firstly because it shared the same formula and secondly because "nobody knows what entropy really is" [1]. This mathematical analogy with a physical quantity allowed the use of techniques from statistical mechanics and helped the development of information theory. However, it was not until the remarkable results of Szilard, Landauer and Bennett that it was realized that we can interpret information as a physical resource and we can use it to extract thermodynamical work. In the words of Charles Bennett: “Computers may be thought of as engines for transforming free energy into waste heat and mathematical work” [2]. Information is physical and we can employ physics tools to study information theory and vice versa. This is one of the reasons why quantum information seems such a promising field.

On the one hand, the development of information theoretic techniques allowed an efficient manipulation and transmission of large amounts of data with a certifiable security provided by cryptographic protocols. On the other hand, quantum mechanics permitted the mastery

of semiconductors and solid state materials and thus the mass production of the microchips and all the electronics necessary to the construction of modern telecommunication systems. The parallel and independent progress of these two fields led Humanity straight to the current Information Age and the building of one of the greatest architectures of our History: Internet.

Internet is the global telecommunication network of interconnected computers that uses a specific Internet Protocol Suite to allow communication between the devices. Internet has had a radical impact on our world, enabled secure communications at arbitrary distances and it plays a crucial role in most of the current human activities. Quantum Information promises to enhance the features of Internet and even develop new functionalities that are simply unattainable with classical technologies [3]. Such a Quantum Internet would work in parallel to the classical one that we have today, allowing quantum communication among arbitrary devices around the globe. Several intriguing applications have already been studied, including device-independent cryptography, secure authentication, clock synchronization, exponential savings in communication, quantum sensor networks and blind delegated quantum computing [4]. However, as with any revolutionary new technology, the most important applications have yet to be imagined.

We finally arrived to the main topic of this thesis. Quantum networks are a very promising technology and their study interpolates between fundamental research and real-world applications [5]. Many physical systems, such as solid state materials and large molecules like proteins can indeed be modeled as quantum networks. The underlying structure of some quantum systems can deeply influence their properties and the theoretical study of quantum networks can help the understanding of many important phenomena such as localization of coherent excitations [6], phase transitions [7], Bose-Einstein condensate [8] and quantum transport [9]. Moreover, understanding the distribution of entanglement in complex quantum structures can assist the development of efficient quantum algorithms for distributed computation [10] and even play a role in the study of decoherence free subspaces [11] and quantum gravity [12]. Finally, the main subject of this manuscript will be quantum communication networks, in which several quantum devices placed at different geographical locations are interconnected by quantum channels. Needless to say, in order to develop large scale quantum communications and build a quantum internet it is compulsory to grasp the potentialities of quantum networks and exploit all their exceptional features.

There is still a long road ahead before the full development of a quantum internet and still there is skepticism about its actual potentialities, however small-scale quantum networks have already been implemented [19] and all the preliminary stages of quantum internet seem to have interesting use-cases. In the very first place, it should allow the performance of Quantum Key Distribution (QKD) among its nodes. While standard cryptography provides secure communications based on mathematical assumptions or on the presumed technological limitations of the adversaries, that could reveal incorrect, QKD is based on physical experimentally tested principles. Stephen Wiesner was the first to propose the idea

of a quantum cryptographic protocol that could be used to produce unforgeable quantum money [20], although his paper was rejected by IEEE Information Theory journal. His approach was then formalized by Bennett and Brassard who devised the first QKD protocol named BB84 [13]. Many developments followed these first discoveries and quantum cryptography became one of the most active fields of quantum information.

The world's first quantum key distribution network was the DARPA Quantum Network [14], that became fully functional in 2003, operating among 10 optical nodes across Boston and Cambridge for three years. Since then, several of these incipient forms of quantum internet have been implemented and new ones are currently being deployed even with some limited commercial applications. In 2017, the first satellite-to-ground QKD was finally established [15] which could acutely boost the scaling of these networks, that is currently severely limited by the absence of efficient quantum repeaters. In addition, many research laboratories are studying and implementing quantum networks with new remarkable attributes that go beyond simple QKD [16].

In this manuscript, we will be interested in three different levels of quantum internet, with distinct architectures and increasing stages of complexity. For each of these levels we will propose a quantum protocol that achieves a functionality that would be impracticable or impossible on the current classical Internet. Along with mathematical rigor, the criterion will be that of practicality, we will thus analyse the properties of the protocols in realistic conditions and, for the first of these, we will present an experimental implementation.

We do not know yet what will be the actual architecture of quantum internet, however we do know that the substrate for the quantum information carriers will be photons! Electromagnetic waves have in fact always been the privileged medium for telecommunications. Photons can travel long distances at the maximum speed allowed by the laws of physics without losing coherence, they interact very little with the molecules of atmosphere, can efficiently be transported in waveguides and they can be distributed and manipulated easily with our current technology. In addition, light has always been of major importance in quantum mechanics since its very first conception and the language of quanta is in large part borrowed from classical optics. As a consequence, we will dedicate a significant part of the attention to the study of quantum optics and the properties of quantum states of light.

This thesis is divided in two distinct parts. The first part is devoted to the review of the mathematical tools and techniques required to understand the subjects of our works. Advanced topics in quantum information, quantum optics, computer science and network theory will be covered, however the reader with familiarity with any or all of these arguments can skip the corresponding sections without any complication. Specifically, chapter 1 will be dedicated to the concepts concerning quantum mechanics and quantum optics, whereas chapter 2 deals with Computer Science and Networks. In the second part, we will explore the properties of quantum networks and explain the protocols we devised. Our journey through the various stages of Quantum Internet begins in chapter 3 with the simplest communication architecture, an end-to-end quantum channel between two agents.

We will show a protocol that allows a simple quantum client to verify the solution of a complex mathematical problem provided by an untrusted server without having access to the full solution. We will present the infeasibility of such scheme without quantum resources and the first experimental demonstration of a computational quantum advantage in the interactive setting. Chapter 4 presents our second stage of quantum Internet, that is set on a larger quantum network in which all the agents are connected to a central node that distributes a quantum state. The protocol that we developed implements an electronic-voting scheme that exploits an untrusted multipartite entangled quantum source to carry on an election without relying on election authorities, whose result is publicly verifiable without compromising the robustness of the scheme and that can be readily implemented with state-of-the-art technology. Finally, in chapter 5 we show the last stage of quantum internet, where we will examine arbitrary complex topologies of quantum networks, characterizing their correlations, estimating the scaling of their cost while the networks grow and evaluating the performances of a routing protocol.

Although this thesis was devoted to the main topic of developing communication protocols for quantum internet, part of the efforts of this doctorate were employed to another project, presented in appendix A. In this work, we show how we can use quantum states of light as batteries, testing the efficiency and power of the charging procedure when the battery is immersed in a noisy environment.

It is now time to stop shooting the breeze, so fasten your seat belt and get ready to begin our road trip through quantum optical networks.

Part I

Background

Chapter 1

Quantum Toolbox

1.1 The principles of Quantum Mechanics 10
1.1.1 First Postulate: physical states 10
1.1.2 Second postulate: physical quantities 11
1.1.3 Third postulate: measurement 11
1.1.4 Fourth postulate: dynamics 12
1.1.5 Fifth postulate: composite systems 12
1.2 Quantum states of light 13
1.2.1 From Maxwell to Dirac 13
1.2.2 Fock states 18
1.2.3 Coherent states 19
1.2.4 Squeezed states 20
1.2.5 Two modes squeezed light 22
1.2.6 Multipartite entangled states 25
1.2.7 Measuring light: discrete vs. continuous variables 26
1.2.8 Gaussian States 28

1.1 The principles of Quantum Mechanics

Quantum Mechanics provides the most accurate description of the non-relativistic physical properties of Nature at the atomic and subatomic scale. The first successful formalization of the description of the atomic spectra was supplied by Heisenberg's matrix mechanics, which is the first formal theory of quantum mechanics. Later the same year, Schrödinger created an equivalent formalism based on wave mechanics. We call the Heisenberg picture the formulation in which operators carry the time dependence, whereas the Schrödinger picture is the one in which the states are time dependent. Another important formulation that we will use in this thesis is the Dirac picture (or interaction picture), in which both the states and operators depend on time. The following axioms are formulated in the Schrödinger picture, which has the most intuitive physical interpretation, however they can be equivalently stated in all the possible representations of the quantum theory. The following principles are in essence based on the standard *Dirac-Von Neumann axioms*, introduced by Dirac [21] and Von Neumann [22], with a modern interpretation drawn from [23].

1.1.1 First Postulate: physical states

"Each physical system is associated with a complex Hilbert space $\mathcal{H}$ in which a scalar product is defined. The state ψ of an isolated system at fixed time is described by a unit-norm vector in $\mathcal{H}$. "

States in the Hilbert space can be conveniently represented through Dirac's bra-ket notation. The state ψ can be expressed with a ket $|\psi\rangle$, its dual vector is called a bra $\langle\psi|$, while the scalar product with state ϕ is $\langle\phi|\psi\rangle$. The linearity of the Hilbert space implies that any linear combination of states belonging to $\mathcal{H}$ is a physical state of the system. So for example, if both $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ then

$$\alpha |\psi\rangle + \beta |\phi\rangle \in \mathcal{H}, \forall \alpha, \beta \text{ s.t. } |\alpha|^2 + |\beta|^2 = 1. \tag{1.1}$$

Furthermore, if two vectors only differ by a global phase factor they represent the same physical state, e.g. $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ are the same state for all real θ.

The building block of digital information is the *bit* which takes one of the possible Boolean values $\{0, 1\}$. Conversely, the unit digit of quantum information is the qubit, which describes the simplest non-trivial quantum system, that has a Hilbert space with dimension 2 and is spanned by any orthonormal basis with two vectors, such as $\{|0\rangle, |1\rangle\}$. Such *computational basis* is the basic element of quantum computation and it can be implemented on a large number of physical systems.

1.1.2 Second postulate: physical quantities

"Every physical quantity $\mathcal{A}$ is described by a linear self-adjoint operator $\hat{A}$ acting on $\mathcal{H}$. The eigenvalues of $\hat{A}$ form a basis for the Hilbert space."

The operator $\hat{A}$ is called an observable and represents some property of a physical system that, in principle, can be measured. The fact that it is self-adjoint (or Hermitian) implies that its eigenvalue spectrum is real. The eigenvalues of $\hat{A}$ correspond to the possible values of the dynamical variable associated to the physical quantity $\mathcal{A}$. In many cases, the degrees of freedom of a quantum system are quantized, meaning that the spectrum of the associated observable is discrete. Discrete spectra are usually associated with systems that are bound in some sense (mathematically, confined to a compact space). The position and momentum operators have continuous spectra in an infinite domain, but a discrete (quantized) spectrum in a compact domain [24] and the same properties of spectra hold for angular momentum, Hamiltonians and other operators of quantum systems.

A self-adjoint operator with a discrete spectrum can be expressed in terms of its eigenvalues a_n and the corresponding orthogonal projection onto the space of eigenvectors with eigenvalue a_n:

$$\hat{A} = \sum_n a_n \left|a_n\right\rangle \left\langle a_n\right| = \sum a_n \hat{A}_n, \tag{1.2}$$

where $\hat{A}_n = \left|a_n\right\rangle \left\langle a_n\right|$ are the projectors on the eigenstate $\left|a_n\right\rangle$. For unbounded operators in an infinite-dimensional space, the definition of self-adjoint and the statement of the spectral theorem are more subtle and we refer to the book of Serafini [25] for a formal definition.

1.1.3 Third postulate: measurement

"The measurement of an observable $\hat{A}$ on a quantum state $\left|\psi\right\rangle$ yields an outcome a_n, that is an eigenvalue of $\hat{A}$ with corresponding eigenvector $\left|A_n\right\rangle$, with a priori probability

$$P(a_n) = \left\langle\psi|A_n\right\rangle \left\langle A_n|\psi\right\rangle = \left\langle\psi\right| \hat{A}_n \left|\psi\right\rangle . \tag{1.3}$$

If the outcome a_n is attained, then the normalized quantum state just after the measurement is $\frac{\hat{A}_n|\psi\rangle}{P(a_n)^{1/2}}$. "

A measurement is some process in which information about the state of a physical system is acquired by an observer. In quantum mechanics this process is intrinsically random and the set of possible outcomes is given by the eigenvalues of the observable quantity, while the probability of measuring that outcome is the square of the scalar product between the state and the eigenvector associated to the outcome. Just after the measurement the state *collapses* in the corresponding eigenstate and if a second measurement is immediately repeated the same outcome is deterministically obtained. If many quantum systems are all identically prepared in the state ψ, then the expectation value of the outcome will be

$$\langle\hat{A}\rangle = \left\langle\psi\right| \hat{A} \left|\psi\right\rangle . \tag{1.4}$$

1.1.4 Fourth postulate: dynamics

"The equation of motion of a quantum system $|\psi(t)\rangle$ evolving in time is governed by the Schrödinger equation

$$i\hbar\frac{d}{dt}|\psi\rangle = \hat{H}(t)|\psi\rangle\,, \tag{1.5}$$

where i is the imaginary unit, $\hbar$ is the reduced Planck constant[1] and $\hat{H}(t)$ is the time dependent self-adjoint operator associated to the Hamiltonian of the system."

If the system's Hamiltonian does not depend on time the equation becomes an eigenvalue equation

$$\hat{H}|\psi\rangle = E|\psi\rangle\,, \tag{1.6}$$

where E is the energy of the system and $|\psi\rangle$ an eigenvector of $\hat{H}$. In *Schrödinger picture*, the state of a system at time t evolved from the initial state $|\psi_0\rangle$ at time $t = 0$ following equation 1.5 is given by

$$|\psi(t)\rangle = \hat{U}(t)|\psi_0\rangle\,, \tag{1.7}$$

where $\hat{U}(t)$ is a unitary operator, such that the product with its conjugate transpose is the identity $\hat{U}(t)\hat{U}^\dagger(t) = \mathbb{1}$. In the case where $\hat{H}$ is time independent we can express $\hat{U}(t) = e^{-\frac{i}{\hbar}t\hat{H}}$.

1.1.5 Fifth postulate: composite systems

"The Hilbert space of a composite system is constituted by the tensor product $\otimes$ of the Hilbert spaces of its components. "

The composite state Ψ of ψ_1 and ψ_2 can be expressed in many ways:

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = |\psi_1\psi_2\rangle\,. \tag{1.8}$$

An operator acting on $|\Psi\rangle$ will be the tensor product of the operators acting on the Hilbert spaces of the two systems

$$\hat{O}_{12}|\Psi\rangle = \hat{O}_1 \otimes \hat{O}_2|\Psi\rangle = \hat{O}_1|\psi_1\rangle \otimes \hat{O}_2|\psi_2\rangle\,. \tag{1.9}$$

If a composite system can be expressed as a tensor product of the components, like in equation 1.8, then it is called separable. The majority of the states in a composite Hilbert space are not separable, for instance

$$\frac{1}{\sqrt{2}}(|\psi\rangle_1|\phi\rangle_2 + |\phi\rangle_1|\psi\rangle_2), \tag{1.10}$$

[1] $\hbar = \frac{h}{2\pi} = 1.0545718 \times 10^{-34}$ m^{2}kg/s, where h is the Planck constant.

where the subscripts specify the subsystem. This is called an entangled state, which is a superposition of two or more separable states, and plays a crucial role in many applications of quantum theory.

Isolated quantum systems are called pure states and can be expressed with the ket notation. However, real systems are never perfectly isolated and must interact with an environment that decreases their purity and adds randomness to their description. In this case, the states can be identified with the so-called density matrix

$$\hat{\rho} = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| , \tag{1.11}$$

where p_i is the classical probability of the system being prepared in the state $|\psi_i\rangle$. If the quantum state is pure, its density matrix reduces to $\hat{\rho} = |\psi\rangle \langle\psi|$.

1.2 Quantum states of light

Historically, the first attempts to the description of quantum mechanics only dealt with the motion of microscopic particles under the effect of classical fields. Despite its unintuitive consequences, that defied the most brilliant minds of the past century and contributed to its popularization, the resulting theory was indeed a prodigy of mathematical elegance, in which from a set of simple axioms it was possible to derive some of the most spectacular predictions of science, that laid down the foundations for the technological development that we are enjoying nowadays.

Nonetheless, that tells only the first part of the story, the one that physicists like to call *first quantization*. In order to go further ahead and understand all the recent progresses that lead us to a deeper comprehension of the quantum world, we need to abandon the single particle description and embrace the dynamical picture of interaction and forces among the tiny constituents of our Universe. In other words, we need a *quantum field theory*.

In the following paragraphs we will bridge the gap between the physical radiation field, in which information will be encoded, and its quantum representation. In order to do so, we need to start from the equations that revealed the true essence of light and reach those that showed its quantum traits. In literature we find a plethora of approaches to the quantization of the electromagnetic field [21], [26]–[29], whereas for procedures akin to quantum information processing we suggest [25], [30].

1.2.1 From Maxwell to Dirac

The Maxwell's equations form the foundations for classical electromagnetism, optics and electrical circuits. In vacuum they read:

$$\begin{cases} \nabla \cdot \boldsymbol{E} = 0, \\ \nabla \cdot \boldsymbol{B} = 0, \\ \nabla \times \boldsymbol{E} = -\partial_t \boldsymbol{B}, \\ \nabla \times \boldsymbol{B} = \frac{1}{c^2} \partial_t \boldsymbol{E}. \end{cases} \tag{1.12}$$

The first striking consequence of these equations is that they can be cast in the form of a wave equation for the electric and magnetic field, whose velocity matches the speed of light $c = (\mu_0 \epsilon_0)^{-1/2}$. This led Maxwell to propose that light and radio waves are propagating waves of the electromagnetic field at different frequencies.

The energy of the free electromagnetic field in a region of space of volume V at time t is given by

$$H_R = \frac{\epsilon_0}{2} \int_V [E^2(\boldsymbol{r}, t) + c^2 B^2(\boldsymbol{r}, t)] d^3\boldsymbol{r}. \tag{1.13}$$

A suitable choice to describe the field of quantized radiation is to consider light confined in a volume of finite size V with periodic boundary conditions. Under this condition the state is described by a discrete succession of dynamical values rather than a continuum and is represented mathematically, in the base of linearly polarized plane waves, by a particularly simple expression:

$$\boldsymbol{f}_j(\boldsymbol{r}, t) = \boldsymbol{\epsilon}_j e^{i(\boldsymbol{k}_j \cdot \boldsymbol{r} - \omega_j t)}, \tag{1.14}$$

where the wave vectors $\boldsymbol{k}_j$ assume discrete values allowed by the boundary conditions, $\omega_j = ck_j$ is the angular frequency of the wave and $\boldsymbol{\epsilon}_j$ is a unit polarization vector perpendicular to the wave vector $\boldsymbol{k}_j \cdot \boldsymbol{\epsilon}_j = 0$. For simplicity, a global index j was used for wave vector and polarization. A normalized solution of the Maxwell's equations, like the one of equation 1.14, is called a *mode* of the electromagnetic field. The time independent ortho-normality relation reads

$$\int_{V' > V} \boldsymbol{f}_j^*(\boldsymbol{r}, t) \cdot \boldsymbol{f}_l(\boldsymbol{r}, t) = V \delta_{jl}. \tag{1.15}$$

The linearity of equations 1.12 implies that any electric and magnetic fields that satisfy the periodic boundary conditions can be expressed as a linear combination of the modes 1.14

$$\begin{aligned} \boldsymbol{E}(\boldsymbol{r}, t) = \boldsymbol{E}^+(\boldsymbol{r}, t) + \boldsymbol{E}^-(\boldsymbol{r}, t) = \sum_j A_j (\alpha_j \boldsymbol{f}_j(\boldsymbol{r}, t) + \alpha_j^* \boldsymbol{f}_j^*(\boldsymbol{r}, t)), \\ \boldsymbol{B}(\boldsymbol{r}, t) = \boldsymbol{B}^+(\boldsymbol{r}, t) + \boldsymbol{B}^-(\boldsymbol{r}, t) = \sum_j \frac{A_j}{c} (\alpha_j \bar{\boldsymbol{f}}_j(\boldsymbol{r}, t) + \alpha_j^* \bar{\boldsymbol{f}}_j^*(\boldsymbol{r}, t)), \end{aligned} \tag{1.16}$$

where the electric and magnetic fields were split in positive and negative frequency parts, $\bar{\boldsymbol{f}}_l = \boldsymbol{k}_l \times \boldsymbol{f}_l / k_l$ denotes the modes of the magnetic field, A_n are real constants with the

electric field physical dimension[2] and α are dimensionless complex valued amplitudes depending on the initial conditions. The absolute value of this complex amplitude represents the intensity of the field and will in turn be proportional to the number of photons. Notice that the discreteness of the field modes was explicitly imposed by the boundary condition of finite volume. If we take the limit $V \to \infty$ we recover the free propagating field with a continuity of modes. A comprehensive discussion of the optical modes of quantum fields can be found in Ref. [31].

We can now define two new dynamical variables

$$\begin{cases} q_n = 2A_n\sqrt{\frac{\epsilon_0 V}{\omega_n}}\mathrm{Re}[\alpha_n] = \sqrt{2}\mathrm{Re}[\tilde{\alpha}_n] \\ p_n = 2A_n\sqrt{\frac{\epsilon_0 V}{\omega_n}}\mathrm{Im}[\alpha_n] = \sqrt{2}\mathrm{Im}[\tilde{\alpha}_n] \end{cases}, \tag{1.17}$$

where we redefined the complex amplitudes of the field as $\tilde{\alpha}_n = A_n\sqrt{\frac{\epsilon_0 V}{2\omega_n}}\alpha_n$. Now, if we substitute 1.16 into equation 1.13 employing the ortho-normality relation 1.15, and rewrite it as a function of the variables of eq. 1.17, the total energy of the electromagnetic field becomes explicitely the hamiltonian of the harmonic oscillator:

$$H_R = \frac{1}{2}\sum_n \omega_n(q_n^2 + p_n^2). \tag{1.18}$$

Everything we did so far resides in the domain of classical Electromagnetism. The standard procedure to quantize a classical theory, the so-called *canonical quantization* was introduced in 1926 by Paul Dirac in his doctoral thesis [32] and was employed by himself to develop the theory of Quantum Electro-Dynamics [21], described by Richard Feynman as "the jewel of physics" for its extremely accurate predictions of the interaction between radiation and matter and for being the very first theory to achieve a full agreement between quantum mechanics and special relativity [33].

We will now present a simplified derivation of the quantized electromagnetic field akin to the one originally handed out by Dirac. It all starts with one simple assumption, *the correspondence principle* formulated by Bohr, stating that the behavior of a quantum system must reproduce classical mechanics in the limit of large quantum numbers [34]. Accordingly, we begin with the hamiltonian equations of motion of the classical field:

$$\frac{df(\boldsymbol{q},\boldsymbol{p})}{dt} = \{f, H\}_{PB} + \frac{\partial f}{\partial t}, \tag{1.19}$$

where we introduced the time independent hamiltonian H, which is the total energy of the system, and a dynamical quantity of the system f function of the $2N$ canonical variables

[2] Of order $10^{-2}[V]/[m]$ for a mode in a typical laser-gas cavity [27].

$\boldsymbol{q} = \{q_i\}_{i=1}^N$ and $\boldsymbol{p} = \{p_i\}_{i=1}^N$, for a system with N degrees of freedom, and the Poisson's bracket defined as

$$\{f, g\}_{PB} = \sum_{i=1}^{N} \left(\frac{\partial f}{\partial q_i} \frac{\partial g}{\partial p_i} - \frac{\partial f}{\partial p_i} \frac{\partial g}{\partial q_i} \right). \tag{1.20}$$

The canonical coordinates describe in phase space the dynamics of the system governed by the hamiltonian H and by definition satisfy the following relations:

$$\{q_i, q_j\}_{PB} = 0,\ \{p_i, p_j\}_{PB} = 0,\ \{q_i, p_j\}_{PB} = \delta_{ij}, \tag{1.21}$$

where δ_{ij} is the Kronecker delta.

Overlooking some mathematical details that are unimportant for our purposes, we can reduce the process of canonical quantization to two essential operations[3]:

1. All the dynamical quantities associated to the observables of the system are mapped into hermitian operators: $f(\boldsymbol{q}, \boldsymbol{p}) \longrightarrow \hat{f}(\hat{\boldsymbol{q}}, \hat{\boldsymbol{p}})$;
2. all the Poisson brackets are deformed and mapped into operator's commutation relation: $[\hat{f}, \hat{g}] = i\hbar\{f, g\}_{PB}$, where i is the imaginary unit and $\hbar$ is the reduced Planck constant.

The commutator $[\hat{f}, \hat{g}] = \hat{f}\hat{g} - \hat{g}\hat{f}$ can be applied to the canonical variables to derive the canonical commutation relation [4]

$$[\hat{q}_i, \hat{p_j}] = i\hbar\delta_{ij}. \tag{1.22}$$

From these equation, considering $\hat{q}$ and $\hat{p}$ as conjugated canonical variables, we can recover the well-known Heisenberg uncertainty principle

$$\Delta q \Delta p \geq \frac{\hbar}{2} \tag{1.23}$$

that gives a lower bound on the product of the standard deviations of complementary variables. The hermitianity of the quantum operators ensures that their eigenvalues, that correspond to the possible values of a measurement, are real. The commutator of two hermitian operators must be purely imaginary, which justify the necessity of the imaginary unit. In

[3] Although this is the naive approach initially proposed by Dirac, it was later noted by Hip Groenewold that a general systematic correspondence between quantum commutators and Poisson brackets could not hold consistently [35]. The consistent correspondence mechanism between the quantum commutator and the deformation of the poissonian brackets (today called the Moyal bracket), and in general between quantum operators and classical observables can be implemented through the Wigner-Weil transform.

[4] The uniqueness of the canonical commutation relation between the position and momentum operators is guaranteed in its exponential form by the Stone-von Neumann theorem [36].

addition, the presence of the reduced Planck constant lets us recover the classical case when the quantum numbers associated are much larger than the Planck constant, such that $\hbar \sim 0$.

We have now all the ingredients to quantize the free propagating electromagnetic field. It can be easily verified that the variables 1.17 satisfy the Hamilton's equations 1.19 and are thus the canonical variables of our classical electromagnetic theory. We can thus map these variables into hermitian quantum operators acting on the Hilbert space of the electromagnetic field and representing its complementary observables. The hamiltonian governing the dynamics of the field propagating in free space will hence become

$$\hat{H}_R = \frac{\hbar}{2} \sum_n \omega_n (\hat{Q}_n^2 + \hat{P}_n^2), \tag{1.24}$$

where the dimensionless operators $\hat{Q}_n := \hat{q}_n/\sqrt{\hbar}$ and $\hat{P}_n := \hat{p}_n/\sqrt{\hbar}$ satisfy the canonical commutation relation $[\hat{Q}_i, \hat{P}_j] = i\delta_{ij}$ and are thus subject to the Heisenberg uncertainty principle. As a consequence, the measurement outcome of the field will fluctuate even when its expectation value is null. We will show in the following that these fluctuations can be used to encode and process quantum information.

Quantum harmonic oscillator

It should not surprise us that equation 1.24 is the hamiltonian of the quantum harmonic oscillator. Indeed, it is a well known fact that the harmonic oscillator is described by one of the few dynamical equations that can be solved analytically and, in the words of the physicist Sidney Coleman, "The career of a young theoretical physicist consists of treating the harmonic oscillator in ever-increasing levels of abstraction".

In order to characterize the properties of the quantum harmonic oscillator, we will make use of the ladder operators method developed by Dirac, that allows the extraction of the energy eigenvalues without directly solving the differential equations of motion. From equation 1.17 we notice that the canonical variables are proportional to the real and imaginary parts of the complex amplitudes of the electromagnetic field, whose modulus represents the intensity of the light. These amplitudes become in turn quantum operators after the quantization mapping and are related to the quadrature operators through a unitary transformation:

$$\begin{cases} \hat{a}_n := \frac{\hat{Q}_n + i\hat{P}_n}{\sqrt{2}} \\ \hat{a}_n^\dagger := \frac{\hat{Q}_n - i\hat{P}_n}{\sqrt{2}} \end{cases} . \tag{1.25}$$

These operators are not hermitian, since $\hat{a}_n$ and its adjoint $\hat{a}_n^\dagger$ are not equal. If we evaluate their commutator we get $[\hat{a}_n, \hat{a}_n^\dagger] = 1$, while if we cast them into the hamiltonian 1.24 we end up with

$$\hat{H}_R = \sum_n \hat{H}_n = \sum_n \hbar\omega_n (\hat{a}_n^\dagger \hat{a}_n + 1/2) \tag{1.26}$$

.

1.2.2 Fock states

Let us now consider a single mode of the field by dropping the index n and evaluate their commutator with the so called number operator $\hat{N} := \hat{a}^\dagger \hat{a}$

$$[\hat{N}, \hat{a}^\dagger] = \hat{a}^\dagger, \; [\hat{N}, \hat{a}] = -\hat{a}. \tag{1.27}$$

If we take an eigenstate $|m\rangle$ of the number operator such that $\hat{N}|m\rangle = m|m\rangle$, the commutation relation yields

$$\hat{N}\hat{a}^\dagger |m\rangle = (\hat{a}^\dagger \hat{N} + [\hat{N}, \hat{a}^\dagger])|m\rangle = (m+1)\hat{a}^\dagger |m\rangle .$$

The state $\hat{a}^\dagger |m\rangle$ is still an eigenstate of the number operator, with eigenvalue increased by 1. Similarly

$$\hat{N}\hat{a}|m\rangle = (m-1)\hat{a}|m\rangle .$$

Given the fact that the number operator commutes with the single mode hamiltonian operator $\hat{H} = \hbar\omega(\hat{N} + 1/2)$ this property has the following interesting consequence

$$\hat{H}\hat{a}^\dagger |m\rangle = (E_m + \hbar\omega)\hat{a}^\dagger |m\rangle ,$$

where $\hat{H}|m\rangle = E_m|m\rangle = \hbar\omega(m + 1/2)|m\rangle$. In linear algebra $\hat{a}^\dagger$ and $\hat{a}$ are called ladder operators because, as we have seen, they allow to increase or decrease the eigenvalue of the number operator. In quantum field theory they are referred to as creation and annihilation operators respectively and they represent the generation or absorption of particles, which correspond to quanta of energy or to excitations in the particle field. Since the square of the length of ket $\hat{a}|m\rangle$ is just $\langle m|\hat{N}|m\rangle \geq 0$ we have that the hamiltonian is lower bounded $E_m \geq \frac{\hbar\omega}{2}$. Let $|0\rangle$ be an eigenstate of $\hat{H}$ corresponding to the lowest eigenvalue $\frac{\hbar\omega}{2}$, so that

$$\hat{a}|0\rangle = 0. \tag{1.28}$$

Starting from this state, that we assume normalized, we can form a succession of states

$$|0\rangle , \quad \hat{a}^\dagger |0\rangle = |1\rangle , \ldots \frac{1}{\sqrt{m!}}\hat{a}^{\dagger m}|0\rangle = |m\rangle \tag{1.29}$$

that are all eigenstates of the hamiltonian with eigenvalues $E_m = \hbar\omega(m + 1/2)$, extending to infinity. The kets in eq. 1.29 are called Fock states and correspond to the stationary states of the harmonic oscillator. They represent the number of excitations, or particles, in a given mode. The normalization comes from the fact that

$$\langle 0|\hat{a}^m(\hat{a}^\dagger)^m|0\rangle = m\langle 0|\hat{a}^{m-1}(\hat{a}^\dagger)^{m-1}|0\rangle = m!. \tag{1.30}$$

Since all the dynamical variables in our problem can be expressed in terms of the ladder operators, these must form a complete set. Thus, any state in the Hilbert space of the harmonic oscillator can be expressed as a linear combination of the Fock states:

$$|\psi\rangle = \sum_m \psi_m |m\rangle = \sum_m \frac{\psi_m}{\sqrt{m!}}(\hat{a}^\dagger)^m |0\rangle . \tag{1.31}$$

In strike contrast with their simple theoretical description, the experimental production of the Fock states is rather involved. The vacuum state $|0\rangle$ of a mode of frequency ω is trivially produced if we consider an optical system at temperature $T \ll \hbar\omega/k_B$. The preparation of the first excited state, or single photon state, $|1\rangle$, on the other hand, is already challenging to produce. Faint laser pulses can approximate single photons in some applications [37], however they cannot show antibunching, namely the effect of producing a predictable (sub-poissonian) statistics in the photon number distribution whose variance is smaller than its mean [38], and other typical quantum signatures. On-demand single emitters, such as single molecules, Rydberg atoms, diamond colour centres and quantum dots often suffer from low emission efficiency. Finally, heralded single photons can be created by first generating a photon pair and then using the detection of one of the photons to isolate the other one. These sources rely on the non-linear optical process of parametric downconversion (PDC) in bulk crystals and waveguides, and four-wave mixing (FWM) in optical fibers. To the present day, these sources represent the workhorse of single photon production, although their mechanism is inherently probabilistic. An extensive review of the subject of single photons production and detection is found in Ref. [39].

1.2.3 Coherent states

As a consequence of the quantization procedure, one can describe in the interaction picture or in the free-field Heisenberg picture the quantum field of a free propagating monochromatic wave satisfying Maxwell's equations as

$$\hat{\boldsymbol{E}}(\boldsymbol{r},t) = \boldsymbol{E}^{+}(\boldsymbol{r},t) + \boldsymbol{E}^{-}(\boldsymbol{r},t) = \boldsymbol{f}_j(\boldsymbol{r},t)\hat{a} + \boldsymbol{f}_j^{*}(\boldsymbol{r},t)\hat{a}^{\dagger}. \tag{1.32}$$

Glauber and Sudarshan, developing the quantum theory of optical coherence, remarked that the eigenstates of the positive frequency part of the electric field operator are of crucial importance in optics as they display the maximal degree of coherence [26]. They are called coherent states and are eigenstates of the annihilation operator

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,, \tag{1.33}$$

with the eigenvalue $\alpha = |\alpha|e^{i\theta} \in \mathbb{C}$. These states, that were originally formulated by Schrödinger in his attempt to search for solutions to the Schrödinger equation that satisfy the correspondence principle [40], represent the simplest and most common case of states living in an infinite dimensional Hilbert space. They can be expressed in the Fock state basis as a sum over all possible occupation numbers

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. \tag{1.34}$$

The state $|\alpha\rangle$ can be obtained from the vacuum through the displacement operator

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle = \exp\left(\alpha\hat{a}^{\dagger} - \alpha^{*}\hat{a}\right)|0\rangle\,. \tag{1.35}$$

The probability distribution of the number of photons in the state is Poissonian

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{e^{-\mu}\mu^n}{\sqrt{n!}}, \tag{1.36}$$

with mean photon number $\mu = \langle\alpha|\hat{N}|\alpha\rangle = |\alpha|^2$ and variance $(\Delta\mu)^2 = |\alpha|^2$. This implies that in the limit of large μ we recover the detection statistics of a classical stable wave. Furthermore, the mean values of the operators $\hat{Q}$ and $\hat{P}$ follow the classical trajectory of the harmonic oscillator and their standard deviations minimize the uncertainty principle. For these reasons the coherent states are often dubbed as quasi-classical states. Nonetheless, these states are broadly used in quantum information protocols, notably but not exclusively in quantum key distribution experiments [41], for the ease of their preparation and manipulation, for which classical techniques and technologies can be put to use. Their hidden quantum nature can in fact be unveiled when examining the scalar product between two coherent states, that reads

$$\langle\alpha|\beta\rangle = e^{-|\alpha-\beta|^2}. \tag{1.37}$$

This means that these states become approximately orthogonal only for $|\alpha - \beta| >> 1$, e.g. in the classical limit, while for low photon numbers they are never perfectly distinguishable.

From equation 1.25 we can derive the time-ordered square of the quadrature operators $\hat{Q}^2$ and $\hat{P}^2$ from which we can compute the quadrature variances of the coherent state:

$$(\Delta Q)^2 = (\Delta P)^2 = \frac{1}{2}. \tag{1.38}$$

Hence, coherent states not only saturate the uncertainty principle, but their noise property are perfectly balanced in the two quadratures. Coherent states will be the main subject of chapter 3, while in the next section we will study a different class of quantum states that, while minimizing the Heisenberg principle, have an unequal expectation value of the variances of the quadrature operators.

1.2.4 Squeezed states

The quadrature of an electromagnetic field is said to be squeezed if it has a standard deviation strictly smaller than that of a coherent state. In order to obey the uncertainty principle, the other quadrature needs to have a standard deviation larger than that of a coherent state, e.g. it is anti-squeezed. The single mode squeezed vacuum state is defined by

$$|\xi\rangle := \hat{S}(\xi)|0\rangle = \exp\left[\frac{1}{2}\left(\xi\hat{a}^2 - \xi^*(\hat{a}^\dagger)^2\right)\right]|0\rangle, \tag{1.39}$$

where $\hat{S}(\xi)$ is the squeezing operator and $\xi = se^{i\phi}$ is the complex squeezing parameter. The squeezed vacuum state is generated by the degenerate parametric down conversion in an optical parametric oscillator, or via four-wave-mixing [42]. These non-linear optical

processes implement an interaction that is quadratic in the ladder operators, effectively transforming each photon $|n\rangle_I$ of the input pump into indistinguishable photon pairs at the output $|2n\rangle_O$. To see why this would imply a quadrature squeezing let us consider the superposition state of a vacuum and a two photon number state,

$$|\psi\rangle = C\left(|0\rangle - \frac{s}{\sqrt{2}}|2\rangle\right), \tag{1.40}$$

where the normalization factor $C = 1 + O(s^2)$ for $s \ll 1$. The mean value of the position operator $\hat{Q} = (\hat{a} + \hat{a}^\dagger)/\sqrt{2}$ is zero in this state, while its variance equals

$$(\Delta Q)^2 = \langle\psi| \frac{(\hat{a} + \hat{a}^\dagger)^2}{\sqrt{2}} |\psi\rangle = \frac{1}{2} - s + O(s^2). \tag{1.41}$$

Hence the state $|\psi\rangle$ is squeezed in position for positive s. If we write the state in 1.39 in the Fock basis we can see that it can be expressed as a superposition of number states with even photon number

$$|\xi\rangle = (\text{sech}s)^{1/2} \sum_{n=0}^{\infty} \left[-\frac{1}{2}e^{i\phi}\text{tanh}s\right]^n \frac{[(2n)!]^{1/2}}{n!} |2n\rangle . \tag{1.42}$$

We can use this expression to evaluate the expectation values of the various combinations of ladder operators. In particular we have that the average photon number is

$$\langle\hat{N}\rangle = \langle\xi| \hat{a}^\dagger\hat{a} |\xi\rangle = \text{sinh}^2 s, \tag{1.43}$$

which is independent of the phase ϕ. The mean photon number vanishes in the absence of squeezing $s = 0$, reducing to the ordinary vacuum state, but increases sharply as the magnitude of the squeezing parameter increases. The photon number variance is accordingly

$$(\Delta N)^2 = 2\langle\hat{N}\rangle(\langle\hat{N}\rangle + 1). \tag{1.44}$$

The photon number statistics of a squeezed vacuum state is thus super-poissonian. On the other hand, the expected value of the ladder operators on this state is null and as a consequence the first moment of the quadratures is 0. Their variances, however, read

$$(\Delta Q)^2 = \frac{1}{2}\left[e^{2s}\text{sin}^2(\phi/2) + e^{-2s}\text{cos}^2(\phi/2)\right] \tag{1.45}$$

$$(\Delta P)^2 = \frac{1}{2}\left[e^{-2s}\text{sin}^2(\phi/2) + e^{2s}\text{cos}^2(\phi/2)\right] \tag{1.46}$$

If we fix $\phi = 0$ we have $(\Delta Q)^2 = 1/(2\Delta P)^2 = \frac{e^{-2s}}{2}$, hence normally when we have a positive squeezing parameter we are considering a state squeezed in the $\hat{Q}$ quadrature and

for small s we recover equation 1.41. In any case, the uncertainty principle is saturated for all values of s and ϕ.

Another important class of quantum states is constituted by the coherent squeezed states, which are simply displaced squeezed vacuum states:

$$|\alpha, \xi\rangle = \hat{D}(\alpha)\hat{S}(\xi)\,|0\rangle \tag{1.47}$$

The squeezed coherent state retains the reduced noise of the squeezed vacuum but it also acquires the non-zero signal of the coherent state and can give rise to a sub-Poissonian photon statistics, which is a genuinely quantum effect [43]. Figure 1.1 resumes the attributes of generalized coherent states in phase space, evidencing their noise features.

The reduced variance of squeezed light finds notable uses in many quantum information processing applications [44] and in optical high-precision measurements, in which it helps improving the signal-to-noise ratio without increasing the optical power. For example, squeezing was employed to enhance the measurement sensitivity in spectroscopic measurement of atomic cesium [45] and to improve the new generation of gravitational wave detectors VIRGO in Italy [46] and LIGO in the United States [47].

1.2.5 Two modes squeezed light

We showed above one of the most common methods to produce squeezing. Spontaneous parametric down-conversion (SPDC) is a nonlinear optical process in which a photon of a powerful laser field propagating through a second-order non-linear optical medium may split into two photons of lower energy. The frequencies, wave vectors and polarizations of the generated photons are governed by phase-matching conditions. Single-mode squeezing, such as that in the above example, is obtained when SPDC is degenerate and the two generated photons are indistinguishable in all their parameters: frequency, direction, and polarization. The quantum state of the optical mode into which the photon pairs are emitted exhibits squeezing. If, on the other hand, we let the SPDC to be implemented in a non-degenerate configuration , the output of the interaction with the non-linear medium will be pairs of distinguishable photons. As a consequence of the conservation of the energy, the momentum and the angular momentum of the incident photons of the pump, the output pairs will be correlated in frequency, wavevector and polarization. Essentially, all the degrees of freedom of the photons share non-classical correlations and we refer to the two electromagnetic modes as entangled. This state can be written in the Fock basis as

$$|\xi_{AB}\rangle := \hat{S}_2(\xi)\,|00\rangle_B = \exp\left[-\left(\xi\hat{a}\hat{b} - \xi^*\hat{a}^\dagger\hat{b}^\dagger\right)\right]|00\rangle = \mathrm{sech}s\sum_{n=0}^{\infty}\left[-e^{i\phi}\tanh s\right]^n|nn\rangle\,, \tag{1.48}$$

where $\hat{a}$ is the annihilation operator acting on mode A and $\hat{b}$ is the annihilation operator acting on mode B, and we used the compact notation $|nn\rangle = |n\rangle_A \otimes |n\rangle_B$. If the individual

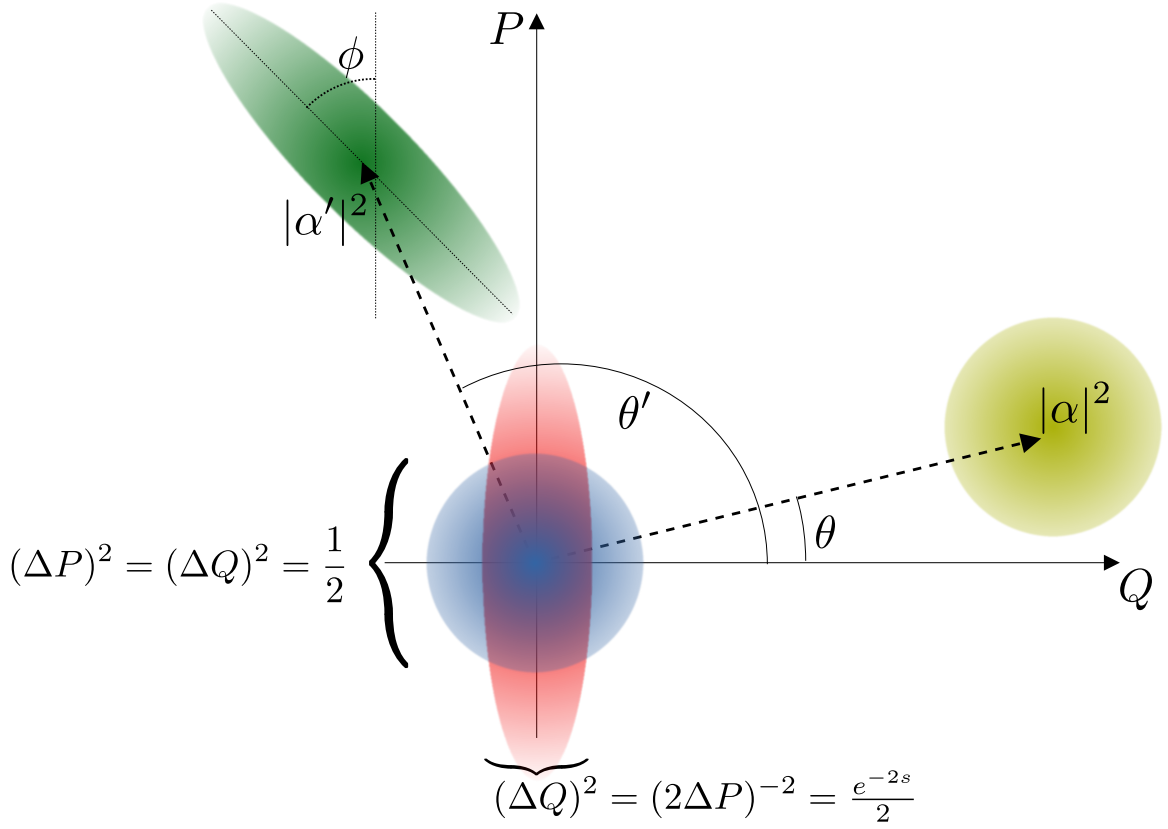


Figure 1.1: Schematic representation in phase-space of the vacuum state (blue), the squeezed vacuum (red), the coherent state (yellow) and the squeezed coherent state (green).

modes of this entangled state were considered separately and delivered at two different position to two agents, Alice and Bob, they would appear as a classical statistical mixture. This can be seen by tracing out the mode B from the overall state:

$$\hat{\rho}_A = Tr_B\left[|\xi_{AB}\rangle\langle\xi_{AB}|\right] = \sum_{n_B}\langle n_B|\xi_{AB}\rangle\langle\xi_{AB}|n_B\rangle = \text{sech}^2 s\sum_{n_A=0}^{\infty}\left[\tanh s\right]^{2n_A}|n_A\rangle\langle n_A|\,. \tag{1.49}$$

By symmetry, the state in the individual mode B will be identical. This is a thermal state of light, where the diagonal density matrix indicates a classical statistical distribution of the photon numbers with no quantum coherence. It represents a quantum description of classical chaotic light, incapable of giving rise to interference and with stochastic fluctuations in the amplitude following a Gaussian probability distribution. As a consequence of the entanglement however, even though the outcome of a measurement performed by Alice is completely random, the state of Bob after Alice's detection is perfectly predictable. Conversely, the variance of the quadratures in the individual mode is

$$(\Delta Q_A)^2 = (\Delta Q_B)^2 = (\Delta P_A)^2 = (\Delta P_B)^2 = \frac{1+R^4}{4R^2}, \tag{1.50}$$

with $R = e^s$. Thus each mode of the overall state exceeds the vacuum fluctuations for all $s > 0$. Nonetheless, if we consider the operator $\hat{Q}_{AB} = \frac{\hat{Q}_A - \hat{Q}_B}{\sqrt{2}}$ we have a variance of

$$(\Delta Q_{AB})^2 = \frac{e^{-2s}}{2}, \tag{1.51}$$

which is below that of a vacuum state for all $s > 0$. Thus, even though each individual mode presents a noise in the quadratures that grows with s, the fluctuations in the difference of the quadratures are suppressed. The same thing happens for the sum of the momentum quadratures.

For infinite squeezing $s \to \infty$ the positions of A and B are completely uncertain, but at the same time precisely equal, whereas the momenta are uncertain but precisely opposite. This state is the basis of the famous quantum non-locality paradox in its original formulation of Einstein, Podolsky and Rosen [48]. The three scientists argued that by choosing to perform either a position or momentum measurement on her portion of the state, Alice remotely prepares either a state with a certain position or one with a certain momentum at Bob's location. But according to the uncertainty principle, certainty of position implies complete uncertainty of momentum, and vice versa. In other words, by choosing the setting of her measurement apparatus, Alice can instantly and remotely, without any interaction, prepare at Bob's station one of two mutually incompatible physical realities. The authors used this argument to claim that the quantum particles must contain some hidden variables that decide the outcome of their measurement. This apparent contradiction to basic principles of causality has challenged quantum mechanics as complete description of physical reality and triggered a debate that continues to this day [49].

In general, non-linear optical process have a particularly weak coupling constant that makes the probability of generating photon pairs very low, thus with a small squeezing parameter. If we take $s \ll 1$ we can neglect the higher order terms in the series of equation 1.48 and the resulting two mode squeezed state will be approximately

$$|\xi_{AB}\rangle \underset{s\ll 1}{\simeq} \frac{1}{\sqrt{1+s^2}}(|00\rangle + s\,|11\rangle). \tag{1.52}$$

This is a coherent superposition of both modes being in a vacuum state and in a single photon state. In particular, if we assume a Type-I SPDC process, the two single photons will be in the same polarized state, that we can assume being a balanced superposition of vertical and horizontal polarized states $|d\rangle = |h\rangle + |v\rangle$. If we separate the two modes spatially and measure the mode B with a single photon detector, a click in the detector would herald the presence of a single photon in mode A, effectively post-selecting the states without a vacuum. Before doing that, we can prepare another two modes squeezed vacuum $|\xi_{CD}\rangle$ with

modes C and D diagonally polarized $|d\rangle$, and make these two states interfere in a polarized beam splitter. The bosonic nature of photons will make the indistinguishable states exit from the same output of the beam splitter, preparing the whole state of the four modes in a superposition of all modes being vertically polarized, all modes being horizontally polarized and all modes being vacuum. If we measure modes B and D, disregarding the states that have no photons and thus produce no clicks in a single photon detector, we can subtract the vacuum from the state. The resulting state will be an entangled state of modes A and C

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|hh\rangle + |vv\rangle), \tag{1.53}$$

which is a superposition of both photons being in the horizontal and vertical polarizations. In photonic quantum information processing, the polarization of a single photon is often used to encode a single bit $\{0, 1\}$, so we can express state $|\phi^+\rangle$ in the computational basis by setting $|h\rangle \rightarrow |0\rangle$ and $|v\rangle \rightarrow |1\rangle$. In this case, the kets $|0\rangle$ and $|1\rangle$ do not represent the number of photons in the state, but exclusively the information thereby encoded, hence state $|\phi^+\rangle$ should not be confused with the state 1.52. From now on, to avoid ambiguity, we will explicitly specify when a state is expressed in the Fock basis.

The state 1.53 is called a Bell pair and is the single photon version of the EPR pair. The Bell states are four specific entangled states that constitute an orthonormal basis for the Hilbert space of two qubits and can be expressed in the computational basis as

$$\begin{aligned} |\phi^\pm\rangle &:= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \\ |\psi^\pm\rangle &:= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \end{aligned} \tag{1.54}$$

In literature, the EPR state and the Bell states are often regarded as the same thing. However, while Bell explicitly used the states 1.54 , hence exploiting the discrete degrees of freedom of qubits, in the EPR article the authors refer to position and momentum of particles, thus continuous non-commuting variables. We will discuss in a dedicated section the difference between the discrete and continuous variables formalisms and how to adress them operationally.

If, like with the EPR, the individual states of the Bell pair are given to Alice and Bob at distant positions, the outcomes of their measurements are at the same time perfectly random and perfectly correlated with each other. In a seminal paper from 1964 [50], John Bell used these states together with simple probability theory as a counter argument against the EPR point of view, showing that no local hidden variable theory can predict these correlations.

1.2.6 Multipartite entangled states

Similarly to the EPR pairs, Bell states find applications in a number of quantum communication scenarios, such as superdense coding [51] and quantum teleportation [52]. The

working principle is the entanglement that enables the possibility to yield shared randomness at arbitrary distance among two agents. If we wish to extend this property to a greater number of participants we need a multipartite quantum state. We can obtain such state by letting quantum systems interact in some manner. The easiest way to do this with linear optics is to use a beam splitter with two different quantum modes as input. For example, the two modes squeezed state can be obtained by mixing two single modes coherent states squeezed in position and momentum respectively in a balanced beam splitter.

A significant multipartite state that will be prominent in chapter 4 is the GHZ state, named after Greenberger, Horne and Zeilinger, who studied its properties in 1989 [53]. A GHZ state with N particles in a Hilbert space of dimension 2 is expressed in the computational basis as

$$|GHZ\rangle = \frac{|0\rangle^{\otimes N} + |1\rangle^{\otimes N}}{\sqrt{2}}. \tag{1.55}$$

In simple words, it is a quantum superposition of all subsystems being in state 0 with all of them being in state 1. This state is non bi-separable, meaning that every possible bi-partition of this state is entangled. GHZ states are used in several protocols in quantum communication and cryptography, for example, in secret sharing [54], for their capability to distribute correlated randomness among many agents.

1.2.7 Measuring light: discrete vs. continuous variables

In the previous paragraphs we described light fields under different aspects, emphasizing either the discrete degrees of freedom, such as polarization, or the continuous ones, such as quadratures. Some quantum states, like the Bell states of equation 1.54, are naturally described in terms of a finite discrete set of kets. These states are most suited to encode quantum information in the form of qubits and are thus akin to yield digital quantum computation and communication. The enormous advantages provided by the usage of digital data, owing to the trailblazing discoveries of Shannon on coding and of Turing on computation and the following revolution in Information Technology, were naturally inherited by Quantum Information science. The latter, in fact, is usually instructed in terms of qubits and logic gates, whereas the first problems in a course of Quantum Mechanics typically deal with the continuous time evolution of the position of a quantum state, in order to facilitate the transition from Classical Physics. The paradigm of digital Quantum Information processing is commonly termed Discrete Variables (DV).

In Quantum Theory, the description of a state reflects the physical quantity we want to study and thus the measurement apparatus used to estimate it. All observables define a complete orthonormal basis for the Hilbert space of a quantum system, that can always be described in terms of the eigenvectors of the associated Hermitian operator. In Quantum Optics the DV formulation of Quantum Information operationally translates to the employment of Single Photon Detectors (SPD). In contrast to a normal photodetector, which generates an analog signal proportional to the flux of photons, a single-photon detector

emits a measurable electric pulse every time a photon is detected. Moreover, SPDs can sharply increase the signal-to-noise ratio [55] and the time resolution of the optical signal [56]. On the other hand, their functionality is intrinsically probabilistic and they are normally able only to detect the presence of "at least" one photon and not to actually resolve the photon number. This is one of the limits to the scaling of Quantum computing with single photons, also known as Linear Optical Quantum Computing. In this computing model, the qubit is produced as a superposition of two modes of the electromagnetic field (typically orthogonal polarizations), is processed with linear optics and then measured with SPDs. The projective operator of such detectors is expressed in the Fock basis as:

$$\hat{D} = \mathbb{1} - |0\rangle\langle 0| = \sum_{i\geq 1} |i\rangle\langle i|, \tag{1.56}$$

with degenerate eigenvalues 0 and 1. Thus, the probability of detecting a photon on a coherent state will be

$$Pr(\alpha) = \langle\alpha|\hat{D}|\alpha\rangle = 1 - e^{-|\alpha|^2}. \tag{1.57}$$

This formula will be helpful in chapter 3. SPDs can be used, as we said, to herald single photons and even to generate entangled states. However, when dealing with linear optical quantum computing, it is necessary to process the states before the measurement and then post-select only the instances in which the outcome revealed the presence of photons.

When we quantized the electromagnetic field we favoured as a natural choice the phase-space description, in which the quadratures of the field can take any real value. This is the typical case of bosonic particles such as photons. In modern telecommunications, information (either digital or analog) is transmitted by modulating the amplitude and the phase of the quadratures of the optical carrier. The technologies and techniques developed in the years by electrical engineers could be employed to study and exploit the properties of non-classical light. This is the standpoint of the Continuous Variables (CV) paradigm, that aims at taking advantage of the continuity of the degrees of freedom of the quantum states to perform analog quantum computation, notably exploiting the non-commutativity of the quadratures of a single mode electromagnetic field. In practice, this is done by measuring the states with homodyne detection. This is a technique that allows to extract information encoded in the modulation of an oscillating signal by comparing it with a Local Oscillator that would be identical to the signal if it carried null information. In Quantum Optics, homodyne detection is used to measure a weak quantum signal field $\boldsymbol{E}_S$ by letting it interfere with the strong classical local oscillator $\boldsymbol{E}_L$, in a balanced beam-splitter, whose action is:

$$(\boldsymbol{E}_S, \boldsymbol{E}_L) \rightarrow (\frac{\boldsymbol{E}_S + \boldsymbol{E}_L}{\sqrt{2}}, \frac{\boldsymbol{E}_S - \boldsymbol{E}_L}{\sqrt{2}}). \tag{1.58}$$

If we measure the two outputs of the beam-splitter with standard photodiodes (not SPD), assuming perfect detection efficiency the difference between the measured photocurrents will be:

$$\hat{N}_- = |\alpha_L|\left(\hat{a}e^{-i\theta} + \hat{a}^\dagger e^{i\theta}\right) \propto \hat{Q}_\theta, \tag{1.59}$$

where the local oscillator is assumed to be a coherent state with complex amplitude $\alpha_L = |\alpha_L|e^{i\theta}$ and $\hat{Q}_\theta$ is the generalized quadrature, reducing to $\hat{Q}$ for $\theta = 0$ and to $\hat{P}$ for $\theta = \pi/2$. For more details on homodyne detection in single and multi modes states of light and its application to continuous variables quantum information consider the following review by Lvovsky and Raymer [57].

Both these paradigms, DV and CV, are completely equivalent and each one can be described in terms of the other. While in the DV formulation the building block for information processing is the simplest non-trivial quantum state, the qubit which is formed by a coherent superposition of two orthogonal modes, in CV the most elementary quantum state is a single mode of the quantum harmonic oscillator, that we call qumode. Be that as it may, all quantum objects have both discrete and continuous degrees of freedom and the neglect of part of them at the end of the day inevitably results in decoherence and thus the loss of quantum information. It is therefore crucial to bear this in mind when choosing one of the two formalisms.

1.2.8 Gaussian States

Continuous variables quantum states are, in essence, states described by variables that obey the canonical commutation relation in eq. 1.22 [25]. In quantum field theory, this is the typical case of bosonic systems like photons and is thus the privileged formalism to describe quantum optics, whereas fermions would obey the anticommutation relation. It can be easily shown that the algebra of canonical commutating variables does not allow a representation through finite size matrices, unlike fermionic states such as electrons. As a consequence CV states necessarily live in infinite dimensional Hilbert spaces even when a finite set of modes is considered. Accordingly, the description of the dynamics or the general properties of such states is often simply intractable. There is however a crucial class of CV states, characterized by a Gaussian distribution in the phase-space and thus called Gaussian states, that considerably simplifies the mathematical requirements to be described.

Gaussian states are ordinarily produced in a vast number of experimental setups in quantum optics [58], trapped ions [59], opto-mechanics [60], atomic ensembles [61] and certain superconducting systems [62] and we have already encountered a few examples, such as coherent and squeezed states. The restriction to Gaussian states severely limits the potentialities allowed by an infinite dimensional Hilbert space and is often criticized on the account of the fact that Gaussian states can be described by a classical probability distribution and can be efficiently simulated on a classical computer [63]. Be that as it may, Gaussian states possess many intriguing quantum properties and play a significant role in the development of quantum technologies, for instance in continuous variables quantum key distribution (CVQKD) [64] and in quantum metrology [65].

Any Hamiltonian that is at most quadratic in the canonical quadratures $\hat{\mathbf{Q}}$ and $\hat{\mathbf{P}}$ implements a Gaussian operation, hence preserving the Gaussian nature of the phase-space dis-

tribution of the system [66]. If the input state is Gaussian, it will stay Gaussian during the time evolution and it can be completely characterized by the first two moments of the quadratures

$$\bar{\mathbf{r}} = Tr[\rho_G \hat{\mathbf{r}}], \tag{1.60}$$

$$\sigma = Tr[\rho_G \{(\hat{\mathbf{r}} - \bar{\mathbf{r}}), (\hat{\mathbf{r}} - \bar{\mathbf{r}})^T\}], \tag{1.61}$$

where $\{A, B\} = AB + BA$ is the anticommutator of the operators A and B, ρ_G is the density matrix of the Gaussian state and $\hat{\mathbf{r}} = (\hat{Q}_1 ... \hat{Q}_N, \hat{P}_1 ... \hat{P}_N)^T$ (xp-ordering [25]).

Instead of analysing the evolution of the density matrix of an infinite dimensional Hilbert space, we can focus on the dynamics of the first and second moments of the canonical variables, satisfying the commutation relation

$$[\hat{\mathbf{r}}, \hat{\mathbf{r}}^T] = i\Omega = i \begin{pmatrix} \mathbf{0} & \mathbb{1} \\ -\mathbb{1} & \mathbf{0}, \end{pmatrix} \tag{1.62}$$

where Ω is a $2N \times 2N$ skew-symmetric matrix associated to the N dimensional Hilbert space. Equivalently, one can write

$$\sigma + i\Omega > 0, \tag{1.63}$$

which is the phase-space formulation of Heisenberg uncertainty principle, also called Robertson-Schrödinger uncertainty relation [67].

The most general second-order Hamiltonian can be written as

$$\hat{H} = \frac{1}{2} \hat{\mathbf{r}}^T H_m \hat{\mathbf{r}} + \hat{\mathbf{r}}^T \mathbf{r}, \tag{1.64}$$

where $\mathbf{r}$ without the hat is a $2N$ dimensional real vector and H_m is a symmetric $2N \times 2N$ matrix known as Hamiltonian matrix. Accordingly, the general Gaussian state density matrix is

$$\hat{\rho}_G = \frac{e^{-\beta \hat{H}}}{\mathrm{Tr}[e^{-\beta \hat{H}}]}, \tag{1.65}$$

where the parameter $\beta = 1/k_B T$ represents the inverse temperature up to the Boltzmann constant and in the limit $\beta \to \infty$ we recover the purity of the state.

The linear term in the Hamiltonian $\hat{\mathbf{r}}^T \mathbf{r}$ implements a displacement in the mean values of the quadratures, such as the displacement of the vacuum to obtain a coherent state in eq. 1.35. On the other hand, the quadratic term $\hat{\mathbf{r}}^T H_m \hat{\mathbf{r}}$ acts on the covariance matrix of the state. The covariance matrix of a Gaussian state encodes the noise properties of the system as well as the correlation among different modes. Given our definition of canonical operators the covariance matrix of the vacuum is $\sigma_0 = \frac{1}{2}\mathbb{1}$, however there is not a coherent

definition in the literature so it is always necessary to carefully check which notation was adopted.

If we are interested exclusively in the noise properties and correlations of our system we can neglect the linear terms in the Hamiltonian and consider a quadratic Hamiltonian of the form $\hat{H} = \hat{\mathbf{r}} H_m \hat{\mathbf{r}}^T$. The evolution in Heisenberg picture of the vector operators $\hat{\mathbf{r}}$ under this Hamiltonian is given by

$$\dot{\hat{\mathbf{r}}} = \Omega H_m \hat{\mathbf{r}}. \tag{1.66}$$

Disregarding the first moments and considering solely the evolution of the covariance matrix σ the evolution of the state from the vacuum after a time t is implemented by

$$S_H = e^{\Omega H_m t}. \tag{1.67}$$

The operator S_H, naturally preserving the symplectic form under congruence $S_H \Omega S_H^T = \Omega$ in order to satisfy the commutation relations, is by definition a symplectic matrix of the real symplectic group $\mathcal{S}_{2N,\Re}$. A complete analysis of the real symplectic group and its applications to optics and quantum mechanics can be found here [68].

We can obtain the most general pure Gaussian state covariance matrix by applying S_H by congruence to the vacuum covariance matrix

$$\sigma = S_H \sigma_0 S_H^T = \frac{S_H S_H^T}{2}. \tag{1.68}$$

In quantum optics the physical process underlying the production of such states relies on spontaneous parametric down conversion. We can consider, as a specific example, a mode-locked femto-second laser that outputs ultra-short pulses, whose spectrum in the Fourier space is a frequency comb constituted of several frequency components peaked in ω_{p0}. This pump is fed into a $\chi^{(2)}$ non-linear crystal, spawning the parametric process that can be approximated[5] by the following interaction Hamiltonian

$$\hat{H}_I = i\hbar g \sum_{jk} L_{jk} \left(\hat{a}_j^\dagger \hat{a}_k^\dagger - \hat{a}_j \hat{a}_k \right), \tag{1.69}$$

where $\hat{a}_j^\dagger$ and $\hat{a}_j$ are the ladder operators, respectively creating and destroying a photon in the j^{th} field mode, g is a squeezing parameter per unit time and the summation is over all the possible modes. The *joint spectral amplitude* L_{jk}, which is the product of the laser pump amplitude α_p and the phase matching function $f_{m,n}$, describes the probability that a photon at frequency ω_p is converted in two photons at frequencies ω_j and ω_k. From energy conservation, $\omega_p = \omega_j + \omega_k$ which gives rise to the correlation between the modes

[5]The actual Hamiltonian is an integral over all the possible frequencies for pump signal and idler. Since we have a comb we can think about it as a sum, discretizing the frequencies.

j and k. Moreover, the conservation of momentum and angular momentum correlate the wavevector and the polarization as well.

Casting the definition of ladder operators 1.25 into equation 1.69 we obtain

$$\hat{H}_I = \hbar g \sum_{jk} L_{jk} \left(\hat{Q}_j \hat{P}_k + \hat{P}_j \hat{Q}_k \right) = \hbar g \hat{\mathbf{Q}} L \hat{\mathbf{P}} + \hat{\mathbf{P}} L \hat{\mathbf{Q}}. \tag{1.70}$$

Singular value decomposition allows one to write the symplectic transformation in the so called Bloch-Messiah decomposition [31] as a product of three matrices, an orthogonal, a diagonal and an orthogonal $S_H = O\Delta O'$, which can be interpreted as a basis rotation, a squeezing in the diagonal basis and another rotation. The mode-basis in which the covariance matrix is diagonal and each component is independently squeezed is named the supermode basis. In [69], [70] where the pump and the phase matching function can be described by a Gaussian spectral profile, the supermode basis corresponds to Hermite-Gauss spectral modes. [6]. The squeezing values of Δ can be derived from the eigenvalues of the Hamiltonian $\hat{\mathcal{H}}_I$, while the orthogonal matrix O can be interpreted as a measurement basis change or, equivalently, as a passive linear optical transformation. The other orthogonal matrix O' is simplified in the product $S_H S_H^T$ and can be disregarded:

$$\sigma = \frac{S_H S_H^T}{2} = \tfrac{1}{2} O \Delta^2 O^T \tag{1.71}$$

State-of-the-art ultrafast laser technology allows the possibility of shaping the spectral profile of femto-second coherent pulses. Furthermore, one can engineer the dispersion properties of the crystal to get the quasi-phase matching conditions by creating a periodic structure in the nonlinear medium. These techniques permit an optimal control on the laser pump amplitude α_p and the phase matching function f_{jk} respectively, therefore an excellent manipulation of the joint spectral amplitude L_{jk} and consequently on the squeezing matrix Δ can be obtained.

The temporal modes in the pulse can then be addressed and measured through homodyne detection. By pulse shaping the local oscillator spectral profile, one can change the measurement basis and select the mode that will be measured at the same time, enabling the creation of arbitrary connections between the qumodes of the state. Although we focused the attention on a specific quantum optical implementation, there are many different techniques that allows a practical manipulation of Gaussian states and the mathematical formalism described above can be applied to all such cases.

[6] If they are not exactly Gaussian (the phasematching is a sinc function) they can also be considered Hermite-Gauss for all practical purposes.

We completed our first review chapter about the description of the quantum states of light that will be employed in our protocols. We can now proceed to the second chapter that is focused on Computer Science topics, notably on the formalization of algorithms and the theory of networks.

Chapter 2

Computer Science Toolbox

2.1 Algorithms . . . 34
2.1.1 Computational time . . . 35
2.1.2 NP complete problems . . . 36
2.1.3 Interactive proof systems . . . 40
2.2 Networks . . . 42
2.2.1 Complex networks . . . 43
2.2.2 Technological networks . . . 45
2.2.3 Information networks . . . 46
2.2.4 Social networks . . . 48
2.2.5 Biological networks . . . 49

2.1 Algorithms

Several centuries ago, in the region of modern-day Iraq, an influential mathematical treatise started to circulate. The book provided an exhaustive account of solving for the positive roots of polynomial equations up to the second degree and it was entitled "The Compendious Book on Calculation by Completion and Balancing", also known as "Al-jabr". It was the first text to teach algebra as an independent discipline, in an elementary form and for its own sake, and it was used until the sixteenth century as the principal mathematical textbook of European universities. The author, who was a prominent polymath, bears a prestige that overcomes his yet vast mathematical production. His name al-Khwarizmi, formerly latinized to *Algorithmi*, baptized a foundational method in science and one of the most impactful branches of modern mathematics and computer science [71].

An algorithm is an unambiguous finite set of instructions that are required to perform some specific task, solve a general class of mathematical problems, or perform a computation. It is an effective procedure that can be expressed in a well-defined formal language in a finite amount of space and time. In other words, whoever the agent executing the algorithm is, they should be able to understand it and implement it in bounded time. For example, if the agent is a person and the algorithm is a recipe written in English, they could use it to prepare a delicious meal in time for dinner. Conversely, if the agent is a computer and the algorithm is a program written in Python, they can compile the program and execute it to recognize pictures of cats on the internet very efficiently. Ultimately, anything a computer can do reduces to computing a mathematical function on some input values. There is a humongous number of protocols that can estimate some remarkably complex functions and deal with some of the most intractable mathematical problems. However, the time required to perform these computations, although limited, is not necessarily small and this is a crucial aspect both for the formal description and classification of the algorithms and for their impact on society. Some of the most insightful problems would require a time that exceeds the life expectation of the Sun to be accomplished on the finest existing super-computer. In spite of the fact that the average computer speed doubles every 18 months, as stated by Moore's law, this trend will eventually stop before such problems become tractable [72]. The recent theoretical and experimental progresses in the field of quantum computation have shown that quantum mechanics can, in some measure, change this paradigm. Nonetheless, to understand how to use it properly, we need to learn how to classify algorithms based on the number of elementary computer operations.

The treatment of the theory of computational complexity of the following paragraphs is based on these references [73]–[75], in particular the discussion of NP-completeness hinges on [76].

2.1.1 Computational time

According to the legend, the game of chess has its origin in India between 400 and 600 CE. The mythical brahmin Sissa would have invented the game to entertain and teach the king who, in turn, gratefully questioned the wise priest what he would desire as a reward. The old man requested that the monarch place one grain of rice on the first square of the chessboard, two on the second and so on, doubling the number of grains for each square up to the 64th. The naive ruler was delighted that he could so easily fulfil his mentor's request but he soon had to realize the impossibility of the test. Only on the last square of the chessboard, there would be $2^{63} = 9,223,372,036,854,775,808$ grains of rice, enough to overwhelm the whole surface of India and its inhabitants. The astute Sissa had tricked the king and thought him a valuable lesson on exponential growth [77].

This myth is exemplary to showcase the importance of efficient algorithms. Imagine you want to build a program that breaks a password expressed as a Boolean string of N variables. If you have absolutely no information, your best option is to brute force all the 2^N possible combinations. Notwithstanding, if you find out that the password has some structure you could employ this additional information to restrict the number of operations, which might be, with some luck, a polynomial in N. In this case, we would say that the algorithm is *efficient* regardless of the type of polynomial we are considering. In fact, any polynomial, even if it has a huge exponent and a large constant, will always be smaller than an exponential if we take N big enough. In practice, although for small N the inefficient algorithm may be faster, its running time on any computer will be asymptotically intractable.

Expressing running time in terms of basic computer operations is a big simplification. As a matter of fact, the execution time of any of such steps depends crucially on the specific details of the architecture on which it is performed and may change dramatically from one execution to another and even from one step to the next one. It would be impossible to take into account all these minutiae and, at the same time, provide a general result that applies to any processor. This leads to yet another simplification, which is the neglect of the smaller order terms of the polynomial and of the constant factor.

In order to formalize all this and provide an operational way to compute the computational time of a protocol, we can introduce the *Big O* notation, also called Bachmann-Landau notation, that characterizes functions according to their growth rates:

Definition 2.1.1. *Let $f(n)$ and $g(n)$ be functions from positive intergers to positive reals. We say $f = O(g)$ (f is big Oh of g) if there is a constant c and a positive integer n' such that $f(n) < cg(n)$ for all $n > n'$.*

The functions $f(n)$ and $g(n)$ can be thought of as running times of two different algorithms with input size n. Different functions with the same growth rate may be represented using the same O notation. The letter O is used because the growth rate of a function is also

referred to as the *order*. For instance, the function $h(n) = 10n^5 + 500n + 1000log(n)$ is of the order n^5, $h = O(n^5)$. The big O notation usually only provides an upper bound on the growth rate of the function, thus it is sometimes necessary to refer to other symbols to describe other types of bounds on asymptotic rates. The ones that will be used in this manuscript are:

- $f = \Omega(g)$, when $g = O(f)$;
- $f = \Theta(g)$, when $f = O(g)$ and $f = \Omega(g)$.

2.1.2 NP complete problems

We now have a formal approach to analyze algorithms based on their efficiency. This method can be used to classify mathematical problems in *complexity classes* depending on their usage of time (or even memory and space) resources. The complexity of a problem is the running time of the best algorithms that allow solving the problem as a function of its input size, which is the number of variables n required to fully specify the instance of the problem. The complexity of a class of problems, on the other hand, is the complexity of the hardest instance of a set of problems. Hence, if we define A a specific set of mathematical problems that shares some general similarities and for which we know that the best algorithm to solve them runs in polynomial time, then the computational complexity of the class A is polynomial. However, if there is a set B in which even just one instance of the problems that takes a number of operation that is greater than any polynomial, than the computational complexity of B is not polynomial and it is generally referred to as exponential.

The existence of polynomial time algorithms is far from being meaningless. Most exponential time algorithms are merely variations of a brute force search across all possible solutions, whereas polynomial time algorithms are generally enabled only through some deeper insight into the structure of a problem. These algorithms exemplify the power of mathematical intuition, providing a general approach to solve some important problems on a machine, whose performances strongly improve with the enhancement of computer technology and whose running time does not explode for slightly larger instances of the same problem. For all these reasons there is a widely accepted unspoken agreement that a problem has not been "well-solved" until a polynomial time algorithm is known for it. The set of problems for which an efficient algorithm is known is called **P**:

Definition 2.1.2. *A problem is in **P** if its solution is a YES/NO answer (decision problem) that can be found by an algorithm on a computer in polynomial time.*

In the previous example we would have said that $A \in \mathbf{P}$ while $B \notin \mathbf{P}$. Conveniently, the complexity class **P** contains a lot of helpful natural problems such as checking if a word is a palindrome, sorting a dictionary in alphabetical order, testing if a number is prime and multiplying matrices.

Nonetheless, there are many problems with crucial applications for which a polynomial time algorithm is not known. Among these, we have the coloring of a geographical map using k colors (graph coloring), filling a backpack of limited capacity with the most valuable items from a list (knapsack problem) and finding the shortest round trip to visit a list of cities (traveling salesman problem). These problems may look simple if pictured on a small scale, but becomes extremely complex when many variables are in play. Furthermore, they are pivotal in many use-cases of scheduling, logistics and optimization.

Among all the possible formulations of mathematical instances, those that lie in **P** are relatively few. An important complexity class, though, is constituted by the set of decision problems, for which the answer is YES or NO, whose solution can be verified efficiently:

Definition 2.1.3. *A problem is in **NP** if it is a decision problem for which, if we are given a proof, a computer can verify in polynomial time if it is or not a solution.*

While **P** clearly stands for *polynomial*, **NP** is the abbreviation of *non-deterministic polynomial*, meaning that it can be efficiently solved on a non-deterministic Turing machine[1]. We can safely assert that **P** is contained in **NP**, however deciding whether a problem is in **NP** but not in **P** may sound a bit arbitrary. As a matter of fact, we claim that a problem is not contained in **P** on the grounds that nobody could find an polynomial time algorithm to solve it yet. It might be the case that one day we will find an efficient solution to all the problems contained in **NP**, causing the so-called *collapse of the polynomial hierarchy*. In spite of that, it is largely believed that this is not the case and that, ultimately

$$\mathbf{P} \neq \mathbf{NP} \tag{2.1}$$

Proving or disproving this conjecture is one the major problems of computer science and of math in general. It is one of the seven Millennium Prize Problems selected by the Clay Mathematics Institute, each of which carries a 1,000,000 US $ prize for the first correct solution.

There are a few examples of problems that were incorrectly believed not to be solvable in efficient time, such as linear programming [78] and the primality test [79]. A huge breakthrough in the field was caused by the discovery of an efficient quantum algorithm for integer factorization by Peter Shor [80]. This finding yields outstanding direct implications both for science and for our every-day life. In fact, the most widely used cryptographic algorithm, the RSA, is based on the hardness of factoring a big number in primes [81]. In a world where a quantum device is able to carry out Shor's algorithm for an arbitrary input size it will be necessary to switch several widely-used asymmetric cryptographic protocols to post-quantum cryptographic schemes or to quantum key distribution [82].

[1] A non-deterministic Turing machine is a theoretical model of computation in which, at each elementary step, more possible actions can be taken. In principle, it is as if during the computation each time the computer needs to take a decision the number of machines is doubled, until one of the computers find the correct solution. If the fastest of these theoretical computers finds the solution in polynomial time, then the problem was in **NP**.

On these grounds, what are the evidences that make us think that equation 2.1 is correct, e.g. that some specific problems do not have efficient algorithms? Well, at the very least we have the intuitive argument that in our everyday experience there are problems that are hard to solve but for which the solutions are easy to verify. This is the position argued by Scott Aaronson who stated [83]:

> "If P = NP, then the world would be a profoundly different place than we usually assume it to be. There would be no special value in "creative leaps," no fundamental gap between solving a problem and recognizing the solution once it's found."

Equation 2.1 is a cornerstone of the theory of **NP complete** problems, which will be a key topic in our discussion of chapter 3. However, overconfidence in an unproven mathematical assumption should never be advocated, and proofs of $\mathbf{P} = \mathbf{NP}$ are being explored as well. A few paragraphs above, before defining **NP**, we cited three special problems: graph coloring, knapsack and traveling salesman. It can be proved that there is an efficient algorithm that transforms each of these problems in any of the other two. This algorithm is called *reduction* and it is a widely used instrument in computational complexity theory to show that some problems are at least as difficult as some others. The pivotal result of NP completeness theory is that all the hardest problems in **NP** can be reduced from one to any other, in fact they can all be thought of as different representations of the same problem.

Definition 2.1.4. *A problem is **NP complete** if it can be reduced to the hardest problem in **NP**.*

A direct consequence of NP completeness theory is that if one finds a polynomial time algorithm for an **NP complete** problem, than equation 2.1 is obviously false! This is apparently not believed to be the case, however it would be the right way to proceed if one wanted to see the collapse of the polynomial hierarchy and, along with, in case equation 2.1 holds and stands tall, we have a practical tool to bound the computational complexity of many problems.

Which is, then, the hardest problem that can be efficiently verifiable? This question is answered by a fundamental unproven assumption in computational complexity theory, namely the exponential time hypothesis, formulated by Impagliazzo and Paturi [84], which implies equation 2.1 but it is more general and has important consequences for computation, communication and structural complexity theories.

Conjecture 2.1.1. *(The exponential time hypothesis) The 3-SAT problem cannot be solved in subexponential time in the worst case.*

The 3-SAT is a Boolean satisfiability problem, namely the problem of determining if there exists a string of boolean variables that satisfies a given formula. The hardness of these

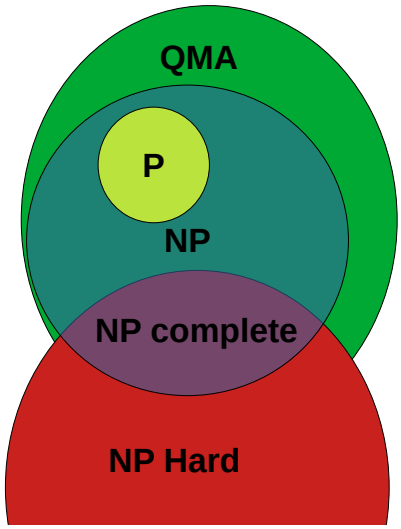


Figure 2.1: Diagram of the complexity class relations.

types of problems is an immediate consequence of Cook-Levin theorem that reads

Theorem 2.1.1. *(Cook-Levin theorem) The boolean satisfiability problem is NP-complete, meaning that it is in **NP** and every problem in **NP** can be reduced to it in polynomial time.*

In a 3-SAT, specifically, the boolean formula is a conjunction of clauses or propositions composed by three variables out of the N different inputs describing the problem, and each clause is satisfied if at least one of the three variables is True. The instance of the problem is fulfilled if and only if one can find an assignment that gratifies every clause. If we choose any instance with $N/3$ clauses in which every variable appear just once, the problem is trivially solvable. However, when we increase the number of clauses and the variables appear multiple times across different parts, the complexity of the problem manifestly explodes. To the time when this thesis is being written, and to the knowledge of the author, the best-known practical SAT solvers can provide a complexity of $O(1.307^N) = O(2^{0.4N})$ [85]. This is the computational complexity of the hardest problem in **NP**. Inasmuch as every problem in **NP** can be turned into a 3-Sat through a reduction algorithm with a polynomial overhead, we can use this specific problem as a benchmark to draw conclusions for the whole class. Importantly, for reasons that will turn out evident in the succeeding chapter, when performing the reduction to the 3-Sat we can assure that the resulting instance is a *balanced formula*, meaning that each of the N boolean variable appear in the same constant number of clauses.

One last important class of problems is the set of **NP hard** problems, which contains all the problems that are at least as hard as the 3-SAT, but are not necessarily contained in **NP** and are not even necessarily decision problems. The relation among the complexity classes is resumed in fig. 2.1.

2.1.3 Interactive proof systems

So far, we described **NP** as the class of mathematical problems with a YES or NO answer that can be found without effort if one is given a proof. The proof of any mathematical statement, e.g. whether a given system of coupled partial derivatives equations admits a real solution, can always be provided as an ordered series of symbols that either supply a procedure to simplify the problem, for example decoupling the equations, or a specific instance that confirms or reject the assertion, such as a real solution of the equations. In all cases, we can model the act of proving a mathematical declaration as the interaction of two agents: a *prover* who wants to convince a *verifier* with incontrovertible logic of the solution to the problem, providing some *certificate*, which is any string of symbols of bounded length. If the above proposition seems overcrowded, the readers can easily convince themselves how easy it is, sometimes, to convince oneself. In this circumstance, the verifier will always accept the proof if provided with the correct witness and reject otherwise.

The example just described constitutes an *Interactive proof system*, which is a powerful computational model and an extensively studied field of complexity theory. In general, the form of the interaction is not necessarily required to be a unidirectional message from the prover to the verifier, and can be as well a series of questions/answers between the two agents. In addition, the restriction to the case in which the verifier deterministically accepts or rejects the proof is awfully limiting, whereas allowing the interaction protocol to be a randomized algorithm turns out to be a pretty powerful tool. A randomized algorithm is an algorithm that uses a degree of randomness as part of its own logical execution. This randomness is usually provided as ancillary aleatory bits that guide some of its actions with the goal of finding the correct solution on average. Probabilistic algorithms revealed to be crucial to effectively cope with many **NP** problems and, in some cases, they are the only practical means of solving a problem.

In literature we find a fancy notation to describe probabilistic interactive proof systems. The almighty malicious prover is called Merlin, who is computationally unbounded and will employ every resource and every ace up the sleeve to convince the limited but honest verifier, Arthur, through a probabilistic protocol, to be in possession of the solution of the problem, regardless of the fact that the problem might not have a solution. In this scenario, we require that two important properties are met:

- *Completeness:* if Merlin provides the correct certificate, Arthur will accept the proof with probability larger than $\mathcal{C}$, e.g. $\mathcal{C} = 2/3$.
- *Soundness:* if Merlin cannot provide the right certificate or the instance is not satisfiable, then Arthur will accept the proof with probability smaller than $\mathcal{S}$, e.g. $\mathcal{S} = 1/3$.

Randomized algorithms let us define a generalized class of problems that can be probabilistically verified using some random bits and a witness that is potentially smaller than the input size of the problem N:

Definition 2.1.5. *The class of problems with Probabilistically Checkable Proofs* $\mathbf{PCP}[r(N), q(N)]$ *refers to the set of problems that can be verified, with completeness and soundness, through a randomized algorithm by using at most* $r(N)$ *random bits and by reading at most* $q(N)$ *bits of the complete* N *bits proof.*

This class has a broad influence when studying the algorithmic complexity of approximate optimization problems. Furthermore, the *PCP theorem* states that

$$\mathbf{NP} = \mathbf{PCP}[O(\log(N)), O(1)] \tag{2.2}$$

In other words, every decision problem in **NP** has probabilistically checkable proofs that require at most a constant complexity of bits to be read and logarithmic randomness complexity.

NP completeness theory and Interactive proof systems, upheld by Cook's and PCP theorems respectively, stand tall as pillars of the modern theory of algorithms. Their immersion in the compass of quantum theory and the inclusion of its counter-intuitive logic is a long way from being petty, nonetheless it is a necessary step for the full development of a quantum computation theory.

In the following chapter, we will explore the quantum analog of the Merlin Arthur proof system, which defines a brand new complexity class called **QMA**, as Quantum Merlin Arthur.

Definition 2.1.6. *A problem is in* ***QMA***$(\mathcal{C}, \mathcal{S})$ *if there is a quantum verifier who receives a proof in the form of a quantum state* $|\psi(x)\rangle$ *with a number of qubits that is a polynomial of the input size* $p(N)$ *such that:*

- *if* x *is a solution of the problem, there is a state* $|\psi(x)\rangle$ *such that Arthur accepts the proof with probability at least* $\mathcal{C}$*;*
- *if* x *is not a solution of the problem, Arthur accepts any proof with probability at most* $\mathcal{S}$*.*

In plain English, the proofs have to be verifiable in polynomial time on a quantum computer, such that if the answer is indeed YES, the verifier accepts a correct proof with probability larger than $\mathcal{C}$, and if the answer is NO, then there is no proof which convinces the verifier to accept with probability larger than $\mathcal{S}$. If a problem admits such proof system for some $\mathcal{C}$ and $\mathcal{S}$ then it belongs to **QMA**.

This ends our discussion on algorithms. Our last topic to review deals with networks in general and complex networks in particular, that will be an important subject of chapter 5.

2.2 Networks

Broadly speaking, a network is a collection of points, which we call *nodes* or vertices, joined in pairs by lines, which we call *edges*. Networks are studied in the form of a mathematical graph theory, which is one of the primary cornerstones of discrete mathematics. Euler's celebrated 1735 solution of the Königsberg bridge problem [86] is often cited as the first true proof in the theory of networks, and during the twentieth century graph theory has developed into a substantial body of knowledge. In the following we will use the terms networks and graphs to describe the same thing, however the first one is usually employed to describe physical systems whereas the latter typically refers to mathematical objects.

Network theory aims at studying how the topology of the pattern of interactions between different parts of a system affects the behavior of the system itself. For instance, the structure of the connections between computers on the Internet can strongly influence the routes that data take over the network and hence the efficiency with which the network transports those data. Unless we know something about the structure of these networks, we cannot hope to understand fully how the corresponding systems work.

A graph simplifies the representation of a system by reducing it to an abstract structure or topology that can capture the essence of the patterns of links, although the systems studied in principle can have many other important aspects that are not captured by the network. Some of these nuances can be enhanced by labeling the nodes or edges in order to endow the network with some attributes, such as names or strengths of interactions. However, the reduction of a full system to a network representation usually implies some loss of information about the system itself. Thus, the most fundamental question in network theory is perhaps the following: how does the structural feature of the network affect the practical issue under exam?

Over the years, network analysts developed a cornucopia of mathematical and statistical tools to simulate, analyze and visualize large networks. One of the simplest representations of a finite graph is its *adjacency matrix*, whose elements indicate whether pairs of vertices are adjacent or not in the graph. If the graph is undirected (i.e. all of its edges are bidirectional), the adjacency matrix is symmetric. Its values can be boolean (0 or 1) if it only indicates the presence of an edge, or real, if it denotes, for instance, its strength. We will see that in some special cases, quantum networks can be represented with a complex valued adjacency matrix.

Another significant notion in graph theory is the *degree distribution*. The degree of a vertex in a network is the number of edges the node has to other vertices and the degree distribution $P(k)$ is then defined to be the fraction of nodes in the network with degree k. Thus if there are N nodes in total in a network and N_k of them have degree k, we have $P(k) = \frac{N_k}{N}$. The degree distribution is, in general, a probability distribution. In the long run, in fact, the attention moved from regular networks, with deterministically generated periodic structures, to a broader class of graphs with aleatory connections. The *Random*

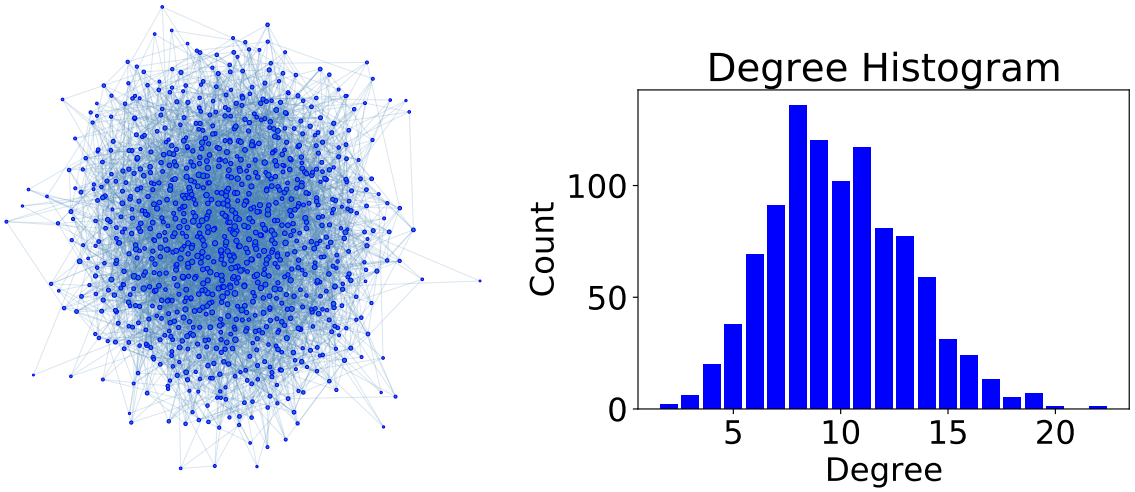


Figure 2.2: Example of a random network: simulation of a $\mathcal{G}_{ER}(N = 2000, p = 0.002)$. The size of each node in the graph showed on the left is proportional to its degree. On the right we can see the poissonian degree distribution typical of this topology.

Graphs are closely associated with the names of Paul Erdős and Alfréd Rényi, who formalized the properties of the network topology that now goes under their names [87]. The $\mathcal{G}_{ER}(N, p)$ is the ensemble of random graphs in which each pair of the N vertices has a probability p of sharing a link, having on average $\langle k \rangle = \binom{N}{2} p$ edges. The degree distribution of the Erdős-Rényi graph is a binomial

$$P(k) = \binom{N}{2} p^k (1-p)^{N-1-k}, \tag{2.3}$$

which becomes Poissonian in the limit of large N if we keep $\langle k \rangle$ fixed. From a mathematical perspective, random graphs are used to answer questions about the properties of typical graphs. Specifically, any graph $g \in \mathcal{G}_{ER}(N, p)$ appears with probability:

$$\Pr[g] = p^{\langle k \rangle} (1-p)^{\binom{N}{2} - \langle k \rangle}. \tag{2.4}$$

One instance of this topology is shown in figure 2.2, where we plotted the graph representation with nodes and edges and its degree distribution. Notice that all nodes are connected and have a degree larger than 0, whereas no node has a degree larger than 22. The Erdős-Rényi model is the simplest model that incorporates a statistical distribution in its definition. Its assumption, namely that the probability of each edge is uniform and independent, is however not adequate to describe real complex networks.

2.2.1 Complex networks

The study of the random graph by mathematicians lead to the discovery and rigorous proof of many important results, both approximate and exact. Yet, the most interesting features

of real-world networks that have boosted the research of the last few years are not encountered in the Erdős-Rényi model and one of the main objectives of network theory is now to show how real networks are not like random graphs. Real networks reveal some aspects that are not shared by regular nor random networks. They are definitely not deterministic but posses a number of very predictable non-trivial features that can be used to find both the intrinsic mechanism that guided their formation and the possible ways in which their infrastructure could be harnessed to achieve certain goals.

Most networks in the real world have a degree distribution very different from 2.3. Most are highly right-skewed, meaning that a large majority of nodes have low degree but a small number, known as *hubs*, have unusually high degree. Unlike the random graph of figure 2.2, many networks are found to contain a small but significant number of hubs. For instance, in the World Wide Web typically only a few websites have a very large number of links. It is often found in social networks that a small fraction of individuals possess an unusual number of acquaintances, way larger than the average. In most metabolic processes there is a small number of metabolites that are always present. Hubs, despite being scare in number, can have an excessive impact on the behaviour and the performances of networked systems, as shown by a broad selection of theoretical and experimental results, notably on the resilience of the network and transport processes and the investigation of the effects of hubs is a major topic of research in recent years [88].

Due to their degree distribution, random graphs do not show hubs which are instead typical of *scale-free networks*. While the Erdős-Rényi graph has a vanishing ratio of nodes with a large k, empirical data shows that real networks have fat-tailed degree distributions [89], approximating a power-law for large values of k

$$P(k) \sim k^{-\gamma}, \ k \gg 1, \tag{2.5}$$

for some positive constant γ, whose value lies typically between 2 and 3, although values a little outside this range are possible and are observed occasionally.

Another remarkable attribute of complex networks that plays a major role in our everyday life is the so called *small-world effect*, which is the observation that most pairs of vertices in naturally occurring networks seem to be connected by a short path. Such circumstance was put into evidence by a famous sociological experiment conducted in 1967 by Milgram [90] and popularized by a notorious play named "Six degrees of separation" written by American playwright John Guare:

> "I am bound, you are bound, to everyone on this planet by a trail of six people."

The study and verification of the small-world effect has been performed in a large number of different networks [88] and its impact has obvious implications for the dynamics of processes taking place on networks. For example, although often students at a school mostly know people from their own class, many of them have experienced how fast can a rumor spread across the whole academy as a consequence of the small-world effect. In addition, it

affects also the number of "hops" performed through the internet by a packet sent among two distant computers, the time and the ease it takes for a virus to circulate throughout a population, the number of journey legs necessary for a traveler to move by train or plane, and so forth. In practice, the nearly instantaneous exchange of data from anywhere in the globe is a capacity that we owe to the result of the small-world effect.

The notion of network is very general and abstract and some of the most different natural systems and phenomena can be described in a similar fashion in terms of nodes and edges. We can broadly organize complex networks into four broad categories: technological networks, information networks, social networks, and biological networks.

2.2.2 Technological networks

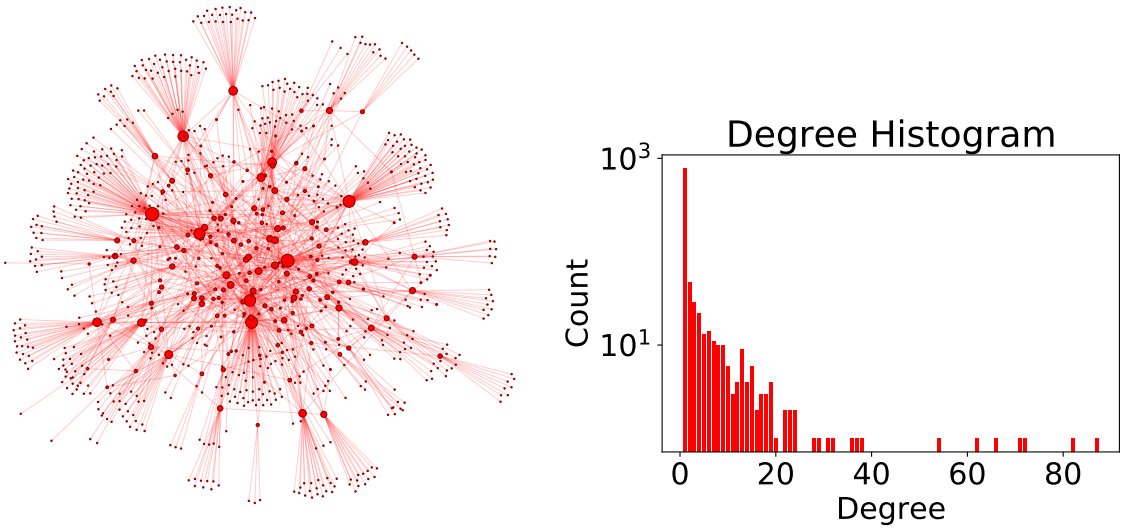


Figure 2.3: Example of a technological network: simulation of a $\mathcal{G}_{AS}(N = 2000)$. The size of each node in the graph showed on the left is proportional to its degree. On the right we can see the power-law degree distribution typical of this topology, where the y-axis is in log-scale.

The first type of networks we will consider are technological networks. These are artificial networks designed typically for distribution of some merchandise or resource, such as electricity or information. Examples include telecommunication networks such as the telephone network, streets, rail lines, or airline routes networks and resource distribution networks such as water lines, oil or gas pipelines, or sewerage pipes and the electricity grid. The archetype of this category is however the global scale network formed by data connections among computers, also known as the Internet. In spite of the fact that the Internet is a fabricated and scrupulously engineered network, because the many different groups that built it had almost no centralized supervision and only poor knowledge of each other's operations, it has been necessary to carry out experimental measurements in order to re-

construct our best current data on its topology, in the absence of any common repository of knowledge about its whole structure.

The Internet has the function of transferring data between computers (and other devices) around the world, which is done by splitting the data into different packets and shipping them across the network from node to node until they reach their designed target. It is thus straightforward to remark that the structure of the internet plays a key part on the performance of such distribution and that by knowing this structure we can address one of the most relevant questions of this context: how should we choose the route by which data are transported? This process is called routing and will be a subject of study in chapter 5.

Since the number of devices connected to the internet is humongous and subject to continuous change it is necessary to examine the structure of the network at a coarse-grained level, which usually comprehends the level of routers, networking devices that perform traffic directing functions on computer networks, or "autonomous systems" (AS), that are a collection of computers whose networking is handled locally on behalf of a single administrative entity, exchanging data between other AS over the public Internet. Typical examples of autonomous systems are the computers at a single company or university.

In figure 2.3 we show an example of the simulation of the AS internet topology based on the work of Elmokashfi, Kvalbein, and Dovrolis [91]. Interestingly, they proposed a topology simulator that uses only the total number of nodes N as parameter and generates a random Internet graph $\mathcal{G}_{AS}(N)$ accordingly. The plots show the appearance of a few large hubs with more than hundred connections, whereas the great majority of vertices are end-nodes with only one edge that links them to the network. In this way we have an intrinsic hierarchical structure that resembles that of the actual Internet, in which we have in a first level the set of network backbone providers (NBPs), who are primarily national governments and major telecommunications companies, then the second level composed of Internet service providers (ISPs) commercial companies, governments, universities, and others who contract with NBPs for connection to the backbone and then provide that connection to end users, who form the third level. Another noteworthy quality of this model is that the network's *average shortest path length*, namely the mean number of hops necessary to go from any node to any other node, is approximately constant (~ 4 hops) with the size of the network.

2.2.3 Information networks

Information networks are artificial networks of data. The emblem of this class is the World Wide Web, accessible over the physical (but distinguished) network of the Internet, in which vertices are web pages identifies by their Uniform Resource Locators (URLs) and edges are the hyperlinks connecting them. Unlike the Internet, the Web is a purely software construct and there is no physical structure. However, its influence on our society is on no account negligible and most people nowadays rely extensively on the Web, both for their work and for their every-day life. As stated by Newman [92]:

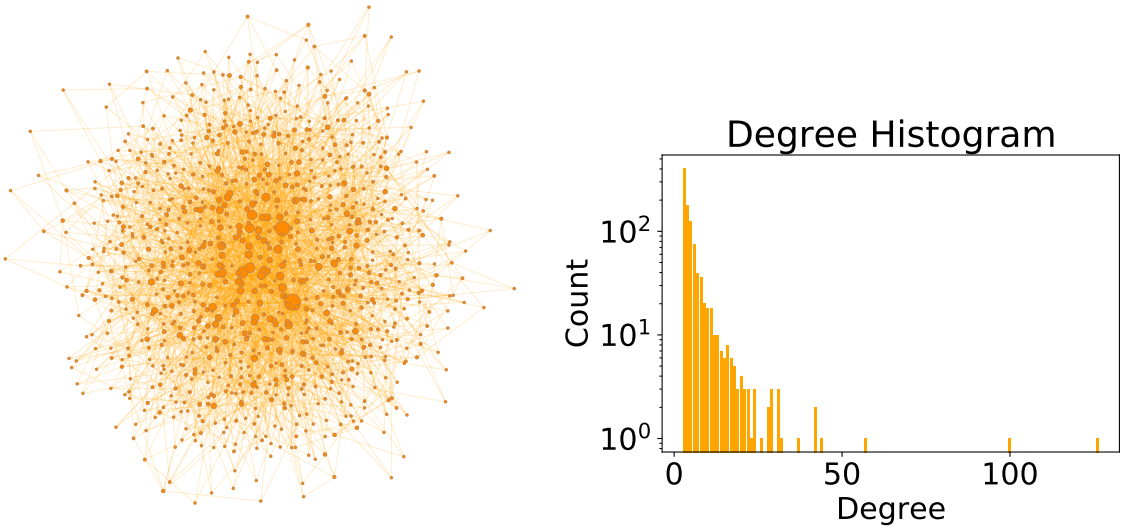


Figure 2.4: Example of an information network: simulation of a $\mathcal{G}_{BA}(N = 2000, K = 3)$. The size of each node in the graph showed on the left is proportional to its degree. On the right we can see the power-law $P(k) \sim k^{-3}$ degree distribution typical of this topology, where the y-axis is in log-scale. There are 993 nodes with degree of 2 and only one with degree 136.

> " Arguably, the structure of the Web could be said to reflect the structure of human knowledge. What's more, people tend to link more often to pages they find useful than to those they do not, so that the number of links pointing to a page can be used as a measure of its usefulness. "

This consideration emphasizes one of the most important aspects of the Web structure, namely the growth by *preferential attachment*. Preferential attachment means that the more connected a node is, the more likely it is to receive new links, establishing a local simple mechanism for the appearance of large hubs. Albert and Barabási [93] invented a renowned algorithm, the Barabási-Albert model (BA), for the generation of scale-free random networks using preferential attachment, purposely to mimic the structure of the web and similar networks. The BA topology $\mathcal{G}_{BA}(N, K)$ requires an additional parameter to the number of nodes N. The network, shown in figure 2.4, begins with K nodes connected to one vertex. Then we progressively add one node with K links, where the probability that the new node is connected to node i is

$$p(i) = \frac{k_i}{\sum_i k_i}, \tag{2.6}$$

where k_i is the degree of node i. Thus the total number of edges in the network is simply $(N - K)K$, however their distribution is random and nodes with larger degrees will have the tendency to attract new links. Although this simple model fails at describing some properties of the Web (e.g. it produces an un-directed graph), it captures the salient features

of the growth of many complex networks. Other types of information networks include citations networks and words co-occurance.

2.2.4 Social networks

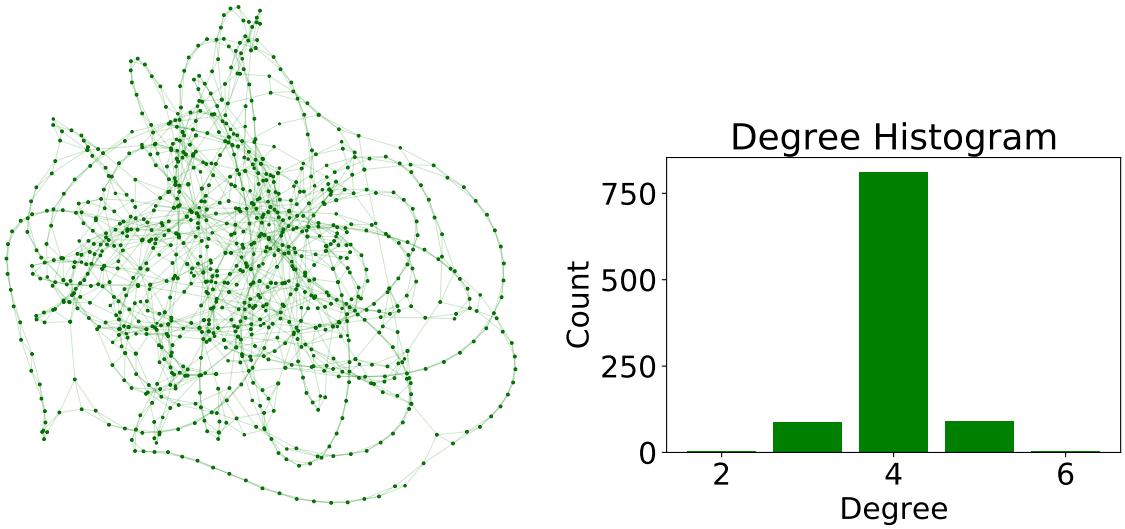


Figure 2.5: Example of a social network: simulation of a $\mathcal{G}_{WS}(N = 2000, Q = 4, \beta = 0.05)$. The size of each node in the graph showed on the left is proportional to its degree. On the right we can see that unlike other complex networks the degree distribution does not follow a power law.

Social networks are often considered as a subclass of Information networks, however it is one of the largest categories and definitely the first that has been studied extensively. Sociologists have, in fact, a long tradition of empirical study of these kind of networks, in which the nodes are constituted by people or groups of people and edges can represent friendship, communication, collaboration, or any sort of social connections. The spread of online social networking companies has largely facilitated the analysis of networks of people. Many of such companies, including Facebook, that at the time of writing has 2.85 billion users, exploit their vast data resources to do scientific research on social networks, typically for commercial purposes.

A property typical of social networks is the clustering, which is the tendency of some nodes in a graph to create tiny groups with a high density of edges. In order to include this feature into the generation of a random network with the small-world property, Watts and Strogatz [94] developed a model that interpolates between a randomized structure close to ER graphs and a regular ring lattice. In the Watts-Strogatz model $\mathcal{G}_{WS}(N, Q, \beta)$, shown in figure 2.5, we first construct a graph with N nodes and $\frac{NK}{2}$ edges where each node has exactly K neighbors, then with probability β we rewire each edge connecting it with another node chosen uniformly at random while avoiding self loops and link duplications.

The underlying ring structure of the WS produces a locally clustered network, whereas the random rewiring of the links significantly reduces the average path lengths.

2.2.5 Biological networks

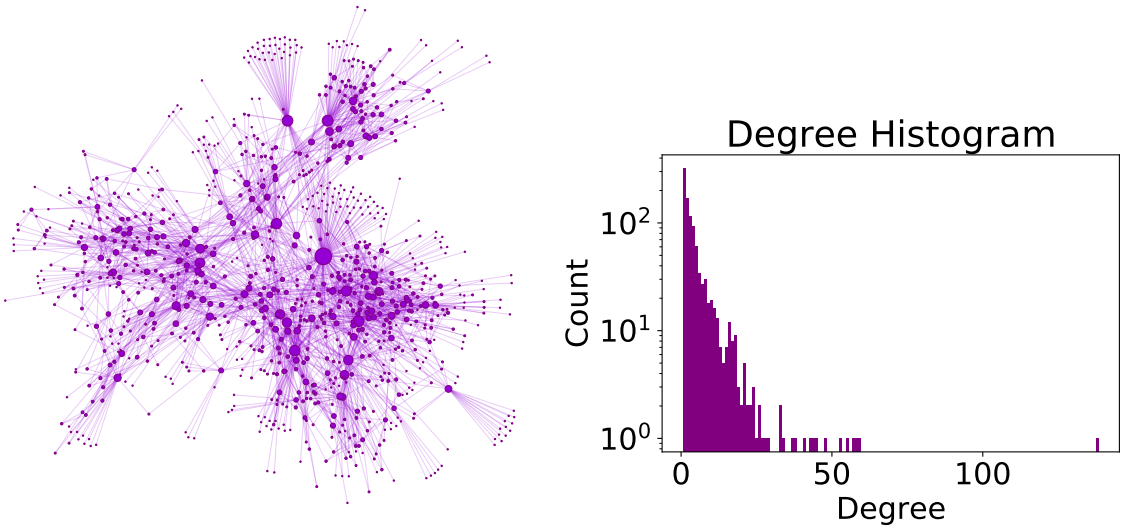


Figure 2.6: Example of a biological network: simulation of a $\mathcal{G}_{PP}(N = 2000, \sigma = 0.4)$. The size of each node in the graph showed on the left is proportional to its degree. On the right we can see the power-law degree distribution typical of this topology, where the y-axis is in log-scale.

So far we presented types of networks that are either built by humans or related to them. The greatest majority of complex networks, however, are naturally generated by other living forms. As a matter of fact, networks appear in range of different settings in biology. We can account for physical networks, like the connections between neurons in a brain, or more abstract networks, such as the "food web", in which the nodes are animal species that are linked if one of the species eats the other. Yet another class is formed by biochemical networks, which includes metabolic networks, genetic regulatory networks and protein-protein interactions networks. The latter (PP), also called interactome, represents the physical association among proteins present in a living cell, where proteins are vertices, and their interactions are undirected edges. PPs are fundamental to the cellular processes and also the most thoroughly analyzed networks in biology, playing a crucial role in the study of evolutionary dynamics. In figure 2.6 it is shown an example of an interactome, based on the work of Ispolatov, Krapivsky, and Yuryev [95]. In this model $\mathcal{G}_{PP}(N, \sigma)$ the nodes are added by randomly choosing a target node and the replica is connected to each neighbor of the target node. Then, each link emanating from the replica is activated with probability σ. This model has a rich behavior based on the value of σ and correctly simulate some properties of real PPs, e.g. the scale-freeness, when $\sigma \sim 0.4$.

We have now completed the review chapters and can proceed to the original research that is the main focus of this thesis. As was explained before, we will look into the details of three practical algorithms that occur on quantum networks at three different stages of complexity. This will give us an insight on how we can employ the theory developed in these first two chapters to derive new techniques in quantum communication scenarios with no classical equivalent, while probing the underlying properties of regular and complex networks endowed with a quantum optical substrate.

Part II

Protocols

Chapter 3

Quantum verification of NP problems

3.1 What is quantum advantage 54
3.2 Coping with NP-completness 57
3.2.1 2-out-of-4 Sat 57
3.2.2 Previous work 58
3.2.3 Sketch of the scheme 60
3.3 The verification protocol 61
3.3.1 Quantum proofs encoded in coherent states 61
3.3.2 The verification test 63
3.3.3 Classical complexity of verification 66
3.3.4 Dealing with practical imperfections. 67
3.3.5 Experimental results 72
3.4 Discussion 78

The Internet is a huge complex network of interconnected computers carrying a myriad of digital information resources and services that are at the core of the current human epoch, the information age. However, its building blocks are simple end-to-end connections between two separated units. In this chapter, we will explore the first stage of the future quantum Internet by looking at a quantum communication scheme between two agents with very different qualities: one is a powerful but untrusted quantum server providing a cloud service, whereas the other is a simple user who is accessing the data center online. In this scenario, we will provide a protocol to efficiently verify the solution to an NP-complete problem revealing only limited information about the proof. It will be shown that such a simple architecture can already provide highly desirable potential applications, for example, the users would be able to verify the dubious information they receive from the powerful quantum server without ever having access to the full solution. Such proof systems could then contribute to protocols like secure identification, authentication or even blockchain [96] in a future quantum Internet. On the other hand, this result demonstrate a simple way to empirically achieve computational quantum advantage, the first in an interactive setting, a long-standing moonshot in the field, believed to be possible only with a considerable technological leap.

3.1 What is quantum advantage

In 1981, during one of his acclaimed lectures, Richard Feynman pointed out the intractability of simulating some quantum phenomena. The memorable quote [97]

> *"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."*

had a prominent influence on the following generations and is largely retained to have been the kickoff for the field of Quantum Computation and Information. Since then, the rush towards the Holy Grail of showing a quantum advantage has only intensified and many proposals have been taking turns on stage. At the time of writing these lines, the race has culminated with two major breakthroughs.

In October 2019 a collaboration of Google and NASA scientists claimed to have reached quantum supremacy with an array of 54 superconducting qubits [98]. The quantum processor, called Sycamore, would have completed a task in 200 seconds that, Google claims, would take a state-of-the-art supercomputer 10,000 years to finish. In December 2020, the Chinese photon-based Jiuzhang processor, developed by the University of Science and Technology of China, achieved a processing power of 76 qubits using 50 input single-mode squeezed states and was 10 billion times faster than Sycamore, making it the second computer to attain quantum supremacy [99]. The USTC group estimated that it would take 2.5 billion years for the Sunway TaihuLight supercomputer to perform the same calculation. If the claims upheld the diffused skepticism, these results would constitute a milestone for

the field of Quantum Information.

At this point, someone may be confused by the terminology with good reasons. There are, in fact, several terms, such as superiority, supremacy or advantage, that ultimately all refer to the same thing. In this book, we will favor the use of quantum advantage, on account of the fact that a quantum supremacy would imply the obsolescence of classical information processing devices. Anyway, what is exactly quantum advantage? The idea was coined by John Preskill in a seminal article [100] and is defined as the following:

Definition 3.1.1. *Quantum advantage is the empirical act of demonstrating that a programmable quantum device can solve a problem that no classical computer can solve in any feasible amount of time.*

In the practice, it is about finding a task that is easy for a quantum machine and hard for a classical one. However, this statement has many subtleties that require deeper discussion. In the first place, the demonstration must be empirical, *id est* experimental. If this may sound completely obvious to a physicist, it is groundbreaking for a computer scientist. It is somewhat like asking to experimentally prove a mathematical assertion, or even using a physics experiment to probe the ultimate computational capacity of the Universe. Be that as it may, the gap between the ultimate theoretical ideas in quantum computing and their factual implementation is gargantuan and has only recently started to be bridged. Another relevant aspect to comment is the programmability of the quantum device. In other words, we should be able to write-in some arbitrary input and read-out the desired output. If this was not so, then we could claim that any sort of naturally occurring chemical reaction could be seen as a kind of computational quantum advantage. As a consequence, we require that the quantum device is in large measure controllable and, in addition, the task it is trying to perform should be impractical, in the computational complexity terms described in the previous chapter, for any machine that does not require a quantum description.

There have been many proposals for schemes that should be impossible to simulate on a classical computer and easily implemented on a quantum system, however there are three in particular that seemed to be the most promising candidates.

Sampling random quantum circuits is the task performed by the Sycamore quantum processor to harness quantum advantage. Essentially, it consists in applying random logic gates to a set of qubits and measuring the outcome in the computational basis. The vastness of the Hilbert space is such that it is very hard for a classical machine to predict the output state if the circuit depth and the number of quibits is large enough, while sampling the probability distribution of the outcomes is straightforward if we directly use a quantum system. *Boson sampling* is the problem solved by the Jiuzhang processor. It was introduced by Aaronson and Arkipov [101] who found a correspondance between the problems of sampling from the probability distribution of identical bosons scattered by a linear interferometer and that of evaluating expectation values of permanents of matrices. This task is naturally suited for photonic platforms thanks to the bosonic nature of light particles, however the specific

choice of the physical information carriers is irrelevant and any type of boson, e.g. Cooper pairs in a superconducting circuit, would do the job. Another interesting candidate is *quantum annealing*, that is a quantum method to solve combinatorial optimization problems by finding the global minimum of a complex function. The process is based on encoding the function's information in a quantum system energy eigenstates and then letting it thermalize in order to reach the global minimum state of its Hamiltonian. Quantum annealers are currently being implemented by D-Wave system and looks like a promising way to implement quantum computing task with useful applications, however no claims on quantum speedup have been announced yet.

These results are by all means precious contributions to the field of Quantum Information, boosting the development of sophisticated quantum technologies and paving the way for a complete implementation of a Universal Quantum Computer. Nonetheless they all suffer from some major drawbacks that must be taken into account. Primarily, the benchmark against classical computing is unquestionably not a bed of roses and, at its heart, there is the difficult task of correctly choosing the appropriate mathematical assumptions, e.g. what is the classical complexity of the problem at hand and how much time would the best existing supercomputer take to implement it. These assumptions can be bulky and delicate to deal with and can lead to serious fallacies in the claims, like in the case of the IBM's researchers response to Google's quantum advantage experiment [102]. Another aspect that turns out to be crucial when dealing with theoretical models of quantum computation is that even though in the ideal scenario the asymptotic gap between the computational time of the quantum and classical cases is apparent, in a realistic implementation with noise and limited input sizes it may be very equivocal. In addition, even if all these problems were properly tackled, there is still the crucial hurdle of the certification of the claim of quantum advantage. Strictly speaking, if the problem under consideration belongs to **NP**, e.g. we want to factorize large numbers, then it should be easy to verify the correctness of the output from the quantum hardware. However, this is certainly not the case for the sampling of an exponential size probability distribution, like Boson and Random circuit samplings. In those cases, when the instance is such that the simulation on a classical machine is simply intractable, we do not have a clear way to certify the legitimacy of the solution. Finally, the lack of useful applications even in perspective for these new technologies is an evident hot potato. Obviously, science is for science's sake and these results are fundamental for the progress of quantum information, having disrupted the last doubts on the possibility that a quantum device can outperform all classical technologies for some task. However, we need to be able to step on these landmarks and turn over a new leaf otherwise their influence on the future of the field will stop here.

In this chapter, we study the power of quantum technologies to provide a computational advantage in an *interactive setting*, where first we allow two parties to interact in a predefined manner, and then we look at the time it takes for one of them to resolve a specific computational task when they can use quantum or classical resources. Specifically, we study the task of verifying NP-complete problems, in particular whether a set of boolean

constraints have a satisfying assignment to them or not, when an untrusted party provides some limited information about the solution of the problem. For this task, we show that we can achieve a quantum advantage exploiting experimental techniques involving coherent states, linear optics and single-photon detection.

Before explaining this further let us remark a few properties of our result: first, the quantum hardware we use is simple and the demonstration can be readily reproduced in well-equipped quantum photonics labs; second, our task is inherently verifiable since the output is a YES/NO answer and not a sample from an exponential size distribution (we emphasize here that the quantum machine in our scenario is certainly not solving NP-complete problems but merely verifies whether a solution exists or not with limited information about the possible solution); third, the benchmarking against the best classical methods is based only on the assumption that NP-complete problems do not have sub-exponential algorithms, a well-known and widely accepted computational assumption [103], that we revised in chapter 2; and finally, while previously experimentally demonstrated computational tasks are typically tailor-made for showing quantum advantage with no direct connection to useful applications, the fast verification of NP-complete problems with bounded information leakage could potentially lead to interesting applications, including in server-client quantum computing, authentication systems, ethical behaviour enforcement and blockchain technologies [96]. At the same time, we stress that the computational advantage we achieve is not in the standard computational model where a single classical or quantum machine receives an input and computes an output, but in the interactive setting, where we first allow interaction with a second party before trying to resolve the computational task at hand.

3.2 Coping with NP-completness

Before going through the details of our results on the demonstration of a quantum computational advantage in this interactive setting, let us revise some of the fundamental concepts of NP verification and take a deeper look at the past literature.

3.2.1 2-out-of-4 Sat

In the previous chapter we discussed the importance of the class of NP-complete problems, which contains some of the most interesting problems both from a theoretical point of view and in practice. Such problems include the Traveling Salesman Problem, Satisfiability, and many problems related to combinatorial optimization, scheduling, networks, etc. As we said earlier, the main characteristic of these problems is that while it is very difficult to find a solution, and in many cases even approximate the optimal solution, it is easy to verify a solution if someone provides one to us, even if this is an untrusted party. Moreover, the theory of NP-completeness shows that all these different problems are related to each other through reductions, meaning that it suffices to study one of them in order to say something interesting about the entire class of problems.

Let us then focus on 2-out-of-4 SAT, which can be obtained through a reduction of a 3-SAT, the canonical NP-complete problem. The 2-out-of-4 SAT problem consists of a formula of N boolean variables in a conjunction of clauses, where each clause is satisfied if and only if exactly two of the four variables forming the clause are True. The task is to decide whether there exists an assignment to the variables $(x_1, x_2, \ldots, x_N)$, which satisfies all clauses of the formula, in other words for every clause two variables must be True and the other two must be False. We assume without loss of generality that our 2-out-of-4 SAT instance meets the following two conditions. First, it is a balanced formula, meaning that every variable occurs in the same constant number of clauses, and second, it is a Probabilistically Checkable Proof (PCP), i.e., either the formula is satisfiable, or for any assignment at least δ fraction of the clauses is unsatisfiable, for some constant $\delta > 0$. These conditions can always be guaranteed using a polynomial overhead in N and the theory of PCPs. Thus any NP-complete problem can be reduced to a balanced 2-out-of-4 SAT instance that is probabilistically checkable.

For the verification of such a 2-out-of-4 SAT instance, we would like the verifier, Arthur, to accept a correct proof (a truth assignment of the variables that satisfies the formula) given by a prover, Merlin, with high probability, say $\mathcal{C} \geqslant 2/3$. We formerly called this the completeness property of the verification scheme. If, on the other hand, the formula is not satisfiable, then for any potential proof he receives, Arthur must accept the proof with low probability, say $\mathcal{S} \leqslant 1/3$. This is the soundness property of the verification scheme. For a 2-out-of-4 SAT problem of size N, the best algorithms for finding a solution run in time exponential in N (using some sort of clever brute force search for a solution) [85], while the verification of a potential solution takes time linear in N. One important property of NP-complete problems is that if we accept that the best algorithms for solving an NP-complete problem are exponential in N, then if one has found or has been provided with part of a solution, for example the truth assignment to a subset of the variables of size $t < N$, then in the worst case the remaining time to complete the solution is still exponential in $(N - t)$ [103].

3.2.2 Previous work

The use of quantum protocols for verification in this so-called interactive proof setting was first employed in [104], which introduced the concept of Quantum Merlin Arthur. Since then, QMA problems have been intensively studied [105]–[109]. As we have seen in chapter 2, they are the quantum analog to NP problems in computational complexity theory and have the same completeness and soundness properties as the ones described above with the proofs encoded in quantum states.

By the results of [109], we know that quantum Merlin Arthur interactive proof systems can be used to verify NP-complete problems more efficiently than the classical ones. In particular, it was shown that a quantum verifier who receives $O(\sqrt{N})$ unentangled copies of a quantum proof can verify efficiently the 2-out-of-4 SAT instance by performing a num-

ber of tests/measurements on these states. Note that the assumption that the proofs are unentangled is crucial. Here, the quantum proof is the state $\frac{1}{\sqrt{N}}\sum_{i=1}^{N}(-1)^{x_i}|i\rangle$, i.e., the quantum state on $\log_2 N$ qubits encoding the values of the assignment $(x_1,\ldots,x_N)$ as amplitudes. The information Arthur receives about the classical solution cannot be more than $O(\sqrt{N}\log_2 N)$ bits of information, since this is the number of qubits he receives, nevertheless, the verification becomes efficient in the quantum case: for the same amount of revealed information a classical verification protocol would require exponential time while it takes polynomial time for the quantum protocol to perform the task. We remark that one can see the quantum advantage either as a computational advantage, as we do in our work, where we ask how long the verification will take in the quantum and classical case if we fix the size of the message sent by the prover, or as an information advantage, where we ask what size of quantum or classical message is needed if we fix the time of the verification to be polynomial in the input size. We stress again that, in both cases, the advantage is not about solving NP-complete problems, but about verifying them with limited information. In Ref.[110], it was first shown that in theory it is possible to implement such a verification protocol with single photons and linear optics, albeit a practical implementation is and will probably continue to be out of reach for photonics technology due to the extremely large number of elements in the proposed scheme shown in figure 3.1.

Here, we overcome this limitation by proposing a quantum verification test that maintains the properties of the original one and at the same time uses new conceptual tools that make it practical. This allows us to provide the first experimental demonstration of an efficient quantum verification scheme for NP-complete problems, and hence a strong provable quantum advantage for this task based on the assumption that finding a solution to NP-complete problems takes exponential time on a classical computer. More precisely, we experimentally demonstrate how a quantum Arthur who receives an unentangled quantum proof of size $\widetilde{O}(N^{3/4})$ (where $\widetilde{O}$ denotes the order up to logarithmic terms) can verify 2-out-of-4 SAT instances in time linear in N, while a well-known assumption is that any known classical algorithm takes time exponential in $(N-\widetilde{O}(N^{3/4}))$. The core idea of our protocol that enables us to perform the verification with coherent states and a simple linear optics scheme is based on the Sampling Matching problem defined and implemented in [111]. This is particularly appealing from a practical point of view because of the relative ease of preparation and manipulation of coherent states, which combined with linear optics transformations have made them attractive candidates for proving quantum advantage in communication complexity and security [112]–[118]. The use of the Sampling Matching is also one of the main conceptual differences of our current protocol with respect to the work of [110], which provided a verification protocol with single photons and which cannot readily be made to work simply by mapping the single photons into coherent states.

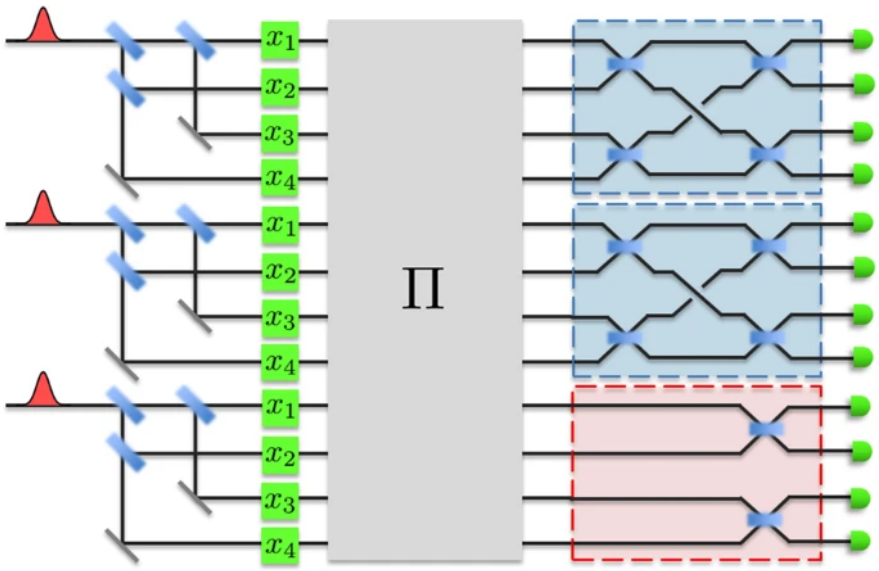


Figure 3.1: Complete setup for the 2-out-of-4 SAT verification with linear optics (figure taken from Ref. [110]). The prover, Merlin, prepares three copies of a single photon state in equal superposition. The satisfying assignment x is encoded in the optical modes with the phase shifters (green). The verifier, Arthur, after deciding which of the three tests they are going to perform and which proofs they randomly picked, then applies a permutation Π on the set of modes. After the permutation, they attach either four-mode interferometers for the satisfiability test (blue), or 50:50 beamsplitters to each pair of modes (red) for the other two tests. Depending on the pattern of clicks observed in the detector they decide whether to accept or reject depending on the pattern of clicks observed. The number of optical elements increases with the input size of the problem.

3.2.3 Sketch of the scheme

In order to explain the importance of our result let us first go back to the classical case and describe a possible scheme for verification. Since we know that in case the formula is not satisfiable then for any assignment at least a constant δ fraction of the clauses are not satisfied, then for verification it suffices for Arthur to pick a random clause, obtain the values of the four variables and check whether the clause is satisfied or not. By repeating this for a small constant number of clauses, Arthur can verify with high probability whether the instance is satisfiable or not, and moreover, the information Arthur receives about the solution is very small (just the value of the variables in a few clauses). We can also see this protocol in a slightly modified version, which will be closer to our quantum verification protocol based on Sampling Matching. Instead of having Arthur pick uniformly at random a small number of clauses out of all possible clauses to verify, we can assume that Arthur picks each clause with some probability so in the end the expected number of clauses he picks is the same number as in the initial protocol.

There is of course a well-known issue in these schemes. Once Merlin knows which clause Arthur wants to test, he can easily adapt the values of the variables to make this clause

satisfiable. Arthur cannot force Merlin to be consistent across the different clauses, namely to keep the same value for each variable in the different clauses. One way to remedy this would be by having Merlin send the entire assignment to Arthur (which is the usual verification protocol), but in this case Arthur gets all the information about the classical solution. Another solution is through interactive computational zero-knowledge proofs, where one uses cryptographic primitives, i.e., bit commitment, in order to force the behaviour of Merlin, but such schemes necessitate communication between Arthur and Merlin and only offer computational security [119]. Thus in the classical world, it is impossible to have a protocol with a single message from Merlin to Arthur that performs verification while at the same time Arthur does not learn the entire classical solution.

In the quantum world, using coherent states and a new efficient linear optics scheme based on the Sampling Matching, we can experimentally demonstrate exactly that: a quantum Arthur can efficiently verify instances of NP-complete problems (in time linear in the size N) while at the same time receiving only a small amount of information about the solution (theoretically of order $\widetilde{O}(N^{3/4})$). To show this advantage experimentally it was sufficient to use sequences of a few thousand coherent pulses, corresponding to a proof size N from 5000 to 15000, with an average mean photon number per pulse on the order of 1, and standard InGaAs single-photon detectors.

We are now ready to give the details of our quantum verification protocol, analyze its completeness and soundness, and provide the results of our experimental demonstration.

3.3 The verification protocol

3.3.1 Quantum proofs encoded in coherent states

In the first step of our verification protocol, Merlin sends the quantum proof to Arthur. We consider here that if the instance is satisfiable then an honest Merlin will use coherent states to encode the proof, exploiting the coherent state mapping introduced in [112], [113]. More precisely, he encodes his proof $x = (x_1, x_2, ..., x_N)$ in a time sequence of N weak coherent states. He does this by applying the displacement operator $\hat{D}_x(\alpha) = \exp(\alpha\hat{a}_x^\dagger - \alpha^*\hat{a}_x)$ to the vacuum state, where $\hat{a}_x = \frac{1}{\sqrt{N}}\sum_{k=1}^{N}(-1)^{x_k}\hat{a}_k$ is the annihilation operator of the entire coherent state mode, and $\hat{a}_k$ is the photon annihilation operator of the k^{th} time mode. Hence,

$$|\alpha_x\rangle = \hat{D}_x(\alpha)\,|0\rangle = \bigotimes_{k=1}^{N} |(-1)^{x_k}\alpha\rangle_k\,, \tag{3.1}$$

where $|(-1)^{x_k}\alpha\rangle_k$ is a coherent state with mean photon number $\mu = |\alpha|^2$ occupying the k^{th} time mode. Thus, the state $|\alpha_x\rangle$ has a mean photon number $|\alpha_x|^2 = N|\alpha|^2$, with the photons distributed over the entire sequence of N modes. As formerly explained in chapter 1, varying the parameter α controls how many photons are expected to be in the state; for example for $\alpha = 1$, every coherent state in the sequence has on average one photon, while

if we take $\alpha = 1/\sqrt{N}$, then on average only one photon will be present in the entire sequence.

In the single-photon version of the original protocol [109], [110], Merlin prepares $O(\sqrt{N})$ unentangled copies of a state that consists of a single photon in N modes, i.e., a state in an N-dimensional Hilbert space. This implies that during the protocol the information revealed to Arthur is at most $O(\sqrt{N}\log_2 N)$ bits of information. Then, a number of tests are performed on these states to check that they are equal, uniform, and that they satisfy the boolean formula. For the equality, a SWAP test is performed between different copies of the proofs; for testing that the amplitudes of the states are roughly uniform, a test based on the Hidden Matching problem is performed; for satisfiability, the parity of four variables that belong to the same clause is measured in order to check whether the specific clause is satisfied. Each test is performed with some probability and if the test is successful, then Arthur accepts the instance as satisfiable.

An important feature of our protocol is that by using the Sampling Matching method we are able to combine the above tests into a single test and all copies of the proofs into a higher mean photon number sequence of N coherent states, which we also assume to be unentangled. By sending coherent states with a higher mean photon number $|\alpha|^2$ we essentially increase the probability of measuring each variable and thus the information conveyed by Merlin; this is important for the uniformity and satisfiability parts of our verification test as we will see later. Increasing $|\alpha|^2$ instead of sending multiple copies of the same state also allows us to avoid the necessity of applying the equality test that was ensuring that the copies are the same. On the other hand, the unentanglement assumption for the sequence of coherent pulses is necessary as it was in [Refs.[108], [109]], since otherwise Merlin could potentially try to correlate the detections of specific parts of the proof that are satisfiable, although the whole proof is not.

We prove in the following that theoretically the average photon number for each of the N coherent states that the honest Merlin sends when the instance is satisfiable is of the order of $|\alpha|^2 = O(N^{-1/4})$, which makes the information Arthur gets about the classical solution to be $\widetilde{O}(N^{3/4})$. In high level, this also implies that any classical verification algorithm with the same amount of information will take time exponential in $(N - \widetilde{O}(N^{3/4}))$, which becomes large enough for practical sizes of N. This is because Arthur can always enumerate over all possible proofs Merlin sends and perform the verification for each one of them. It will take him time exponential in $\widetilde{O}(N^{3/4})$ to enumerate over all possible proofs (since the information in them is less than $\widetilde{O}(N^{3/4})$) and thus if the verification for each of them takes time less than exponential in $(N - \widetilde{O}(N^{3/4}))$ then this would imply a fast algorithm for NP.

Once Arthur receives the quantum proof as a sequence of unentangled coherent states from Merlin, he performs the verification by applying a verification test. We assume that Merlin can behave dishonestly in any way possible, apart from having to send unentangled states. Let us now describe this verification test and how it can be performed in a linear optical setting.

3.3.2 The verification test

As we discussed previously, the original verification test [109] consists in first testing that the copies of the proofs are the same (which we have avoided by sending a single sequence of coherent states), and then that the amplitudes of each of these states are close to uniform. This test is necessary in order to show that Arthur can actually check all possible clauses with roughly uniform probability. Otherwise, Merlin can just force Arthur to always measure some specific subset of variables (the ones that can satisfy some corresponding subset of clauses) and thus convince Arthur of the validity of the assignment, even though no assignment exists that satisfies all clauses.

Here, we deal with this in a different way. Again, we want to ensure that Arthur will measure each clause with some probability, meaning that Merlin cannot force Arthur to measure only a specific subset of variables and clauses. This is where we use the idea of Sampling Matching [[111]], which was introduced as a practical version of Hidden Matching, the problem performed in the original uniformity test. Instead of interfering Merlin's coherent states with themselves, we in fact input in an interferometer Merlin's sequence of coherent states in one arm, and a new sequence of coherent states prepared by Arthur in the other arm. This is also the main difference with the single-photon protocol in [Ref. [110]].

More specifically, the test as depicted in Fig. 3.2 is the following. When Arthur receives the state $|\alpha_x\rangle$ from Merlin with the mean photon number $|\alpha_x|^2$ predefined by the protocol, he generates his local state in the form of a sequence of uniform coherent pulses, with the same mean photon number. In particular, Arthur creates the state

$$|\alpha_0\rangle = \bigotimes_{k=1}^{N} |\alpha\rangle_k \,, \tag{3.2}$$

such that $|\alpha_0|^2 = |\alpha_x|^2$. He then sequentially interferes each of honest Merlin's coherent states with his local coherent states in a balanced beam splitter (BS) and collects the outputs in the two single-photon detectors, D_0 and D_1. At each time step k, the input state in the beam splitter is $|(-1)^{x_k}\alpha\rangle_k \otimes |\alpha\rangle_k$, while at the output modes we have,

$$|\frac{((-1)^{x_k}+1)\alpha}{\sqrt{2}}\rangle_{D_0,k} \otimes |\frac{((-1)^{x_k}-1)\alpha}{\sqrt{2}}\rangle_{D_1,k} \,. \tag{3.3}$$

Then, the probability of getting a click on each of the single-photon detectors at the k^{th} time step of the verification protocol is:

$$P_{\text{det}}^{(k)} = \begin{cases} 1 - e^{-|\alpha|^2((-1)^{x_k}+1)^2/2} & \text{on } D_0 \\ 1 - e^{-|\alpha|^2((-1)^{x_k}-1)^2/2} & \text{on } D_1. \end{cases} \tag{3.4}$$

One way of understanding the above test is to note that it is guaranteed that Arthur receives a value for each variable with at least some probability, due to the photons in his

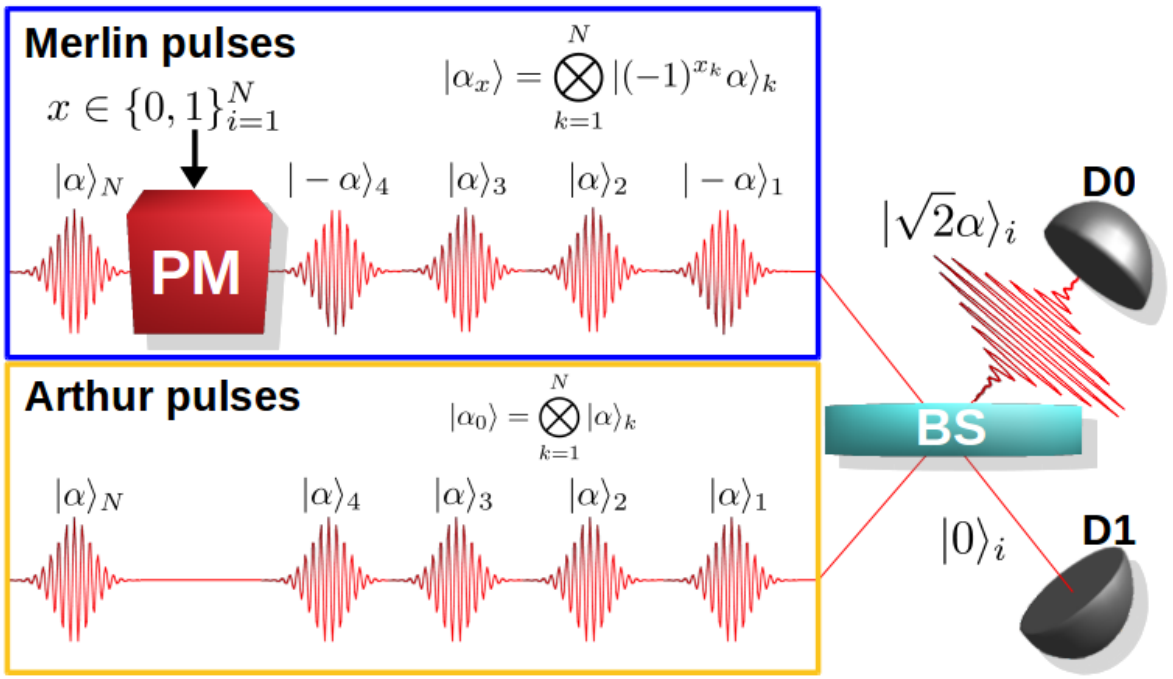


Figure 3.2: **The Sampling Matching scheme (SM).** Merlin creates his coherent state quantum proof by sequentially encoding his proof x into the coherent pulses. Under the SM scheme, Arthur interferes Merlin's coherent state quantum proof with his local state consisting of a sequence of N pulses. He observes the clicks in two single-photon threshold detectors D_0 and D_1 to decide whether Merlin's proof state is correct.

own state. This way, Merlin cannot choose exactly for what variables Arthur will obtain a value. Thus, Arthur will end up obtaining the values of a subset of variables that is random enough (meaning Merlin cannot deterministically choose it) so that when he considers the clauses whose variables are in this subset, then either all of them will be satisfied in the YES-instance, or sufficiently many of them will not be satisfied in the NO-instance.

Now, if Merlin wants to send a value for a specific variable x_k to Arthur, then he can do it perfectly, since by constructing an honest coherent state of the form $|(-1)^{x_k}\alpha\rangle_k$, only one of the two detectors of Arthur has non-zero probability of clicking. On the other hand, if Merlin sends any state $|\beta\rangle$, then after the interaction with Arthur's coherent state $|\alpha\rangle$ one important thing is true: no matter what Merlin's state is, there is still a probability of a detector click, which is at least $1 - e^{-|\alpha|^2}$ due to the photons in Arthur's coherent state and the fact that we only perform linear optics operations that preserve the number of photons. In other words, Arthur obtains a value for each variable with some probability independent of Merlin's message, and this value can be fixed by Merlin if he honestly sends a state that encodes a value.

After recording the results of his measurements, Arthur assigns values to the variables in the following way: if the detector D_0 clicked, then the value is 0, if the detector D_1 clicked then the value is 1, while he leaves the variables unassigned if no click was observed. Then,

Arthur checks for each clause for which he has assigned a value to all four variables whether it is satisfied or not, namely if exactly two out of the four variables in the clause have value 1. In the ideal case where there are no errors, Arthur will accept if all clauses are satisfied and reject if any clause is not satisfied. In the presence of non-ideal experimental conditions, we will see that Arthur will use a threshold and accept if at least that fraction of clauses are satisfied or else he will reject.

We are now ready to analyze the completeness of the protocol, namely the probability Arthur accepts assuming that the 2-out-of-4 SAT instance is a satisfiable instance, in which case Merlin prepares a proof state in the form $|\alpha_x\rangle$ for a satisfying assignment x. Then, we discuss the soundness of the protocol, namely the case in which the instance has no satisfying assignment and where Merlin still wants Arthur to accept his proof and acts dishonestly. He will then try to send some general quantum state to trick Arthur, while, as we said, here we make the same type of assumption as in the original work of Aaronson *et al.*[[109]], namely that Merlin still sends a sequence of unentangled states. Later, we will complete the analysis by looking at the protocol under non-ideal experimental conditions and see what level of noise the interferometric setup can tolerate in order to maintain a positive gap between the completeness and soundness probabilities.

The completeness corresponds to the probability that Arthur accepts the proof of Merlin in the case of a satisfiable instance, where Merlin sends the correct quantum state. As we have described, Arthur will retrieve the values of a number of variables that are encoded in the phases of Merlin's sequence of coherent states by using his own local coherent states and the interferometric setup shown in Fig. 3.2. As long as Merlin honestly encodes the satisfying assignment into his coherent states then only one detector has non-zero probability of clicking and thus Arthur will never get a wrong value. Thus the only probability of rejecting comes from Arthur not obtaining the values of the four variables of any clause.

To estimate this probability, and hence the completeness, we remark again that the unentanglement promise guarantees that the probability of detecting a photon in each of the pulses in the sequence is independent of the remaining pulses of the sequence, since the pulses are unentangled between them. Furthermore, the probability of measuring a particular variable is independent of which clause Arthur is going to verify later on. If we now denote as $p_h \geq 1 - e^{-2|\alpha|^2}$ the probability that a detector clicks during a time step in an honest run (see Eq. (3.4)), then the probability that a specific clause is measured (meaning all four variables in the clause are measured) is at least p_h^4 (where we have used the independence remarks above).

We have also assumed that the instance is balanced and each variable appears in a constant number of clauses, which implies that the number of clauses in an instance of the problem is $O(N)$.

Taking into account the above, we see that the probability that Arthur does not obtain the values of the four variables for any clause in an instance is at most $(1 - p_h^4)^{O(N)}$. This can

be made arbitrarily small, and therefore the completeness arbitrarily close to 1, as long as $p_h^4 = O(N^{-1})$ for a large enough constant, which in turn implies that it suffices to take $|\alpha|^2$ on the order of $O(N^{-1/4})$ with a large enough constant. Note that by taking $|\alpha|^2$ on the order of $O(N^{-1/4})$, the verifier is expected to receive $\widetilde{O}(N^{3/4})$ clicks in the detectors. This is higher than the $O(\sqrt{N})$ bits in the original protocol of [Ref. [109]], where one can choose a specific measurement (depending on the clauses) to always get the value of a clause and hence check satisfiability. In fact the $O(\sqrt{N})$ is needed to prove the uniformity of the state. In our case, the way we achieve a good probability of measuring all variables in a clause of the instance is by increasing the $|\alpha|^2$ to ensure we are measuring enough variables, and that number needs to be now $\widetilde{O}(N^{3/4})$ to make the probabilities work out. We will see later that experimentally we will pick specific values for N and $|\alpha|^2$ that keep the completeness higher than 0.9.

We are going to show now that if the 2-out-of-4 SAT is a NO instance, then the soundness of the protocol, namely the probability of Arthur accepting the proof, is small enough no matter the strategy of the prover as long as the promise of unentanglement holds. For this, we highlight again two important features of our test and the properties of the SAT instances we are dealing with. First, at least a δ fraction of the clauses are unsatisfiable for any assignment of variables, and second, the probability of measuring a particular variable is lower bounded by the fact that Arthur inputs an honest coherent state into the interferometer, even if Merlin sends no photon in his corresponding state.

We can then bound the probability that Arthur measures the values of some variables and finds a clause that contains them and is not satisfied. We have already seen that the minimum probability of Arthur obtaining a value for any variable, no matter what Merlin sends, is $p_d \geq 1 - e^{-|\alpha|^2}$. Then, following the same rationale as before, since a constant δ fraction of clauses are unsatisfied for any assignment, we can conclude that the probability of measuring the values of four variables that make a clause unsatisfied is at least δp_d^4. Assuming again that there are $O(N)$ clauses in an instance, the probability that Arthur does not find any unsatisfied clause is at most $(1 - \delta p_d^4)^{O(N)}$. So again we just need to pick $|\alpha|^2$ large enough in order to make the soundness small enough. In particular, since δ is a constant, we can pick as before $|\alpha|^2 = O((\delta N)^{-1/4}) = O(N^{-1/4})$ and make soundness arbitrarily small. We will see later that experimentally we will pick values for N and $|\alpha|^2$ that keep the soundness lower than 0.6.

3.3.3 Classical complexity of verification

Our quantum verification test takes time $O(N)$ to implement, since Arthur receives a sequence of N pulses that he interferes with his own coherent states and then he simply calculates the number of satisfied clauses (from the $O(N)$ of them) before accepting or rejecting. To compare our test with classical resources in terms of complexity, we are making here a well founded assumption that any classical algorithm for solving 2-out-of-4 SAT runs in time exponential in the instance size N, e.g. the exponential time hypothesis.

In particular, we consider the classical complexity to be of the form $2^{\gamma N}$ for some constant $\gamma \leq 1$. Shöning's algorithm for 3-SAT takes time $(4/3)^n$ on average for instances of size n [120], while the best-known practical SAT solvers can provide a complexity of $O(1.307^N) = O(2^{0.4N})$ [85]. We have also discussed previously that if the information that Arthur gets about the proof is t bits, then the running time of the classical algorithm remains exponential in $(N - t)$.

The value of t, namely the bits of information Arthur obtains about the proof during the verification of a YES instance, can be easily upper bounded for our test by the number of detector clicks during the verification procedure. We want to remark here that in our setting we have an honest Arthur who tries to verify the instance and we do not have to consider a cheating Arthur as in the case of standard cryptographic settings. The expected number of clicks in Arthur's detectors depends on the parameter $|\alpha|^2$, namely the average number of photons per pulse. In particular we have that the number of clicks is $O(N(1 - e^{-|2\alpha|^2}))$ and for our value of $|\alpha|^2 = O(N^{-1/4})$ we have that the information obtained by Arthur is at most $\widetilde{O}(N^{3/4})$. Thus, by picking large enough N it is easy to make the difference $(N - \widetilde{O}(N^{3/4}))$ also large enough.

We will see later that experimentally we will keep this difference larger than 1000. This is an arbitrary choice that nonetheless is more than sufficient to confirm that the classical computation would be unfeasible. For example, given a difference of 150, we can calculate that we would need a 45-digit number of operations to verify the SAT instance: even with processors working at 10 GHz and operated by 10 billion people, and repeating the operation in 10 billion planet Earth copies, parallelizing somehow the whole process, it would be necessary to wait around the age of the Universe to be able to classically verify such instances.

To summarize the above, in the setting that we have described we define the notion of quantum advantage for verifying NP-complete problems of size N with bounded information when three conditions are fulfilled:

1. The verification of the proof by a quantum Arthur takes time linear in N;
2. The obtained completeness is high enough and soundness low enough, where in our case we have set $\mathcal{C} > 0.9$ and $\mathcal{S} < 0.6$;
3. The number of bits of information on the proof that Arthur obtains is much smaller than N, in our case at least 1000 bits smaller, so that the classical complexity of performing the same task is such that it is effectively unfeasible.

3.3.4 Dealing with practical imperfections.

Let us now consider how we can take into account practical imperfections in our verification test in view of its experimental implementation for demonstrating a quantum advan-

tage as we have defined it above.

Up till now we have assumed that Arthur measures the values of the variables perfectly when Merlin is honest. In a practical setting, however, this may not be the case due to errors coming mainly from the imperfect visibility of the interferometric setup and the finite quantum efficiency and dark counts of the single-photon detectors.

There is a simple way to remedy the verification test in order to deal with such imperfections. Arthur performs the same measurements and assigns values to the variables in the following way: when only one detector clicks then he assigns the corresponding value to the variable, i.e., he assigns the value 0 if he registers a click in detector D_0 and nothing in D_1 and vice versa; when both detectors click (which can occur in practice due to the imperfections) then he assigns a uniformly random value to the variable; when no detector clicks then the variable remains unassigned. Note that the fact of picking a random value for a variable in case of double clicks, instead of ignoring this variable, helps avoiding the case where Merlin would input a large number of photons to force double clicks for the variables that he would not want Arthur to measure. Once Arthur assigns the values to the variables, he looks at the clauses for which all four variables have been assigned a value and checks if the clause is satisfied, namely if exactly two out of four variables have the value 1. Knowing the experimental parameters, we can calculate the expected fraction of satisfied clauses in the YES instance (which should be only slightly less than 1 for photonic systems with low loss and errors) and the one in the NO instance (which should be much less than 1 for instances with large enough δ and small enough errors). Arthur can now define an appropriate threshold for the number of satisfied clauses above which he accepts and below which he rejects, and assuming an appropriate gap between the number of satisfied clauses in the YES and NO instances we can then guarantee a large gap between completeness and soundness using simple Chernoff bound calculations.

We will try now to find an experimental parameter regime where we can show quantum advantage. For this, we first make one more assumption about the dishonest Merlin, which is that he always sends states that have the correct mean photon number $\mu = |\alpha|^2$ specified by the protocol, while he can freely choose the assignment values in order to trick Arthur to accept. Note that here we are not trying to define a general interactive proof (Arthur-Merlin) system; we are trying to construct a specific computational task for experimentally demonstrating quantum advantage. Thus, we add on top of the unentanglement assumption the assumption of states with the appropriate mean photon number so as to make the implementation of this task simpler. This essentially corresponds to a dishonest Merlin who can only cheat "classically", in the sense that he can choose whatever assignment he wants for the variables encoded in the quantum states and then send states of the form in Eq. (3.1) (see also Fig. 3.2). This is an assumption that is only needed in order to perform our proof of principle experiment but it is not needed for any of the previous analysis of the protocol, including about completeness and soundness. In fact, even without this assumption we can find a parameter regime where the experimental demonstration is possible, albeit these parameters were just out of reach with our photonics setup but can very well be achieved

in the near future. We will also discuss later how Arthur may in fact be able to force this behaviour of Merlin, namely instead of assuming that dishonest Merlin sends states with the correct mean photon number, Arthur can verify this himself by slightly changing the protocol itself. In any case, we emphasize again that our goal here is to define a specific theoretical scenario and a concrete computational task for which we can show a quantum advantage.

We denote the imperfect visibility of Arthur's interferometer by ν (with $\nu = 1$ in the ideal case) and the dark count probability of the single-photon detectors by p_{dark}. As we will justify later, the effect of the random detection events due to the dark counts can be neglected. To understand the effect of the imperfect visibility, we see that, for example, for an input state in the beam splitter at the k^{th} time step $|\alpha\rangle_k \otimes |\alpha\rangle_k$ (corresponding to $x_k = 0$), the output state will be $|\sqrt{2\nu}\alpha\rangle_{D_0,k} \otimes |\sqrt{2(1-\nu)}\alpha\rangle_{D_1,k}$, hence there is a non-zero probability of a click in the wrong detector (D_1 in this case). We can then calculate the probability of detecting a photon in the correct and wrong detector (and nothing in the other) as follows,

$$\begin{aligned} p_c &= (1 - e^{-2\nu|\alpha^2|})e^{-2(1-\nu)|\alpha^2|}, \\ p_w &= (1 - e^{-2(1-\nu)|\alpha^2|})e^{-2\nu|\alpha^2|}. \end{aligned} \tag{3.5}$$

Moreover, we calculate the probability of a click in both detectors as,

$$p_{dc} = (1 - e^{-2\nu|\alpha^2|})(1 - e^{-2(1-\nu)|\alpha^2|}). \tag{3.6}$$

These double clicks do not contain any information but, as we have explained, they will be used by Arthur to pick a random value for the variable, so they play a role in the verification test. Note that the average number of expected detector clicks is given by $(p_c+p_w+p_{dc})N \approx p_h N$ (with an equality for negligible p_{dark} as in our case). Note also that all quantities depend on $|\alpha|^2$ and ν, but we have neglected the effect of the losses in the system, as we will also justify later.

Let us now calculate, taking into account the above, the expected number of satisfied measured clauses Arthur should obtain in the YES and NO instances. In the YES instance, all clauses are satisfied by the assignment, and the probability that Arthur measures a satisfied clause will be the sum of three terms,

$$p_Y = (p_c + p_{dc}/2)^4 + (p_w + p_{dc}/2)^4 + 4(p_c + p_{dc}/2)^2(p_w + p_{dc}/2)^2. \tag{3.7}$$

The first term is the probability of getting four correct values for the four variables; the second of getting four wrong values; and the third is the sum of the probabilities of two correct and two wrong values in a way that the 2-out-of-4 clause remains satisfied.

In the NO instance, we upper bound the probability of measuring a satisfied clause as follows,

$$p_N \leq p_h^4 - \delta p_Y - (1 - \delta)(p_h^4 - p_Y). \tag{3.8}$$

This is the probability of measuring a clause (for negligible p_{dark}) minus the probability of measuring an unsatisfied clause. To provide a bound on the latter we note that, for any assignment, there is at least a δ fraction of unsatisfiable clauses that will not be satisfied if measured correctly, namely with probability p_Y, and a fraction $1-\delta$ of satisfiable clauses that will be unsatisfied if measured incorrectly, namely with probability $p_h^4 - p_Y$.

It is then straightforward to find the expected number of measured satisfied clauses $T_{\mathcal{C}}$ in the YES instance and $T_{\mathcal{S}}$ in the NO instance, by multiplying the above probabilities with the number of clauses that we assume is some constant (greater than 1) times N. Thus, we have $T_{\mathcal{C}} - T_{\mathcal{S}} \geq (p_Y - p_N)N$. Our experimental values will be such that $T_{\mathcal{C}} - T_{\mathcal{S}}$ is a large enough number to allow us to use Chernoff bounds to guarantee a sufficiently large gap between completeness and soundness.

More specifically, we define a threshold for Arthur's verification as $T = (T_{\mathcal{C}} + T_{\mathcal{S}})/2$, in other words Arthur accepts if and only if at least T measured clauses are satisfied. By a simple Chernoff bound we can then see that the completeness can go arbitrarily close to 1 and the soundness arbitrarily close to 0 by properly tuning the value of $|\alpha|^2$, and again as $|\alpha|^2 = O(N^{-1/4})$. More precisely, we use the following inequalities for completeness and soundness,

$$\mathcal{C} = \Pr[\text{correct measured clauses} \geq T] \geq 1 - e^{-\frac{(T_{\mathcal{C}} - T_{\mathcal{S}})^2}{4T_{\mathcal{C}}}} \tag{3.9}$$

$$\mathcal{S} = \Pr[\text{correct measured clauses} \geq T] \leq e^{-\frac{(T_{\mathcal{C}} - T_{\mathcal{S}})^2}{4T_{\mathcal{S}}}}. \tag{3.10}$$

To illustrate how this analysis allows us to identify an experimental parameter regime where it is possible to demonstrate a quantum advantage for our verification task, we show in Fig. 3.3 theoretical bounds for the fraction of measured satisfied clauses in the YES and NO instances, as well as the gap between the completeness and soundness, as a function of the mean photon number $\mu = |\alpha|^2$, for $N = 10000$, $\nu = 0.91$, $\delta = 0.15$, and negligible dark counts. We can see that for our aforementioned target gap, where we want to keep the completeness above 0.9 and the soundness below 0.6, there is a region of μ where quantum advantage can be shown for the chosen parameters.

Let us now discuss the more general scenario where the dishonest Merlin may send any unentangled state (including with no or many more photons). This is a more complicated case to analyze, but we do know that whatever Merlin does, Arthur will still receive a value for a variable from the photons he inputs himself in the interferometer, which is at least $p_d = 1 - e^{-|\alpha|^2}$. If we drop the assumption that Merlin will only send coherent states with the correct mean photon number, we can still find a region with a positive gap between completeness and soundness, albeit with more stringent experimental conditions that were not fulfilled in our setup, in particular with respect to the required visibility, but that we believe can be fulfilled in the near future.

Note also that Arthur could potentially try to force Merlin to send states with the correct mean photon number by creating the pulses himself, sending them over to Merlin who

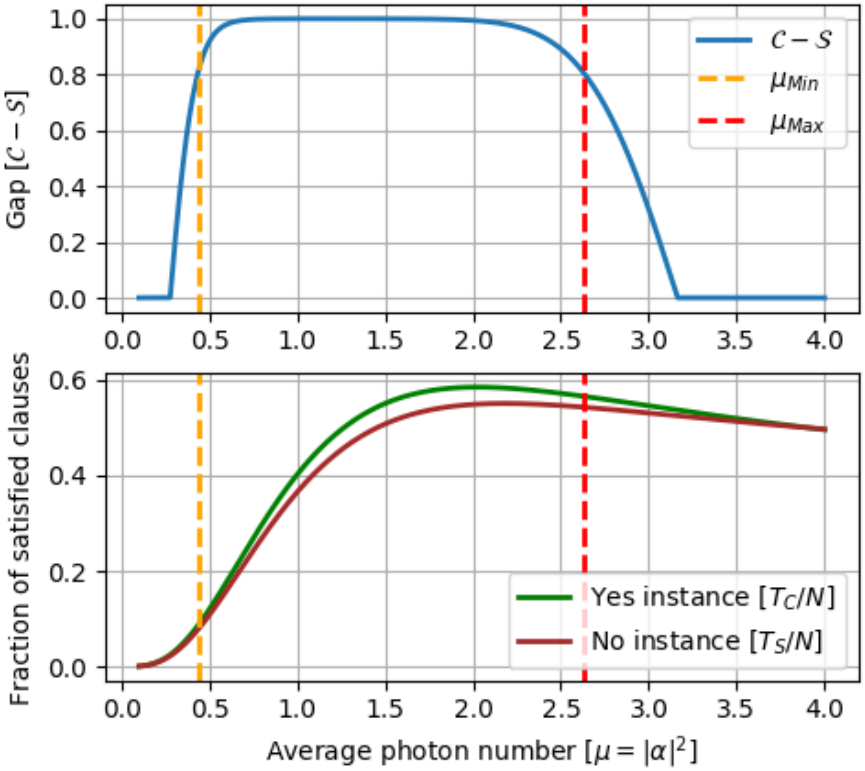


Figure 3.3: **Numerical results.** (Top) Gap between completeness and soundness as a function of the mean photon number $\mu = |\alpha|^2$, for $N = 10000$, $\delta = 0.15$, $\nu = 0.91$. The two vertical lines correspond to the minimum and maximum μ in order to have at the same time completeness $\mathcal{C} > 0.9$ and soundness $\mathcal{S} < 0.6$. (Bottom) Fraction of measured satisfied clauses as a function of μ. As the mean photon number increases the number of satisfied clauses in the NO instance overcomes the one in the YES instance.

prepares the state with the setup of Fig. 3.2 and returns it. Arthur can use random timings for his pulses impeding Merlin from injecting more photons and also use part of the pulses in order to count the number of clicks and convince himself that Merlin is not sending fewer photons over. Again, we do not need to do any of this for our demonstration of a quantum advantage, since we are free to define the computational task ourselves, namely verification of NP problems for a specific type of interactive proof systems, without having to deal with general cryptographic considerations and dishonest behaviours. Nevertheless, this would provide a simple solution in case one might want to use our protocol in practical scenarios, for example for server-client verification.

Last, we claim that losses are not important in our setting. Again, this is a verification scenario where an honest Arthur tries to efficiently verify an NP instance with the "small" help of an untrustful Merlin. Hence, Arthur and Merlin can jointly measure the potential losses during a calibration phase before the actual verification starts and increase the power of their pulses by the factor $1/\eta$, where η includes the channel and detection efficiency. Thus, we do not have to worry here about an Arthur that can use the losses to his benefit.

To summarize the above and in preparation for the description of our experimental implementation, we provide below a step-by-step outline of the protocol:

Protocol NP Verification

Input: Instance of the NP-complete problem and all its relevant parameters: N, δ, etc., after the reduction to a 2-out-of-4 SAT;
Goal: Verification of the solution;

1. Merlin and Arthur jointly perform a pre-calibration of the optical setup, finding the values of the visibility ν_N and the transmittivity η;
2. Arthur computes the minimum value of the mean photon number number μ_N in order to satisfy the quantum advantage conditions 1-3 and communicates it to Merlin in order to tune the amplitude of his pulses; he also computes the threshold T for accepting a proof;
3. Arthur sends a signal to Merlin to trigger the protocol;
4. Merlin encodes his proof in the phases of the pulses which are then sent to Arthur;
5. Arthur interferes Merlin's pulses with his own and assigns a value x_k each time he registers a measurement in the k^{th} pulse:
   - $x_k = 0$ for a click in detector D_0 and no click in D_1;
   - $x_k = 1$ for a click in detector D_1 and no click in D_0;
   - x_k is randomly assigned if both detectors click.
6. For all the measured bits that form a clause, Arthur checks the satisfiability;
7. If the number of satisfied clauses is greater than T, Arthur accepts the proof, otherwise he rejects.

3.3.5 Experimental results

We now have all the ingredients to describe the experimental implementation of our verification test and the assessment of the quantum advantage for this task. As we defined previously, we need to satisfy three conditions to show quantum advantage. We need the verification procedure to take time linear in N, to have completeness and soundness such that $\mathcal{C} > 0.9$ and $\mathcal{S} < 0.6$, and that the number of clicks Arthur registers is much smaller than the input size N.

First, as we will see, in our experiment we use indeed a train of coherent pulses of size N and some simple classical post-processing of the measurement results, so our test satisfies condition 1. In fact, the real time to run the verification procedure for N between 5000 and 14000 was a fraction of a second for the quantum part, a few seconds for the classical post-processing and a couple of minutes for the calibration procedure for each run.

Second, we will show that our verification procedure has high completeness, i.e., when the instance is satisfiable and Merlin sends to Arthur a satisfying assignment encoded in the coherent states, then Arthur accepts with high probability. For the same experimental parameters we will then use our theoretical analysis that upper bounds the maximum soundness of our protocol for any strategy of Merlin, and ensure that the soundness is much lower than the experimentally demonstrated completeness, thus proving condition 2 of quantum advantage.

In fact, to simplify the classical pre- and post-processing, we experimentally perform a modified version of the test, where we do not sample balanced and probabilistically checkable YES instances with planted satisfying assignments (this is far from being straightforward), but we generate uniformly random N-bit strings (for several values of N) that correspond to satisfying assignments. Note that a uniform distribution of the satisfying assignments is the hardest case for the problem, since with any other distribution, Arthur would already have some information about the possible solutions to the problem. After that, we check the number of the variables for which Arthur obtains the correct value, the number of wrong values, and the number of undefined variables. From these numbers we compute the expected number of satisfied and unsatisfied clauses Arthur will get on a random YES instance, and using the threshold that has been defined in the calibration phase of the experiment described below, we conclude whether Arthur would accept or reject the instance, thus estimating the completeness of our protocol.

Finally, the measurements events of Arthur are also used to ensure that condition 3 for quantum advantage is satisfied.

Let us now provide more details on our experiments. The experimental setup is shown in Fig. 3.4. The coherent light pulses are generated using a continuous wave laser source emitting light at 1560 nm followed by an amplitude modulator (AM), at a rate of 50 kHz and with a pulse duration of 10 ns. An unbalanced beam splitter is used to monitor the pulse power and a variable optical attenuator (VOA) to set the mean photon number at the desired level. We then use a balanced beam splitter (S) to direct the coherent pulses to Arthur and Merlin. Following the scheme for the verification test shown in Fig. 3.2, Merlin impinges his proof on the phase of the pulses using a phase modulator (PM). Arthur and Merlin then both use a set of variable optical attenuators to finely tune and equalize the power of the signals entering the output balanced beam splitter of the interferometer (I). The pulses are finally detected by two InGaAs single-photon detectors (D_0 and D_1) and the measurement results are collected by Arthur. The experiment is controlled by a data acquisition card and the data is analyzed with dedicated software.

We perform several preliminary measurements and calibrations before moving on with the verification test. In particular, we calibrate the voltage level needed to induce a π-phase shift, V_π, with the phase modulator off line. Phase drifts may occur during the experiment and affect the obtained visibility, hence requiring real-time phase correction techniques [111]. In our case the time scale of the drift (on the order of 5 s) was much longer

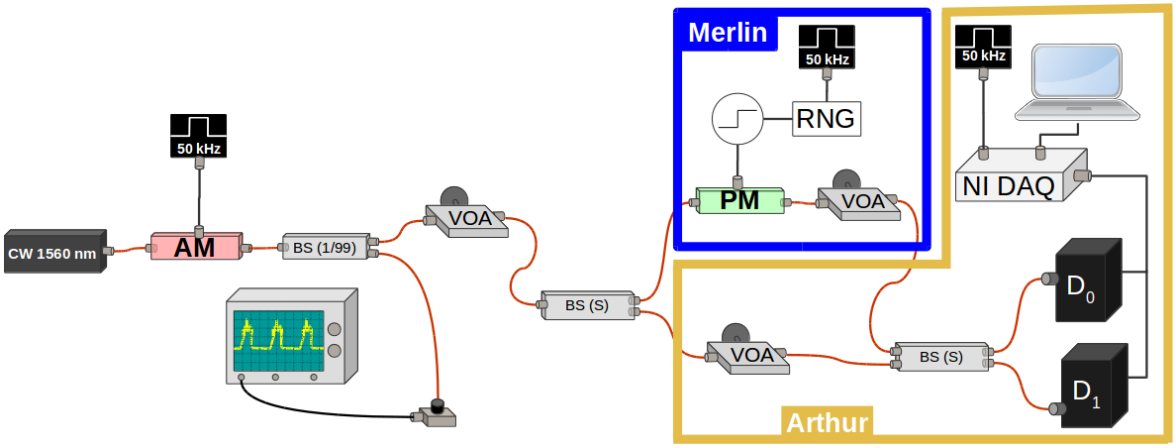


Figure 3.4: **Experimental setup.** A coherent light source operating at a wavelength of 1560 nm (Pure Photonics) together with an amplitude modulator (AM) are used to generate coherent pulses at a 50 kHz repetition rate and with a 10 ns pulse duration. Using a beam splitter with 1/99 ratio, we monitor the pulse power with a photodiode and send the small fraction of the beam to the rest of the setup. The beam is further attenuated before being split with a balanced beam splitter (BS) and sent to Merlin and Arthur. The former encodes the proof in the phases of his pulses using a phase modulator (PM). They both use attenuators to fine tune and equalize the photon number in their paths and the pulses are then interfered on the output beam splitter (I) before been detected by InGaAs avalanche photodiode single-photon detectors (IDQuantique). The measurement outcomes are collected using a National Instruments data acquisition card and analyzed with dedicated software.

than the duration of each run of the protocol (around a fraction of a second) and it was therefore not necessary to use such feedback loops. Arthur and Merlin also need to carefully equalize the power of their pulses before interfering them, as required by our test. To do this, Arthur calibrates the losses in Merlin's path by first removing his signal, measuring detection events due to Merlin's signal only, for several values of the mean photon number, and then minimizing the clicks on one of the detectors with his signal reconnected. This procedure also allows Arthur and Merlin to determine the losses in their setup, and hence the efficiency η, which includes the channel efficiency $\eta_{\text{channel}} \approx 38\%$, and the quantum efficiency of the single-photon detectors, $\eta_{\text{det}} \approx 25\%$. As we have explained, this parameter does not play a direct role in our verification test.

Importantly, the above calibration procedure allows Arthur to evaluate the visibility of the interferometer, which is central to the assessment of the performance of our test. Indeed, we use this estimation as benchmark for the expected number of satisfied clauses in the YES and NO instances, and correspondingly define a threshold for accepting a proof, as we have detailed previously. A low visibility will increase the number of errors so that we will need to increase δ in order to verify the solution with sufficient completeness and soundness.

In our experiment, we use the nominal value $\nu_N = 0.93$, as well as $\mu_N = 1.31$, and set correspondingly $\delta = 0.15$. These values are chosen such that in our theoretical estimations

$\mathbf{N}$	ν	μ	$\mathbf{s}_{\text{clk}}$	$\mathbf{c}_{\text{clk}}$	$\mathbf{d}_{\text{clk}}$	$\mathbf{N}-\mathbf{t}_{\text{clk}}$	$\mathbf{T}$	$\mathbf{S}_{\text{cl}}$
5000	0,87	1,29	3657	3505	964	1343	2254	2227
6000	0,93	1,30	4834	4741	719	1166	2717	3231
7000	0,94	1,34	5670	5582	848	1330	3232	3904
8000	0,92	1,29	6203	6062	1195	1797	3613	4030
9000	0,92	1,30	6974	6813	1363	2026	4088	4546
10000	0,95	1,15	8045	7929	947	1955	4111	5082
11000	0,93	1,30	8675	8524	1515	2325	4996	5789
12000	0,93	1,30	9632	9466	1476	2368	5437	6471
13000	0,95	1,30	10636	10496	1405	2364	5902	7320
14000	0,94	1,29	11135	10950	1807	2865	6801	7437

Table 3.1: **Summary of experimental data.** In each run we increase the input size N by 1000. The table shows: the actual visibility ν in each run; the average number of photons per pulse μ; the number of measured single clicks s_{clk} and those that were in the correct detector c_{clk}; number of double clicks d_{clk}, which correspond to randomly assigned variables; the missing bits to complete the solution; the threshold of correct measured clauses for accepting a proof T; the number of satisfied clauses in the experiment S_{cl}. The parameters $\delta = 0.15$, $\nu_N = 0.93$ and $\mu_N = 1.31$ are kept fixed in the theoretical analysis of the experiment.

(see Fig. 3.3) the conditions $\mathcal{C} > 0.9$ and $\mathcal{S} < 0.6$ are satisfied at the same time for all the values of N that we will be using. The value of δ will be fixed for all the runs; however, we experimentally measure the actual visibility in each case. We remark that here we are using a single laser to generate the pulse sequences of Arthur and Merlin, which is optimal for obtaining high visibility values. Nevertheless, it is still possible to use this setup for assessing the performance of our test for demonstrating a quantum advantage since all actions required by the test, as shown in Fig. 3.2, are performed independently.

We finally remark that the dark count probability in our setup is $p_{\text{dark}} \sim 10^{-3}$, and hence the effect of dark counts can safely be considered negligible for our values of ν and μ. In fact, for our choice of parameters, we have $p_c, p_w, p_{dc} \gtrsim 10^{-2}$ as can be easily seen from Eqs. (3.5).

We are now ready to analyze our verification test enabling Arthur to verify efficiently that a given 2-out-of-4 SAT instance is satisfiable. As we have explained, we assume that Merlin acts honestly and only the environment will lead to errors that will make Arthur reject a correct proof. After performing the preliminary calibrations, Merlin starts the test by encoding his proof on his coherent pulse sequence. Here, as a proof, we generated a random Boolean string of N variables (for several values of N). Arthur records all clicks t_{clk} including single and double clicks on both detectors. We denote the single clicks as s_{clk}. He assigns a bit 0 or 1 to variable x_k if the pulse at time step k resulted in a single click in detector D_0 or in a single click in detector D_1, respectively. For the double clicks, he assigns a random value to the corresponding variable, while we leave all other variables undefined.

For computing the completeness of the verification, we need to decide if Arthur would have accepted or rejected the specific run of the verification test. Had we fixed a specific instance then Arthur would just check with the values of the variables that he has obtained, how many clauses are satisfied and how many clauses are not, and depending on the threshold T he would accept or reject. Note that Arthur can indeed compute the value of T given the experimental values of μ and ν.

As we said, in order to avoid the complications of sampling such classical instances in a fair way, we decide whether Arthur accepts or rejects the instance using the same threshold T, but estimating the number of clauses Arthur would have found satisfied or not, through the number of correct variable values he really obtained through the experiment. Since the instances are assumed to be balanced, this is equal on expectation over random instances to the corresponding calculations on the clauses.

In other words, from the number of all single clicks s_{clk}, the number of single clicks that correspond to the correct variable value c_{clk}, and the number of double clicks that are randomly assigned dc_{clk}, we can infer the probabilities $p_{dc_{\text{exp}}} = \frac{t_{\text{clk}}}{N}$, $p_{c_{\text{exp}}} = \frac{c_{\text{clk}}}{N}$ and $p_{w_{\text{exp}}} = \frac{s_{\text{clk}} - c_{\text{clk}}}{N}$, from which we can compute the expected number of satisfied clauses in the YES and NO instances using Eqs. (3.7) and (3.8). Note that the expected numbers are sufficiently far from the threshold so that we do not expect the variance of the number of satisfied clauses (for each specific instance) to affect the completeness. For these experimental parameters we also compute the soundness, which is in fact very close to 0, see Fig. 3.5.

In order to prove the third condition for the quantum advantage, if the proof is accepted, we count the number of variables for which Arthur has no information, i.e., $N - s_{\text{clk}}$, which is the information that Arthur is missing to complete the solution. We remark again that a double click in both detectors does not provide any information to Arthur and we also assume that all single clicks reveal the true variable value. With only classical resources, Arthur would need a computational time of $2^{\gamma(N-s_{\text{clk}})}$, for some prefactor γ (for SAT solvers around 0.4). As we have explained, here we claim quantum advantage if $N - s_{\text{clk}}$ is larger than 1000, but it is clear that for any given threshold one can reach quantum advantage by increasing N and improving ν.

In Table 3.1 we summarize our experimental data for fixed δ, slightly varying μ, and ν evaluated for every input size N. We include the number of single clicks, correct clicks, double clicks, missing bits, as well as the threshold T and the number of computed satisfied clauses in each case. As we can see, the number of bits Arthur still misses at the end of the protocol increases with N, which means that the problem is becoming more and more difficult for classical computation as N increases. Moreover, starting from $N = 6000$, we see that the computed number of satisfied clauses is much bigger than the threshold, hence the completeness is very close to one.

Finally, in Fig. 3.5 we compare the simulations with a typical run of the experiment for various N fixing the nominal photon number μ_N, visibility ν_N and the constant δ. Notice

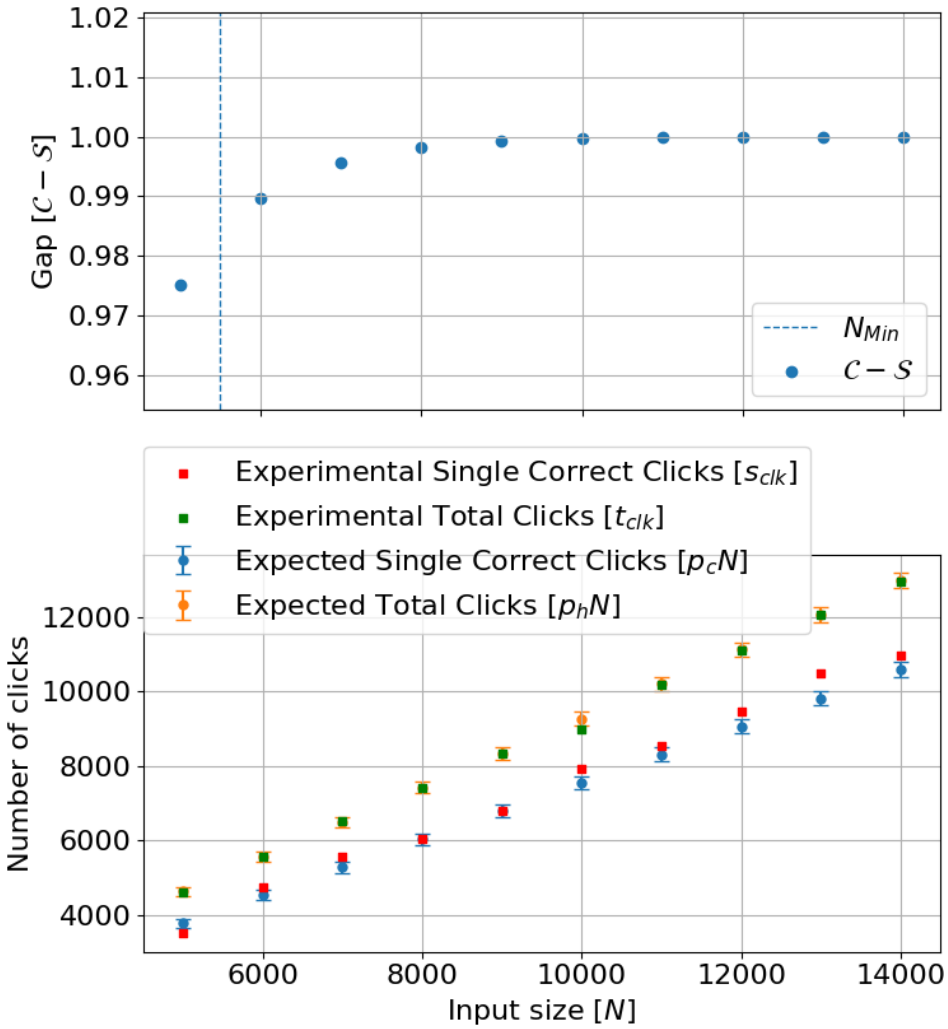


Figure 3.5: **Experimental data.** (Top) Plot of the gap as a function of N when simulating the protocol with the nominal parameters of $\nu_N = 0.93$, $\mu_N = 1.31$ and $\delta = 0.15$. The vertical line bounds the region for quantum advantage. (Bottom) Number of clicks as a function of N. The correct bits are clicks in the correct detector or in both detectors with half probability and total clicks is the total number of measured pulses. Each square corresponds to one run of the protocol whereas the dots with error bars are numerical. Because each pulse gives a poissonian probability distribution in the number of photons, the error bar is given by $2\sqrt{\#\text{clks}}$ which is twice the root mean square of the poissonian.

how the gap between completeness and soundness increases with N and very fast becomes almost 1. In the experimental runs shown in the figure, the only point for which we cannot show quantum advantage is the one at $N = 5000$, since the gap between completeness and soundness is not large enough. This is due to a low level of visibility that induced a too large number of incorrect detections in this case.

3.4 Discussion

The result of this chapter is an experimental demonstration of a computational quantum advantage in the interactive setting with linear optics. The simplicity of our experimental implementation, in addition to the powerful algorithmic idea of the Sampling Matching, exemplifies the power of linear optics, and in particular of coherent state mappings, not only for communication but also for computational tasks. Differently from the other forms of computational quantum advantage, that are tailor-made to challenge the capacities of traditional computing beyond their capabilities and to promote the progress of quantum platforms, this work enhances the efficacy of the already existing quantum photonics to harness quantum advantage.

It will be interesting to investigate further applications of linear optics, in particular in the frame of near-term quantum technologies. Moreover, we would like to argue that our computational task, that of efficiently verifying NP-complete problems with limited leakage of knowledge about the proof, is a step closer to useful applications, even though it remains for the time being a theoretical scenario. In fact, one can start imagining applications in a near-term quantum cloud, where a powerful quantum server might have the ability to perform some difficult computation, and the much less powerful client can verify the validity of the computation, without the server needing to reveal all the information to the client. Such limited-knowledge proof systems could also have applications in a future quantum internet, similarly to classical zero-knowledge proofs that can be used for identification, authentication or blockchain. In addition, we could picture the same scenario in which, although, the client is not interested in getting to know the whole solution but only to know if there is one, in order to proceed with some computation. In this case, Merlin (or the quantum server) does not need to care about the privacy of the solution and only wants to perform the verification scheme with the least amount of energy, therefore the lowest average photon number per pulse, similarly to [121]. Even though the advantage would be only polynomial its relevance could be fundamental for a society that is clashing with the reality of the energetic unsustainability of the internet.

It still remains an open question to find the first concrete real-world application of quantum computers and our results show that linear optics might provide an alternative route towards that goal.

Chapter 4

Quantum electronic voting

4.1 Why electronic voting is still a bad idea . . . 81
4.2 Quantum e-voting protocol . . . 82
4.2.1 Notation . . . 82
4.2.2 High level protocol description . . . 83
4.2.3 Subroutines . . . 85
4.2.4 Quantum e-voting pseudo code . . . 90
4.3 E-voting protocol Analysis . . . 91
4.3.1 $(\sigma_H, \sigma_D, \gamma)$-Correctness . . . 93
4.3.2 ζ-Privacy . . . 94
4.3.3 Authentication . . . 96
4.3.4 Double voting . . . 96
4.3.5 Verifiability . . . 96
4.3.6 Receipt freeness . . . 97
4.3.7 Additional candidates . . . 97
4.3.8 Proof of Theorem 1 . . . 99
4.3.9 Proof of Theorem 2 . . . 100
4.3.10 Proof of Theorem 3 . . . 104
4.4 Discussion . . . 105

The simplest possible quantum connection already revealed some significant features that are unmatchable with classical techniques. Nonetheless, one link is hardly a network and, although the preparation and measurement of a single quantum state already provides non-trivial crucial qualities, some of the most important properties of quantum systems arise only when we drop the assumption of unentanglement and we unveil the nature of multipartite quantum states.

When two physical systems interact, they can end up being correlated. Entanglement, is a quantum superposition of correlations that occurs when quantum systems interact in some specific manner. When a subsystem of a multipartite quantum state is measured, it will yield an outcome that is at the same time perfectly random and perfectly correlated with the outcomes produced by the measurement of the other parts of the whole entangled state, regardless of the distance between these parts. This outstanding trait of inseparable many bodies quantum states can be engineered to produce shared randomness on-demand among distant users who can employ this resource to perform multipartite communication and computation.

Some of the most ambitious quantum protocols that are allowed by the presence of distributed entanglement are anonymous transmission [122], which enables two nodes to communicate a message in an untrusted network anonymously, byzantine agreement [123], that allows a network of n agents, who could in part be faulty or malicious, to reach agreement on a single bit of data and secret sharing [124], that allows to transfer a quantum state (or a classical message encoded as quantum state) only with the consent of a certain fraction of the agents. One of the most desirable technologies that quantum information promises to revolutionize is, however, *electronic voting*.

Electronic voting is a useful but challenging internet-based protocol that despite many theoretical approaches and various implementations with different degrees of success, remains a contentious topic due to issues in reliability and security. In fact, the very definition of security in electronic voting is ambiguous, which explains why almost all the proposed schemes were subsequently declared insecure. All the different implementations performed by the governments of different countries in the last years attired the critics of specialists [125] and the 2006 American documentary *Hacking democracy* revealed how easily an electronic voting system can be exploited to manipulate the result of a public election.

Here we present a quantum protocol that exploits an untrusted source of multipartite entanglement to carry out an election without relying on election authorities, simultaneous broadcast or computational assumptions, and whose result is publicly verifiable without compromising the robustness of the scheme. The level of security depends directly on the fidelity of the shared multipartite entangled quantum state, and the protocol can be readily implemented for a few voters with state-of-the-art photonic technology.

4.1 Why electronic voting is still a bad idea

Electronic voting, or e-voting, is a functionality built on top of the Internet or any distributed network that allows performing large-scale elections in a secure and verified way, even in the presence of distrusted authorities or dishonest agents. The benefits of such a functionality include a faster and simpler way to carry out elections resulting in higher public participation (*i.e.*, a higher number of voters), reduction of election costs, and accessibility for people with disabilities. Furthermore, e-voting offering information-theoretic security guarantees in principle the security and honesty of the elections even in the case of corrupted officials or a coalition of dishonest agents. However, the adoption of a protocol that uses a public network to accomplish elections also increases the possibilities for fraud by manipulating the results or violating privacy [126]. Moreover, even though it may not be possible for such a protocol to be infringed, the agents would need to trust devices and programs they did not author and, most likely, not even understand [127]. Finally, it is also necessary to take into account the cost of implementing the elections with advanced technology.

Classical e-voting systems are based on computational assumptions and might not be secure against quantum or other adversaries. Moreover, there have been serious criticisms against commercial e-voting systems due to insecurities [128]. In recent years, several quantum e-voting protocols have been proposed, announcing perfect security also in dishonest scenarios. However, none of these was able to provide a rigorous mathematical definition of the properties required, such as privacy, verifiability, and correctness, as well as to identify proper corruption models suitable for this scenario. As a matter of fact, in [129], the authors discovered vulnerabilities in all previously proposed quantum e-voting schemes. Let us also mention the work in [130], where a lattice based post-quantum cryptographic protocol achieving computational security was suggested. This may however be undesirable for e-voting because privacy cannot be guaranteed in the long term. For these reasons it is paramount to find schemes based on information-theoretic security, rather than computational assumptions, in order to ensure honest elections also in the presence of dishonest authorities with unbounded (or much bigger than publicly known) computational power. This level of security for an e-voting scheme was announced in [131], which proposed a protocol exploiting only classical resources. However, the requirement of a simultaneous broadcasting channel makes it impractical even for a small number of voters, or turns the security back to computational if the simultaneous broadcasting channel is simulated via usual channels.

Here we describe and formalize several properties required by an electronic voting system to be secure and propose a quantum protocol that satisfies these properties even in the presence of computationally unbounded adversaries and without necessarily trusting the devices that execute the elections. Another benchmark is that of practicality, in the sense that we want the protocol to be implementable with technology that is already or soon-to-be available and hence that it is possible to carry out a demonstration at least for a

few voters. Our protocol fulfils the above requirements, at the expense on relying on the generation and manipulation of a Greenberger-Horne-Zeilinger (GHZ) state with as many particles as voters, which is the major limitation to its scalability. We note, however, that here the number of voters can refer not to the total number of voters in the election, but the number of voters within each polling station, since, as in the classical case, we can aspire to provide privacy of each vote within each such polling station.

Our protocol utilises a multipartite entanglement verification scheme [132]–[134] as a subroutine as well as classical subroutines useful for anonymous transmission in communication networks. It is inspired by the self tallying quantum anonymous voting protocol proposed in [135], the particularity of which resides in the absence of a tallier and any election authority. Although this protocol was proven insecure in [129], by employing the multipartite entanglement verification scheme of [132] and simplifying the quantum resource requirements using ideas of [131], we devise an efficient quantum protocol and rigorously prove its security. Furthermore, even though sharing an N-party GHZ state for big N needed for large-scale elections is today still technologically out of reach, we note that applications for small number of voters are already feasible and important, and so are applications where one can use multiple small-scale GHZ states to mimic an election with a large number of polling stations. Similarly to the proposal of [135], such a protocol can also be used as an anonymous chat board, where one party can write a message visible to anyone but no one can deduce who sent it (similar to one party being able to vote without anyone being able to deduce whose vote that is), or even as a form of anonymous distributed computation.

4.2 Quantum e-voting protocol

In the general setting of our protocol, a source of N-qubit GHZ states, $|GHZ\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$, is situated at the central node of a star-graph quantum network, whose edges are the communication links needed for the distribution of the entangled qubits to N agents. Even though voters do not have to trust the multipartite entangled photon source, it should be capable of producing high fidelity quantum states to pass the verification test at the heart of the protocol in the honest case, and with a high enough rate to ensure the elections can be performed in an efficient way. Each agent only needs to be able to receive, perform unitary operations, store for a short time, and measure single photons. A particular feature of our protocol is that it does not require talliers or other election authorities, as all the votes are announced publicly and anonymously and so each voter can verify that the tally is correct. However, as we will see later, if a voter detects malicious behaviour, they can abort the protocol using the appropriate subroutine at the end of the election.

4.2.1 Notation

Before describing the protocol, let us lay out some useful notation.

- N: the total number of participants to the election;
- $\mathbf{W} = \{1, 2, \ldots, N\}$: the set of all the voters. $\mathbf{W_H}$ and $\mathbf{W_D}$ the sets of honest and dishonest voters respectively;
- $\mathbf{V} = \{v_k\}_{k \in W}$: the set of *votes*. Each voter v_k's value is the index of the candidate for which they want to vote;
- K: the number of eligible candidates;
- $\mathbf{C} = \{0, 1, \ldots, K-1\}$: the set of candidates. We first assume $\mathbf{C} = \{0, 1\}$; the generalization to more candidates is shown in the dedicated section.
- $\mathbf{B} = \{b_k^j\}$: the bulletin board encodes all the anonymous votes to be tallied.
- $\mathbf{E} = \sum_k \mathbf{B}$ is the set of votes resulting by summing the rows of the bulletin board. Errors or dishonest players may induce some b_k to be different from v_k.
- $\mathbf{T} = \{t_i\}_{i \in C}$ the tally, a vector whose elements represent the number of votes for the corresponding candidate. It can always be computed as a vector valued function of the bulletin board $f(\mathbf{B}) = \mathbf{T}$.
- $\mathbf{R} = \{r_i\}_{i \in \mathbf{C}}$ is the result of the elections with the actual set of voters $\mathbf{V}$. It is the histogram of the real voters preferences.

4.2.2 High level protocol description

Let us now describe the protocol, referring to a number of classical and quantum subroutines when it is necessary. The pseudo-code of each of the subroutines is provided in 4.2.3, while in 4.2.4 we show in detail the pseudo code of the whole quantum e-voting protocol and Fig. 4.1 we provide a simple instance of the voting procedure. We will assume in the following that the election admits only two possible candidates, '0' and '1', while the generalization to additional candidates is described later.

In the first phase of the protocol, each agent $k \in [N]$ needs to obtain a secret, unique index $\omega_k \in [N]$ that indicates the round the agent becomes the voting agent. To do this, the agents perform the UniqueIndex subroutine.

Subsequently, the second phase consists of as many rounds as the voters and at each round one agent votes according to the order based on the secret indices shared in the first phase of the protocol.

Each voting round $\ell \in [N]$ starts with the voting agent (namely the agent k who has received the unique index $\omega_k = \ell$) deciding repeatedly to perform one of two actions according to some random coins they flip locally: Verification of the source or Voting. The probability of this decision is guided by a parameter M, which equals the number of coins, so that the probability the coins return 'all heads' (which corresponds to Voting) is 2^{-M}.

In order to notify everyone anonymously of the outcome of the coin flip, all agents then perform a LogicalOr subroutine with input 0 except the voting agent whose input depends on the result of the coin flip: if the result was not 'all heads' the agent inputs 1, announcing anonymously Verification to the other agents, otherwise the agent inputs 0 announcing Voting. For the LogicalOr protocol performed in this phase, we will assume for simplicity that if the voting agent inputs 1, then the probability that the outcome is 1 is equal to 1, which corresponds to the choice of a very small security parameter for this subroutine (see Lemma 2 in 4.2.3).

When Verification is announced, following the corresponding protocol the voting agent first performs the RandomAgent subroutine in order to choose a verifier anonymously; this is necessary because the verifier needs to communicate publicly with the other agents so if their identity is the same as the one of the voting agent, the voter's privacy would be violated. Then, they all proceed with the Verification test of the multipartite quantum state distributed by the untrusted (or just faulty) source. In the ideal case, where the quantum state is created and distributed with no errors and all the operations are perfect, if the state does not pass the Verification test the protocol is aborted. In any realistic implementation, however, the protocol cannot abort as soon as there is any error. In practice, at each voting round, during the verification tests before Voting, each honest agent k counts the number of trials and rejections when they are the verifier, computes the practical parameter $\delta_k = \frac{\text{rejections}_k}{\text{trials}_k}$, and if this is larger than a predetermined threshold δ, the entire protocol is aborted.

When Voting is announced, the agents proceed with the corresponding subrtoutine, which returns an N-dimensional binary vector encoding the voting agent's preference. The underlying idea here is that if all qubits of the shared GHZ state are measured in the Hadamard basis, the sum of the outcomes d_k modulo 2 of all agents is always zero. Then, at this round, all agents will just perform a Hadamard measurement on their qubit, while the voting agent k will XOR the outcome of the Hadamard measurement with their vote intention v_k. This implies that when everyone follows the protocol, the parity of all announced outcomes in the round is equal to the vote intention v_k.

Then, a new round starts, the $(\ell+1)$-th round, where it is the turn of agent k' with index $\omega_{k'} = \ell + 1$ to be the voting agent. After all voting rounds have completed and everyone has proceeded with Voting, all agents publicly broadcast their own updated vectors and all together will form an $N \times N$ bulletin board $\mathbf{B}$. By computing the parity of each row (corresponding to each round) we get the vote vector $\mathbf{E}$ (since as we said the parity of each row is equal to the vote of the voting agent) from which the tally $\mathbf{T}$ can be calculated easily by everybody. Since the indices are unique and secret, each agent can verify that their vote is correct without revealing their choice. If an agent wants to abort the protocol because of suspected fraud (*e.g.*, the tally does not agree with their vote intention) they can input their objection anonymously during the LogicalOr procedure that follows, where the security parameter defines how many agents on average should raise an objection before the election is actually aborted.

$$d_1 = \begin{pmatrix}0\\1\\1\\0\end{pmatrix}, d_2 = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}, d_3 = \begin{pmatrix}1\\1\\1\\1\end{pmatrix}, d_4 = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \longrightarrow \mathbf{B} = \begin{pmatrix}0 & 0 & 1 & \mathbf{1}\\ 1 & \mathbf{1} & 1 & 0\\ \mathbf{0} & 0 & 1 & 0\\ 0 & 1 & \mathbf{0} & 0\end{pmatrix} \longrightarrow \mathbf{E} = \begin{pmatrix}0\\1\\1\\1\end{pmatrix}, \mathbf{T} = \begin{pmatrix}1\\3\end{pmatrix}$$

Figure 4.1: Example of the voting procedure according to our e-voting scheme with 4 voters who vote in the order $(4, 2, 1, 3)$. At the end of all rounds each voter has a list of 4 Hadamard measurement outcomes d_k, and for each round the four outcomes sum to 0 modulo 2. The voters express their vote by adding their vote (0 or 1) to the row corresponding to their secret index (in bold), then broadcast the resulting vector and all together they form the bulletin board $\mathbf{B}$. Here the votes where $(0, 1, 1, 1)$. Then they sum each row of $\mathbf{B}$ to compute the election vote set $\mathbf{E}$, from which is computed the tally $\mathbf{T}$. In this example candidate '1' won the election.

4.2.3 Subroutines

Let un now take a look at the specific subroutines employed in the Quantum e-voting protocol. The LogicalOr, RandomBit and RandomAgent subroutines are classical anonymous protocols taken from [131] and used in [122]. In particular, the last two are based on the first one, which performs the logical OR of all the agents' inputs. It will thus output 1 with high probability if and only if at least one agent had input 1. The RandomBit subroutine employs the LogicalOr to produce shared randomness, *i.e.*, a random bit publicly announced according to some probability distribution. This can be used a number of times in order to draw an agent at random among the voters through RandomAgent.

Protocol LogicalOr

Input: N agents, N boolean variables x_i, security parameter $S = (1-2^{-\Gamma})^{\Sigma} \in (0, 1)$.
Output: $y = \bigvee_i^N x_i$.
Resources: Classical communication and random numbers.

Description:

1: Decide N random orderings, such that each voter is the last once. For each ordering repeat Σ times the following.
2: Each voter k gives an input x_k.
3: If $x_k = 0$ set $p_k = 0$, otherwise toss Γ coins and set p_k to 1 if the result is 'all heads' and to 0 otherwise.
4: Then each voter generates uniformly at random an N-bit string $r_k = r_k^1 r_k^2 ... r_k^N$, such that $\bigoplus_{i=1}^N r_k^i = p_k$.
5: Voter k sends r_k^i to voter i for all i, keeping r_k^k for themselves.
6: Each voter sums the received bits and broadcasts the parity $z_i = \bigoplus_{k=1}^N r_k^i$ according to the ordering.
7: Compute the parity of the original bits $y = \bigoplus_i z_i$.

8: From this everyone can also compute the parity of all other inputs except their own $w_k = \bigoplus_{i=1}^{N}(z_i \otimes r_k^i)$.
9: Repeat Σ times from step 4: each time repeat with p_k as new inputs.
10: If at least once in the Σ repetitions for the various orderings $y = 1$, this is the output of the protocol, otherwise it is $y = 0$.

The LogicalOr functionality is implemented probabilistically by assigning a random value p_k to all inputs $x_k = 1$, while $p_k = 0$ if $x_k = 0$. Then the parity of the p_k is computed anonymously for various orderings, such that each voter is last once, and for repetitions for each ordering. Since the inputs of the parity are random, if at least one voter has input 1, the output of the parity will be 1 at least once through all the repetitions. The orderings are necessary for the voters to broadcast their computation asynchronously, while at the same time avoiding that the last agent changes their output to corrupt the result. This subroutine has two additional parameters as input Σ and Γ that in turn define the security parameter S. Σ indicates the number of times the protocol needs to be repeated for each ordering, while Γ specifies the number of coins that each voter has to toss to assign the value p_k, which will be 1 only if the result is 'all heads'. As a consequence, the security parameter $S = (1-2^{-\Gamma})^{\Sigma}$ can take any value in the open interval $(0, 1)$ and represents the probability of the protocol giving the incorrect answer.

The following lemmas are taken from Ref. [131].

Lemma 1. *(Reliability) No one can abort the LogicalOr protocol.*

If someone refuses to broadcast, it is assumed that the output of the protocol is 1.

Lemma 2. *(Correctness) If all the inputs are $x_i = 0$, the LogicalOr protocol outputs $y = 0$ with probability 1. If M agents input 1 in the protocol then we will have $y = 1$ with probability at least $P = 1 - S^M$.*

Lemma 3. *(Privacy) The most an adversary can know in the protocol is the logical Or of the other participants.*

These properties are also guaranteed in the following subroutines that are based on LogicalOr.

Protocol RandomBit

Input: Security parameter S to be used in LogicalOR.
Output: The voting agent anonymously announces a random bit uniformly at random.
Resources: Classical communication and random numbers.

Description: Perform the LogicalOr with security parameter S where the voting agent inputs a random bit according to D and the other agents input 0.

Protocol RandomAgent

Input: Security parameter S to be used in RandomBit.
Output: The voting agent anonymously chooses an agent uniformly at random.
Resources: Classical communication and random numbers.

Description: Repeat RandomBit $\log_2 N$ times.

UniqueIndex is used to anonymously distribute a secret random index to each voter. Note that here it is a classical protocol while in [135] it was necessary to use another entangled quantum state to achieve the same goal. This protocol is polynomial in the number of the operations and completely guarantees the privacy. In order to achieve this functionality we proceed in the following way. The protocol is composed of N rounds.In the first step of each round all agents perform the LogicalOr protocol with inputs 0 if they already have an index, otherwise they will input 1 with probability $1/t$ and 0 with probability $1 - 1/t$, where t is the number of agents that do not have an index yet. If there is any agent with input 1 the output of LogicalOr will be $y = 1$. Each agent with input $x_k = 1$ can verify at this point if there is a collision by tracking the parity of all other inputs w_k. If for any of the Σ repetitions in every ordering $w_k \neq 0$, then they know that there is someone else with input 1. At the end of each LogicalOr everybody performs another LogicalOr protocol that acts as an anonymous notification, in which they input 0, unless no collision was detected. Everyone then repeats the first LogicalOr; this time those who previously had input 0 will stay the same, while the others toss a coin and decide their inputs accordingly. This is repeated until there is only one agent j with input 1, while $w_j = 0$ throughout all repetitions of LogicalOr. When the notification LogicalOr is performed, agent j will be the only with input 1, announcing that the index ω_j was assigned and the round is over. Then this is repeated from the first step, the agents who already have an index always set their input to 0 and the protocol terminates when the last notification LogicalOr output is 0, announcing that all indices have been assigned. If at any time $y = 0$, then there is no one with input 1, and the protocol should be repeated from the beginning of the last LogicalOr, with the same inputs until someone gets an index.

Protocol UniqueIndex

Input: Security parameter S to be used in LogicalOR, N random boolean variables x_i.
Output: Each agent k has a secret unique index ω_k.
Resources: Classical communication and random numbers.

Description:

1: Beginning of round $R = 1$.
2: Perform LogicalOr with inputs $x_k = 0$ if they already have an index, otherwise they input $x_k = 0$ with probability $1 - 1/(N - R)$ and $x_k = 1$ with probability $1/(N - R)$.
3: If $y = 0$ repeat from step 2.
4: If an agent k has a bit $x_k = 1$ and $w_k = 0$ they know they are the only one and has been assigned the secret index corresponding to the round $\omega_k = R$, otherwise there is a collision.
5: [notification] Everybody performs a LogicalOr with input 0, unless they received the index in this round, in which case they input 1.
6: If the output of LogicalOr is 0, no index was assigned and we repeat from step 2.
7: If the output of LogicalOr is 1, the index was assigned and we repeat from step 2 with $R+ = 1$.
8: Repeat from step 2 until all indices have been assigned.

Where w_k (not to be confused with ω_k) was defined in the LogicalOr protocol and represents the parity of all the inputs except the one with index k.

Verification is the same protocol as in [132], where a test is performed by all the agents and the quantum state will pass it with a probability that grows with the fidelity between the input state and an ideal GHZ state.

Protocol Verification

Input: A quantum state distributed and shared by N parties, security parameter S for RandomAgent.
Output: If the state is a GHZ state $\rightarrow$ YES.
Resources: Classical communication, random numbers, quantum state source, quantum channels.

Description:

1: Everyone executes RandomAgent to choose uniformly at random one of the voters to be the *verifier*.
2: The verifier generates random angles $\theta_j \in [0, \pi)$ for all agents including themselves, such that the sum is a multiple of π. The angles are then sent out to all the agents.
3: Agent j measures in the basis $\left[|+_{\theta_j}\rangle, |-_{\theta_j}\rangle\right] = \left[\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta_j}|1\rangle\right), \frac{1}{\sqrt{2}}\left(|0\rangle - e^{i\theta_j}|1\rangle\right)\right]$ and publicly broadcasts the result $Y_j = \{0, 1\}$.
4: The state passes the verification test when the following condition is satisfied:

if the sum of the randomly chosen angles is an even multiple of π, there must be an even number of 1 outcomes for Y_j, and if the sum is an odd multiple of π, there must be an odd number of 1 outcomes for $Y_j : \bigoplus_j Y_j = \frac{1}{\pi}\sum_i \theta_i$.

With Voting a voter can express their preferred candidate. The state that will be used for voting is equivalent to a GHZ state up to a local Hadamard transform applied by each agent to their own particle. Once the GHZ state is measured in the Hadamard basis, the outcomes will always sum up to $0 \mod 2$. This can be seen by direct application of the N-dimensional Hadamard $\mathcal{H}^{\otimes^N} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes ... \otimes \mathcal{H}_N$, where each of the transforms $\mathcal{H}_j$ acting on the 2-dimensional Hilbert space of the j-th voter's particle is expressed in the computational basis as

$$\mathcal{H}_j = \frac{1}{\sqrt{2}}\left[\left(|0\rangle_j + |1\rangle_j\right)\langle 0|_j + \left(|0\rangle_j - |1\rangle_j\right)\langle 1|_j\right].$$

It is easy to show that if we apply the Hadamard to the GHZ state we obtain:

$$\begin{aligned}\mathcal{H}^{\otimes^N}|GHZ\rangle &= 2^{-N}\left[\bigotimes_{i=1}^{N}\left(|0\rangle_i + |1\rangle_i\right) + \bigotimes_{i=1}^{N}\left(|0\rangle_i - |1\rangle_i\right)\right] = \\ &= 2^{-N}\left[\sum_{\{k_i=0,1\}_{i=1}^N} |k_i\rangle^{\otimes_i^N} + \sum_{\{k_i=0,1\}_{i=1}^N} (-1)^{\sum k_i}|k_i\rangle^{\otimes_i^N}\right] = \\ &= 2^{-N/2}\sum_{\sum k_i = 0_{\mathrm{mod}2}} |k_i\rangle^{\otimes_i^N}.\end{aligned}$$

So, by measuring each particle in the Hadamard basis, we are assured that the sum of the outcomes will be 0 modulo 2.

Protocol Voting

Input: Voting agent preference v_k.
Output: All agents get one row of the bulletin board.
Resources: Classical communication, GHZ source, quantum channels.

Description:

1: Each agent measures the state they received in the Hadamard basis and records the outcome.
2: The outcomes of the measurement of each voter k is d_k. Then we know that $\sum_k d_k = 0 \mod 2$.
3: The voting agent performs an XOR between the outcome d_k and their vote v_k: $d_k \to B_k = d_k \oplus v_k$. However, this alone will still appear as a random string.
4: Every agent publicly broadcasts d_k which gives one line $\mathbf{b_k}$ of the bulletin board

$\mathbf{B} = \{\mathbf{b_k}\}$.

4.2.4 Quantum e-voting pseudo code

The pseudo code for the entire protocol is given below.

Protocol Quantum e-voting

Input: N agent votes $\mathbf{V} = \{v_k\}_{k\in[N]}$, security parameter S used in Phase 3, ϵ: accepted distance from the perfect GHZ, δ: threshold for verification, η: probability of failure of verification.
Output: The candidate with majority votes or Abort.
Resources: Classical communication, random numbers, N-qubit GHZ source, quantum channels.

Description:

1. Phase 1 [getting unique secret indices]:
   - The agents perform UniqueIndex until each agent receives a secret unique random index ω_k.
2. Phase 2 [casting votes]:
   For $\ell = 1$ to N [voting round ℓ]:
   (a) The voting agent is the agent k with $\omega_k = \ell$.
   (b) Repeat
      (i) The source distributes to each of the N agents one qubit of the GHZ state.
      (ii) All agents $j \in [N]$ set $\text{rejections}_j = \text{trials}_j = 0$;
      (iii) The voting agent tosses $\log_2 \left[\frac{16N\epsilon^2}{(\epsilon^2-4\delta)^2} \ln\left(\frac{1}{\eta}\right)\right]$ coins;
      (iv) The agents perform LogicalOr, where output 1 indicates Verification and output 0 indicates Voting, and where everyone except the voting agent inputs 0; if the coin toss is 'all heads' the voting agent also inputs 0, otherwise the voting agent inputs 1;
      (v) If Verification is chosen, the agents perform RandomAgent and the voting agent picks anonymously an agent $j \in [N]$ to be the verifier. Agent j increment trials_j by 1 and if Verification outputs reject: agent j increment rejections_j by 1.
   until Voting is announced.
   (c) If for any $j \in [N]$ $\delta_j = \frac{\text{rejections}_j}{\text{trials}_j} > \delta$, the protocol Aborts.
   (d) Perform Voting. The outcome is one row of the bulletin board $\mathbf{B}$.
3. Phase 3 [verification of results]:

- All agents perform LogicalOr with security parameter S, and with input 1 if their vote is not the same as the vote in the tally $\mathbf{T}$ for the round in which they were the voting agent, else with input 0.
- If LogicalOr outputs 1, Abort the protocol, else the candidate with the majority votes according to the tally wins the elections.

4.3 E-voting protocol Analysis

We now analyze our quantum e-voting scheme and show that it possesses a number of desired properties even in the non-ideal case where the quantum source is imperfect or can be manipulated by colluding adversaries.

If the quantum states being used in the protocol are perfect GHZ states and the agents behave honestly, all the operations are anonymous and hence the e-voting scheme is perfectly correct and private. In any realistic scenario, however, the state used will have some imperfections, due to the source itself, the photon distribution, storage and measurement that may result in some errors in the tally, for example the sum of the outcomes of a round will not be 0 mod 2. We account for all the possible imperfections assuming that the fidelity between the state used in the protocol $|\psi\rangle$ and the perfect GHZ state $|GHZ\rangle$ is $F(|\psi\rangle, |GHZ\rangle) = \sqrt{1-\epsilon^2}$ for some $\epsilon > 0$. Note that the state produced by the source could be a mixed state, but as discussed in [122], for the security it suffices to upper bound the cheating probability of any pure state, since this would also bound the cheating probability for any mixed state. For this reason we analyze below the case where the state produced by the source is a pure state.

Since the source or the state itself can further be intercepted and modified by an adversary in order to gain advantage over the privacy of the honest voters, we need to implement a mechanism that allows anyone to check the legitimacy of the state being used with high probability. An efficient multipartite entangled state verification protocol was devised in [132], [133] and applied to an anonymous transmission protocol in [122]. This is the Verification subroutine used in the protocol (see 4.2.3 for details). While in the ideal case we would abort the protocol as soon as the test failed once, in a realistic implementation we need to keep track of the number of failures and at the end check if the failures are too many with respect to what was expected, which would imply that there was a malicious manipulation of the source. This is what is performed in Phase 2 of the protocol.

In [132], the authors prove that the probability of a state $|\psi\rangle$, whose trace distance with the GHZ state is $\mathcal{D}(|\psi\rangle, |GHZ\rangle) = \epsilon$, to pass the verification test when an honest verifier is in the presence of dishonest agents who can perform local unitaries and communicate with each other is $P(|\psi\rangle) \leq 1 - \epsilon^2/4$. The main idea of our practical e-voting protocol is that the states produced by the source and potentially manipulated by the dishonest agents will be verified a large number of times in order to ensure that the state that will be eventually

used for the voting part will be very close to the GHZ state. Then we will prove that states close to the GHZ state offer almost perfect privacy for the e-voting scheme.

We start by proving the following theorem that in high level states that with high probability if the verification procedure succeeds, then the state used for the e-voting part must be close to the GHZ state:

Theorem 1. *Let C_ϵ be the event that the protocol does not abort and the state used for Voting is such that $F(|\psi\rangle, |GHZ\rangle) \leq \sqrt{1-\epsilon^2}$, for some $\epsilon > 0$. Then,*

$$P(C_\epsilon) \leq e^{-\frac{2^M(\epsilon^2-4\delta)^2}{16N\epsilon^2}}, \tag{4.1}$$

where δ is the threshold for the ratio of rejections over trials above which the protocol is aborted, M is the number of coins the agent has to toss to choose between Verification and Voting and N is the number of agents.

The proof of Theorem 1 is provided in section 4.3.8, at the end of the chapter. Note that the honest voters do not know how many corrupt agents there are and that if a dishonest agent is the verifier, the test always passes. We can make the probability of using a state that is ϵ-far in trace distance from the ideal one arbitrarily small by increasing the number of repetitions, as long as we have $\delta = (1-\alpha)\epsilon^2/4$ for an $\alpha \in (0,1)$; more precisely, by taking $M = \log_2 \left[\frac{16N}{\alpha^2\epsilon^2} \ln\left(\frac{1}{\eta}\right)\right]$ we can make $P(C_\epsilon) \leq \eta$ for any small parameter $\eta > 0$. Moreover, we see that for the same choices of δ and M, we also have the property that the protocol accepts with high probability states that are a bit closer to the perfect GHZ state, which is important so that the protocol will not always abort. Indeed, it is easy to see with Chernoff bounds that states that are $\epsilon\sqrt{\frac{1-\alpha}{1+\alpha}}$-away from the GHZ state have probability almost 1 to pass the verification test.

Hence, we can assume for the remaining of the discussion that with high probability $F(|\psi\rangle, |GHZ\rangle) \geq \sqrt{1-\epsilon^2}$. In this case, we prove that for each round of the protocol, the identity of the voting agent remains almost secret:

Theorem 2. *At any round $\ell \in [N]$ with voting agent k (who has unique index $\omega_k = \ell$), if the agents use a state $|\psi\rangle$ such that $F(|\psi\rangle, |GHZ\rangle) \geq \sqrt{1-\epsilon^2}$ to perform Voting, then for the optimal strategy that any subset of malicious agents $\mathcal{D}$ can use to guess the identity of the voting agent k correctly, we have*

$$\forall j \in W_H,\ \Pr[\mathcal{D} \text{ guess } j] = \begin{cases} \frac{1}{H} + \tilde{\epsilon} & \text{for } j = k \\ \frac{1-\tilde{\epsilon}}{H} & \text{for } j \neq k, \end{cases} \tag{4.2}$$

where $\tilde{\epsilon} = \sqrt{\epsilon^2 + \epsilon^4}$, W_H is the set and H the number of honest agents.

This theorem is simply based on Theorem 2 of [122]. The difference is that, instead of a sender who anonymously chooses between Verification and Anonymous Transmission,

we have a voting agent who anonymously chooses between Verification and Voting. The probabilities for the other agents come from the fact that all the agents that are not voting perform exactly the same transformation on the state, so it is impossible for the dishonest parties to distinguish between them, hence the probability of guessing their identity is the same. The proof of Theorem 2 is provided in 4.3.9.

The last property we prove shows that if the agents are all honest and use a state close to the GHZ state for voting, then the probability there is an error in the tally is small:

Theorem 3. *If at round ℓ the agents are honest and use a state $|\psi\rangle$ such that $F(|\psi\rangle, |GHZ\rangle) \geq \sqrt{1-\epsilon^2}$ to perform Voting, then the probability that there is an error in the tally in the ℓ-th round is upper bounded by ϵ,*

$$P_\ell^{er} \leq \epsilon. \tag{4.3}$$

The proof of Theorem 3 is provided in 4.3.10. The above three theorems allow us to formalize and prove a number of important properties for our e-voting scheme, namely correctness, privacy, authentication, no double voting, verifiability, and receipt freeness. Note that in [136], the authors show that there exist sets of properties that are incompatible in any voting system, meaning that not all of them can be fulfilled simultaneously by any protocol. However, one can remove the incompatibility by defining approximate versions for the properties or making computational assumptions about the voters' behaviour. Indeed, here, given that we want to allow for imperfect sources of quantum states in order to have a practical protocol that is robust to some level of noise, we define approximate versions of some of these properties for our e-voting protocol, as we explain in the following.

4.3.1 $(\sigma_H, \sigma_D, \gamma)$-Correctness

The correctness of a protocol implies that when no adversary interferes, the election should be carried out correctly, and that in the presence of adversaries, if the election tally is far from the real votes, then the election is rejected with high probability. These two requirements can be expressed as two properties of the voting scheme:

- *σ_H-completeness:* if all agents are honest, the election result is accepted with probability more than σ_H,

$$\Pr[\text{election accepted}] \geq \sigma_H. \tag{4.4}$$

- *(σ_D, γ)-soundness:* the probability that the election result is accepted, given that the set of the votes $\mathbf{E}$ computed from the bulletin board $\mathbf{B}$ resulting from the election is more than γ-away from the real votes $\mathbf{V}$, is smaller that σ_D,

$$\Pr[\text{election accepted} \mid \tfrac{1}{N}||\mathbf{V} - \mathbf{E}||_1 \geq \gamma] \leq \sigma_D. \tag{4.5}$$

The use of an imperfect state may result in some errors in the final tally (see Theorem 3), and this is why we define a notion of approximate correctness. In particular, the probability that

the e-voting is validated is the probability that the LogicalOr subroutine in Phase 3 outputs 0 despite some voters announcing a wrong entry in the tally. Note that Theorem 3 ensures that at each round we can have an error with probability at most ϵ, while it can also be proven (see Lemma 2 in 4.2.3) that during LogicalOr, if j agents input 1 (which corresponds to their vote being tallied wrongly) the probability that LogicalOr outputs 0 is S^j, for the parameter S defined by the e-voting protocol. Summing over all the combinations we get:

$$\Pr[\text{election accepted}] = \sum_{j=0}^{N} \Pr[j \text{ inputs } 1] \Pr[\text{ LogicalOr outputs } 0 | j \text{ inputs } 1] = \sum_{j=0}^{N} \binom{N}{j} \epsilon^j (1-\epsilon)^{N-j} S^j = [1-\epsilon(1-S)]^N .$$

We can then define the σ_H parameter for our e-voting protocol as

$$\sigma_H = [1-\epsilon(1-S)]^N , \tag{4.6}$$

and we can see that by choosing $S = 1 - \chi/(\epsilon N)$ for some small constant χ we can make σ_H close to 1.

Consider now the events $A = \{\text{The protocol produced more than } N\gamma \text{ errors}\}$ for $0 \leq \gamma \leq 1$ and $B = \{\text{The elections are validated}\}$. Then we have $P(B|A) \leq S^{N\gamma}$ and we can define the σ_D parameter of our protocol as

$$\sigma_D = S^{N\gamma}. \tag{4.7}$$

If we assume that γ is a small fraction λ greater than the expected number of errors, namely $\gamma = (1+\lambda)[\epsilon(1-\eta)+\eta]$, we can make σ_D close to 0.

In conclusion, our e-voting protocol with inputs $S, \epsilon, \delta, \eta, N$ and for a small constant $\lambda > 0$, is $([1-\epsilon(1-S)]^N , S^{N(1+\lambda)[\epsilon(1-\eta)+\eta]}, (1+\lambda)[\epsilon(1-\eta)+\eta])$-correct, where the first parameter tends to 1 and the second to 0 for an appropriate parameter S.

4.3.2 ζ-Privacy

The privacy of the election scheme implies that each vote must remain secret with high probability. More precisely, with high probability, for any voter k, the probability that any subset of malicious parties $\mathcal{D}$ that deviates from the honest protocol can guess the vote v_k of the voter is at most ζ more than in the case they just have access to the bulletin board and to their own votes. In other words,

$$\forall k, \quad \Pr[v_k|\mathcal{D}] - \Pr[v_k|\mathbf{B}, v_j \in \mathbf{V}_D] \leq \zeta. \tag{4.8}$$

Theorems 1 and 2 ensure that by repeating the Verification test a significant number of times at each voting round, the voting only happens with a shared state that is close to a GHZ state, which guarantees almost perfect anonymity. In practice, by having each agent record the frequency of failures of the test, they can deduce the practical parameter $\delta_k = \frac{\text{rejections}_k}{\text{trials}_k}$ and in case this is above the predetermined threshold δ, which is an input of the protocol, the protocol is aborted. Otherwise, the rounds proceed normally and all agents vote. Note that δ is linked to the expected fidelity of the state produced by the GHZ source, as explained earlier.

We have also seen that by taking the appropriate parameters, we can have that with probability at least $(1-\eta)$, Eq. (4.2) from Theorem 2 holds. This is the case the event C_ϵ (see Theorem 1) is false. In case C_ϵ is true, which happens with probability at most η, we can assume that the anonymity is totally violated.

One needs to be careful here because the definition of privacy is not the same as the one of anonymity. More specifically, anonymity ensures that the honest voters' secret indices, or the round in which they voted, remain secret, whereas privacy implies that their vote remains a secret. Of course, the violation of anonymity implies the disclosure of privacy, however a malicious agent can gather information about someone's vote also by looking at the distribution of the other votes and the anonymity of the other voters. Taking Eq. (4.2) into account and considering that among the H honest voters, H_0 voted for candidate '0' and the others H_1 voted for candidate '1', such that $H = H_0 + H_1$, we have that the probability of a subset of dishonest agents guessing correctly the vote of agent k that is '0' (same for '1') is the probability that they can guess that agent k is part of the subset H_0, in other words that agent k voted in one of the rounds where the vote was cast as '0'. Theorem 2 tells us how much the dishonest agents can guess if a particular agent was the voter in a particular round, depending on whether the agent was actually the voter or not. Hence, assuming that the event C_ϵ does not hold for any round, we have

$$\begin{aligned}\Pr[\mathcal{D} \text{ guesses } v_k = 0] =& \tfrac{1}{H} + \tilde{\epsilon} + (H_0 - 1)\tfrac{1-\tilde{\epsilon}}{H} = \\ &= \tfrac{H_0}{H} + \tfrac{H+1-H_0}{H}\tilde{\epsilon} \leq P[v_k = 0|\mathbf{B}] + \tilde{\epsilon},\end{aligned}$$

where we used the fact that $\frac{H_0}{H}$ is the distribution of the votes given by the public bulletin board and that $H_0 \geq 1$. Given that the event C_ϵ happens for each round with probability at most η we have that for the final privacy,

$$\Pr[\mathcal{D} \text{ guesses } v_k = 0] \leq \tag{4.9}$$

$$\leq P[v_k = 0|\mathbf{B}] + (1-\eta)^N\tilde{\epsilon} + (1-(1-\eta)^N), \tag{4.10}$$

which proves Eq. (4.8) in the non-ideal case.

In conclusion, our e-voting protocol with inputs $S, \epsilon, \delta, \eta, N$ is ζ-private with ζ-private with $\zeta = (1-\eta)^N\epsilon\sqrt{1+\epsilon^2} + (1-(1-\eta)^N)$, which tends to 0 for small enough η and ϵ.

4.3.3 Authentication

Only eligible voters are allowed to vote. Our e-voting protocol as described here does not provide authentication, which should be taken care by the physical implementation of the protocol. For electronic voting machines authentication might be provided by an official ID, whereas for voting directly through the internet authentication would require some digital signature scheme.

4.3.4 Double voting

Each voter can vote at most once. Double voting is taken care of easily if the number of voters is known in advance, which in fact is necessary in our scheme in order to prepare the shared quantum state. If N agents declare they want to vote, we will have an $N \times N$ bulletin board, each row of which corresponds to one vote. A null vote can be treated as an additional candidate and will be discussed below. A dishonest voter might try to intercept all the transcripts, modify the bulletin board by adding a column and a row with another vote without changing the sum of each row, but this would result in a evident $(N+1) \times (N+1)$ matrix that will be rejected by the honest voters. At the same time, if a dishonest voter keeps the same number of rows and columns but tries to vote at a round where they are not supposed to be voting, then either the vote will not change or if the vote in the ballot changes from the intended vote of the honest voting agent, then this will be captured by the LogicalOr subroutine protocol in Phase 3 of the protocol.

4.3.5 Verifiability

Each voter can verify that their vote has been counted correctly. More precisely, a protocol is called verifiable if there exists a function g specified by the protocol, such that every voter can apply the function g on the bulletin board and a private witness w_k (the witness corresponds to the vote and the secret voting index of the voter) and get back 1 if and only if their vote was counted correctly. In other words,

$$\exists g \text{ s.t. } \forall k \; \exists w_k \text{ s.t. } \forall \mathbf{B}: \quad g(\mathbf{B}, w_k) = \quad 1 \iff v_k \text{ was counted in the tally} \tag{4.11}$$

The verifiability, thus, demands the existence of a function that, given the bulletin board $\mathbf{B}$ and the voter's secret index ω_k returns 1 if v_k was counted in the tally and 0 otherwise.

The verifiability is inherent in the protocol, as the tally is performed by the voters themselves. The bulletin board produced as an output of the protocol is public and can always be checked by everyone, however it appears as a random set of votes. Each row j corresponds to the vote v_k of agent k whose secret unique index is $\omega_k = j$, and thus each agent can easily verify their own vote and only that one. If the vote in the bulletin board differs from the actual intended vote v_k, as a consequence of a dishonest behaviour or an imperfection in the quantum state, the agent can reject the result through the LogicalOr subroutine in Phase 3.

4.3.6 Receipt freeness

A voter cannot prove how they voted, in order to avoid vote selling. A receipt is a witness w_k defined as:

$$\exists g \text{ s.t. } \forall k \ \exists v_k \ \exists! w_k \text{ s.t. } \forall \mathbf{B} \ \ g(\mathbf{B}, k, v_k, w_k) = 1 \tag{4.12}$$

If there is no receipt, then the protocol is called receipt-free. As long as their index stays secret all the agents can always deterministically verify their votes, without getting their privacy violated, and without producing any receipt of their vote which could be used for vote selling.

4.3.7 Additional candidates

So far we assumed that there were only two candidates, '0' or '1', which is suitable for referendum type of elections.

If there are K candidates, each candidate identifier will have $\log_2 K$ digits and each election can provide the preference for at most 1 digit of each voter. If we repeat the whole protocol $\log_2 K$ times, keeping the same secret index for each voter at all times, we end up with a greater election votes vector $\underline{\mathbf{E}} = \mathbf{E}^{(1)}\mathbf{E}^{(2)}...\mathbf{E}^{(\log_2 K)}$ formed by the election vote vector of each election by summing the row of the corresponding bulletin board $\mathbf{E}^{(i)} = \sum_k \mathbf{B}^{(i)}$. So the sub-election 1 will result in a vector $\mathbf{E}^{(1)} = e^{(1)}_{\omega_1} e^{(1)}_{\omega_2} ... e^{(1)}_{\omega_N}$, where $e^{(1)}_{\omega_k}$ is the value of the first digit of the preference of voter k, with secret index ω_k, and so on for all the other sub-elections. If we want to perform an election with 3 candidates and 7 voters, allowing also the possibility of a null vote, which will be candidate $(0, 0)$, we need to carry out 2 sub-elections, and result in the following table:

$$\underline{\mathbf{E}} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \\ 0 & 0 \\ 0 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix},$$

where two agents voted for candidate 3, candidates 1 and 2 received one vote each and the rest of the voters decided not to express a preference.

The only properties that are affected by the additional candidates are correctness and privacy. This is because they are the only ones that are probabilistic and that actually depend on the use of an imperfect state in the different rounds. Authentication, double voting, verifiability and receipt freeness will thus remain unchanged even in the scenario with many candidates. In particular, the correctness is affected because repeating the elections multiple times increases the probability of having an error at some point. We can assume that the agents perform the LogicalOr protocol with security parameter S to notify an error only

at the end of all the repetitions of the elections. By Theorem 3, the probability that for any agent at least one bit of the final tally will be incorrect is $\epsilon^* = 1-(1-\epsilon)^{\log_2 K}$ and thus the probability that the election is accepted after multiple rounds will be

$$\Pr[\text{election accepted}] = [1-\epsilon^*(1-S)]^N = \sigma_H^*. \tag{4.13}$$

The soundness, on the other hand, is not affected. In fact, if any voter notices more than one incorrect bit in their vote it will count as a single error.

The privacy of the protocol is affected as well. From one point of view, since the number of bits that the dishonest agents need to guess is larger, the probability of violating the anonymity, and thus the privacy, is actually smaller. If, however, we want that each individual bit of the vote remains private, the privacy is decreased by the fact of having multiple rounds of elections. In this case, let us consider the probability of the event X that at some round the malicious agent guesses the preference of the voter k and let us assume that this probability is upper bounded as $P(X) \leq \zeta$. If we repeat the elections $\log_2 K$ times, the probability that event X is true at least once will thus be at most $\zeta^* = 1-(1-\zeta)^{\log_2 K}$. Hence, when dealing with multiple candidates our e-voting protocol with inputs $S, \epsilon, \delta, \eta, N$ is ζ^*-private with $\zeta^* = 1-(1-(1-\eta)^N\epsilon + [1-(1-\eta)^N)]^{\log_2 K}$, which tends to 0 for small enough η and ϵ.

Example.– Let us consider a 4-photons GHZ source that has been calibrated to produce states with fidelity ~ 0.85, which can be produced with current quantum photonics. This corresponds to an expected fraction of rejections $\delta \sim 0.05$. If we now set $\epsilon = 0.6$, it implies that we will never accept states with fidelity lower than ~ 0.8. Although we would like ϵ to be very small, there is not much more we can do with currently available GHZ sources. In any case, this is not a big deal for the correctness of the protocol. If we fix the non aborting probability $\eta = 0.001$, eq. 4.1 implies that M=12, and thus we will need around 4000 GHZ states to accomplish each voting. Since the production rate of currently available GHZ source is $\sim 8KHz$, the protocol can be carried out in just a few seconds. The actual problem is the privacy, which would be violated with a probability of $\zeta \sim 0.7$. A way to tackle this issue is to amplify the privacy by repeating Q rounds of the *e-voting* and encoding the vote intention of each voter in the parity of the Q outcomes. In this way, each round of the election would encode no information and the malicious agents would require to succeed in each of the rounds, reducing the total probability of violating the privacy to $\tilde{\zeta} = \zeta^Q$. If $Q = 15$, with the previous parameters this would reduce the privacy parameter to $\tilde{\zeta} \sim 0.005$, to the price of repeating more rounds of the elections. Notice that the privacy amplification would have the consequence of increasing the potential number of errors in the outcome of the election. This and other details of the protocol will be tackled in the experimental implementation.

4.3.8 Proof of Theorem 1

Here we prove the soundness of the Verification protocol. For simplicity of the proof, recall that we denote the ideal state by $|\Phi_0^n\rangle$, which can be obtained from the GHZ state by applying a Hadamard and a phase shift $\sqrt{Z}$ to each qubit.

Theorem 1. *Let C_ϵ be the event that the protocol does not abort and the state used for Voting is such that $F(|\psi\rangle, |GHZ\rangle) \leq \sqrt{1-\epsilon^2}$, for some $\epsilon > 0$. Then,*

$$P(C_\epsilon) \leq e^{-\frac{2^M(\epsilon^2-4\delta)^2}{16N\epsilon^2}},$$

where δ is the threshold for the ratio of rejections over trials above which the protocol is aborted, M is the number of coins the agent has to toss to choose between Verification and Voting and N is the number of agents.

Proof. During the protocol, each voter can trust only themselves as they do not know who could be a colluding agent. Thus, although at each round of Verification a verifier is chosen at random and could be an honest voter, we will perform the following analysis assuming we are in the worst case scenario in which the voting agent is the only honest voter and cannot trust anybody else. Thus the average number of rounds of the Verification will be $\langle D \rangle = 2^M/N$. In addition, if we take M large enough, we can make the probability of having at least $D = 2^M/2N$ rounds of Verification, arbitrarily close to 1. Thus, in the following we will assume that $D \geq 2^M/2N$. In any practical implementation of the protocol, however, the other honest agents will also assist the verification and if they count a ratio of rejections larger than δ they can abort the elections, increasing the soundness of the protocol.

Although we allow the malicious source to create any state in any round and even entangle the states between rounds, the optimal cheating strategy, which maximizes the probability of the event C_ϵ, is to create in each round some pure state $|\Psi\rangle$ such that $F'(|\Psi\rangle) = \sqrt{1-\epsilon^2}$, as proven in [132]. In high level, one can first see that an entangled strategy does not help, as it can be replaced by a strategy sending unentangled states as follows. Given some entangled state, for a given round, the probability of passing the test and the fidelity of the state depend only on the reduced state, conditioned on passing previous rounds. The same effect is achieved by sending these mixed reduced states corresponding to each round, without any entanglement.

Next, one sees that by providing a mixed state, the source does not gain any advantage, as a mixed state is a probabilistic mixture of pure states, and the overall cheating probability of this mixed strategy is just a weighted combination of the cheating probabilities of each of the pure states. Then, obviously this mixed strategy is worse than the strategy that always

sends the pure state that has the maximum cheating probability of all states in the mixture. Hence, one can continue the proof by only considering strategies with pure states.

Moreover, since the adversary is just trying to maximize the probability the state $|\Psi\rangle$ used for voting has $F'(|\Psi\rangle) = \sqrt{1-\epsilon^2}$, it is clear that there is no need to send any state with even smaller $F'(|\Psi\rangle)$, since then the probability of failing the test (and therefore the protocol aborting) would just increase. Last, if in any round the source created a state with higher $F'(|\Psi\rangle)$, then this certainly does not contribute to the event C_ϵ, and in fact it may also cause the protocol to abort. Thus, to upper-bound the probability of event C_ϵ with respect to the best attack a malicious source can perform, we only need to consider the case where in each round the malicious source creates some state $|\Psi\rangle$ such that $F'(|\Psi\rangle) = \sqrt{1-\epsilon^2}$.

The protocol takes as input a threshold parameter δ, such that if during their round the voting agent rejects the state more than a δ fraction, then they abort the elections because the source is corrupted. In the limit, the ratio of rejections will tend to the probability of a single state ϵ-far in trace distance from a GHZ to fail the Verification test in the presence of dishonest adversaries, which is [132]:

$$P(\epsilon) \geq \frac{\epsilon^2}{4}. \tag{4.14}$$

Thus, we can use a Chernoff inequality to bound the probability that in D rounds of Verification with a state ϵ-far the ratio of rejections of the voting agent δ_k is smaller than δ, in which case the event C_ϵ is true. In particular, given that the expected number of rejections is at least $D\epsilon^2/4$, the Chernoff bound gives the following inequality

$$P(C_\epsilon) = P(\delta_k \leq \delta) \leq e^{-\frac{D(\epsilon^2-4\delta)^2}{8\epsilon^2}}. \tag{4.15}$$

If we substitute $D \geq 2^{M-1}/N$, we obtain the expression of Theorem 1.

□

4.3.9 Proof of Theorem 2

Next, we prove the anonymity of the protocol as in [122]. Once again, recall that we denote the ideal state by $|\Phi_0^n\rangle$, which can be obtained from the GHZ state by applying a Hadamard and a phase shift $\sqrt{Z}$ to each qubit. The voter's transformation now becomes $\sigma_x\sigma_z$. Further, we also define the state:

$$|\Phi_1^n\rangle = \frac{1}{\sqrt{2^{n-1}}}\Big[\sum_{\Delta(y)=1 \text{ (mod 4)}} |y\rangle - \sum_{\Delta(y)=3 \text{ (mod 4)}} |y\rangle\Big], \tag{4.16}$$

and note that $\sigma_x\sigma_z \left|\Phi_0^n\right\rangle = \left|\Phi_1^n\right\rangle, \sigma_x\sigma_z \left|\Phi_1^n\right\rangle = -\left|\Phi_0^n\right\rangle$.

We consider two cases here: first, when all the agents are honest (Lemma 4), and second, when we have malicious agents who could apply some operation on their part of the state (Lemma 5).

Lemma 4. *If all the agents are honest, and they share a state $\left|\Psi\right\rangle$ such that $F(\left|\Psi\right\rangle, \left|\Phi_0^n\right\rangle) = \sqrt{1-\epsilon^2}$, then for every honest agent i, j who could be the voter, we have that $F(\left|\Psi_i\right\rangle, \left|\Psi_j\right\rangle) \geq 1-\epsilon^2$, where $\left|\Psi_i\right\rangle$ is the state after agent i has applied the voter's transformation.*

Proof. If we have $F(\left|\Psi\right\rangle, \left|\Phi_0^n\right\rangle) = \left|\left\langle\Psi\right|\left|\Phi_0^n\right\rangle\right|^2 = \sqrt{1-\epsilon^2}$, then similarly to [132] we can write the state shared by all the agents as:

$$\left|\Psi\right\rangle = (1-\epsilon^2)^{1/4}\left|\Phi_0^n\right\rangle + \epsilon_1\left|\Phi_1^n\right\rangle + \sum_{i=2}^{2^n-1}\epsilon_i\left|\Phi_i^n\right\rangle, \tag{4.17}$$

where $\sum_{i=1}^{2^n-1}\epsilon_i^2 = 1-\sqrt{1-\epsilon^2}$. If agent i is the voter, then they apply $\sigma_x\sigma_z$, and the state becomes:

$$\left|\Psi_i\right\rangle = (1-\epsilon^2)^{1/4}\left|\Phi_1^n\right\rangle - \epsilon_1\left|\Phi_0^n\right\rangle + \sum_{i=2}^{2^n-1}\epsilon_i'\left|\Phi_i^n\right\rangle. \tag{4.18}$$

Instead, if agent j is the voter and they apply $\sigma_x\sigma_z$, the state becomes:

$$\left|\Psi_j\right\rangle = (1-\epsilon^2)^{1/4}\left|\Phi_1^n\right\rangle - \epsilon_1\left|\Phi_0^n\right\rangle + \sum_{i=2}^{2^n-1}\epsilon_i''\left|\Phi_i^n\right\rangle. \tag{4.19}$$

The fidelity is then given by:

$$\begin{aligned} F(\left|\Psi_i\right\rangle, \left|\Psi_j\right\rangle) &= \left|\left\langle\Psi_i\right|\left|\Psi_j\right\rangle\right|^2 \\ &= |\sqrt{1-\epsilon^2} + \epsilon_1^2 + \sum_{i=2}^{2^n-1}\epsilon_i'\epsilon_i''|^2 \\ &\geq 1-\epsilon^2. \end{aligned} \tag{4.20}$$

□

Lemma 5. *If some of the agents are malicious, and they share a state $\left|\Psi\right\rangle$ such that $F'(\left|\Psi\right\rangle) \geq \sqrt{1-\epsilon^2}$, then for every honest agent i, j who could be the voter, we have that $F(\left|\Psi_i\right\rangle, \left|\Psi_j\right\rangle) \geq 1-\epsilon^2$, where $\left|\Psi_i\right\rangle$ is the state after agent i has applied the voter's transformation.*

Proof. Recall that our fidelity measure is given by $F'(|\Psi\rangle) = \max_U F(U|\Psi\rangle, |\Phi_0^n\rangle)$. Let us now denote by $|\Psi'\rangle = U|\Psi\rangle$ the state after the operation U which maximizes this fidelity has been applied. As in [132], we can write this state in the most general form as:

$$|\Psi'\rangle = |\Phi_0^k\rangle|\psi_0\rangle + |\Phi_1^k\rangle|\psi_1\rangle + |\chi\rangle, \tag{4.21}$$

where note that $|\chi\rangle$ contains both honest and malicious parts, of which the honest part is orthogonal to both $|\Phi_0^k\rangle$ and $|\Phi_1^k\rangle$.

We want to find the closeness of the states $|\Psi_i\rangle, |\Psi_j\rangle$, which are the states after the $\sigma_x\sigma_z$ operation is applied to $|\Psi'\rangle$ by either agent i or j who is the voter. These states are given by:

$$\begin{aligned} |\Psi_i\rangle &= |\Phi_1^k\rangle|\psi_0\rangle - |\Phi_0^k\rangle|\psi_1\rangle + |\chi'\rangle, \\ |\Psi_j\rangle &= |\Phi_1^k\rangle|\psi_0\rangle - |\Phi_0^k\rangle|\psi_1\rangle + |\chi''\rangle. \end{aligned} \tag{4.22}$$

The fidelity is then given by:

$$\begin{aligned} F(|\Psi_i\rangle, |\Psi_j\rangle) &= |\langle\Psi_i||\Psi_j\rangle|^2 \\ &= |\langle\psi_0||\psi_0\rangle + \langle\psi_1||\psi_1\rangle + \langle\chi'||\chi''\rangle|^2. \end{aligned} \tag{4.23}$$

However, although the overall state $|\Psi'\rangle$ is normalized, the malicious agents' part of the state is not. Thus, we need to determine a bound on $\langle\psi_0||\psi_0\rangle$ and $\langle\psi_1||\psi_1\rangle$. We have:

$$F(|\Psi'\rangle, |\Phi_0^n\rangle) = |\langle\Phi_0^n||\Psi'\rangle|^2 \geq \sqrt{1-\epsilon^2}. \tag{4.24}$$

It was shown in [132] that we can write for any k, n:

$$|\Phi_0^n\rangle = \frac{1}{\sqrt{2}}\Big[|\Phi_0^k\rangle|\Phi_0^{n-k}\rangle - |\Phi_1^k\rangle|\Phi_1^{n-k}\rangle\Big], \tag{4.25}$$

and using this, we get:

$$\begin{aligned} &\frac{1}{2}|(\langle\Phi_0^{n-k}||\psi_0\rangle)^2 + (\langle\Phi_1^{n-k}||\psi_1\rangle)^2 \\ &\quad - 2\langle\Phi_0^{n-k}||\psi_0\rangle\langle\Phi_1^{n-k}||\psi_1\rangle| \geq \sqrt{1-\epsilon^2}. \end{aligned} \tag{4.26}$$

Using the triangle inequality, we have:

$$\frac{1}{2}\Big[|\langle\Phi_0^{n-k}||\psi_0\rangle|^2 + |\langle\Phi_1^{n-k}||\psi_1\rangle|^2\Big] \geq \sqrt{1-\epsilon^2}. \tag{4.27}$$

Using the Cauchy-Schwarz inequality, we have:

$$\begin{aligned} \langle\psi_0||\psi_0\rangle + \langle\psi_1||\psi_1\rangle &\geq |\langle\Phi_0^{n-k}||\psi_0\rangle|^2 + |\langle\Phi_1^{n-k}||\psi_1\rangle|^2 \\ &\geq \sqrt{1-\epsilon^2}. \end{aligned} \tag{4.28}$$

Since the overall state $|\Psi'\rangle$ is normalized, we have $\langle\chi'|\,|\chi''\rangle \leq 1 - \sqrt{1-\epsilon^2}$. Thus, we get our expression for fidelity as:

$$\begin{aligned} F(|\Psi_i\rangle, |\Psi_j\rangle) &= |\langle\psi_0|\,|\psi_0\rangle + \langle\psi_1|\,|\psi_1\rangle + \langle\chi'|\,|\chi''\rangle|^2 \\ &= \left(|\langle\psi_0|\,|\psi_0\rangle| - |\langle\psi_1|\,|\psi_1\rangle + \langle\chi'|\,|\chi''\rangle|\right)^2 \\ &\geq 1 - \epsilon^2 - \epsilon^4 = 1 - \tilde{\epsilon}^2, \end{aligned} \tag{4.29}$$

where $\tilde{\epsilon} = \sqrt{\epsilon^2 + \epsilon^4}$. □

We are now ready to prove Theorem 2.

Theorem 2. *At any round $\ell \in [N]$ with voting agent k (who has unique index $\omega_k = \ell$), if the agents use a state $|\psi\rangle$ such that $F(|\psi\rangle, |GHZ\rangle) \geq \sqrt{1-\epsilon^2}$ to perform Voting, then for the optimal strategy that any subset of malicious agents $\mathcal{D}$ can use to guess the identity of the voting agent k correctly, we have*

$$\forall j \in W_H,\ \Pr[\mathcal{D} \text{ guess } j] = \begin{cases} \frac{1}{H} + \tilde{\epsilon} & \text{for } j = k \\ \frac{1-\tilde{\epsilon}}{H} & \text{for } j \neq k, \end{cases} \tag{4.30}$$

where W_H is the set and H the number of honest agents.

Proof. We will now show that if the agents share close to the GHZ state, then the voter remains anonymous. From Theorem 1, we saw that the probability that the state used for voting satisfies $F'(|\Psi\rangle) \leq \sqrt{1-\epsilon^2}$ is given by $\Pr[C_\epsilon] \leq \eta$ for the honest agents, where η depends on the number of runs of the verification protocol. Thus, by doing enough runs, we can make this very small, and so we have that the state used for voting will be close to the GHZ state, as given by $F'(|\Psi\rangle) \geq \sqrt{1-\epsilon^2}$.

From the previous proof, we see that if $F'(|\Psi\rangle) \geq \sqrt{1-\epsilon^2}$, the distance between the states if agent i or j was the voter is $D(|\Psi_i\rangle, |\Psi_j\rangle) \leq \tilde{\epsilon}$. A malicious agent who wishes to guess the identity of the voter would make some sort of measurement to do so. Thus, we wish to find the maximum success probability of a measurement that could distinguish between the H states that are the result of the voter (who can only be an honest agent) applying the $\sigma_x\sigma_z$ transformation.

The success probability of discriminating between H states is given by $\sum_{i=1}^{H} p_i \mathrm{Tr}(\Pi_i\rho_i)$. From Lemma 5, we know that the distance between any two states after the voter's transformation is upper-bounded by $\tilde{\epsilon}$. Thus, if we take $|\alpha\rangle = |\Psi_j\rangle$, then we know that any of these H states is of distance $\tilde{\epsilon}$ away from this same state $|\alpha\rangle$.

For any POVM element P, we can write the trace distance between two states ρ, σ as

$\mathrm{Tr}\big[P(\rho-\sigma)\big] \leq D(\rho,\sigma)$. Thus, we have for a POVM element Π_i and for states $|\Psi_i\rangle, |\alpha\rangle$:

$$\mathrm{Tr}(\Pi_i |\Psi_i\rangle \langle\Psi_i|) - \mathrm{Tr}(\Pi_i |\alpha\rangle \langle\alpha|) \leq \tilde{\epsilon}. \tag{4.31}$$

Assuming that each honest agent has an equal chance of becoming the voter, the probability that the malicious agents can guess the identity of the voter is bounded by:

$$\begin{aligned}
\Pr[\text{guess}] &= \sum_{i=1}^{H} \frac{1}{H} \mathrm{Tr}(\Pi_i |\Psi_i\rangle \langle\Psi_i|) && (4.32)\\
&\leq \frac{1}{H} \sum_{i=1}^{H} \Big[\mathrm{Tr}(\Pi_i |\alpha\rangle \langle\alpha|) + \tilde{\epsilon}\Big] && (4.33)\\
&= \frac{1}{H} \mathrm{Tr}\Big[\sum_{i=1}^{H} \Pi_i |\alpha\rangle \langle\alpha|\Big] + \frac{1}{H} H\tilde{\epsilon} && (4.34)\\
&= \frac{1}{H} \mathrm{Tr}(|\alpha\rangle \langle\alpha|) + \tilde{\epsilon} && (4.35)\\
&= \frac{1}{H} + \tilde{\epsilon}. && (4.36)
\end{aligned}$$

As we said, the probabilities for the other agents come from the fact that all the agents that are not voting perform exactly the same transformation on the state, so it is impossible for the dishonest parties to distinguish between them, hence the probability of guessing their identity is the same.

□

4.3.10 Proof of Theorem 3

Theorem 3. *If at round ℓ the agents are honest and use a state $|\psi\rangle$ such that $F(|\psi\rangle, |GHZ\rangle) \geq \sqrt{1-\epsilon^2}$ to perform Voting, then the probability that there is an error in the tally in the ℓ-th round is upper bounded by ϵ,*

$$P_\ell^{er} \leq \epsilon.$$

Proof. At each round, only one vote is declared. The state $|\psi\rangle$ maximizing this probability can be at most ϵ-far in trace distance. Knowing that $Tr[\Pi(\rho-\tau)] \leq D(\rho,\tau)$ for any POVM Π, the probability of having one error using the state $\rho = |\psi\rangle \langle\psi|$, instead of the correct state $\tau = |GHZ\rangle \langle GHZ|$ is

$$P_\ell^{er} = Tr[\Pi_\ell \mathcal{H}^{\otimes^N} \rho] \leq Tr[\Pi_\ell \mathcal{H}^{\otimes^N} \tau] + D(\rho,\tau) = \epsilon,$$

where Π_ℓ is some operator that evaluates the distance from the correct ℓ-th output of the state measured in the Hadamard basis, $\mathcal{H}^{\otimes^N}$ is the product of local Hadamard applied by

each voter and we used the fact that if we measure the correct state it is impossible to have an error. □

4.4 Discussion

We have described and analyzed a practical quantum e-voting scheme and provided approximate definitions of correctness and privacy, which make it appropriate for realistic non-ideal scenarios. The quantum e-voting protocol that we have described achieves information-theoretic security without requiring trust in the quantum source or in any election authority. Previously proposed classical schemes, such as the one in Ref. [131], also achieve information-theoretic security, however the requirement of trusting authorities and simultaneous broadcasting could make it impractical. A small-scale election demonstration of our protocol can be implemented with currently available quantum photonic platforms and with the improvement of these technologies a voting scheme for board meetings and similar scenarios may be attainable in the near future. When GHZ states of a thousand photons, with high fidelity and a reasonable repetition rate, become available and can be well controlled, it will be possible to implement the protocol at a metropolitan level and then as a consequence, with a subdivision into regular elections, at a national level. Although this is certainly challenging, all the future applications of quantum information protocols will have to meet similar obstacles and this protocol might be one of the first practical use cases of quantum technologies to meet realization.

Chapter 5

Quantum Complex Networks

5.1 What is a CV network . . . 108
5.2 Arbitrary Gaussian Network . . . 110
5.2.1 Gaussian quantum states . . . 110
5.2.2 Graph states as quantum networks . . . 111
5.3 Interplay between squeezing and symplectic spectra . . . 113
5.4 A resource theory of Squeezing . . . 114
5.5 Squeezing cost for network generation . . . 115
5.5.1 Regular Networks . . . 115
5.5.2 Complex Networks . . . 118
5.6 Quantum teleportation Gaussian Networks . . . 122
5.7 Multi-path entanglement . . . 124
5.7.1 Graphical Calculus . . . 124
5.7.2 Parallel enhancement of entanglement . . . 125
5.8 Routing protocol . . . 129
5.9 Discussion . . . 134

So far we explored two important use-cases of photonic quantum communication channels, one involving two users with different attributes and one that engages an arbitrary number of agents without a central authority. In those cases, the protocols themselves required a pre-established specific structure of the quantum connections that is far from the complex shape of modern day internet. In the third and last stage of our study on quantum networks we will investigate the capabilities provided by highly multimode entangled quantum systems with arbitrary shapes, evaluate their cost and the limitations of their experimental realization and set up a protocol able to distribute entanglement among any two nodes in the network to allow quantum communications.

As we have seen there are several ways to supply quantum communication channels, including simple optical fibers and entangled photons. An appealing approach to study photonic quantum networks is given by continuous variables graph states, an interesting class of Gaussian quantum states that, under certain condition, can provide a substrate for universal quantum computation [137]. This type of quantum states can readily be produced in some well equipped photonic labs, however their ideal version requires an infinite amount of squeezing, which is unphysical as it would imply infinite energy.

In this chapter we study continuous-variable graph states as quantum communication networks, exploring graphs with regular and complex networks shape distributed among different agents, simulating a CV based quantum internet. Since, as we said, the main limitation to construct these optical systems is finite squeezing, we show their cost as a global measure of squeezing and number of squeezed modes that are necessary to build the network. We show that the trend of the squeezing cost presents a non-trivial scaling with the size of the network strictly depending on its topology. Notice that for these states the amount of squeezing is directly linked with the energy of the system, thus the squeezing cost can provide a lower bound on the intrinsic energetic cost necessary to produce this type of quantum network.

Finally, we devise a routing protocol based on local quadrature measurements for reshaping the network in order to perform teleportation protocol between two arbitrary nodes of the networks. The *Routing* protocol, which is based on wire-shortening over parallel paths among the nodes, improves the final entanglement between the two nodes in a considerable amount of cases, and it is particularly efficient in running-time for complex sparse networks.

5.1 What is a CV network

Photonics quantum networks are essential resources for quantum communication and information protocols, they represent an essential part of the future quantum internet where quantum states of light will allow for the efficient distribution and manipulation of information [138]–[140]. In this chapter we explore continuous-variable (CV) entangled states with regular and complex network topologies, that are distributed among different agents.

Continuous-variable quantum states span on infinite dimensional Hilbert spaces, so allowing for the encoding of larger amount of information when compared to Discrete Variables (DV). Moreover, generation and measurement of CV states requires only coherent control on classical laser source and weakly non-linear materials, along with coherent (homodyne) detection which, differently from photon counting detectors, can be highly efficient at room temperature and easily integrated in classical communication networks. However, CV encoding in quantum networking/routing protocols has not been extensively studied yet.

Our model aims at reproducing the existing photonic platforms with realistic experimental constraints, such as limited amount of squeezing, but without taking into account propagation losses [1]. At the same time we probe their capabilities while the scaling of the network increases beyond the capacities allowed by the state-of-the-art technology. In particular we explore the cost of different networks topologies in term of number of needed squeezers at fixed number of nodes in the networks and of the global amount of squeezing.

We then explore their potentialities to perform efficient quantum communications between two arbitrary nodes when assisted with a given class of Gaussian Local Operations and Classical Communication (GLOCC) by all the agents in the network. A typical approach of quantum networking and routing consists in distributing photonics states like single-photons, Bell pair or Gaussian state and then use synchronous local operations that build the wanted entanglement structure between the agent [139], [141]–[144]. We rather consider the case where a preexisting CV multipartite entangled state is distributed among the players and then local operations reconfigure the entanglement connections, similarly to some protocol in the DV case [145]. The choice is motivated by the fact that multimode entangled states can be directly generated via optical platform [70], [146]–[149] and their shape can be easily manipulated [69], [150]. The chapter is structured as it follows. In section 5.2 we briefly revise Gaussian quantum states, their generation by quadratic Hamiltonian and their decomposition, that we already discussed in section 1.2.8 of chapter 1. We then introduce the Gaussian quantum networks studied in this chapter. In section 5.4 we revise a resource theory of squeezing and in section 5.5 we will adopt it in order to estimate the cost of expanding the network. Although in entangled qubits networks the resource usage is always proportional to the number of links, we show that in CV Gaussian networks the trend of the squeezing cost is vastly richer, presenting non-trivial scaling with the size of the network strictly depending on its topology. We present as well a few instances of the full squeezing spectra — i.e. the needed amount of squeezers with the required squeezing values — of regular and complex networks, showing that some topologies are equivalent up to a linear optical transformation.

In section 5.6 we propose a CV architecture for the quantum internet based on the Gaussian

[1] This work is focused on the capabilities of pure CV quantum states to act as quantum networks and the resources needed for their generation. Of course propagation losses can be included in the model in future works. Also generation losses can be very low, so that the hypothesis of pure states is a realistic one, and propagation losses can be mitigated by considering local (short distances) networks.

network previously described. We simulate quantum communication protocols through the network by letting the spatially separated agents present at each node perform a homodyne measurement on their optical mode and look for the optimal measurement strategy to maximize the negativity of the entangled pair shared by the two users who want communicate, Alice and Bob. We prove a compelling result that could have potential applications, notably that when multiple entangled paths connect Alice to Bob the optimal measurement strategy allows to increase the negativity in the final pair. This *parallel enhancement of entanglement* can be used to increase the quality of quantum communications in some selected network topologies.

Lastly, in section 5.8, we employ our previous findings to implement an heuristic routing protocol for distributing and boosting the entanglement between two arbitrary agents. The algorithm we provide, on the one hand, is much more efficient than directly checking all possible combinations of quadrature measurements and, on the other hand, it always provides higher negativity than the classical scheme, which is directly employing the shortest path between Alice and Bob and neglect the parallel channels.

5.2 Arbitrary Gaussian Network

5.2.1 Gaussian quantum states

The generation of continuous variables multimode entangled states has been demonstrated in several optical setups. In such experiments we recover networks structures as naturally appearing entanglement correlations [70], reconfigurable Gaussian interactions [150], or imprinted cluster states [69], [146], [149], [151].

These quantum states produced via parametric processes and linear optical transformation are characterized by Gaussian statistical distribution of the quadratures of the involved optical modes [31]. The quadratures $\hat{Q}_j$ and $\hat{P}_j$ of the j^{th} mode are canonical conjugate variables, such that $[\hat{Q}_j, \hat{P}_k] = i\hbar\delta_{j,k}$, associated to the quantum harmonic oscillator describing the light mode. In this work we adopt the following relation with creation and annihilation operators $\hat{\mathbf{a}}^\dagger = (\hat{\mathbf{Q}} - i\hat{\mathbf{P}})/\sqrt{2}$ and $\hat{\mathbf{a}} = (\hat{\mathbf{Q}} + i\hat{\mathbf{P}})/\sqrt{2}$, such that the variance of the vacuum quadratures is normalized to $1/2$.

The produced states can then be completely characterized by the first two moments of the quadratures $\bar{\mathbf{r}} = \mathrm{Tr}[\rho\hat{\mathbf{r}}]$ and $\sigma = \mathrm{Tr}[\rho\{(\hat{\mathbf{r}} - \bar{\mathbf{r}}), (\hat{\mathbf{r}} - \bar{\mathbf{r}})^T\}]$, where ρ is the density matrix of the Gaussian state and $\hat{\mathbf{r}} = (\hat{Q}_1 ... \hat{Q}_N, \hat{P}_1 ... \hat{P}_N)$.

Parametric processes are described by quadratic Hamiltonians $\hat{\mathcal{H}}_I = \hat{\mathbf{r}} H \hat{\mathbf{r}}^T$, whose dynamics is implemented on the quadratures by $S_H = e^{\Omega H t}$, as

$$\mathbf{r}' = S_H \mathbf{r}_0 \tag{5.1}$$

where $\Omega = \left(\begin{smallmatrix} 0 & \mathbb{1} \\ -\mathbb{1} & 0 \end{smallmatrix}\right)$, $\mathbf{r}_0$ are quadratures of the initial state and $\mathbf{r}'$ are the quadratures of the

final state. Since any pure Gaussian state can be obtained by the application of a quadratic Hamiltonian H to the vacuum, the most general pure Gaussian state covariance matrix is given by applying S_H by congruence to the vacuum covariance matrix $\sigma_0 = \mathbb{1}/2$:

$$\sigma = S_H \sigma_0 S_H^T = \frac{S_H S_H^T}{2}. \tag{5.2}$$

In section 1.2.8, we showed how to adopt the Bloch-Messiah decomposition to express the covariance matrix as a product composed by an orthogonal matrix O and a diagonal matrix Δ:

$$\sigma = \frac{S_H S_H^T}{2} = \tfrac{1}{2} O \Delta^2 O^T. \tag{5.3}$$

The diagonal matrix Δ contains the information on the minimum number of squeezed modes in the system and their value of squeezing, which will later be used in the chosen resource theory. If we consider a single mode field, the squeezing operation is defined as a Gaussian transformation that reduces the variance of $\hat{P}$ by a factor $10^{-s/10}$, where s, measured in dB throughout this article, is called *squeezing factor*. Squeezing is represented by the local symplectic matrix

$$S_{sq}(s) = \begin{pmatrix} 10^{s/20} & 0 \\ 0 & 10^{-s/20} \end{pmatrix}.$$

The multimode Δ matrix can then be written as

$$\Delta = \mathrm{diag}\{10^{s_1/20}, 10^{s_2/20}, ...10^{s_N/20}, 10^{-s_1/20}, 10^{-s_2/20}, ...10^{-s_N/20}\}. \tag{5.4}$$

This formalism can be used to visualize and manipulate Gaussian quantum states, that are readily available in most well-equipped photonics laboratories and, although the number of modes and their connections is still in large part limited, many efforts are employed to improve the capacities of these systems.

Targeted Gaussian quantum states, including the quantum networks of the next section, can be generated via the two following strategies: i) by tailoring Hamiltonians $\hat{\mathcal{H}}_I$ of multimode parametric processes in order to get the decomposition of Eq. 5.3 corresponding to the desired covariance matrix; ii) by getting a number of single-mode squeezers equal to the the number of elements with $s_j \neq 0$ of Δ in Eq. 5.3 and producing the corresponding s_j squeezed states, that are injected in a linear optic intereferometer corresponding to the orthogonal matrix O in Eq. 5.3.

5.2.2 Graph states as quantum networks

The above formalism can be employed to describe Gaussian graph states, that can be used as CV quantum networks. We at first recall that a network is mathematically described

by a graph $G(V, E)$, which is a set of vertices V (or nodes) connected by a set of edges E. Labeling the nodes of the graph in some arbitrary order, we can define a symmetric adjacency matrix $A = A^T$ whose $(j, k)^{\text{th}}$ entry A_{jk} is equal to the weight of the edge linking node j to node k (with no edge corresponding to a weight of 0). Typically, the adjacency matrix is enough to completely characterize a graph, however we will see that in our case there are other degrees of freedom such as the squeezing of a node and its angle.

We can now describe the quantum networks we use in this work that are called graph-states [152]–[154]. Theoretically, they can be built by entangling a number of squeezed modes of light via CZ-gates, which is a Gaussian operation implementing a correlation of strength g between the $\hat{Q}$ and the $\hat{P}$ of the two modes on which it acts. The corresponding symplectic matrix is

$$S_{CZ}(g) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & g & 1 & 0 \\ g & 0 & 0 & 1 \end{pmatrix}.$$

The graph associated to the graph states identify edges as CZ-gates applied between nodes, that are the squeezed modes, weighted with g.

In order to simplify the many degrees of freedom present in our networks, for the moment we shall assume that all the nodes will be squeezed in $\hat{P}$ by s and all the edges have a correlation strength of g. If we apply a CZ-gate network with adjacency matrix A to a multimode squeezed vacuum σ_s, with squeezing factor s we obtain a Gaussian network with covariance matrix [155]

$$\begin{aligned} \sigma = \begin{pmatrix} \sigma_{qq} & \sigma_{qp} \\ \sigma_{pq} & \sigma_{pp} \end{pmatrix} &= \begin{pmatrix} \mathbb{1} & 0 \\ A & \mathbb{1} \end{pmatrix} \sigma_s \begin{pmatrix} \mathbb{1} & A \\ 0 & \mathbb{1} \end{pmatrix} \\ &= \begin{pmatrix} R\mathbb{1} & RA \\ RA & RA^2 + \mathbb{1}/R \end{pmatrix}, \end{aligned} \tag{5.5}$$

where $R = 10^{s/10}$. The $2N \times 2N$ covariance matrix σ is divided in four $N \times N$ blocks, where the blocks σ_{qq} and σ_{pp} represent the correlations among the different nodes' Q- and P-quadratures, respectively, whereas the blocks $\sigma_{qp} = \sigma_{pq}$ describe the correlations between Q- and P-quadratures.

Bear in mind that the *CZ-gate* operations that theoretically identify the edges of the networks are seldom realized in any laboratory being very challenging to accomplish. What is commonly done, as explained in the previous subsubsection, is the reduction of the covariance matrix of the graph state in 5.5 to the form of Eq. 5.3, that is also a receipt for bulding the graph states from a certain number of squeezed modes (Δ) and linear optics transformations (O).

In this chapter we will focus on the squeezing cost of employing highly multimodes Gaussian systems as quantum networks and discuss some strategies to increase the quality of

quantum communication on these networks in some selected (but realistically relevant) scenarios. Our platform offers a wide range of applications for simulating complex structured quantum systems or implementing quantum information protocols in realistic networks.

5.3 Interplay between squeezing and symplectic spectra

Consider a N-dimensional graph with adjacency matrix A. If we apply a set of CZ-gate to the N modes of a vacuum state according to the structure of A, we end up with a Gaussian graph state with the following $2N$-dimensional covariance matrix:

$$\sigma = \frac{1}{2}\begin{pmatrix} \mathbb{1} & A \\ A & \mathbb{1} + A^2 \end{pmatrix}, \tag{5.6}$$

where we assumed that the vacuum state is normalized to $1/2$. Since A is symmetric, it is always diagonalizable

$$VAV^T = D = \text{diag}(\{D_i\}), \tag{5.7}$$

for some orthogonal matrix V, where $\{D_i\}_{i=1}^N$ is the set of the real eigenvalues of A. It follows that $VA^2V^T = VAV^TVAV^T = D^2$. Let us consider the following matrix

$$W = \frac{1}{\sqrt{2}}\begin{pmatrix} V & V \\ V & -V \end{pmatrix}. \tag{5.8}$$

We can verify easily that $WW^T = \mathbb{1}$, hence W is an orthogonal matrix implementing a basis change that would not change the spectrum of the matrix to which it is applied. If we apply it to σ we get

$$\sigma' = W\sigma W^T = \frac{1}{2}\begin{pmatrix} \mathbb{1} + D + D^2/2 & -D^2/4 \\ -D^2/4 & \mathbb{1} - D + D^2/2 \end{pmatrix}, \tag{5.9}$$

which is a block matrix composed of diagonal matrices. We can permute the rows and columns of the matrix to get a diagonal block matrix

$$\Pi\sigma'\Pi^T = \bigoplus_{i=1}^{N} M_i, \tag{5.10}$$

where Π is a permutation operator, while

$$M_i = \begin{pmatrix} \mathbb{1} + D_i + D_i^2/2 & -D_i^2/4 \\ -D_i^2/4 & \mathbb{1} - D_i + D_i^2/2 \end{pmatrix}. \tag{5.11}$$

In this basis, each block M_i represents a single mode covariance matrix of a pure unentangled Gaussian state. We can hence diagonalize each block independently. In particular, notice that $\det(M_i) = \frac{1}{4}$, thus the eigenvalues of σ are given by

$$\lambda_i^{\pm} = \frac{1}{2}\left(\text{Tr}(M_i) \pm \sqrt{\text{Tr}(M_i)^2 - 4\det(M_i)}\right) = \frac{1}{2}\left(1 + D_i^2/2 \pm \sqrt{D_i^2 + D_i^4/4}\right). \tag{5.12}$$

This equation shows the interplay between the physical resources necessary to experimentally implement a CV graph state and the spectrum of the underlying graph. This implies that we can use spectral graph theory to characterize analytically the physical requirements of building Gaussian networks and thus predict which one will be easier to realize. A first crucial consequence is that different graph states whose underlying graphs are co-spectral, e.g. their adjacency matrices have the same eigenvalues, can be transformed into each other applying passive linear optics. We will see later that the star and diamond networks have this property, making them a relevant class of Gaussian networks for applications. Further results of this relation will be analysed in future works.

Notice that there is as well a simple relation between the adjacency matrix of the graph state and the internal energy difference between the state and the vacuum:

$$\Delta E = E - E_0 = \mathrm{Tr}(\sigma - \sigma_0) = \frac{1}{2}\mathrm{Tr}(A^2). \tag{5.13}$$

This represents a fundamental lower bound on the energy necessary to implement such states.

5.4 A resource theory of Squeezing

The Gaussian bosonic states of subsection 5.2.1 are of particular significance in the theory of continuous variable quantum information, in particular in their quantum optical implementations. They are in fact resources for measurement based quantum computing [152], [154], quantum simulations [150], multi-party quantum communication [69], [156], and quantum metrology [157], [158].

Being interested in the nature of the correlations between such states, the first moments become irrelevant. In any practical realization of a quantum communication protocol with Gaussian states, first moments do play a role, but these are normally managed in the post-processing and do not interfere with the dynamics of the second moments. We can thus assume that our quantum states are fully described by their covariance matrix.

We have seen in the previous section that the squeezing is the essential resource for building Gaussian entangled states. A natural question is thus: what is the squeezing cost of producing a quantum state?

A general resource theory for Gaussian states is provided in [159]. The specific case of squeezing is described in [160] where they show an operational squeezing measure for any symplectic transformations S:

$$F : \mathbb{R}^{2N\times 2N} \to \mathbb{R}, \quad F(S) = \sum_{i=1}^{N} 20\log_{10}(\overset{\downarrow}{s}_i(S)), \tag{5.14}$$

where $\overset{\downarrow}{s}_i$ are the decreasingly ordered singular values of S, while $\log_{10}$ and the factor 20

ensures that the outcome is measured in dB. Using Eq. 1.71, we can then define a squeezing measure for covariance matrices

$$G : \mathbb{R}^{2N\times 2N} \to \mathbb{R}, \quad G(\sigma) = \sum_{i=1}^{N} 10 \log_{10}(\lambda_i^{(+)}(\sigma)), \tag{5.15}$$

where $\lambda_i^{(+)}(\sigma)$ are the the largest eigenvalues of the covariance matrix σ of equation 5.12 and, once again, the factor 10 guarantees that the outcome is measured in dB. This definition can be generalized for arbitrary quantum states, but assumes this particularly simple form for pure Gaussian ones and it works for any number of modes. We will employ it to classify networks topologies, basing on how their squeezing cost scales with the dimension of the network. As we said previously, the implementation of the CZ-gate is not trivial, however in our analysis the actual transformations used to implement the state are irrelevant because the Eq. 5.15 only depends on the final state to which it is applied and not on the single symplectic maps used to implement it.

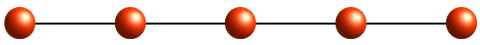
5.5 Squeezing cost for network generation

In this section we apply the results presented above to various topologies of Gaussian networks, to study how their squeezing requirement scales with the size of the network depending on its own structure. As stated in the first section, a node in the network is a a pure continuous variables Gaussian state, that will be called a qumode, and is completely defined by its own covariance matrix.

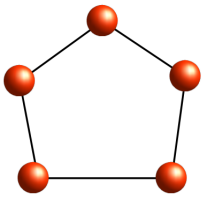
5.5.1 Regular Networks

Let us first discuss some regular network structures. We shall consider the following topologies:

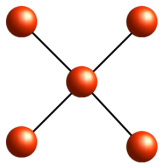
- The *linear graph* $\mathcal{L}_N$, with N nodes and $N-1$ edges, is accomplished by connecting each node in series to the next.



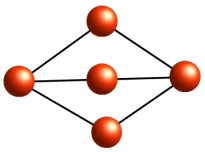
- The *ring graph* $\mathcal{R}_N$, with N nodes and N edges, is a linear graph with a closed loop.



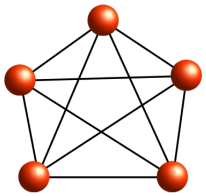
- In the *star graph* topology $\mathcal{S}_N$, with N nodes and $N-1$ edges, every peripheral node is linked to a central node called hub.



- The *diamond graph* $\mathcal{D}_N$, with N nodes and $2(N-2)$ edges, has 2 hubs, each linked to all the $N-2$ central nodes of the network.



- In the *complete* (or *fully connected*) *graph* $\mathcal{F}_N$, with N nodes and $\frac{N(N-1)}{2}$ edges, all nodes are interconnected.



We use the linear graph as a benchmark to see how the squeezing cost scales with the number of nodes and links. In fact, single mode squeezing and the CZ-gate both require a fixed amount of squeezing to be implemented, so we would expect $G(\sigma)$ to scale linearly with the number of links and nodes. This is indeed the case of the graphs in Fig. 5.1. In figure (a), we create a multimode squeezed vacuum with no connections ($g = 0$). We can see how the effect of the squeezing s on each node is that of shifting the average cost. In figure (b) we set the initial squeezing to be null ($s = 0$) and only apply the CZ-gates. It is shown that for large values of N the average cost is constant, hence the total cost is linear in N . We can always set $s = 0$ which would only contribute as a constant shift and see how the effect of the connections influence the squeezing requirement for the network. Let us now see how the total squeezing cost $G(\sigma)$ scales with the number of nodes N for each of the network topologies presented above.

In Fig. 5.2 we can see how the linear graph in blue and the ring graph in orange are superposed, sharing the same squeezing cost, as well as the star graph in green and the diamond in red. The latter two graphs present much less squeezing than the others and do not grow linearly with N .

Fig. 5.3 shows the average cost for each node and each edge respectively. It results that the constant behaviour of the linear and ring topologies is rather an exception and that in general the squeezing required to generate a determined Gaussian network is not simply proportional to the number of nodes or edges but sublinear. The intrinsic connection be-

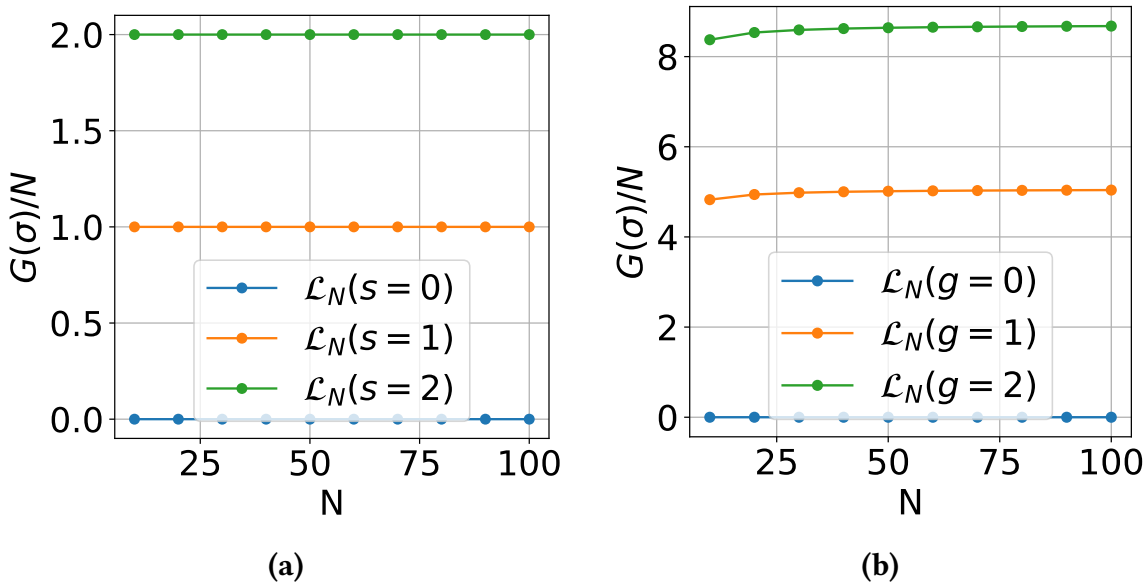


Figure 5.1: Trend of the average squeezing cost for the linear graph $\mathcal{L}_N$ up to $N = 100$: (a) we increase the squeezing s keeping the correlations null $g = 0$ and (b) we increase the correlations g keeping the squeezing null $s = 0$.

tween the squeezing of a Gaussian network and its topology was already put in evidence by *Gu et al.* [154], by proving a relation between the squeezing required to produce a CV graph state and the singular value decomposition of the associated adjacency matrix. As we said, the linear and ring graphs have a constant average cost per edge with the growth of the network, whereas the complete graph seems to be the one with lowest average cost per edge, having also the highest degree of edges.

An objection one could make at this point is that our cost functional $G(\sigma)$ does not fully characterize our Gaussian networks. In fact, two states that have the same squeezing cost are not necessarily equivalent up to an orthogonal transformation. For example, a 10dB single mode squeezed vacuum and a two mode squeezed vacuum with 5dB of squeezing each would have the same cost but cannot be transformed into each other using only passive optics. As a matter of fact, resource theories can seldom give a complete view of the problem in exam, notably in the light of an experimental implementation.

Although the squeezing cost is indeed the most insightful figure of merit to investigate what happens as the size of the Gaussian networks grows, the most complete picture of number of the amount of needed experimental resources is given by the decomposition defined in Eq. 1.71, which gives us the minimum number of squeezed modes and their squeezing value.

In Fig. 5.4 we then show the distribution of the logs of the singular values of the covariance matrix of the regular topologies studied above, for $N = 100$.

Notice that the diamond and the star graphs only have two intrinsic squeezed modes. In

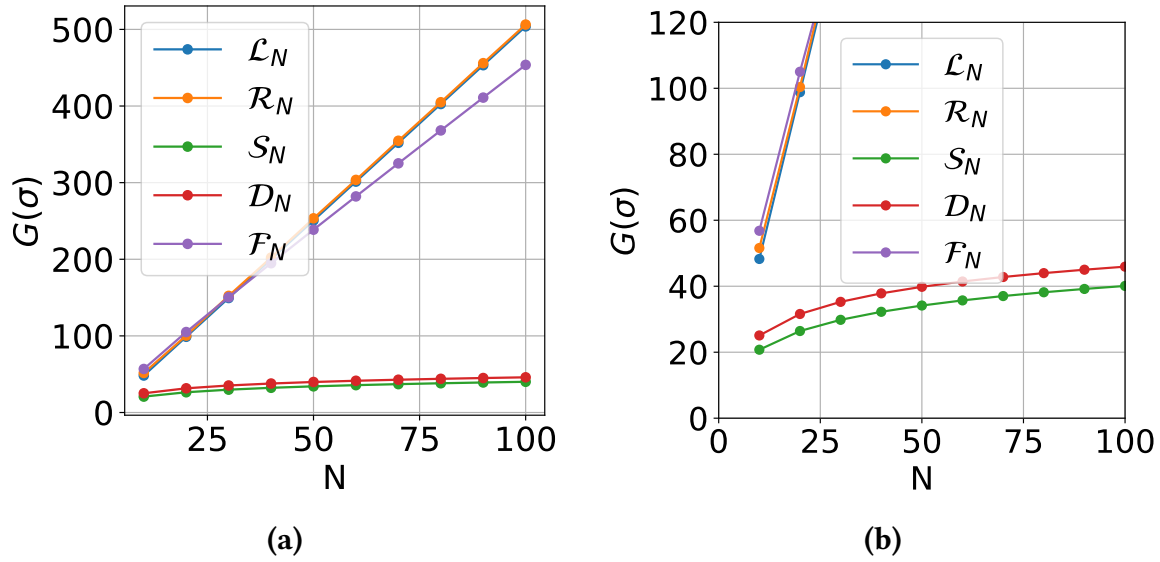


Figure 5.2: (a) Trend of the squeezing cost $G(\sigma)$ for the regular topologies with $s = 0$ and $g = 1$: linear $\mathcal{L}_N$, ring $\mathcal{R}_N$, star $\mathcal{S}_N$, diamond $\mathcal{D}_N$, full $\mathcal{F}_N$ networks up to $N = 100$ nodes. (b) Detail of the diamond and star graphs. These networks do not scale linearly unlike the others.

the specific, the number of squeezers in all the networks grows linearly with N , except the star and diamond, that are built by squeezing only two modes and mixing them with $N - 2$ vacuum modes with passive optics interferometry. A straight consequence, is that these two very different types of networks are completely equivalent up to an orthogonal transformation, which means that they can be exactly reshaped one into the other using linear optics [2]. Interestingly, the first mode of the $\mathcal{F}$ network has the majority of squeezing, while the rest is shared equally among all other nodes.

5.5.2 Complex Networks

So far we described graphs that are built through a deterministic algorithm, though we can also construct a graph based on statistical models [161], [162]. In this subsection we will shortly review the main feautures of random and complex networks explained in section 2.2.1 of chapter 2. The exemplary standard for random networks is the Erdős–Rényi model $\mathcal{G}_{ER}(N, p)$, in which each pair of the N nodes have a probability p to be linked; the network thus has $\binom{N}{2}p$ edges on average [87].

Most of the network properties observed in nature, however, simply cannot be described by regular or random graphs. For this reason, a youthful branch of scientific research is committed to the study of *complex networks*. In the field of network theory, complex networks are a type of graph with non trivial topological features, that are shared by neither

[2] In general any CV graph can be reshaped in any other graph via a symplectic transformation, in this case the symplectic involves only linear optics without any supplementary squeezing.

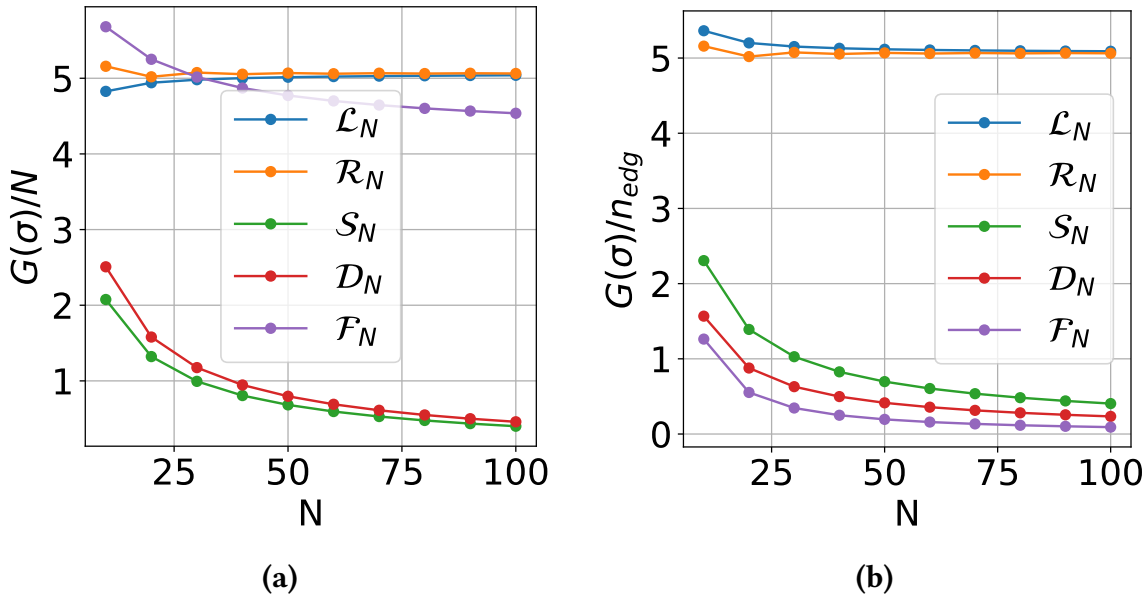


Figure 5.3: Trend of the average squeezing cost for regular topologies with $s = 0$ and $g = 1$: linear $\mathcal{L}_N$, ring $\mathcal{R}_N$, star $\mathcal{S}_N$, diamond $\mathcal{D}_N$, full $\mathcal{F}_N$ networks up to $N = 100$ nodes. (a) Average cost per node $\frac{G(\sigma)}{N}$, (b) average cost per edge $\frac{G(\sigma)}{n_{edg}}$.

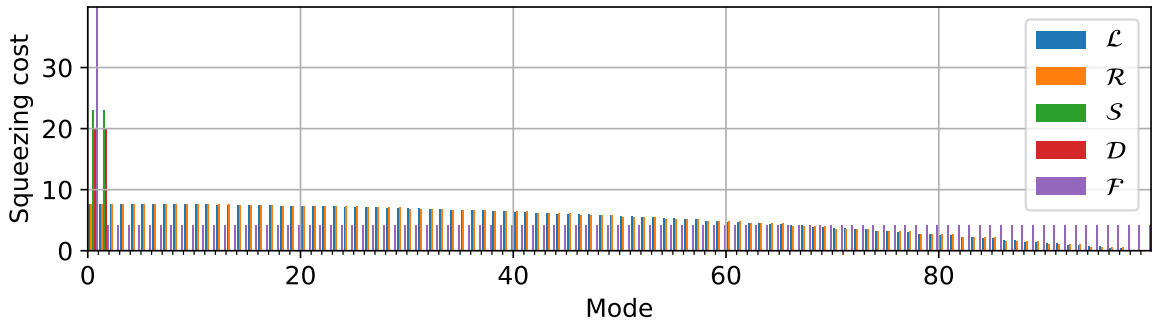
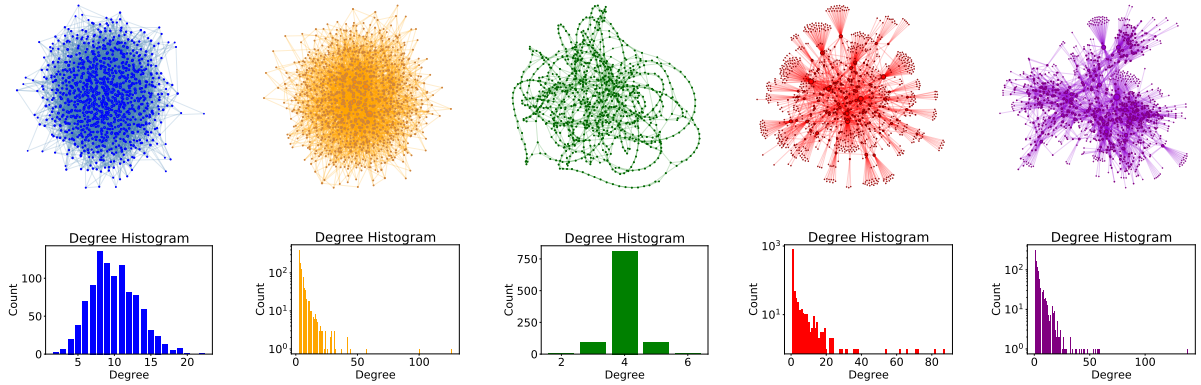


Figure 5.4: Squeezing cost distribution for regular networks: linear $\mathcal{L}_N$, ring $\mathcal{R}_N$, star $\mathcal{S}_N$, diamond $\mathcal{D}_N$, full $\mathcal{F}_N$ networks in the $N = 100$ supermodes, $s = 0, g = 1$. All the networks present some squeezing in each mode except the $\mathcal{S}$ and $\mathcal{D}$ that have an equal amount of squeezing only in the first two modes. The $\mathcal{F}$ network has a large peak of squeezing in the first mode, while the remaining amount of squeezing is equally distributed in the other modes.

regular nor random graphs, but are rather akin to networks modeling real systems [88].

As we have seen in chapter 2, an important class of complex networks is characterized by the *small world* property. These networks exhibit the peculiarity of having a low average path length, which is the mean distance between two arbitrary nodes, and a high clustering, which is a measure of the degree to which nodes in a graph tend to cluster together. The emblematic network presenting this feature is the the Watts–Strogatz model $\mathcal{G}_{WS}(N, \kappa, \beta)$



(a) Erdős–Rényi $\mathcal{G}_{ER}$ (b) Barabasi–Albert $\mathcal{G}_{BA}$ (c) Watts–Strogatz $\mathcal{G}_{WS}$ (d) AS internet $\mathcal{G}_{AS}$ (e) Proteins $\mathcal{G}_{PP}$.

Figure 5.5: Some complex networks and their degree distribution. In the distributions of the BA, AS and PP the y-axis is in log-scale.

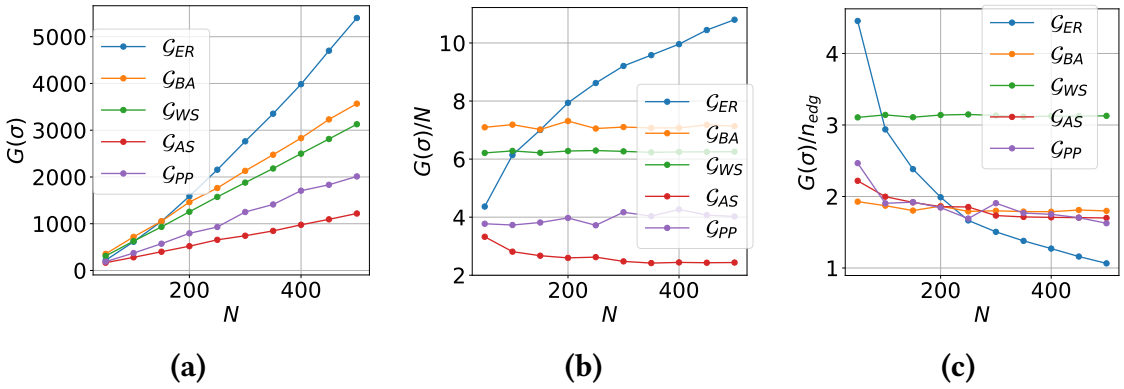


Figure 5.6: (a) Trend of the squeezing cost for complex topologies: Erdős–Rényi $\mathcal{G}_{ER}$, Barabasi–Albert $\mathcal{G}_{BA}$, Watts–Strogatz $\mathcal{G}_{WS}$, AS internet $\mathcal{G}_{AS}$ and Protein–Protein interaction $\mathcal{G}_{PP}$ networks up to $N = 500$ nodes. (b) Average squeezing per node, (c) average squeezing per edge.

[94]. In this model, we first construct a graph with N nodes and $\frac{N\kappa}{2}$ edges where each node has exactly κ neighbors, then with probability β we rewire each edge with another node chosen uniformly at random while avoiding self loops and link duplications.

Another relevant class of complex networks that we previously studied presents the typical aspect of being *scale-free* and having *long-tailed* structures. Scale-free networks show a power law in the degree distribution $P(k) \propto k^{-\gamma}$ for some $\gamma > 0$, which is self-similar at all values of k in the *tail* of the distribution, unlike the ER and WS models that go to zero very quickly and have no tails. This fractal like attribute is well modeled by the Barabasi–Albert model $\mathcal{G}_{BA}(N, K)$, which can also reproduce growth and preferential attachment in networks [93]. This type of graph is the canonical example to reproduce some properties of the *World Wide Web*.

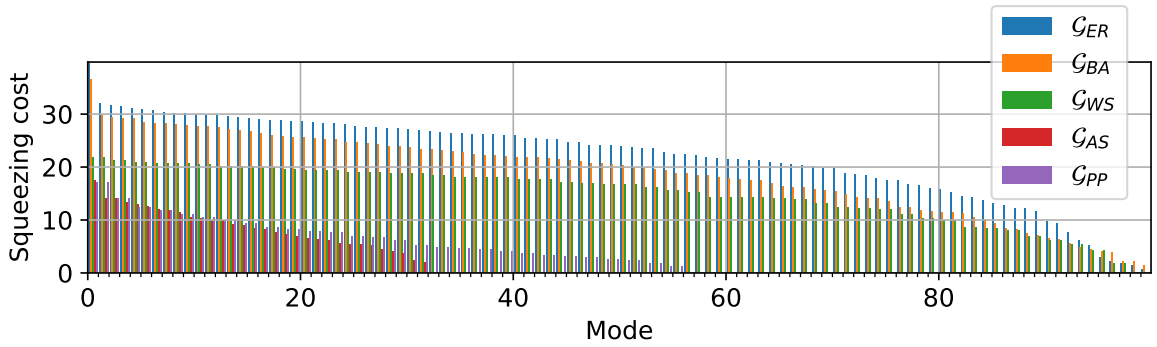


Figure 5.7: Squeezing cost distribution for complex topologies: Erdős–Rényi $\mathcal{G}_{ER}$, Barabasi–Albert $\mathcal{G}_{BA}$, Watts–Strogatz $\mathcal{G}_{WS}$, AS internet $\mathcal{G}_{AS}$ and Protein–Protein interaction $\mathcal{G}_{PP}$ networks in the $N = 100$ supermodes. The trend of the number of modes for each of these networks is shown in Fig. 5.8

Two different classes of complex networks that often present scale-free distributions are constituted by *technological networks* and *biological networks*, that we also revised in chapter 2. As an example of technological network we will consider the Internet Autonomous System (AS) $\mathcal{G}_{AS}(N)$, basing on the work put forward in ref. [91], whereas for the study of a biological network we will examine specifically the protein–protein interaction network model $\mathcal{G}_{PP}(N, \sigma)$ developed in ref. [95].

In Fig. 5.6 we report the trend of the total squeezing cost, average cost per node and average cost per edge as a function of the number of nodes for each of the above complex topologies.

From the plots we notice that the most expensive growth belongs to the ER topology, while the AS seems to be the cheapest, which is a relevant quality in prospect of an actual implementation of the quantum internet. Another interesting feature, that did not emerge for regular networks, is the fact that for the ER the average cost of squeezing per node increases with the size of the graph. It is in part surprising that the complete graph behaves so differently from the ER graph. In fact, even though they are topologically very different, the scaling of the number of edges is similar so one could have expected a similar trend. On the other hand, the cost per node in the BA, WS and PP is approximately constant whereas it slowly decreases for the AS topology. Moreover, we observe that the average price per edge is decreasing for all but the WS topology. The fact that a high connectivity does not imply a high resource usage is a particularly inviting property of Gaussian networks, especially for their applications in quantum communications.

In Fig. 5.7 we show the squeezing cost distribution for the various topologies of complex networks by showing the squeezing cost of all the principal modes. We deduce that the AS is not only the cheapest, but is also the one that has the least number of squeezed modes, turning to a tremendous advantage for experimental applications. This feature is further emphasized in Fig. 5.8, in which we plot the trend of the number of squeezed modes necessary to build the network as a function of N. In this plot we see that the ER, BA and

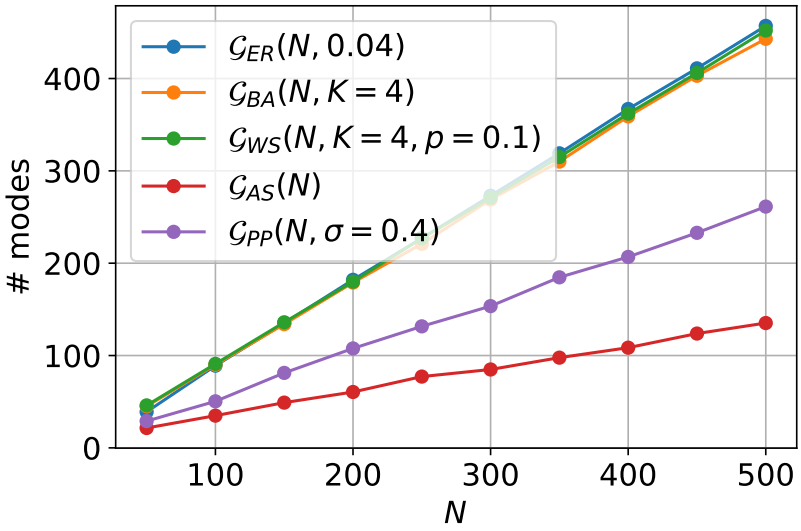


Figure 5.8: Trend of the number of squeezed modes necessary to build the networks versus the number of nodes in the network for complex topologies: Erdős–Rényi $\mathcal{G}_{ER}$, Barabasi–Albert $\mathcal{G}_{BA}$, Watts–Strogatz $\mathcal{G}_{WS}$, AS internet $\mathcal{G}_{AS}$ and Protein–Protein interaction $\mathcal{G}_{PP}$ networks up to $N = 500$ nodes.

WS networks have a similar trend, unlike the PP and AS.

Now that we have characterized the cost of implementing Gaussian quantum networks, we will describe how to use them as a substrate to perform quantum communications.

5.6 Quantum teleportation Gaussian Networks

Quantum entanglement is a paramount resource for quantum information purposes. In particular, bipartite entanglement represents the fundamental requirement that a shared quantum channel should have in order to enable a truly quantum teleportation. In the framework of Quantum Communications, the networks previously described can be seen as distributed Gaussian *quantum teleportation networks* [163], where each pair of nodes can employ the pre-established quantum correlations together with *Local Operations* and *Classical Communications LOCC* to teleport a Gaussian quantum state from one node to the other.

In a naive strategy, the teleportation between two arbitrary nodes can be implemented simply by ignoring all the other nodes and exploiting the residual bipartite entanglement together with classical communications. This strategy is a direct extension of the standard teleportation protocol from two to more stations and is called *non-assisted* protocol [164].

Another set of strategies is based upon a cooperative behavior, where all the other nodes assist the teleportation between the chosen pair (Alice and Bob) by means of LOCC. In fact, if the external nodes perform suitable local measurements and then classically communicate

their outcomes to Bob, the latter can use this additional classical information to improve the process via modified conditional displacements. These strategies are called *assisted* protocols and are the ones that determine what we call networking/routing protocol in this chapter.

According to *Gu et al.* [154] quadrature measurement on a mode of a Gaussian network like the ones we considered so far can be described by two simple rules:

- *Vertex Removal:* a $\hat{Q}$-measurement on a qumode removes it from the network, along with all the edges that connect it.
- *Wire Shortening:* a $\hat{P}$-measurement on a qumode is just a $\hat{Q}$-measurement after a Fourier Transform, which corresponds to a phase rotation of $\pi/2$: $S_F = S_R(\theta = \frac{\pi}{2})$. The node will thus be removed but the phase shift will induce correlations between the neighbouring edges. Thus, measurements in the momentum basis allow us to effectively "shorten" linear graph states.

If two nodes A and B need to teleport a quantum state, they can be helped by the other nodes in the network who will perform these operations in order to increase the strength of the entanglement in the final pair. A typical measure of entanglement is the *negativity*

$$\mathcal{N} = -2\log_2 \nu_-, \tag{5.16}$$

where ν_- is the smallest symplectic eigenvalue of the partially transposed covariance matrix of the pair. Partial transposition is a necessary operation for the PPT criterion [165] and is easily implemented in Gaussian states by changing the sign of the momentum of one of the two subsystems. The negativity is simply connected to another measure of entanglement, which is the fidelity of teleporting a coherent state through that quantum channel

$$\mathcal{F}_{\text{coh}} = \frac{1}{1+\nu_-}. \tag{5.17}$$

Simple classical communication attains at most $\mathcal{F}_{\text{coh}} = \frac{1}{2}$ so a bipartite system presents truly quantum correlations only if $\mathcal{F}_{\text{coh}} > \frac{1}{2}$, or equivalently $\nu_- < 1$ and $\mathcal{N} > 0$.

The symplectic eigenvalues $\nu_\pm$ of a two-mode system can be computed through the invariants of the covariance matrix [166]. More specifically, we can define the *seralian* $\Delta = \det\sigma_A + \det\sigma_B + 2\det\sigma_{AB}$, where σ_A and σ_B are the local covariance matrices of the single-mode sub-systems A and B, and σ_{AB} represents their correlations. From this we can compute the symplectic eigenvalues as:

$$\nu_\pm^2 = \frac{\Delta \pm \sqrt{\Delta^2 - 4\det\sigma}}{2}. \tag{5.18}$$

In Fig. 5.9 we compare the effect of different regular topologies of quantum networks with the purpose of distributing entanglement between two of the furthest nodes inside the

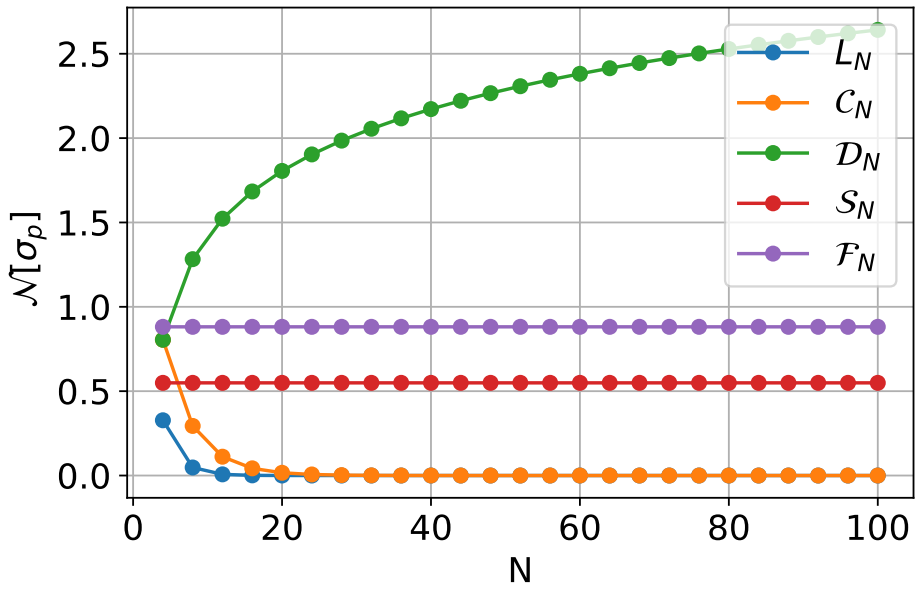


Figure 5.9: Negativity in the final two modes states after that all the other agents have locally measured their node for the regular topologies: linear $\mathcal{L}_N$, ring $\mathcal{R}_N$, star $\mathcal{S}_N$, diamond $\mathcal{D}_N$, full $\mathcal{F}_N$ networks up to $N = 100$ nodes.

network. The simplest cases are the *star* and *complete* networks. In the first case the best *assisted* strategy is to let everyone perform a $\hat{Q}$-measurement on their node except the central one who will make a *wire shortening* to link the final pair. In the complete network A and B are already linked by an edge so it is sufficient to measure the position in all the other qumodes (notice that this strategy outperforms the non-assisted protocol). In both these cases the entanglement is constant with the number of nodes in the network as we would expect, and the wire shortening of the central node in the star graph decreases the negativity with respect to the complete graph [167]. In the linear graph all the nodes have to wire shorten from A to B. Here the negativity quickly decreases with the number of nodes. The decrease of entanglement with the wire shortening seem to be typical in all configurations except the diamond graph, where all the central nodes are $\hat{P}$-measured.

5.7 Multi-path entanglement

5.7.1 Graphical Calculus

In ref. [153] it is provided a unified graphical calculus for all Gaussian pure states that is particularly suited for describing highly multimode Gaussian networks.

In this framework, a N mode Gaussian state is completely described, up to displacements,

by a $N \times N$ complex valued adjacency matrix:

$$Z = V + iU, \tag{5.19}$$

where the real and imaginary part of Z, V and U respectively, are related to the covariance matrix through the following unique decomposition

$$\sigma = \frac{1}{2}\begin{pmatrix} U^{-1} & U^{-1}V \\ VU^{-1} & U + VU^{-1}V \end{pmatrix}. \tag{5.20}$$

Gaussian graph states have a particular simple graphical representation, being

$$Z = A + iD, \tag{5.21}$$

where A is the weighted adjacency matrix of the graph and D is a diagonal matrix that represents momentum squeezing, i.e. for $D = 10^{-2s}\mathbb{1}$ the momentum variance of all modes is reduced by $2s\ dB$.

All symplectic operations can be reproduced in this language, however, since we already know how to represents the resource graph states, we only need to implement the quadrature measurements in $\hat{Q}$ and $\hat{P}$. We can express the state as

$$Z = \begin{pmatrix} t & R^T \\ R & W \end{pmatrix}, \tag{5.22}$$

where t is the target mode we want to measure, W is the subgraph of the untouched modes and R their correlations with the target mode. We have the following two rules:

- $Z \longrightarrow Z_Q = W$ after a $\hat{Q}$ measurement.
- $Z \longrightarrow Z_P = W - \frac{RR^T}{t}$ after a $\hat{P}$ measurement.

Thus, for a measurement in $\hat{Q}$ we remove the node and its link from the graph, whereas for a measurement in $\hat{P}$ we apply a $\pi/2$ phase rotation and then measure $\hat{Q}$.

5.7.2 Parallel enhancement of entanglement

The behaviour of the diamond graph is quite counter-intuitive and might be expected to increase the fidelity of quantum communications. It can be shown that the lowest symplectic eigenvalue for this system goes like

$$\left(\nu_-^{(\mathcal{D}_\mathcal{N})}\right)^2 = \frac{1}{1 + 2NRg^2}, \tag{5.23}$$

where $R = 10^{s/10}$ is the inverse of the squeezing in $\hat{P}$, with squeezing factor s in dB. Hence, the two modes become perfectly correlated in the limit of either infinite squeezing, infinite strength CZ-gate or infinite parallel measurements on $\hat{P}$.

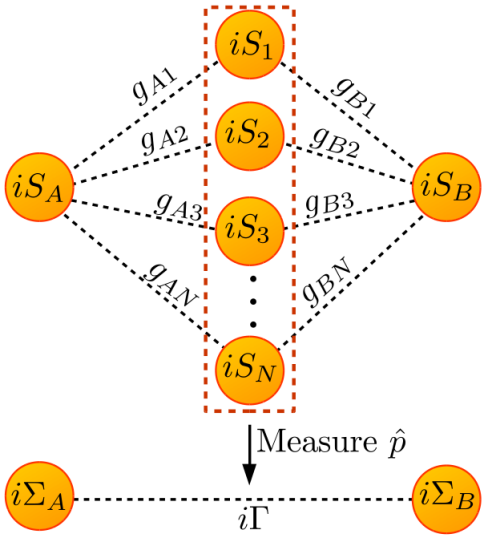


Figure 5.10: Graphical representation of the diamond graph and its parallel enhancement of entanglement.

We can use the rules described in the previous sections to prove Eq. 5.23, that expresses analytically the power of parallel enhancement of entanglement in the diamond network when measuring the central nodes in $\hat{P}$. Let us assume that the nodes A and B are squeezed by a factor S_A and S_B respectively, there are N central nodes and the kth mode has squeezing S_k and is correlated with A and B through a CZ-gate with strength g_{Ak} and g_{Bk}. It can then be easily showed that the final pair will have a purely imaginary adjacency matrix of the form

$$Z_{AB} = i \begin{pmatrix} \Sigma_A & \Gamma \\ \Gamma & \Sigma_B \end{pmatrix}, \tag{5.24}$$

where $\Sigma_A = S_A + \sum_k \frac{g_{Ak}^2}{S_k}$, $\Sigma_B = S_B + \sum_k \frac{g_{Bk}^2}{S_k}$ and $\Gamma = \sum_k \frac{g_{Ak} g_{Bk}}{S_k}$. These result can be derived by direct application of the rule for measuring $\hat{P}$ in the graphical calculus formalism, schematized in figure 5.10.

Employing Eq. 5.19 and 5.20 and noticing that $V = 0$, we can reconstruct the covariance matrix of the final pair:

$$\sigma_f = \begin{pmatrix} \frac{\Sigma_B}{\Sigma_A\Sigma_B - \Gamma^2} & -\frac{\Gamma}{\Sigma_A\Sigma_B - \Gamma^2} & 0 & 0 \\ -\frac{\Gamma}{\Sigma_A\Sigma_B - \Gamma^2} & \frac{\Sigma_A}{\Sigma_A\Sigma_B - \Gamma^2} & 0 & 0 \\ 0 & 0 & \Sigma_A & \Gamma \\ 0 & 0 & \Gamma & \Sigma_B \end{pmatrix}. \tag{5.25}$$

Notice that this state differs from a graph state up to a local phase.

By computing the seralian Δ of the partially transpose covariance matrix of the pair $\tilde{\sigma}_f$ and applying formula 5.18, we can derive the general lowest symplectic eigenvalue of the state

$$\nu_-^2 = \frac{(\sqrt{\Sigma_A\Sigma_B} - \Gamma)^2}{\Sigma_A\Sigma_B - \Gamma^2}. \tag{5.26}$$

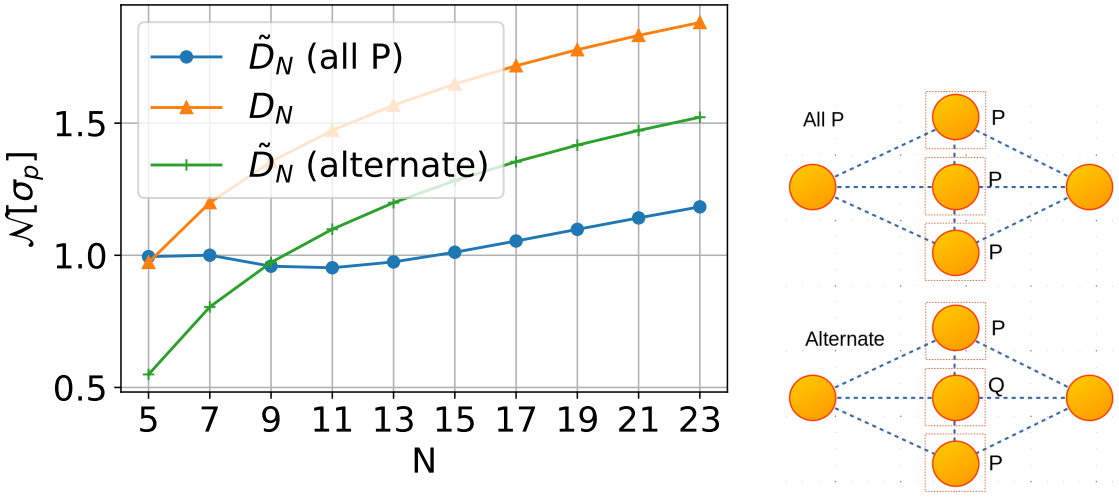


Figure 5.11: Different measurement strategies for two types of diamond network: the standard $\mathcal{D}_N$ we have seen so far and the $\tilde{\mathcal{D}}_N$, in which the central nodes are connected to their neighbors. We apply two different strategies to $\tilde{\mathcal{D}}_N$: one is to measure all the central nodes in P and the other is to alternate a P and a Q measurement. We can see that measuring always in P is not necessarily the optimal strategy. On the right side you can see a scheme of the $\tilde{\mathcal{D}}$ network and the two different measurement strategies.

Finally, if we assume that all the modes are equally squeezed in $\hat{P}$ of a factor $R^{-1} = 10^{2s}$ and all the CZ-gate correlations have a strength g, we arrive to formula 5.23.

This property of the Diamond network, however, is not easily generalized to all graphs that present parallel connections and the quest for the optimal measurement strategy in order to improve the final entanglement is by no means trivial. This is the case, for example, of the $\tilde{\mathcal{D}}$ graph shown in Fig. 5.11, generated by taking the diamond network and add a CZ-gate link between adjacent central nodes. We can see that for $N > 9$ measuring always $\hat{P}$ in this network is not the optimal strategy, whereas a better strategy is to alternate a $\hat{P}$ and $\hat{Q}$ measurement in order to restore a (smaller) diamond network.

Another important figure of merit is the entanglement per squeezing cost, shown in Fig. 5.12 (a). We see that the diamond is the only one that gives the a ratio of entanglement per cost of the network that becomes constant for large N. However, the linear graph is the one that links two nodes that are the furthest away from each other. Conversely, figure 5.12 (b) shows the negativity in the final pair divided by the number of modes in the initial state. Once again, the diamond structure is particularly convenient, yielding the highest negativity while keeping a constant number of independent squeezers.

In order to give a fair comparison between the capacity of the linear network to bridge distant nodes and that of the diamond to increase the final entanglement we need to generalize the diamond graph to a diamond chain graph, $\mathcal{DC}_{K,N}$, where K is the number of parallel branches linking the two hubs that want to perform quantum communications as in figure

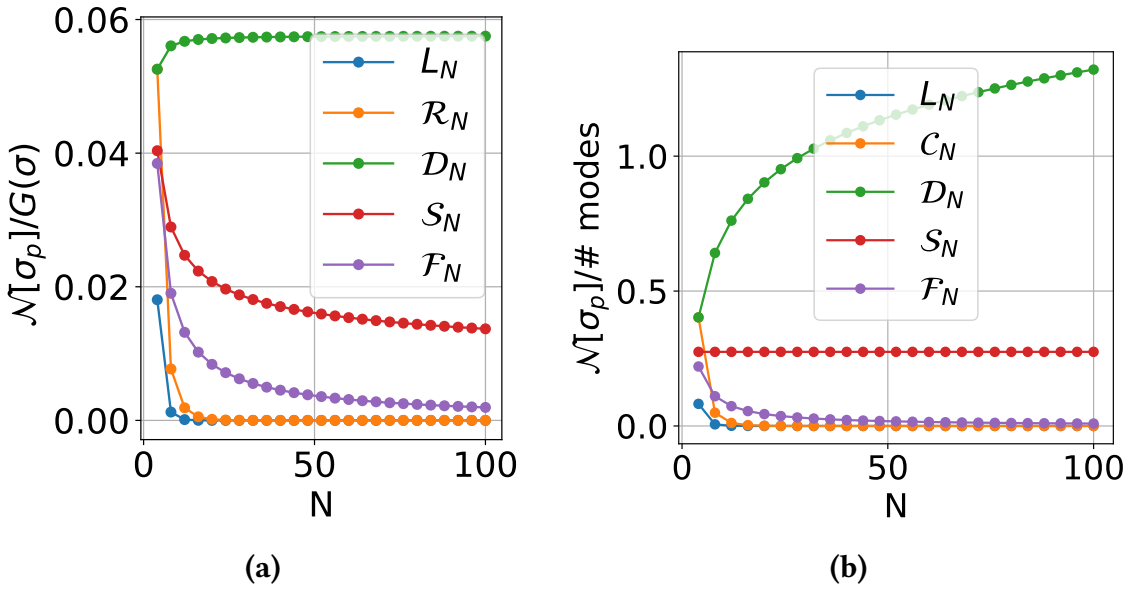


Figure 5.12: Trend of the ratio between the negativity of the final state and (a) the squeezing cost of the initial state or (b) the total numer of modes in the initial state for regular topologies: linear $\mathcal{L}_N$, ring $\mathcal{R}_N$, star $\mathcal{S}_N$, diamond $\mathcal{D}_N$, full $\mathcal{F}_N$ networks up to $N = 100$ nodes.

5.13 (c).

We can then compare the entanglement concentrated using multiple path strategies to link two nodes far away from each other. We can see in figure 5.13 (a) and (b) that the presence of parallel links has indeed the desired effect, despite the quality of the final pair, which still decreases exponentially with the distance. On the other hand, notice that the parallel links can help concentrating more entanglement until the system reaches a plateau and even the additional channels will not allow to increase the negativity. Moreover, the quality-price of this networks, specifically the ratio between the entanglement of the pair after the protocol and the squeezing cost before the protocol, is maximized by the linear graph.

Another important class of networks, notably for measurement based quantum computation, is constituted by grid cluster states that belong to graph shapes that allow for universal quantum computation [168]. Similarly to the diamond network, the presence of ancillary nodes between the emitter and the receiver can improve the quality of the quantum link with respect to the linear network. This, however, is not a general rule and sometimes the presence of additional links can be detrimental. This is the case of the triangular lattice, generated from the square lattice by adding a link between the nodes in the diagonal. There are two ways of generating the triangular and only one of the two decreases effectively the distance between Alice and Bob $\tilde{\mathcal{T}}$. In both cases the result is detrimental, however $\mathcal{T}$ is slightly better than $\tilde{\mathcal{T}}$, while the square lattice $\mathcal{Q}$ seems to be the most effective. This result is shown in figure 5.14.

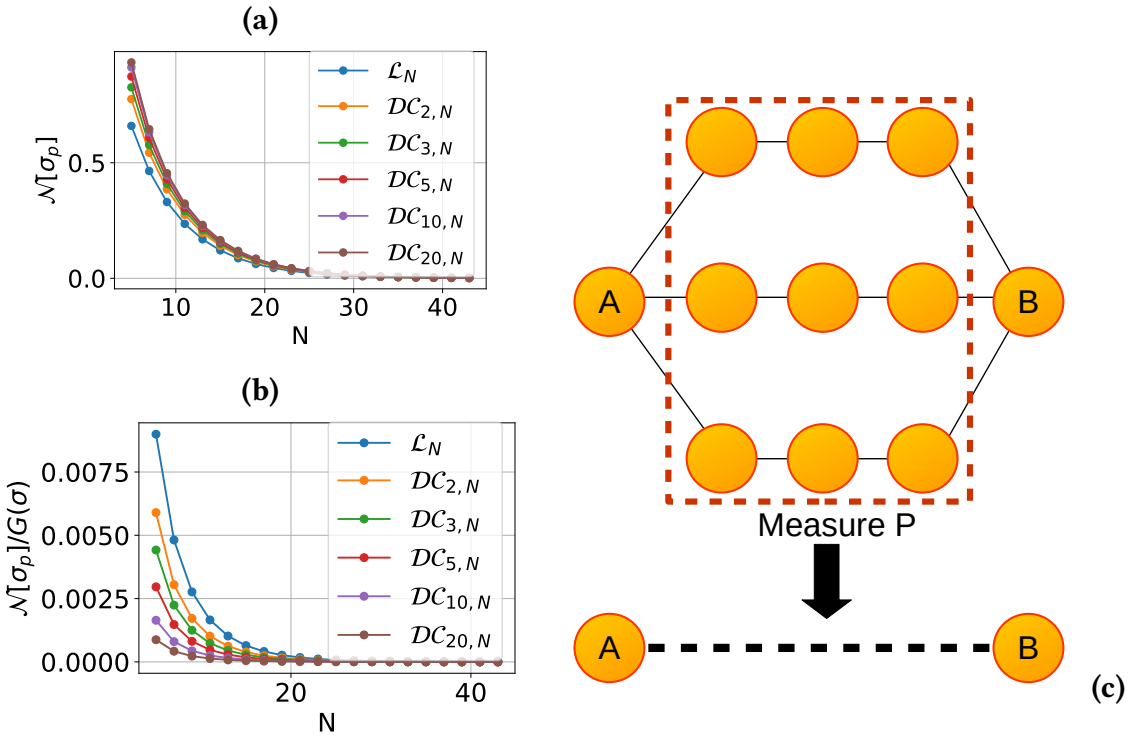


Figure 5.13: (a) Trend of the negativity of the output state for the diamond chain network, for various values of the number of branches K (K=1 is the linear network). (b) Trend of the ratio between the negativity of the final state and the squeezing cost of the initial state for the diamond chains. (c) Scheme of an entanglement routing protocol in a diamond chain with K=3. All the central nodes are measured in P in order to concentrate entanglement between Alice and Bob.

5.8 Routing protocol

In this section we aim at employing the abstract notions on Gaussian graphs developed so far for a specific application: the routing of entanglement. In this scenario, the highly multimode entangled Gaussian state corresponds to a distributed teleportation network, described in the previous section, where each node of the network is supplied with a mode of an electromagnetic harmonic oscillator and is linked to some other nodes in different geographical locations through quadrature correlations, e.g. quantum entanglement. We remark that this type of communication quantum networks is inherently different from the typical qubit networks that are currently being deployed in different metropolitan areas [19]. In those cases, for example, each entanglement link is pairwise between two qubits and as a consequence each node of the network will have to receive, store and measure as many quantum states as neighbors it has. Conversely, in a Gaussian quantum network the same qumode can be entangled with an arbitrary number of other nodes. Moreover, the production of such states, their manipulation to increase the entanglement among two nodes and their measurement to perform quantum teleportation can be achieved deter-

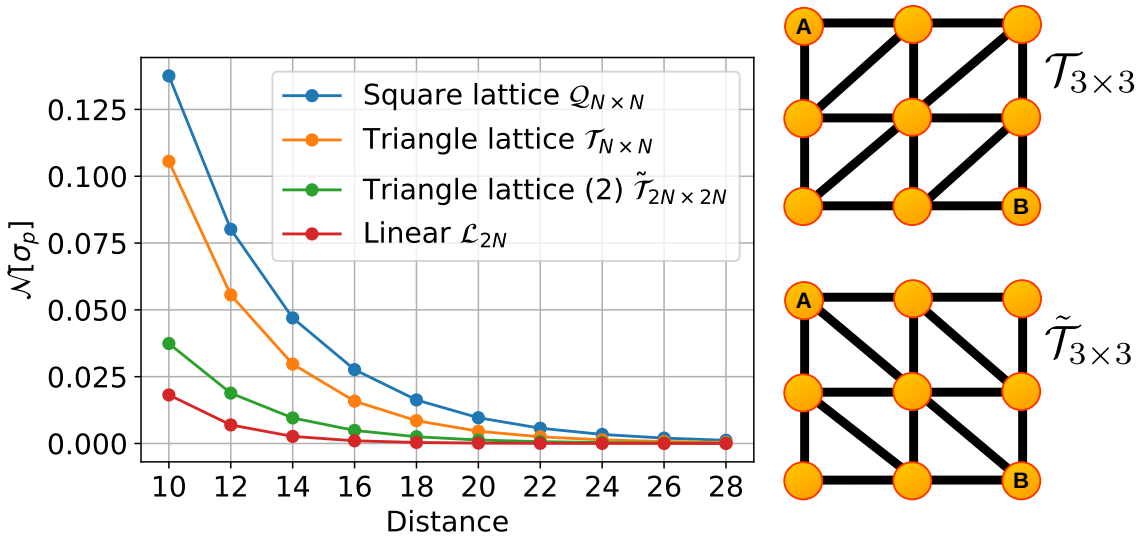


Figure 5.14: Comparison between the entanglement capacity between two nodes at the same distance of three lattices graphs, the square lattice $\mathcal{Q}_{N\times N}$ and the two triangles $\mathcal{T}_{N\times N}$, formed from the square by adding edges on the diagonals in such a way that the distance between A and B is the same, $\tilde{\mathcal{T}}_{N\times N}$ formed by adding edges to the diagonals so that the distance is the same as the linear graph, and the linear graph $\mathcal{L}_N$. In order to compare the networks with the same distance we doubled the size of the $\tilde{\mathcal{T}}$ and the $\mathcal{L}$ graphs.

ministically, unlike the discrete variables case. Nonetheless, qubits networks have been extensively studied over the last years, whereas Gaussian teleportation networks is a very recent emerging field. Our purpose is, thus, not to prove the superiority of the latter, but rather to explore its properties and the differences from the DV schemes in order to get the best of both worlds.

The results of the previous sections highlighted some outstanding properties of Gaussian networks. The most important is the parallel enhancement of entanglement in the diamond graph. If properly used, this feature can most certainly improve the routing of entanglement in regular and complex shaped network. On these grounds, the search for an optimal protocol that exploits all the qualities of these Gaussian networks is very desirable yet arduous, and will be subject of future investigations. Alternatively, we present a naive entanglement routing protocol that takes into account some of these properties and we will apply it to complex topologies, to show that the enhancement of the entanglement with respect to the trivial protocol is, in principle, easily achievable. Imagine we have a distributed network of entangled harmonic oscillators, where each node is honest and can perform classical communication and local homodyne measurement, and we want to establish an entangled pair between two nodes, Alice and Bob, that want to teleport a quantum state or perform QKD. The trivial protocol would be to find the shortest path between them and measure in P all the qumodes along this path and in Q all the others. A careful look at the inner structure of the network, however, might help us increase the strength of the correlation. For example if at any point, two nodes on the path are linked by multiple parallel routes, we can measure

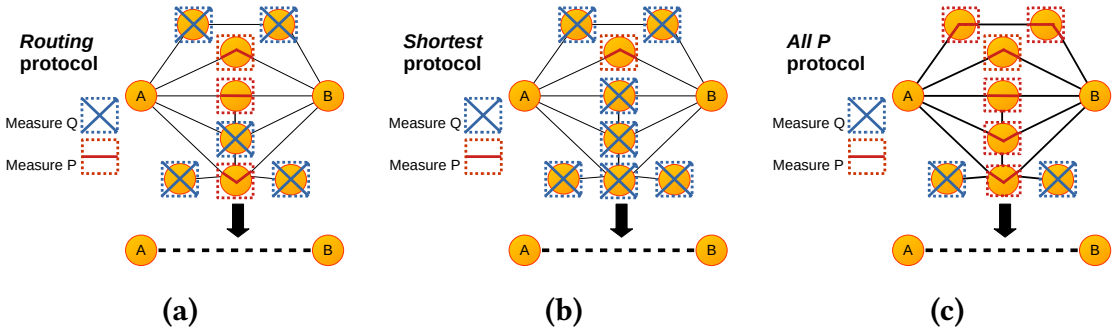


Figure 5.15: Scheme of the three protocols for the entanglement distribution: (a) the *Routing* protocol takes a list of the shortest paths connecting A and B and measures in P those that increase the negativity while the rest is measured in Q; (b) the *Shortest* protocol only consider one of the shortest paths to be measured in P and the rest in measured in Q; (c) the *All P* measures the nodes with only one connection in Q and all the rest in P.

these in P to exploit the parallel enhancement.

In order to show this in practice, we will test the performances of three different routing protocols (shown in figure 5.15 on various complex networks) with the purpose of establishing a highly entangled pair. We choose Alice to be one of the hubs of the graph and evaluate the efficiency of the protocol in delivering entanglement to all the other nodes. The quantum protocol that we propose to exploit the parallel enhancement of entanglement will be simply called *Routing*.

- *Routing*: it takes as input the target node, Bob, lists all the shortest paths connecting it to Alice and measures all the nodes that are not in these paths in the Q quadrature, so that they will not influence the protocol. Among the list of paths it checks one by one those to be measured in P in order to maximize the negativity $\mathcal{N}$ of the final pair, while the rest will be measured in Q.

In the *Routing* protocol, in principle, we could have considered as well parallel paths of longer lengths that might have contributed to improve the negativity. However, in practice it had the only effect of slowing down the performances while not increasing the entanglement for all the cases we considered. The effect of the parallel paths can be appreciated when comparing the negativity produced by *Routing* with that produced by *Shortest*.

- *Shortest*: the difference of the latter is that it only exploits one of the shortest parallel paths, directly measuring everything else in Q.

In some cases the two protocols do not give a substantial difference, either because there are not parallel routes or because these do not help increasing the entanglement, however in many instances the effects of parallel routing are significant. The last protocol we compare with is *All P*.

- *All P*: it measures all the terminal nodes with degree 1 in Q and the rest in P.

This protocol is less effective than the first two but is always the quickest, whereas *Routing* can be computationally very slow on regular networks, which are characterized by long distances and many parallel paths, but becomes very efficient on complex sparse networks.

One instance of this program is given in figure 5.16 that shows the negativity provided by the three different protocols for each node of a $\mathcal{G}_{AS}(N = 1000)$ network. At the beginning of the protocol, we pick Alice as the node, or one of the nodes, with the highest degree. The nodes are then sorted by their distance from Alice and, for the same distance, by the number of all the shortest paths connecting them to Alice. Additionally, the grey column represents the ratio of parallel paths that were useful to increase the entanglement. Notice that nodes at distance 1 cannot show a difference between the *Routing* and the *Shortest* protocols, however many nodes at distance 2 present a greater negativity than those at shorter distance after the *Routing*. This non-trivial effect of improving a channel capacity at larger distances has no classical equivalent.

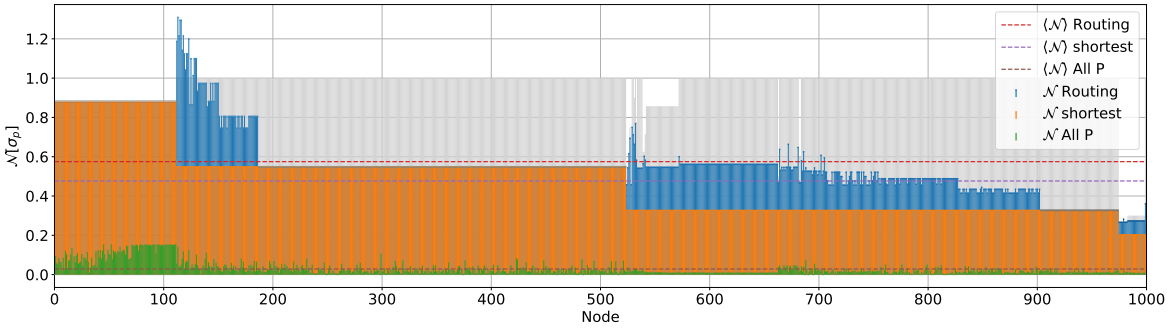


Figure 5.16: Negativity produced by the three different protocols applied to each node of the the $\mathcal{G}_{AS}(N = 1000)$ network. The nodes are labeled in order of distance and of number of paths connecting to Alice. The blue, orange and green stems represent the negativity of the final pair after the *Routing*, *Shortest* and *All P* protocols respectively, while the dashed lines represent the mean value for all the nodes. The color of the marker indicates the distance of the node from A and the grey columns represent the ratio of paths that improved the entanglement in *Routing*. We invite the reader to zoom in the figures in electronic version to appreciate all the details.

In figure 5.17 we show the graph of the network, where the nodes are again sorted by distance and number of parallel paths and the size of each node is proportional to its degree. In this figure Alice is '0' and has a thick red contour. The node with highest negativity and all the paths that improved its entanglement are highlighted with red thick lines.

The same analysis was done in several networks with different sizes and topologies with very different results that we report in figures 5.18, 5.19, 5.20 and 5.21. A property that is not apparent in Fig. 5.17, is that the node with the highest enhancement of entanglement due to the multiple paths is not necessarily the one with the highest negativity in absolute. This is the case of the ER network of Fig. 5.18, in which the node with the highest entanglement, highlighted in green in the graph representation, is at distance 1 while the node with the highest difference in negativity between the *Routing* and the *Shortest* protocols, high-

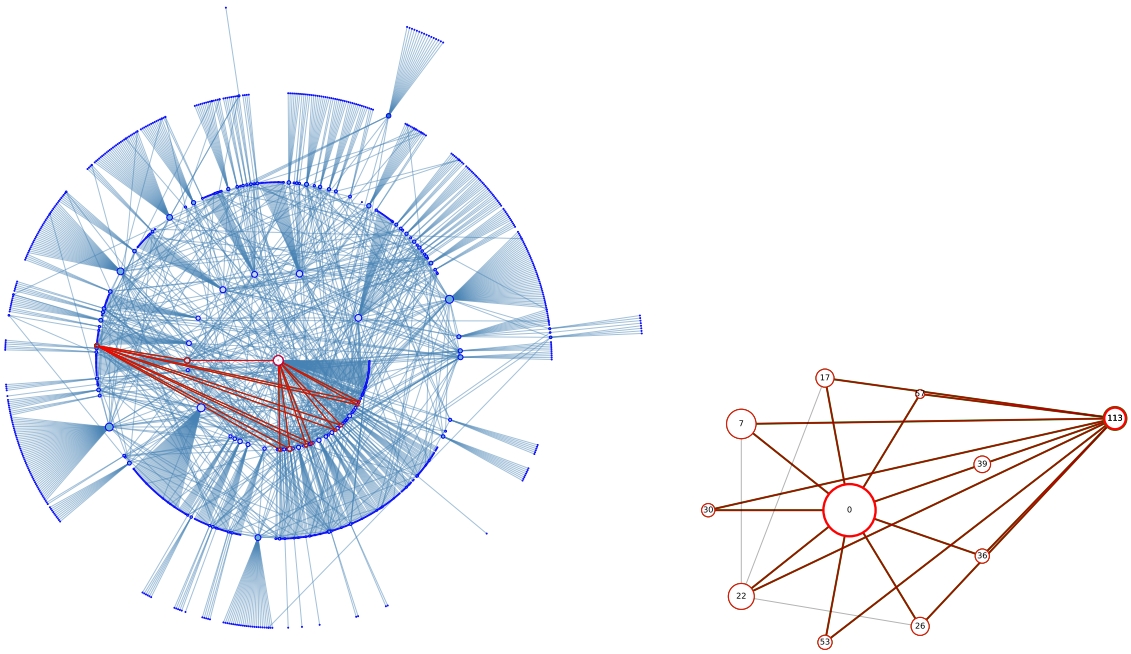


Figure 5.17: Scheme of the $\mathcal{G}_{AS}(N = 1000)$ network on which we performed the protocol and subgraph of the paths connecting to the node with highest negativity. The nodes are set in circles according to their distance from Alice and their size is proportional to the degree. We invite the reader to zoom in the figures in electronic version to appreciate all the details.

lighted in red, is at distance 3. In this case, the structure of the subgraph used throughout the *Routing* is not a diamond chain and the intercorrelations among the parallel branches have limited the increase of the entanglement,as for the $\tilde{\mathcal{D}}_N$ network in Fig. 5.11. In any case, in this network the nodes at greater distances are the ones that are most affected by our protocol and, although in some cases many parallel paths have been disregarded, as shown by the height of the grey column, all the nodes at distance 4 received a substantial enhancement.

The results of the simulation on the BA topology of Fig. 5.19 are similar to the AS, although the first only reaches a distance of 3. The nodes with the highest absolute negativity and the highest negativity difference produced by the *Routing* protocol coincide and are at distance 2 from Alice, whereas this time its subgraph is a diamond with no interconnections. Also in this case distance 2 is favorable to perform quantum communications.

The WS structure of Fig. 5.20, on the other hand, is the worst to apply the *Routing protocol*. Only a few nodes, in fact, were poorly enhanced and mostly at large distances, while the negativity averaged over all the nodes for *Routing* and *Shortest* is comparable. The node 44 at distance 3 is the one that received the greatest boost from our protocol, whereas node 1 (like all the other nodes at distance 1) has the highest negativity.

Finally, the biological network of Fig. 5.21 produced the most interesting results. Once again, many nodes at distance 2 end up having more negativity than those at distance 1, and at this distance the nodes with the same degree have the same negativity that decreases exponentially with their degree. The nodes with highest negativity and highest difference coincide with node 139, which is linked to Alice through 33 intermediate nodes, forming a diamond network with no interconnections.

5.9 Discussion

We have studied Gaussian multimode quantum networks with regular and complex topologies for quantum communication protocols. In particular: i) we have studied their cost in terms of amount of squeezing and number of necessary squeezed modes to build the network; ii) we have established a multi-path routing protocol distributing entanglement between two arbitrary nodes. In details:

- We have shown that the cost of the networks is not always linear with the number of edges and nodes and there are particular (regular and complex) graph shapes that optimize the cost and the number of squeezers over number of nodes/edges in the networks. Among regular networks the diamond and the star graphs need only two squeezed nodes to be built, independently from their number of nodes. Among the complex networks shapes, the Internet Autonomous System model is the most convenient in number of needed squeezed states.
- We have studied the assisted teleportation protocol in Gaussian entangled networks, where a couple of nodes are assisted in the teleportation by local measurements in all the other nodes. This naturally defines a routing protocol in Gaussian networks. In particular we have considered Q and P homodyne quadrature measurements that allow respectively for vertex-removal and wire-shortening.
- The routing is optimized by different measurement schemes in regular networks. In the linear and the diamond networks the best strategy consists in the wire shortening, but the diamond network shows the largest ratio in reached entanglement over cost.
- Inspired by the behaviour of the diamond network we have devised a routing protocol that exploits wire shortening in parallels paths and we have applied it to complex networks graphs. The protocol named *Routing* is compared with *Shortest*, where wire shortening is done only in the shortest path, and *All P*, which removes all the terminal nodes while it wire-shorten all the others. In most cases, the *Routing* improves the entanglement compared with *Shortest.* Also, in terms of computational complexity, the *Routing* is much slower than *All P* in regular networks, where there are long distances between nodes and several parallel paths, but it is very efficient in complex sparse networks.

The devised *Routing* protocol is very general so that it can be applied to arbitrary networks,

and it is particularly efficient for sparse not regular networks. Our simple graph exploration approach would be improved in computational efficiency by real graph-based algorithms, especially if we allow for approximate solutions. Also it would be interesting to allow for non uniform distributions of squeezing s and CZ gate strength g or more general homodyne measurements, i.e. going beyond the two P and Q cases and considering measurements along $Q_\theta = \cos(\theta)Q + \sin(\theta)P$. In addition, it could be interesting to examine a scenario in which the intermediate nodes are dishonest and do not cooperate to perform the routing. Moreover, in order to consider practical implementations, realistic parameters for losses and noise should be included in the model. Finally the routing protocol has been implemented to solve the particular task of creating a perfect EPR pair between two nodes; future protocols will consider general reshaping in arbitrary multiparty states.

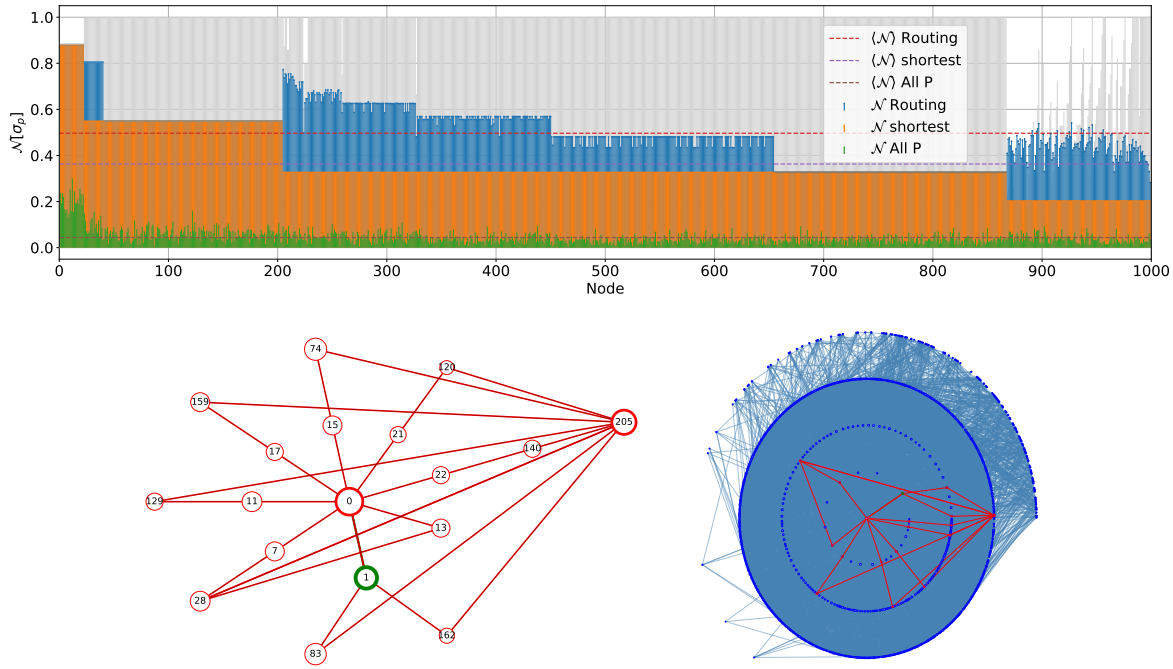


Figure 5.18: Negativity produced by the three different protocols applied to each node of the the $\mathcal{G}_{ER}(N = 1000, p = 0.4)$ network.

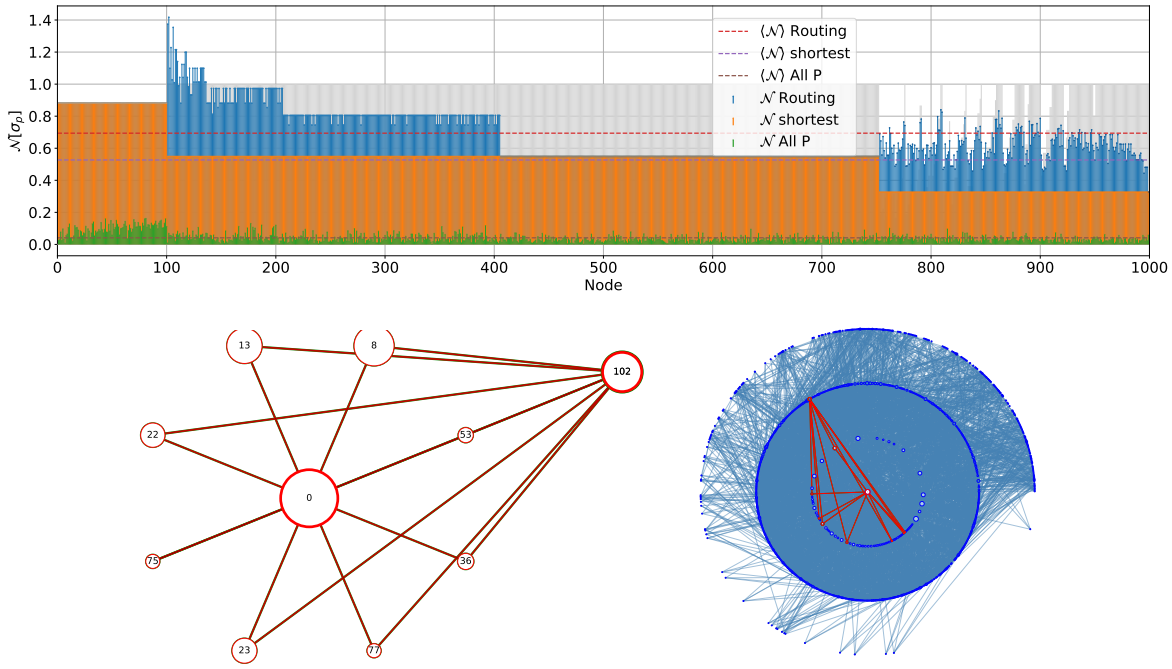


Figure 5.19: Negativity produced by the three different protocols applied to each node of the the $\mathcal{G}_{ER}(N = 1000, p = 0.4)$ network.

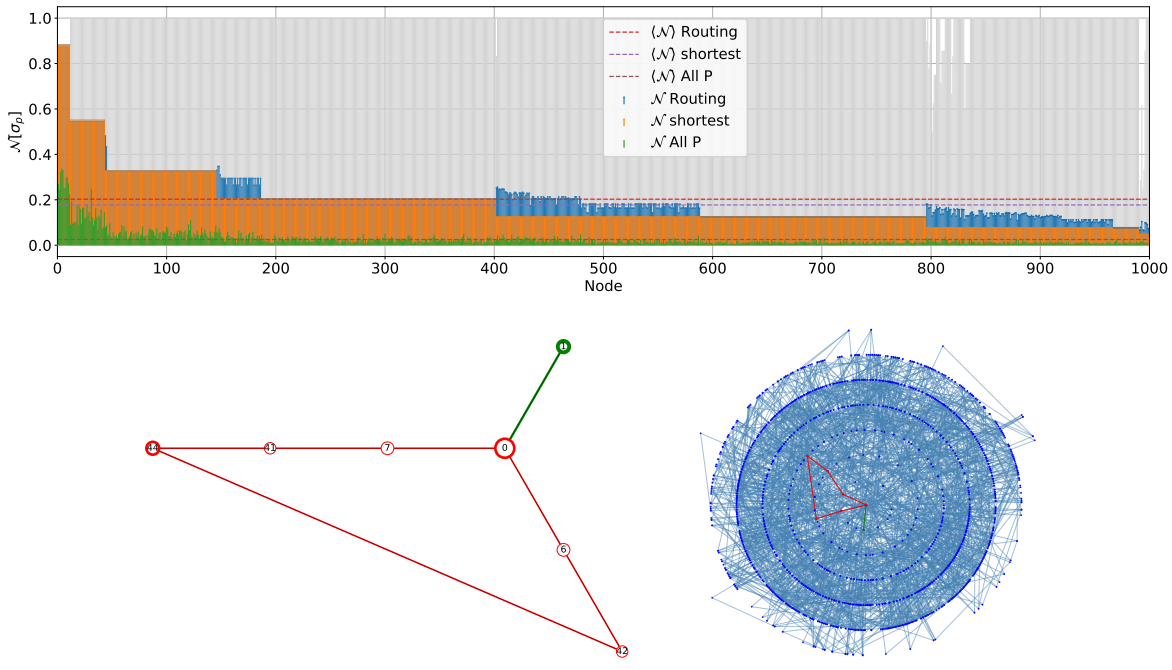


Figure 5.20: Negativity produced by the three different protocols applied to each node of the the $\mathcal{G}_{ER}(N = 1000, p = 0.4)$ network.

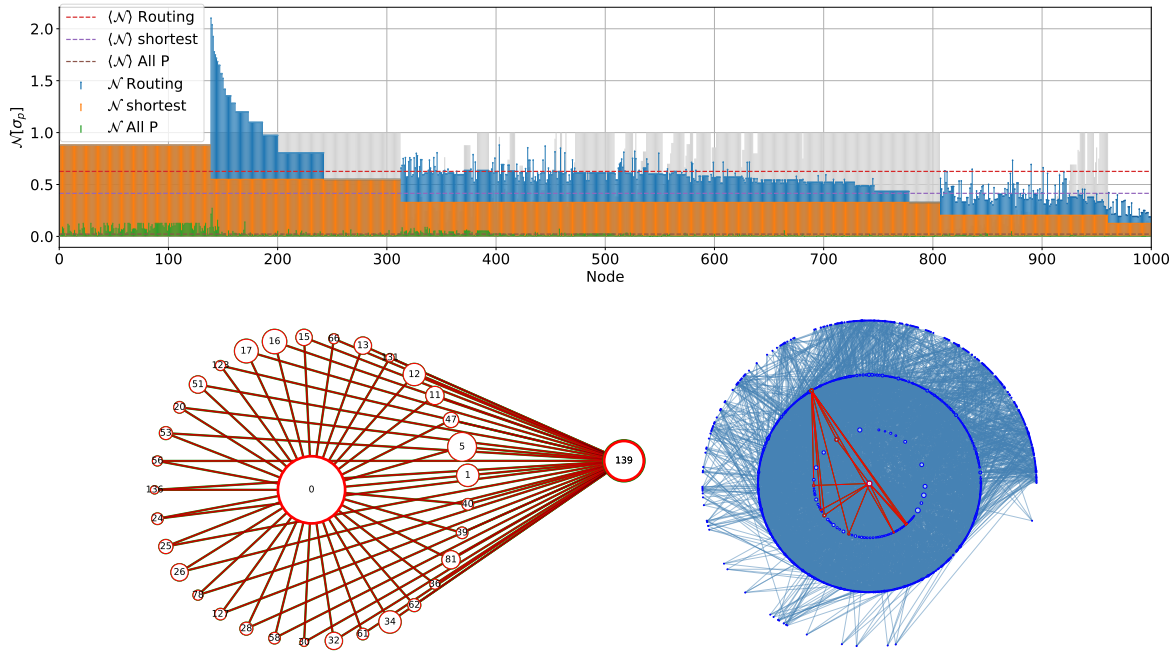


Figure 5.21: Negativity produced by the three different protocols applied to each node of the the $\mathcal{G}_{ER}(N = 1000, p = 0.4)$ network.

Conclusions and Perspectives

This thesis focused on the investigation of selected techniques from quantum optics and their applications to quantum information processing and beyond, with a special regard to their impact on the future quantum internet. The availability of concrete technological resources and the possibility to compare our findings with experiments in realistic scenarios have been the Ariadne's thread guiding our theoretical inquiry through a vast maze of abstract research. In addition, the applicability in the short or mid term of our research in contexts of societal value has been a vital motivation to the pursuit of our studies. Above all, the unsustainable footprint of civilization has become a matter of major concern for a large part of the population. Recent studies [169] estimated that by 2025, Internet and all the Information and Communication Technology industry in general, might use 20% of all electricity generated and emit up to 5.5% of the world's carbon emissions. That amounts to more than the total emissions of many countries, such as US, China and India. As a consequence the improvement of the efficiency of communication and computation promised by quantum technologies could play a crucial role to face the challenge placed by the energetic emergency. Moreover, the progress of photonic technologies offers an alternative way to boost the performances of supercomputers even in the classical paradigm. Nonetheless, throughout this thesis we explored topics that divert from purely applied science, examining some fundamental aspects of computer science and quantum theory, e.g. the effects of topology and measurement on networks of quantum harmonic oscillators.

The first part of the thesis was devoted to the introduction of some preliminary notions and concepts necessary to grasp the main results presented in the second part, that revolved around advanced topics in quantum optics and computer science. In particular, in chapter 1 we described some of the most common quantum states encountered in quantum optics, we showed their theoretical representation and discussed their experimental production. We stressed the difference between the Discrete and Continuous Variables formalisms, revealed their advantages and drawbacks and displayed how to address them operationally. In chapter 2 we introduced the concept of algorithmic complexity and used it to classify protocols based on their efficiency. We presented as well some recent results in the theory of NP completeness, Interactive Proof systems and complex networks.

The second part of this thesis contains the original contributions produced during the doctorate. The works are presented as three different stages of complexity of quantum internet, ranging from a simple connection among two distant nodes, to a regular star-shaped network with an arbitrary number of users, to general complex quantum networks of any shape and dimension. For each of these stages we provide a description of the architecture, the scenario and the physical requirements to implement it, as well as an innovative protocol that can serve for quantum communication purposes in that stage. The actual implications of these results, however, transcend the field of quantum communications and further studies will be necessary in order to fully seize their potentialities.

In chapter 3 we introduced the first of these stages, where we illustrated the results and methodology presented in the paper [170]. In this work we experimentally implemented a Quantum Merlin Arthur Interactive Proof system with linear optics, demonstrating a protocol in which a simple agent can efficiently verify the solution to an NP-complete problem, supplied by the untrusted Merlin, having access to only a fraction of the whole proof. Assuming the exponential time hypothesis, we rigorously proved that in order to perform the same task without quantum resources it would take an exponential time in the input size of the problem. As a consequence, we demonstrated experimentally for the first time a computational quantum advantage in the interactive setting. This type of quantum advantage, unlike the standard proposals of computational advantage, can be certified straightforwardly, requires a number of optical elements that are easily found in most well-equipped photonic laboratories and that is constant in the size of the problem and might bring us a step closer to interesting applications. Although this work is an experimental implementation, the theoretical contribution was fundamental to its development. In fact, the original scheme proposed in [110] could not be implemented with current technology and the necessary simplifications required to rethink the protocol from scratches.

A crucial limit to the applicability of this protocol is the presence of the unentanglement hypothesis, namely the fact that the quantum proofs provided by Merlin need to be isolated separable states, otherwise the completeness and soundness of the verification procedure cannot be guaranteed in a dishonest scenario. It should be noted, however, that coherent states cannot be entangled, thus the only way to induce quantum correlations among the different parts of the proof is to deviate from the coherent regime, for example by adding squeezing. Such deviations, though, would be detected by Arthur during the protocol and it is thus not clear whether the presence of entanglement actually invalidates the correctness of the protocol. An interesting prosecution of this work could be to investigate if the unentanglement promise is indeed not necessary, which would make the verification protocol applicable in a more general cryptographic scenario. Furthermore, as pointed out in [171], the existence of a test that can efficiently distinguish between a product of n quantum states and states which are far from product, given only one copy of the state, is an open question that has many interesting implications in quantum information and computer science. Our work could thus provide an advance in this direction as well.

The second stage of the quantum internet is displayed in chapter 4, where we discussed the results shown in [172]. In this work, we present a quantum photonic architecture that is capable to implement a secure voting system in the presence of realistic noisy conditions and dishonest agents, without requiring a centralized authority that governs the elections or computes the tally. This highly desirable functionality has received the attention of a large part of the classical and quantum community, with many interesting proposals. All of those, however, suffered from some major security flaws when applied to realistic scenarios, or had theoretical requirements out of reach for our current technological disposals. In order to devise a protocol that could guarantee security also in a non-ideal scenario it was necessary to drop the notions of perfect correctness and privacy and define approximate

versions of these properties, in such a way that the probability of fulfilling the properties was directly linked to some measurable experimental parameters.

Although this is a theoretical protocol and the implementation for an actual election might require severe modifications to circumvent the need of a large multipartite entangled state, an experimental execution for a small number of voters can be readily performed with state-of-art photonics. The main challenges to this purpose would be the generation and distribution of a high fidelity GHZ state, with a high production rate. Realistically, a proof-of-principle experiment would require a 4 particles GHZ state with a fidelity larger than 0.9. Further investigations and modifications to the scheme could reduce these requirements. Single photon memories with long enough storage times, in order to allow the complete distribution and the announcement of the verification or voting subroutines, might be another bottleneck for the scaling of the protocol and it could be interesting to devise a prepare-and-measure version that could avoid this problem. Finally, the same scheme could be employed to perform anonymous multipartite computation and there are many other important functionalities that could be based on electronic voting, e.g. byzantine agreement.

The last stage of quantum internet is examined in chapter 5, that reports the results of [173]. We revised the CV formalism and used it to describe Gaussian graph states that will be employed as quantum communication networks. We analyzed the scaling of the squeezing cost and number of squeezers required to implement a selection of regular and complex topologies, showing that building certain structures is more convenient than others. We discovered an interesting feature of CV quantum networks, namely the parallel enhancement of entanglement, that allows to increase the quantum correlations among two nodes of the network by exploiting the measurement of their multiple connections. This allowed to devise a routing protocol to distribute entanglement among two arbitrary nodes of the networks, that shown to be particularly effective for sparse complex networks. We benchmarked this protocol against a simpler scheme that only considers one of the links among the nodes, showing the superiority of the first in many cases, especially for nodes at large distances.

The field of CV quantum networks is largely unexplored and offers a wide range of lines of research. A possible extension of our model could include the effect of general homodyne measurements, with arbitrary phases among the quadratures. This would allow the possibility to train a gradient descent algorithm to find the optimal angle to measure sets of nodes given the global structure. In particular, the existence of an optimal measurement strategy that only depends on the local details of each node, e.g. position and connections, would be particularly appealing for applications. Another possibility might be to endow the nodes with local non-gaussian measurements, that in certain cases could boost the performance of the routing.

Appendix A

Quantum batteries

A.1 Why we need a quantum battery . . . 144
A.2 The system and charging cycle . . . 145
A.2.1 The open dynamics of the quantum battery . . . 147
A.2.2 Energetic considerations . . . 148
A.2.3 Efficient charging process . . . 150
A.2.4 Assessment of charging power and temporal considerations 151
A.3 Closed-system dynamics . . . 154
A.3.1 Channel picture . . . 154
A.3.2 Continuous time evolution . . . 155
A.4 Multimode system . . . 157
A.5 Discussion . . . 157

In this appendix we study a topic that slips away from the main context of this thesis, namely quantum communication networks, however we hope that a curious reader may find it intriguing. Although the applications proposed for this study may differ a lot from those proposed in the previous chapters, the physical system under exam is once again a multimode CV quantum state undergoing a Gaussian evolution, to which the theory developed in chapter 1 applies perfectly. Specifically, we present a scheme for the charging of a quantum battery based on the dynamics of an open quantum system undergoing coherent quantum squeezing and affected by an incoherent squeezed thermal bath. We show that quantum coherence, as instigated by the application of coherent squeezing, are key in the determination of the performance of the charging process, which is efficiency-enhanced at low environmental temperature and under a strong squeezed driving.

A.1 Why we need a quantum battery

Quantum physics proved to have an edge for outstanding applications in computation and cryptography. Whether quantum technologies can help us facing the forthcoming energetic crisis remains however an open question. The efficient storage and distribution of energy far from its production centers is rapidly becoming one of the economic market drivers and a key technological challenge for the grounding of a sustainable green powered society. Batteries have consequently become a vital technology in modern society and many efforts are being dedicated to improving their performances in terms of capacity, energy density, power and life-time [174]. The boost of nanotechnologies has made the miniaturization of these "work reservoirs" a primary matter. As the size of these devices approaches the sub-molecular scale, it becomes reasonable – and indeed appropriate – to formulate a quantum mechanical description of their working principles. One of the core questions in this regard is whether non-classical effects can play a useful role in the improvement of the capabilities of energy-storing systems. This has triggered the drawing of theoretical models able to characterize and quantify quantum advantages in terms of non-equilibrium thermodynamical quantities [175].

Interesting case-studies of quantum batteries leveraging on discrete [176]–[178] and continuous [179] degrees of freedom have been put forward. Needless to say, limiting the study to a unitary charging process severely reduces the application of the models to realistic scenarios. Moreover, the analysis of quantum batteries in the context of open quantum systems may provide additional ways to improve the potentialities of the batteries. In Ref. [180] it was proven for instance that a squeezed thermal reservoir can improve the power and efficiency of a quantum heat engine. Quantum squeezing, which is the effect of reducing the variance of one quadrature below the uncertainty of the vacuum state, has found many applications in many domains, from quantum optics to quantum technologies [43] and grants the possibility of increasing the energy of a bosonic Gaussian system while keeping a null mean value of the fields.

In this work we study the effects of squeezing, both as a coherent charging potential and

as an incoherent squeezed bath, in the charging of a battery initially prepared in a vacuum state. Our findings reveal that both forms of squeezing efficiently charge the quantum battery, however their simultaneous usage requires to accurately tune the parameters of the potential and the bath in order to enhance the performance of the system and avoid that their effects cancel out.

The remainder of the chapter is organized as follows: in Sec. A.2 we introduce the notation, formalize the description of the system and characterize the charging scheme; in Sec. A.2.1 we give details on the open dynamics in terms of its master equation describing the evolution of the system coupled to the environment; in Sec. A.2.2 we discuss the thermodynamic quantities of interest and the operational way to measure them, while Sec. A.2.3 is dedicated to the simulation of the charging cycle. We identify the range of parameters of the Hamiltonian and the bath that allow for an improvement of the efficiency of the battery. Finally in Sec. A.2.4 we bound the quantum speed limit of the charging process to compute the power of the storage device. The investigation reported in this chapter sheds some light on the role that the quantum coherences enforced by the use of squeezing have in the charging process of a quantum battery, thus taking the investigation on the potential quantum advantage for the management of energy-storing devices a step closer to a full grasp.

A.2 The system and charging cycle

In what follows, we consider the battery as a single-mode harmonic oscillator that is initially prepared in a thermal state. Such initial state is *completely passive*, meaning that it is impossible to extract useful work from it through unitaries. Completely passive states can also be found in literature as Gibbs states or KMS states [181].

We shall consider a fully Gaussian framework where the state of the battery evolves according to a quadratic Hamiltonian in the quadrature operators $\hat{x} = \hat{a}^\dagger + \hat{a}$ and $\hat{p} = i(\hat{a}^\dagger - \hat{a})$ [25], [182]. Since the system is Gaussian, we can translate its description in the phase space: its first moments $\langle \hat{r} \rangle = 0$, and its covariance matrix is $\sigma_{ij} = \langle \{r_i, r_j\} \rangle$, with $\hat{r} = (\hat{x}, \hat{p})^T$.We will consider a thermal state whose first moments are null $\bar{x}_\tau = \langle \hat{x} \rangle_\tau = \bar{p}_\tau = \langle \hat{p} \rangle_\tau = 0$, whereas the covariance matrix of second moments is $\sigma_\tau = \coth(\beta\mu/2)\mathbb{1}$ with β the inverse temperature of the system and $\mu = \hbar\omega$, where ω is the frequency of the oscillator. The thermal factor $\coth(\beta\mu/2)$ is linked to the average number of excitation in the bath as $N = \frac{1}{2}\left[\coth(\beta\mu/2) - 1\right] = (e^{\beta\mu} - 1)^{-1}$.

First, we aim at implementing a charging operation for a completely passive state ρ_a prepared by letting the battery thermalize with a reservoir at inverse temperature β_A, whose density matrix can be described by $\rho_A = e^{-\beta_A H_0}/Z_A$. The covariance matrix associated to ρ_A is $\sigma_A = \mathbb{1}(1 + 2N_A)$, where N_A is the number of excitations within the thermal bath.

The stroke AB is used to charge the battery. In this stroke, the Hamiltonian of the system is modified by the presence of a charging potential as (from this point on, we assume units

such that $\hbar = 1$)

$$\hat{H}_{AB} = \hat{H}_0 + \hat{V}_c(t), \tag{A.1}$$

where $\hat{H}_0 = \mu(\hat{x}^2 + \hat{p}^2)/2$ is the Hamiltonian of the oscillator and the charging potential takes the form

$$\hat{V}_c(t) = -\frac{\lambda}{2}\Sigma(\tau_A, \tau_B)(\hat{x}\hat{p} + \hat{p}\hat{x}) \tag{A.2}$$

with $\Sigma(\tau_A, \tau_B) = \Theta(t - \tau_A)\Theta(\tau_B - t)$ resulting from the composition of two Heaviside step functions, $\Theta(t - \tau_A)$ and $\Theta(\tau_B - t)$ with $\tau_B > \tau_A$, so as to result in a constant in the interval $\tau_{AB} = [\tau_A, \tau_B]$. The charging potential is thus a constant parametric potential of strength λ within τ_{AB}, and is null otherwise.

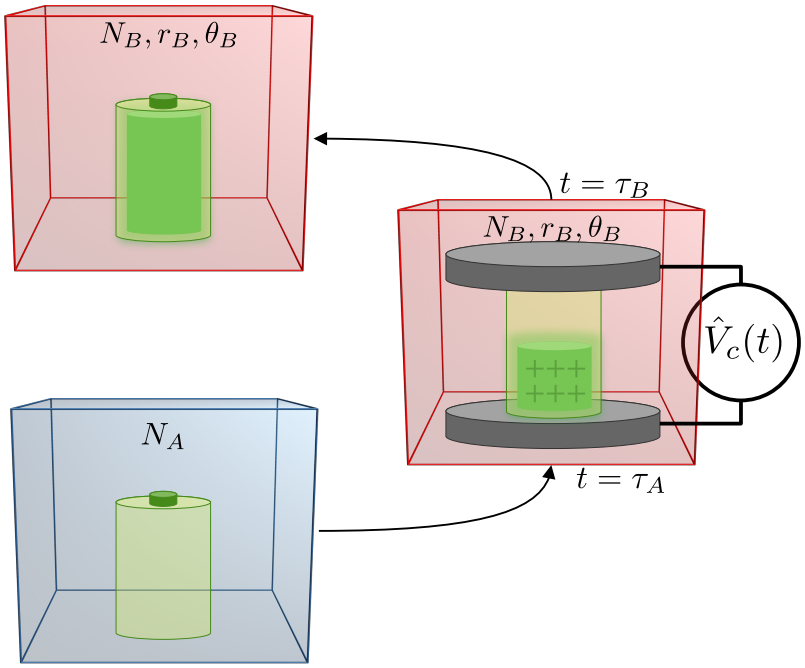


Figure A.1: Scheme of the charging process proposed in this work. Firstly, the discharged battery is prepared by letting the system thermalize with a thermal reservoir having an average number of excitation of N_A. At time $t = \tau_A$ we turn on the interaction with the charging potential $\hat{V}_c(t)$ and with the squeezed thermal bath that has mean excitation N_B, squeezing parameter r_B and squeezing angle θ_B. At time $t = \tau_B$ we turn off the charging potential and the battery is fully charged.

A.2.1 The open dynamics of the quantum battery

In the following, we aim at characterising the dynamics of an open quantum battery. We assume the system to be weakly coupled to a large environment, whose correlation times are much shorter than the system dynamical time scale and we can always consider them to be uncorrelated, thus allowing us to invoke the validity of the Born-Markov conditions. In such a regime, the dynamics can be described with a Lindblad master equation of the form

$$\frac{d\hat{\rho}}{dt} = -i[\hat{H}_{AB}, \hat{\rho}] + \sum_{k=1}^{m} \left(\hat{L}_k \rho \hat{L}_k^\dagger - \tfrac{1}{2}\{\hat{L}_k^\dagger \hat{L}_k, \hat{\rho}\} \right) \tag{A.3}$$

Where $\hat{L}_k$ are the Lindbladian (or jump) operators associated to the non-unitary dynamics.

Let us introduce a bosonic bath B with quadratures $\hat{\mathbf{r}}_{\text{bath}}(t)$ satisfying the quantum *white noise* condition

$$[\hat{\mathbf{r}}_{\text{bath}}(t), \hat{\mathbf{r}}_{\text{bath}}(t')] = i\Omega_N \delta(t - t'), \tag{A.4}$$

where $\Omega_N = \Omega^{\oplus N}$ with $\Omega = i\sigma_y$ is the symplectic form (here σ_y is the y-Pauli matrix). Eq. (A.4) entails the *memoryless* Markovian dynamics, neglecting the correlation of the bath modes at different times. In order to maintain the Gaussian evolution, we can assume a quadratic coupling Hamiltonian $\hat{H}_C = \hat{\mathbf{r}}^T C \hat{\mathbf{r}}_{\text{bath}}^T$ between system and bath. In this situation, the covariance matrix σ and the first moments $\bar{\mathbf{r}}$ of the system obey the following diffusive equations

$$\begin{cases} \dot{\bar{\mathbf{r}}} = A\bar{\mathbf{r}}, \\ \dot{\sigma} = A\sigma + \sigma A^T + D, \end{cases} \tag{A.5}$$

where the drift matrix A and the diffusion matrix D may be derived from the system hamiltonian $\hat{H}_{AB}$ and its coupling C with the environment.

A key ingredient of our proposal is the squeezed nature of the bath being considered. In this case, we can use the linear response theory as developed in [183]. The master equation of a system interacting with a squeezed thermal bath is [180]

$$\tfrac{d\hat{\rho}}{dt} = -\tfrac{i}{\hbar}[\hat{H}_{AB}, \hat{\rho}] + \{\hat{L}_+ \hat{L}_+^\dagger, \hat{\rho}\} + \hat{L}_- \hat{\rho} \hat{L}_-^\dagger - \tfrac{1}{2}\{\hat{L}_- \hat{L}_-^\dagger, \hat{\rho}\} + \hat{L}_+ \hat{\rho} \hat{L}_+^\dagger, \tag{A.6}$$

where the jump operators $\hat{L}_\pm$ read

$$\hat{L}_+ = \sqrt{\tfrac{\Gamma}{2}(N_B + 1)}(\hat{a} \cosh r_B + \hat{a}^\dagger \sinh r_B e^{i\theta_B}),$$
$$\hat{L}_- = \sqrt{\tfrac{\Gamma}{2} N_B}(\hat{a}^\dagger \cosh r_B + \hat{a} \sinh r_B e^{i\theta_B}).$$

Here, Γ is the damping rate, and $N_B = (e^{\beta_B \omega_B} - 1)^{-1}$ is the mean number of excitations of a thermal reservoir at frequency ω_B and inverse temperature β_B. and frequency ω_B, $r_B \geq 0$ is the degree of squeezing of the bath and $\theta_B \in [0, 2\pi]$ is its phase.

Since the system's hamiltonian is quadratic in the quadratures, we can rewrite it as $\hat{H}_{AB} = \frac{1}{2}\hat{\mathbf{r}}^T H_s \hat{\mathbf{r}}$, being careful to distinguish the hamiltonian operator $\hat{H}_{AB}$, acting on the Hilbert space of the system, and its hamiltonian matrix H_s, mixing the quadratures. The Lindbladian operators, conversely, can be written in the form $\hat{L}_k = b_k^T \hat{\mathbf{r}}$. Now, given a master equation such as Eq. (A.6), we can write the drift and diffusion matrix as [183]

$$A = \Omega H_s - \tfrac{1}{2}\mathrm{Im}\left(BB^\dagger\right), \quad D = -\Omega \mathrm{Re}\left(BB^\dagger\right)\Omega \tag{A.7}$$

with $B = (b_1^T, b_2^T, ..., b_m^T) \in \mathbb{C}^{2N\times m}$ taken from the Lindblad operator described above. We can then deduce the form for the matrix B and use it to obtain the drift and diffusion matrices A and D. Plugging these into Eq. (A.5) gives us the dynamical equation for the evolution of the first two moments of our Gaussian system. In what follows, we will focus our study only on vacuum states with null first moments, neglecting the driving of the average value of the quadratures and thus assuming that the quantum state is always fully described by its covariance matrix.

Before describing the dynamics ensuing from Eq. (A.7), we shall identify the conditions under which a steady state satisfying the stationary equation

$$A\sigma_\infty + \sigma_\infty A^T + D = 0 \tag{A.8}$$

exists. Criteria for the existence of such a state are provided by the Routh–Hurwitz stability conditions [184], [185], which affirms that if A is diagonalizable and the real part of its eigenvalues is negative, then the steady state is stable. When applied to the situation described above, this results in the condition

$$\mu^2 - \lambda^2 - \Gamma^2/4 > 0. \tag{A.9}$$

This is the condition for the stability of the steady state. Now we want to find a condition on the matrix D in order to enforce the physicality of the dynamics. Imposing the validity of the uncertainty principle for the bath state covariance matrix σ_{bath} we get a *bona fide* diffusive dynamics condition for D, which in the single mode case can be reduced as

$$\mathrm{Det}[D] \geq \mathrm{Det}[\Omega^T A - A^T \Omega], \tag{A.10}$$

which is always satisfied in our case.

A.2.2 Energetic considerations

The internal energy at time t of a quantum system can be computed as the expectation value of its Hamiltonian $E = \langle \hat{H} \rangle = \mathrm{tr}[\hat{\rho}\hat{H}]$. As mentioned in Sec. A.2, during the charging phase, the Hamiltonian must depend on time in order to change the energy of the system. However, just outside of the charging period, we have $\hat{H}_{AB}(\tau_A^-) = \hat{H}_{AB}(\tau_B^+) = \hat{H}_0$, so that

$$E = \langle \hat{H}_0 \rangle = \frac{\mu}{2}\left(\langle \hat{x}^2 \rangle + \langle \hat{p}^2 \rangle\right) = \frac{\mu}{4}\mathrm{tr}[\sigma] \tag{A.11}$$

This expression allows us to derive the internal energy difference between the charged battery at τ_B and the initial state

$$\Delta E_{AB} = E_B - E_A = \frac{\mu}{4}\left(\mathrm{Tr}[\sigma_B - \sigma_A]\right), \tag{A.12}$$

where σ_j is the covariance matrix of the system at time τ_j.

The first law of thermodynamics implies that, for our open quantum system, such energy change is due to two contributions: the work ΔW done on the system, and the heat ΔQ exchanged with the environment. These contributions take the form

$$\Delta Q = \int_{\tau_A}^{\tau_B} \mathrm{Tr}\left[\dot{\hat{\rho}}(t)\hat{H}(t)\right] \mathrm{dt},\ \Delta W = \int_{\tau_A}^{\tau_B} \mathrm{Tr}[\hat{\rho}(t)\dot{\hat{H}}(t)]\mathrm{dt}, \tag{A.13}$$

which characterize the work ΔW spent in order to change the energy of the system of ΔE and the amount of heat dissipated to accomplish such result [186]. For our choice of the Hamiltonian we have

$$\begin{aligned} \Delta W_{AB} &= -\frac{\lambda}{2}(\sigma_{B_{12}} - \sigma_{A_{12}}), \\ \Delta Q_{AB} &= \frac{\mu}{4}\,\mathrm{Tr}[\sigma_B - \sigma_A] + \frac{\lambda}{2}\left(\sigma_{B_{12}} - \sigma_{A_{12}}\right). \end{aligned} \tag{A.14}$$

The process under consideration is thus not unitary: the thermal bath keeps draining irreversibly quantum information from the system, increasing its entropy and decreasing its purity until it reaches a non-equilibrium steady state.

None of these quantities, however, represents the energy available in the battery to perform useful work. This is due to the second principle of thermodynamics which tells us that in a spontaneous process part of the energy is used for increasing the entropy of the system. Therefore we need to consider the Helmoltz free energy defined as

$$\Delta F = \Delta E - T\Delta S, \tag{A.15}$$

where ΔS is the change of the von Neumann entropy $S = -\,\mathrm{Tr}[\rho \ln \rho]$. For Gaussian systems, this can be cast in the form

$$S = \sum_{i=1}^{N} \left[\frac{\nu_i + 1}{2}\log\left(\frac{\nu_\mathrm{i} + 1}{2}\right) - \frac{\nu_\mathrm{i} - 1}{2}\log\left(\frac{\nu_\mathrm{i} - 1}{2}\right)\right], \tag{A.16}$$

where ν_i is the i^{th} symplectic eigenvalue of the covariance matrix σ. The maximum amount of work that the system can perform in a thermodynamic process is given by $-\Delta F$. We will thus use ΔF_{BA} to characterize the storage capacity of the battery during the discharging process, and the internal energy difference ΔE_{AB} to quantify the energy required to

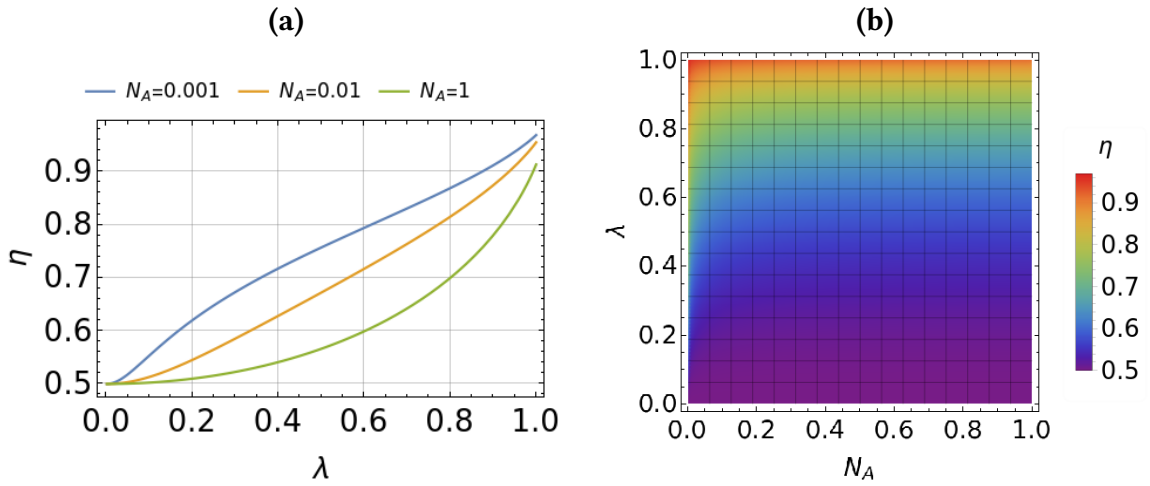


Figure A.2: In panel **(a)** we report the trend followed by the efficiency η with the temperature of the thermal bath $N_A = N_B$, studied against the charging squeezing λ. We have taken $\Gamma = \mu = 1$ and no squeezing of the bath (i.e. $r_B = 0$). Panel **(b)** shows η against λ and N_A.

charge the battery. For the second law, in a thermodynamic cycle we will always have some irreversible energetic waste so we expect in general $\Delta E_{AB} \geq -\Delta F_{BA}$.

In the following we assume $\tau_A = 0$ and $\tau_B = +\infty$, so that the charged state of the battery is reached when the system is in the non-equilibrium steady state of the dynamics, and thus $\sigma_B = \sigma_\infty$. We will go back to study the dynamical evolution in time when we will discuss the charging power and the quantum speed limits.

A.2.3 Efficient charging process

The free energy is a function of state that equals zero at thermal equilibrium. As such, it only depends on the initial covariance matrix of the discharged battery σ_A and the final state of the charged battery σ_B and as a consequence we have that the free energy in the charging stroke equals the free energy in the discharging stroke $\Delta F_{AB} = \Delta F_{BA}$. This means that we do not need to implement the dynamics in the discharging phase in order to characterize the extraction of energy, because this is fully defined by the initial and final state of the charging phase.

In order to compare the performances of the quantum battery in different dynamical situations, we define the following figure of merit for efficiency

$$\eta = \frac{\Delta F_{AB}}{\Delta E_{AB}} = 1 - \frac{\Delta S_{AB}}{\Delta E_{AB}}. \tag{A.17}$$

This corresponds to the ratio between the extractable energy from the battery and the corresponding total internal energy stored in the charged system.

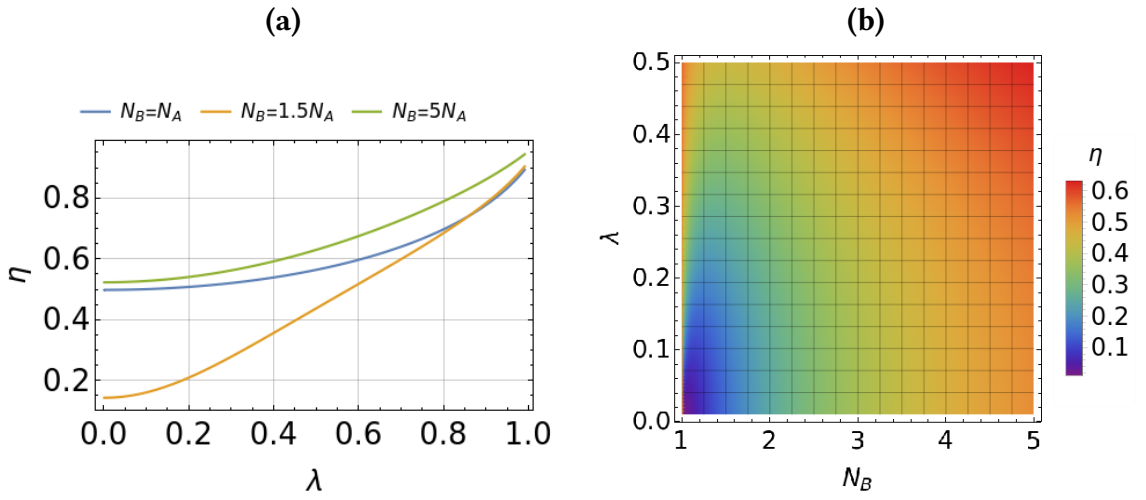


Figure A.3: Trend of the efficiency η with the temperature of the thermal bath N_B and the charging squeezing λ. $N_A = \Gamma = \mu = 1$ and the squeezing bath is switched off $r_B = 0$.

One of the key results of our study is that quantum coherence is a resource for single-mode Gaussian batteries: by increasing the thermal bath temperature N_A, and thus decreasing the initial purity of the system, we also decrease its efficiency, despite the fact that the overall available energy is larger. This is shown in Fig. A.2, where we report the performance of a single-mode quantum battery system coupled to a single-mode thermal reservoir, setting the squeezing parameter of the bath at $r_b = 0$, and taking $N_B = N_A$. Although the dynamical process is non-unitary and the system evolves towards the charged steady-state σ_B, on average there will be no net heat exchange ($\Delta Q_{AB} = 0$) and thus $\Delta E_{AB} = \Delta W_{AB}$. Notice that, although both ΔF_{AB} and ΔE_{AB} disappear in the limit $\lambda \to 0$, the efficiency tends to $\eta = 1/2$, in this limit. This asymptotic behaviour changes non-trivially if we increase the temperature of the bath B, as shown in Fig. A.3.

We now turn on the interaction with the squeezed bath by setting the parameter r_b to a non-null value. The influence of this type of environment is complex and the interplay between the various parameters rich. One would expect that, as we increase the squeezing parameters, λ and r_B, the energy would correspondingly grow. Surprisingly, this is not the case. In fact, the squeezing phase θ_B of the bath plays a crucial role, and in order to properly charge the battery and improve its efficiency, such parameter should be finely tuned, as it can be appreciated from Fig. A.4.

A.2.4 Assessment of charging power and temporal considerations

We now aim at showing the performance of the average power when charging the battery. We define the average power as

$$P = \frac{\Delta F_{AB}}{\Delta t_{AB}}, \tag{A.18}$$

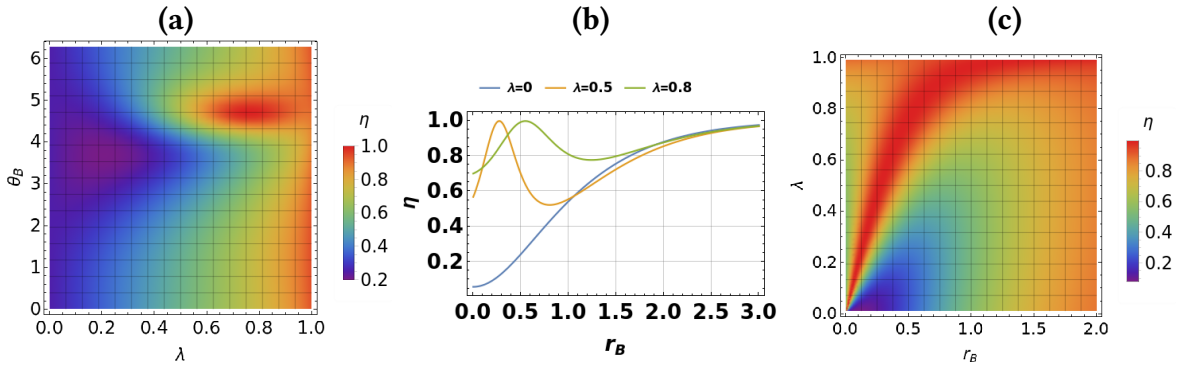


Figure A.4: **(a)** Density plot of the efficiency η plotted against the charging squeezing λ and the phase of the squeezing for the bath θ_B for $r_B = 0.5$. The optimal angle to obtain the maximal efficiency is $\theta_B \sim 3\pi/2$. **(b)** Trend of the efficiency η with the the bath squeezing r_B for various values of the charging squeezing λ. The phase of the bath squeezing is set to its optimal value, while all the other parameters are as in panel **(a)**. **(c)** Density plot of the efficiency η with the charging squeezing λ and the bath squeezing r_B with the optimal choice of phase for the bath squeezing. In all panels we have taken $N_A = N_B = \Gamma = \mu$.

where Δt_{AB} is the average time employed to charge the battery. Although by definition it is required an infinite time for the battery to reach the steady charged state, in the first stages of the dynamics the system evolves much quicker and then it slows down until it asymptotically reaches the final state, thus $\Delta t_{AB} \neq \tau_B - \tau_A = \infty$. In order to bound the time required to perform the charging we will employ the quantum speed limits geometric formalism. The quantum speed limits bound the minimum velocity v_{QSL} of a system to evolve between a state ρ and a state infinitesimally close $\rho + d\rho$ on the Riemannian manifold formed by the set of density matrices of the Hilbert space of a quantum state. The infinitesimal distance between these states is defined through the Bures metric $ds^2 = 2[1 - \mathcal{F}(\rho, \rho + d\rho)]$, where $\mathcal{F}$ is the Ulhmann fidelity.

The problem of bounding the minimal Riemannian speed of an infinite dimensional Hilbert space can be challenging [187]. However, the limitation to a Gaussian dynamics leads to a critical simplification that allows us to efficiently solve the issue. In Ref. [188] some of us showed that, for Gaussian states evolving under Gaussian generators, the instantaneous speed of quantum evolution on the Riemannian manifold is

$$v^2(t) = \frac{1}{4} \sum_j \frac{\partial_t \nu_j}{\nu_j^2 - 1}. \tag{A.19}$$

The integral velocity of the system between τ_A and τ_B is thus

$$V_{AB} = \int_0^\infty v(t) dt. \tag{A.20}$$

This dimensionless quantity embodies the product of the interaction time $\Delta\tau_{AB}$ and the average velocity, which allows us to estimate a lower-bound to the ratio between the average

time of the evolution and the interaction time as

$$\frac{\Delta t_{AB}}{\Delta \tau_{AB}} = \frac{\Delta s_{AB}}{V_{AB}}. \tag{A.21}$$

Here, $\Delta s_{AB} = 2[1 - \mathcal{F}(\rho_A, \rho_B)]$ is the Bures distance between the passive and charged states. Ref. [189] has provided a closed formula for the evaluation of the Ulhmann fidelity between generic Gaussian states as

$$\mathcal{F}_1^2(\sigma_A, \sigma_B) = \frac{1}{\sqrt{\Delta + \Lambda} - \sqrt{\Lambda}}, \tag{A.22}$$

where $\Delta = \det[(\sigma_A + \sigma_B)/2]$ and $\Lambda = 4\Pi_{j=A,B} \det[(\sigma_j + i\Omega)/2]$. This gives us all the tools to compute the average power of our single mode Gaussian battery. Once again, we are going

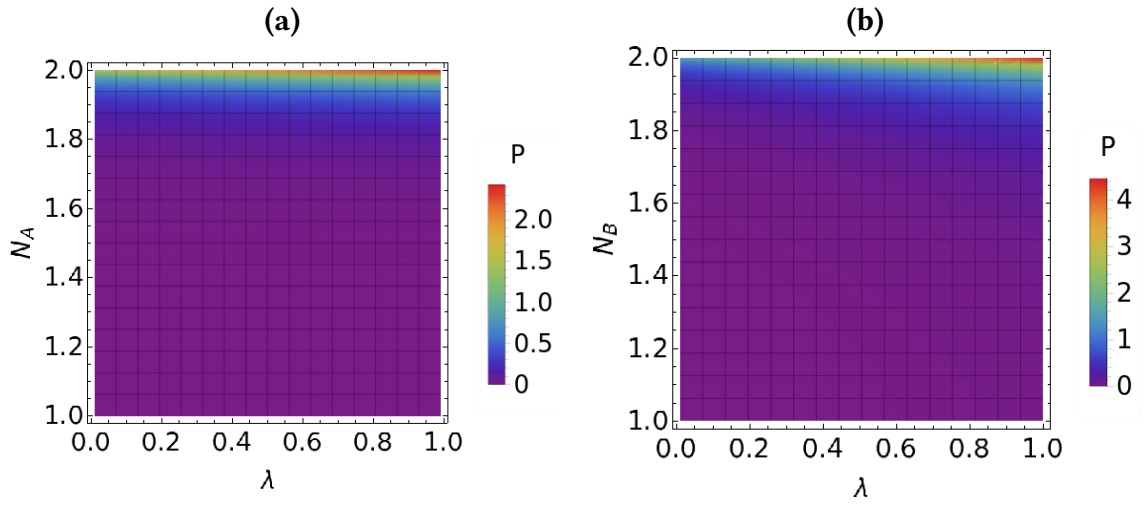


Figure A.5: In panel **(a)** we show the density plot of power P against the mean occupation number $N_A = N_B$ and squeezing λ. In this simulation, we have taken $\Gamma = \mu$ and a thermal bath with $r_B = 0$. Panel **(b)** shows the results of a similar study but for $N_B \geq N_A = \Gamma = \mu$.

to consider the influence of a simple thermal bath, setting the squeezing parameter of the bath $r_B = 0$. We are then going to turn on the charging potential $\hat{V}_c(t)$ with a squeezing strength of λ. The situation where the two baths A and B have the same temperature $N_A = N_B$ is shown in Fig. A.5 **(a)**.

Differently from the case of the efficiency, the higher temperature, and thus a lower quantum coherence, increases the power of the system. While the increment of λ raises the charging power only linearly, the dependence from the initial temperature N_A is actually exponential. Nonetheless, in the limit of $\lambda \to 0$ there would be no charging potential and thus no charging power, whereas a pure quantum state at zero temperature can still store energy if $\lambda > 0$.

In Fig. A.5 **(b)**, we take $N_A = 1$ and let the bath temperature vary to charge the battery with thermal energy. Even though, the dependence of the charging power from the temperature N_B and the squeezing parameter λ is similar to the previous case, the operations performed on the system is conceptually different. In this case, in fact, the energy stored in the battery will increase even if $\lambda = 0$.

Once again, the situation becomes more complex when we turn on the interaction with the squeezing bath $r_B > 0$. In this case, the dynamics strongly depend on the phase of the bath θ_B and there is an interplay between the two squeezing factors that can be optimized in order to increase the power. Interestingly, the optimal value of θ_B to maximise the charging power, as shown in Fig. A.6, is different from the optimal value to maximise the efficiency of the discharging (cf. Fig. A.4).

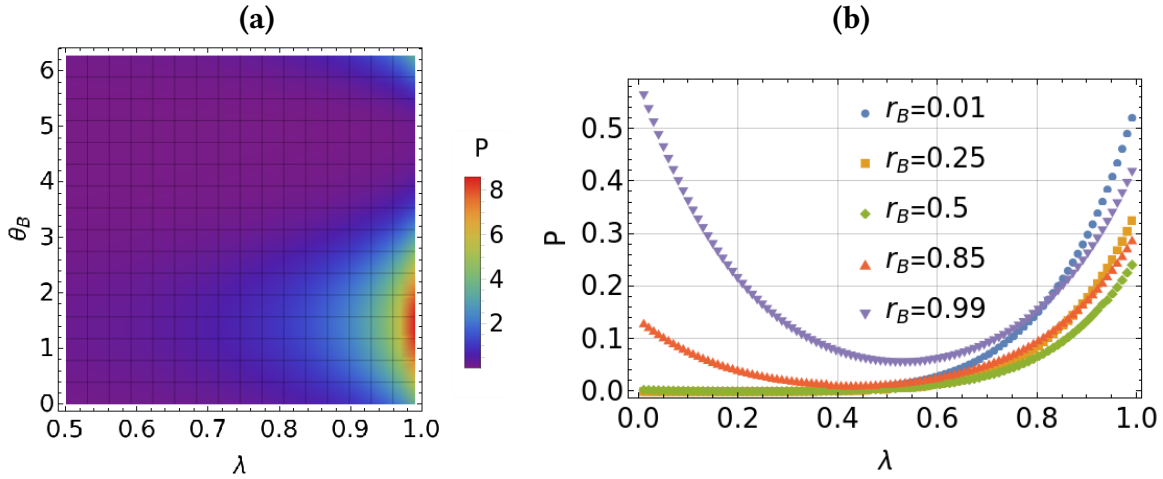


Figure A.6: **(a)** Density plot of power P vs λ and θ_B. $N_A = N_B = \Gamma = \mu = 1$ and the squeezing bath is set to $r_B = 0.5$. In this case the optimal value of the angle is $\theta_B \sim \pi/2$. **(b)** Trend of the power P with λ for various values of r_B. $N_A = N_B = \Gamma = \mu = 1$ and the squeezing bath angle is set to its optimal value $\theta_B = \pi/2$.

This optimal value of θ_B is used in Fig. A.6 **(b)**, where it is shown the trend of the power P with λ for various $r_B > 0$. The behaviour of the system is far from being trivial and while we would expect that the power always increases with λ and r_B, it is not the case of Fig. A.6 **(b)**.

A.3 Closed-system dynamics

A.3.1 Channel picture

We describe the dynamics through a discrete evolution, applying quantum maps to states rather than solving the associated equations of motion in continuous time. In a closed Gaus-

sian system, the evolution of the covariance matrix is described by $\sigma_C = S\sigma_0 S^T$, where $S \in \mathrm{Sp}_{2,\Re}$ (single-mode Gaussian state) is a real symplectic matrix. We will assume that our Gaussian battery has an internal Hamiltonian $\hat{H}_0$ and that S represents the charging process induced by an external potential applied for some time. Note that we are not considering first moments, which do play a role in the energy of the system, by neglecting linear terms in the charging potential. Without loss of generality, we can apply an Euler (or Bloch-Messiah) decomposition $S = OK$, where O is an orthogonal matrix representing a quadrature rotation, K is diagonal representing single mode squeezing and we disregarded the last orthogonal matrix because it commutes with the identity of the thermal state [25], [182].

We can parametrize as $O = \cos\theta\mathbb{1} + i\sin\theta\sigma_y$ and $K = \exp[-r\sigma_z]$ with σ_z the $z-$Pauli matrix. With this at hand, the most general covariance matrix of a Gaussian state reads

$$\sigma_C = (1+2N_A)\begin{pmatrix} e^{-2r}\cos^2\theta + e^{2r}\sin^2\theta & \sin(2\theta)\sinh(2r) \\ \sin(2\theta)\sinh(2r) & e^{2r}\cos^2\theta + e^{-2r}\sin^2\theta \end{pmatrix} \tag{A.23}$$

This provides information on the charged battery. We can now 'unplug' the charger and let the system be driven by its own internal Hamiltonian $\hat{H}_0$. The energy difference is thus given by Eq. (A.11)

$$\Delta E_{AB} = \frac{\mu}{2}(1+2N_A)\sinh(x)^2 \tag{A.24}$$

and its trend against r and N_A is shown in Fig. A.7. Notice that the parameter θ does not contribute to the energy as rotations are passive transformations.

The calculation of the ergotropy of the battery would require an optimization of the charging symplectic transformation. However, fixing the bath parameters, the energy difference always grows with the squeezing, so we can assume that there is a finite amount of energy or time to charge the battery. In this case, the work W coincides with ΔE.

A.3.2 Continuous time evolution

In order to describe the dynamics in time we need to write explicitly the quadratic Hamiltonian of the system, which will be of the form $\hat{H} = \hat{H}_0 + \hat{V}(t)$, where $\hat{V}(t) = \mu(\hat{a}^\dagger\hat{a} + \frac{1}{2}) - i\lambda(\hat{a}^\dagger\hat{a}^\dagger - \hat{a}\hat{a})$ is applied for a time t and then becomes null. By using the definition of canonical conjugate variables, as described previously, we can write the full Hamiltonian from time 0 to t as

$$\hat{H}(t) = \frac{\mu}{2}(\hat{x}^2 + \hat{p}^2) - \frac{\lambda}{2}(\hat{x}\hat{p} + \hat{p}\hat{x}) \tag{A.25}$$

We can see that this Hamiltonian is the sum of a harmonic oscillator part, which implements rotations, and a parametric oscillator part, implementing squeezing through a parametric amplification [25].

Using a bold symbol for the vectorial notation we can write the quadratures as $\hat{\mathbf{r}} = (\hat{x}, \hat{p})^T$, so that we can write any quadratic Hamiltonian as $\hat{H} = \frac{1}{2}\hat{\mathbf{r}}^T H_s \hat{\mathbf{r}}$. In our case $H_s = \mu\mathbb{1} - \lambda\sigma_x$

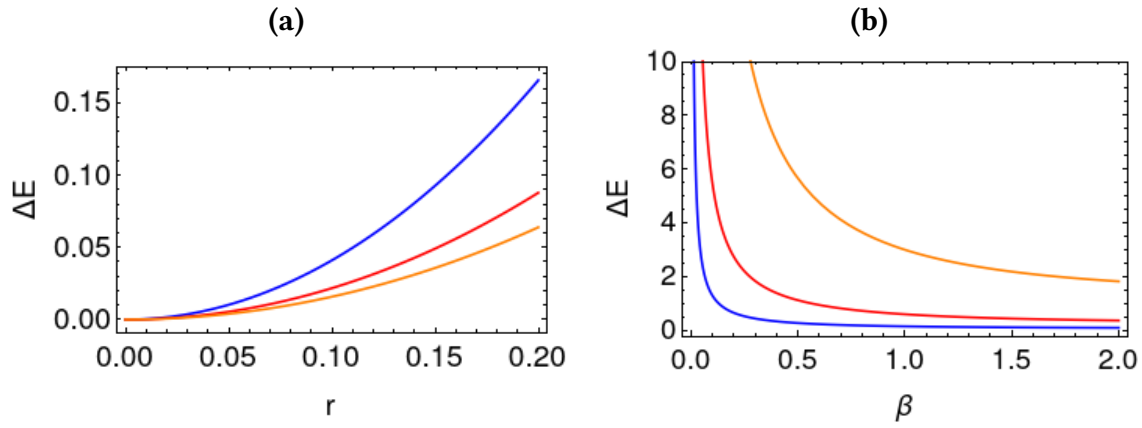


Figure A.7: Trend of the energy difference (in units of μ) for a battery undergoing closed dynamics. **(a)**: Energy difference ΔE as a function of the squeezing parameter r. From top to bottom curve, we have $\beta = 0.5, 1$ and 1.5, respectively. **(b)**: Energy difference against the inverse temperature β for $r = 0.25$, 0.5 and 1 (bottom to top curve, respectively).

with σ_x the $x-$Pauli matrix. Generally speaking, this matrix should satisfy the condition $H_s > 0$ in order to have a bounded spectrum. When this condition is not satisfied, the system cannot have a steady state and will keep gaining energy indefinitely, which is clearly unphysical. The $H_s > 0$ condition implies that $\mu > \lambda$.

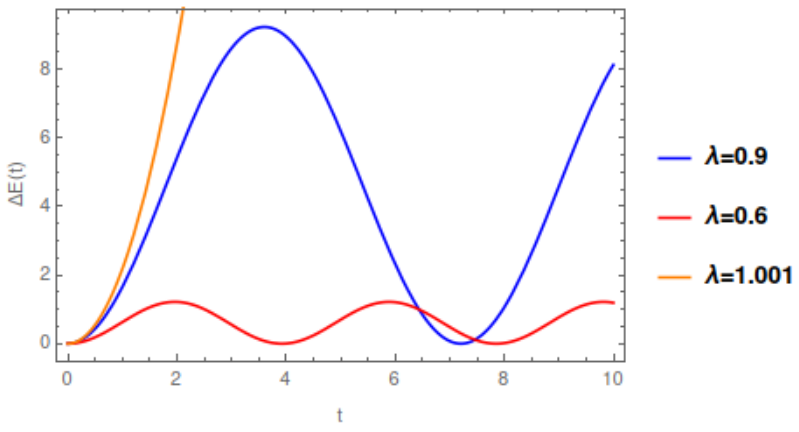


Figure A.8: Trend of energy in time

The continuous-time dynamics of a Gaussian system can be described by the Lyapunov equation

$$\partial_t \sigma = A\sigma + \sigma A^T \tag{A.26}$$

with the drift matrix $A = \Omega H$. As we are considering a closed evolution we can take $C = 0$.

Solving the Lyapunov and computing the energy through Eq. (A.11) we find

$$\Delta E(t) = \frac{\mu\lambda^2(1+2N_A)\sinh^2\left(t\sqrt{\lambda^2-\mu^2}\right)}{\lambda^2-\mu^2}. \tag{A.27}$$

At first sight, this result appear in contradiction with the stability condition $\mu > \lambda$. However we can verify that the solution exists and is continuous for all real values of λ and μ. In fact

$$\Delta E(t) = \begin{cases} \frac{\mu\lambda^2(1+2N_A)\sin^2\left(t\sqrt{\mu^2-\lambda^2}\right)}{\mu^2-\lambda^2} \text{ for } \mu > \lambda, \\ \mu\lambda^2\left(1+2N_A\right)t^2 \text{ for } \mu \sim \lambda. \end{cases} \tag{A.28}$$

The last expression has been found using the Taylor expansion of $\sin(t\sqrt{\lambda^2-\mu^2})$.

In particular we can see how the energy is bounded only inside the stability condition, as predicted by the theory.

A.4 Multimode system

The study on single-mode Gaussian batteries can be readily extended to the multimode case with little differences. Eq. (A.22) for the fidelity of single mode Gaussian states, needs to be generalized to the multimode case using the expression [189]

$$\mathcal{F}^2(\sigma_A,\sigma_B) = \frac{F_{\text{tot}}}{\sqrt[4]{\det(\sigma_A+\sigma_B)}} \tag{A.29}$$

with

$$F_{\text{tot}}^4 = \det\left[2\left(\sqrt{\mathbb{1}+\frac{(\sigma_{\text{aux}}\Omega)^{-2}}{4}}+\mathbb{1}\right)\sigma_{\text{aux}}\right] \tag{A.30}$$

and $\sigma_{\text{aux}} = \Omega^T(\sigma_A/2+\sigma_B/2)^{-1}(\Omega/4+\sigma_A\Omega\sigma_B/4)$.

All the quantities of interest can now be computed following the analysis of the previous section. One can prove, however, that the multimode case can be reduced to the analysis of a product of single modes system and environments. This result comes from the fact that the we only need the symplectic decomposition of the system and environment joint covariance matrix to derive the thermodynamically relevant quantities of our study, and all passive elements that can mix modes, although they can deeply influence the dynamics, would not affect the thermodynamics.

A.5 Discussion

We have illustrated a scheme for the charging of a quantum battery based on the dynamics of an open harmonic system subjected to the effects of a coherent squeezing charging

mechanism, and an incoherent squeezed thermal bath. We have characterized the charging process by tracking its efficiency defined in therm of the fraction of extractable energy over the total energy that can be accommodated in the battery itself. We have demonstrated the key role played by quantum coherence in the charging process, whose efficiency is boosted for a low-temperature environment and strong-coherent squeezing driving.

Bibliography

[1] M. Tribus and E. C. McIrvine, "Energy and information", *Scientific American*, vol. 225, no. 3, pp. 179–190, 1971.

[2] C. H. Bennett, "The thermodynamics of computation—a review", *International Journal of Theoretical Physics*, vol. 21, no. 12, pp. 905–940, 1982.

[3] H. J. Kimble, "The quantum internet", *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[4] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead", *Science*, vol. 362, no. 6412, 2018.

[5] B. Yurke and J. S. Denker, "Quantum network theory", *Physical Review A*, vol. 29, no. 3, p. 1419, 1984.

[6] L. Jahnke, J. W. Kantelhardt, R. Berkovits, and S. Havlin, "Wave localization in complex networks with high clustering", *Physical review letters*, vol. 101, no. 17, p. 175 702, 2008.

[7] A. Halu, S. Garnerone, A. Vezzani, and G. Bianconi, "Phase transition of light on complex quantum networks", *Physical Review E*, vol. 87, no. 2, p. 022 104, 2013.

[8] R Burioni, D Cassi, M. Rasetti, P Sodano, and A Vezzani, "Bose-einstein condensation on inhomogeneous complex networks", *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 34, no. 23, p. 4697, 2001.

[9] O. Mülken and A. Blumen, "Continuous-time quantum walks: Models for coherent transport on complex networks", *Physics Reports*, vol. 502, no. 2-3, pp. 37–87, 2011.

[10] M Rossi, D Bruß, and C Macchiavello, "Hypergraph states in grover's quantum search algorithm", *Physica Scripta*, vol. 2014, no. T160, p. 014 036, 2014.

[11] M. De Ponte, S. S. Mizrahi, and M. H. Y. Moussa, "Relaxation-and decoherence-free subspaces in networks of weakly and strongly coupled resonators", *Annals of Physics*, vol. 322, no. 9, pp. 2077–2084, 2007.

[12] G. Bianconi and C. Rahmede, "Network geometry with flavor: From complexity to quantum geometry", *Physical Review E*, vol. 93, no. 3, p. 032 315, 2016.

[13] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *arXiv preprint arXiv:2003.06557*, 2020.

[14] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the darpa quantum network", in *Quantum Information and computation III*, International Society for Optics and Photonics, vol. 5815, 2005, pp. 138–149.

[15] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, *et al.*, "Satellite-to-ground quantum key distribution", *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[16] R. Van Meter, *Quantum networking*. John Wiley & Sons, 2014.

[17] J. P. Dowling and G. J. Milburn, "Quantum technology: The second quantum revolution", *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 361, no. 1809, pp. 1655–1674, 2003.

[18] C. E. Shannon, "A mathematical theory of communication", *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[19] S. K. Joshi, D. Aktas, S. Wengerowsky, *et al.*, "A trusted node–free eight-user metropolitan quantum communication network", *Science advances*, vol. 6, no. 36, eaba0959, 2020.

[20] S. Wiesner, "Conjugate coding", *ACM Sigact News*, vol. 15, no. 1, pp. 78–88, 1983.

[21] P. A. M. Dirac, *The principles of quantum mechanics*, 27. Oxford university press, 1930.

[22] J. Von Neumann, *Mathematical foundations of quantum mechanics*. 2018 English edition by Princeton university press, 1933.

[23] J. Preskill, "Lecture notes for physics 229: Quantum information and computation", *California Institute of Technology*, vol. 16, no. 1, pp. 1–8, 1998.

[24] E. Lifshitz, LD, and S. L. (JB), *Quantum Mechanics; Non-relativistic Theory*. Pergamon Press, 1965.

[25] A. Serafini, *Quantum continuous variables: a primer of theoretical methods*. CRC press, 2017.

[26] R. J. Glauber, "Coherent and incoherent states of the radiation field", *Physical Review*, vol. 131, no. 6, p. 2766, 1963.

[27] R. Loudon, *The quantum theory of light*. OUP Oxford, 2000.

[28] G. Grynberg, A. Aspect, and C. Fabre, *Introduction to quantum optics: from the semi-classical approach to quantized light*. Cambridge university press, 2010.

[29] A. Furusawa, "Quantum states of light", in *Quantum States of Light*, Springer, 2015, pp. 1–67.

[30] P. Kok and B. W. Lovett, *Introduction to optical quantum information processing*. Cambridge university press, 2010.

[31] C. Fabre and N. Treps, "Modes and states in quantum optics", *Reviews of Modern Physics*, vol. 92, no. 3, p. 035 005, 2020.

[32] P. Dirac. "Dissertation of paul a. m. dirac for ph.d. degree." (1926), [Online]. Available: https://fsu.digital.flvc.org/islandora/object/fsu%3A641.

[33] P. R. Feynman, *QED: The Strange Theory of Light and Matter*. Princeton University Press., 1985.

[34] N. Bohr, "Über die serienspektra der elemente", *Zeitschrift für Physik*, vol. 2, no. 5, pp. 423–469, 1920.

[35] H. J. Groenewold, "On the principles of elementary quantum mechanics", in *On the Principles of Elementary Quantum Mechanics*, Springer, 1946, pp. 1–56.

[36] M. H. Stone, *Linear transformations in Hilbert space and their applications to analysis*. American Mathematical Soc., 1932, vol. 15.

[37] M. Dušek, M. Jahma, and N. Lütkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states", *Physical Review A*, vol. 62, no. 2, p. 022 306, 2000.

[38] H Paul, "Photon antibunching", *Reviews of Modern Physics*, vol. 54, no. 4, p. 1061, 1982.

[39] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited review article: Single-photon sources and detectors", *Review of scientific instruments*, vol. 82, no. 7, p. 071 101, 2011.

[40] E. Schrödinger, "Der stetige übergang von der mikro-zur makromechanik", *Naturwissenschaften*, vol. 14, no. 28, pp. 664–666, 1926.

[41] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states", *Nature*, vol. 421, no. 6920, pp. 238–241, 2003.

[42] R. Loudon and P. L. Knight, "Squeezed light", *Journal of modern optics*, vol. 34, no. 6-7, pp. 709–759, 1987.

[43] A. I. Lvovsky, "Squeezed light", *Photonics: Scientific Foundations, Technology and Applications*, vol. 1, pp. 121–163, 2015.

[44] F. Arzani, "Measurement based quantum information with optical frequency combs", Ph.D. dissertation, PSL Research University, 2018.

[45] E. Polzik, J Carri, and H. Kimble, "Spectroscopy with squeezed light", *Physical review letters*, vol. 68, no. 20, p. 3020, 1992.

[46] F. Acernese, M Agathos, L Aiello, *et al.*, "Increasing the astrophysical reach of the advanced virgo detector via the application of squeezed vacuum states of light", *Physical review letters*, vol. 123, no. 23, p. 231 108, 2019.

[47] M. e. Tse, H. Yu, N. Kijbunchoo, *et al.*, "Quantum-enhanced advanced ligo detectors in the era of gravitational-wave astronomy", *Physical review letters*, vol. 123, no. 23, p. 231 107, 2019.

[48] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?", *Physical review*, vol. 47, no. 10, p. 777, 1935.

[49] B. B. T. Collaboration *et al.*, "Challenging local realism with human choices", *Nature*, vol. 557, no. 7704, pp. 212–216, 2018.

[50] J. S. Bell, "On the einstein podolsky rosen paradox", *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.

[51] C. H. Bennett and S. J. Wiesner, "Communication via one-and two-particle operators on einstein-podolsky-rosen states", *Physical review letters*, vol. 69, no. 20, p. 2881, 1992.

[52] M. Huo, J. Qin, J. Cheng, *et al.*, "Deterministic quantum teleportation through fiber channels", *Science advances*, vol. 4, no. 10, eaas9401, 2018.

[53] D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond bell's theorem", in *Bell's theorem, quantum theory and conceptions of the universe*, Springer, 1989, pp. 69–72.

[54] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing", *Physical Review A*, vol. 59, no. 3, p. 1829, 1999.

[55] H. P. K.K. "Detection questions & answers". (2020), [Online]. Available: https://hub.hamamatsu.com/us/en/ask-engineer/detection-questions-and-answers/index.html (visited on 2020).

[56] W. Becker, "Fast acquisition tcspc flim system with sub–25ps irf width", *Application Note*, 2018.

[57] A. I. Lvovsky and M. G. Raymer, "Continuous-variable optical quantum-state tomography", *Reviews of modern physics*, vol. 81, no. 1, p. 299, 2009.

[58] J. Laurat, G. Keller, J. A. Oliveira-Huguenin, *et al.*, "Entanglement of two-mode gaussian states: Characterization and experimental production and manipulation", *Journal of Optics B: Quantum and Semiclassical Optics*, vol. 7, no. 12, S577, 2005.

[59] W. Chen, J. Gan, J.-N. Zhang, D. Matuskevich, and K. Kim, "Quantum computation and simulation with vibrational modes of trapped ions", *Chinese Physics B*, 2021.

[60] Y. Chen, "Macroscopic quantum mechanics: Theory and experimental concepts of optomechanics", *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 46, no. 10, p. 104 001, 2013.

[61] K Jensen, W Wasilewski, H Krauter, *et al.*, "Quantum memory for entangled continuous-variable states", *Nature Physics*, vol. 7, no. 1, pp. 13–16, 2011.

[62] J.-k. Xie, S.-l. Ma, Y.-l. Ren, X.-k. Li, and F.-l. Li, "Dissipative generation of steady-state squeezing of superconducting resonators via parametric driving", *Physical Review A*, vol. 101, no. 1, p. 012 348, 2020.

[63] S. Lloyd and S. L. Braunstein, "Quantum computation over continuous variables", in *Quantum information with continuous variables*, Springer, 1999, pp. 9–17.

[64] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution", *Nature photonics*, vol. 7, no. 5, pp. 378–381, 2013.

[65] R. Nichols, P. Liuzzo-Scorpo, P. A. Knott, and G. Adesso, "Multiparameter gaussian quantum metrology", *Physical Review A*, vol. 98, no. 1, p. 012 114, 2018.

[66] C. Weedbrook, S. Pirandola, R. García-Patrón, *et al.*, "Gaussian quantum information", *Reviews of Modern Physics*, vol. 84, no. 2, p. 621, 2012.

[67] H. P. Robertson, "The uncertainty principle", *Physical Review*, vol. 34, no. 1, p. 163, 1929.

[68] B. Dutta, N. Mukunda, R. Simon, *et al.*, "The real symplectic groups in quantum mechanics and optics", *Pramana*, vol. 45, no. 6, pp. 471–497, 1995.

[69] Y. Cai, J. Roslund, G. Ferrini, *et al.*, "Multimode entanglement in reconfigurable graph states using optical frequency combs", *Nat. Commun.*, vol. 8, p. 15 645, 2017. DOI: 10.1038/ncomms15645. [Online]. Available: https://www.nature.com/articles/ncomms15645.

[70] J. Roslund, R. M. De Araujo, S. Jiang, C. Fabre, and N. Treps, "Wavelength-multiplexed quantum networks with ultrafast frequency combs", *Nature Photonics*, vol. 8, no. 2, p. 109, 2014.

[71] B. Hughes, "The medieval latin translations of al-khwarizmi's al-jabr", *Manuscripta*, vol. 26, no. 1, pp. 31–37, 1982.

[72] B. Hoefflinger, "Itrs: The international technology roadmap for semiconductors", in *Chips 2020*, Springer, 2011, pp. 161–174.

[73] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. MIT press, 2009.

[74] S. Dasgupta, C. H. Papadimitriou, and U. V. Vazirani, *Algorithms*. McGraw-Hill Higher Education New York, 2008.

[75] S. Arora and B. Barak, *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[76] H. R. Lewis, *Computers and intractability. a guide to the theory of np-completeness*, 1983.

[77] H. J. R. Murray, *A history of chess*. Clarendon Press, 1913.

[78] L. G. Khachiyan, "A polynomial algorithm in linear programming", in *Doklady Akademii Nauk*, Russian Academy of Sciences, vol. 244, 1979, pp. 1093–1096.

[79] M. Agrawal, N. Kayal, and N. Saxena, "Primes is in p", *Annals of mathematics*, pp. 781–793, 2004.

[80] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring", in *Proceedings 35th annual symposium on foundations of computer science*, Ieee, 1994, pp. 124–134.

[81] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[82] E. Diamanti, *A step closer to secure global communication*, 2020.

[83] S. Aaronson. "Reasons to believe". (2006), [Online]. Available: https://www.scottaaronson.com/blog/?p=122.

[84] R. Impagliazzo and R. Paturi, "On the complexity of k-sat", *Journal of Computer and System Sciences*, vol. 62, no. 2, pp. 367–375, 2001.

[85] T. D. Hansen, H. Kaplan, O. Zamir, and U. Zwick, "Faster k-sat algorithms using biased-ppsz", in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, 2019, pp. 578–589.

[86] L. Euler, "Solutio problematis ad geometriam situs pertinentis", *Commentarii academiae scientiarum Petropolitanae*, pp. 128–140, 1741.

[87] P. Erdős and A. Rényi, "On the evolution of random graphs", *Publ. Math. Inst. Hung. Acad. Sci*, vol. 5, no. 1, pp. 17–60, 1960.

[88] M. E. Newman, "The structure and function of complex networks", *SIAM review*, vol. 45, no. 2, pp. 167–256, 2003.

[89] P. Holme, "Rare and everywhere: Perspectives on scale-free networks", *Nature communications*, vol. 10, no. 1, pp. 1–3, 2019.

[90] S. Milgram, "The small world problem", *Psychology today*, vol. 2, no. 1, pp. 60–67, 1967.

[91] A. Elmokashfi, A. Kvalbein, and C. Dovrolis, "On the scalability of bgp: The roles of topology growth and update rate-limiting", in *Proceedings of the 2008 ACM CoNEXT Conference*, 2008, pp. 1–12.

[92] M. Newman, *Networks*. Oxford university press, 2018.

[93] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks", *Reviews of modern physics*, vol. 74, no. 1, p. 47, 2002.

[94] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world'networks", *nature*, vol. 393, no. 6684, pp. 440–442, 1998.

[95] I. Ispolatov, P. L. Krapivsky, and A. Yuryev, "Duplication-divergence model of protein interaction network", *Physical review E*, vol. 71, no. 6, p. 061 911, 2005.

[96] E. Morais, T. Koens, C. Van Wijk, and A. Koren, "A survey on zero knowledge range proofs and applications", *SN Applied Sciences*, vol. 1, no. 8, p. 946, 2019.

[97] R. P. Feynman, "Simulating physics with computers", *International Journal of Theoretical Physics*, vol. 21 (6), 467–488. 1982.

[98] F. Arute, K. Arya, R. Babbush, and et al., "Quantum supremacy using a programmable superconducting processor", *Nature*, vol. 574, pp. 505–510, 2019.

[99] H.-S. Zhong, H. Wang, Y.-H. Deng, *et al.*, "Quantum computational advantage using photons", *Science*, vol. 370, no. 6523, pp. 1460–1463, 2020.

[100] J. Preskill, "Quantum computing and the entanglement frontier", *arXiv preprint arXiv:1203.5813*, 2012.

[101] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics", in *Proceedings of the forty-third annual ACM symposium on Theory of computing*, ACM, 2011, pp. 333–342.

[102] E. Pednault, J. A. Gunnels, G. Nannicini, L. Horesh, and R. Wisnieff, "Leveraging secondary storage to simulate deep 54-qubit sycamore circuits", *arXiv preprint arXiv:1910.09534*, 2019.

[103] G. J. Woeginger, "Exact algorithms for np-hard problems: A survey", in *Combinatorial optimization—eureka, you shrink!*, Springer, 2003, pp. 185–207.

[104] E. Knill, "Quantum randomness and nondeterminism", *arXiv preprint quant-ph/9610012*, 1996.

[105] J. Kempe and O. Regev, "3-local hamiltonian is qma-complete", *arXiv preprint quant-ph/0302079*, 2003.

[106] A. Kitaev and J. Watrous, "Parallelization, amplification, and exponential time simulation of quantum interactive proof systems", in *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, 2000, pp. 608–617.

[107] J. Watrous, "Succinct quantum proofs for properties of finite groups", in *Proceedings 41st Annual Symposium on Foundations of Computer Science*, IEEE, 2000, pp. 537–546.

[108] H. Kobayashi, K. Matsumoto, and T. Yamakami, "Quantum merlin-arthur proof systems: Are multiple merlins more helpful to arthur?", in *International Symposium on Algorithms and Computation*, Springer, 2003, pp. 189–198.

[109] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor, "The power of unentanglement", in *2008 23rd Annual IEEE Conference on Computational Complexity*, IEEE, 2008, pp. 223–236.

[110] J. M. Arrazola, E. Diamanti, and I. Kerenidis, "Quantum superiority for verifying np-complete problems with linear optics", *npj Quant. Inf.*, vol. 4, no. 1, p. 56, 2018.

[111] N. Kumar, I. Kerenidis, and E. Diamanti, "Experimental demonstration of quantum advantage for one-way communication complexity surpassing best-known classical protocol", *Nature Commun.*, vol. 10, no. 1, p. 4152, 2019.

[112] J. M. Arrazola and N. Lütkenhaus, "Quantum fingerprinting with coherent states and a constant mean number of photons", *Phys. Rev. A*, vol. 89, no. 6, p. 062 305, 2014.

[113] ——, "Quantum communication with coherent states and linear optics", *Phys. Rev. A*, vol. 90, p. 042 335, 2014.

[114] F. Xu, J. M. Arrazola, K. Wei, *et al.*, "Experimental quantum fingerprinting with weak coherent pulses", *Nature Commun.*, vol. 6, p. 8735, 2015.

[115] J.-Y. Guan, F. Xu, H.-L. Yin, *et al.*, "Observation of quantum fingerprinting beating the classical limit", *Phys. Rev. Lett.*, vol. 116, p. 240 502, 2016.

[116] R. Amiri and J. M. Arrazola, "Quantum money with nearly optimal error tolerance", *Phys. Rev. A*, vol. 95, no. 6, p. 062 334, 2017.

[117] N. Kumar, E. Diamanti, and I. Kerenidis, "Efficient quantum communications with coherent state fingerprints over multiple channels", *Phys. Rev. A*, vol. 95, no. 3, p. 032 337, 2017.

[118] N. Kumar, "Practically feasible robust quantum money with classical verification", *Cryptography*, vol. 3, no. 4, p. 26, 2019.

[119] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity", *Journal of the ACM*, vol. 38, no. 3, pp. 690–728, 1991.

[120] U. Schöning, "A probabilistic algorithm for k-sat and constraint satisfaction", *IEEE Symposium of Foundations of Computer Science (FOCS)*, 1999.

[121] I. Burenkov, M. Jabir, A. Battou, and S. Polyakov, "Time-resolving quantum measurement enables energy-efficient, large-alphabet communication", *PRX Quantum*, vol. 1, no. 1, p. 010 308, 2020.

[122] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, "Anonymity for practical quantum networks", *Phys. Rev. Lett.*, vol. 122, p. 240 501, 2019.

[123] M. A. Taherkhani, K. Navi, and R. Van Meter, "Resource-aware system architecture model for implementation of quantum aided byzantine agreement on quantum repeater networks", *Quantum Science and Technology*, vol. 3, no. 1, p. 014 011, 2017.

[124] C. Lu, F. Miao, J. Hou, and K. Meng, "Verifiable threshold quantum secret sharing with sequential communication", *Quantum Information Processing*, vol. 17, no. 11, pp. 1–13, 2018.

[125] M. Specter and J. A. Halderman, "Security analysis of the democracy live online voting system", in *30th {USENIX} Security Symposium ({USENIX} Security 21)*, 2021.

[126] H. Bar-El, *Why secure e-voting is so hard to get*, Archived from *Hagai Bar-El on Security* on 2015-09-12.

[127] K. Thompson, "Reflections on trusting trust", *Commun. ACM*, vol. 27, pp. 761–763, 1984.

[128] A. L. Abba, M. Awad, Z. Al-Qudah, and A. H. Jallad, "Security analysis of current voting systems", in *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, IEEE, 2017, pp. 1–6.

[129] M. Arapinis, E. Kashefi, N. Lamprou, and A. Pappa, "Definitions and analysis of quantum e-voting protocols", *ACM Transactions on Quantum Computing*, vol. 2, pp. 1–33, 2021.

[130] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, "A homomorphic lwe based e-voting scheme", in *Post-Quantum Cryptography. PQCrypto 2016. Lecture Notes in Computer Science,*, vol. 9606, Springer, Cham, 2016, pp. 245–265.

[131] A. Broadbent and A. Tapp, "Information-theoretic security without an honest majority", in *Advances in Cryptology – ASIACRYPT 2007. Lecture Notes in Computer Science*, vol. 4833, Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 410–426.

[132] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, "Multipartite entanglement verification resistant against dishonest parties", *Phys. Rev. Lett.*, vol. 108, p. 260 502, 2012.

[133] W. McCutcheon, A. Pappa, B. A. Bell, *et al.*, "Experimental verification of multipartite entanglement in quantum networks", *Nat. Commun.*, vol. 7, p. 13 251, 2016.

[134] R. Yehia, E. Diamanti, and I. Kerenidis, "Composable security for multipartite entanglement verification", *Phys. Rev. A*, vol. 103, p. 052 609, 2021.

[135] Q.-L. Wang, C.-H. Yu, F. Gao, H.-Y. Qi, and Q.-Y. Wen, "Self-tallying quantum anonymous voting", *Phys. Rev. A*, vol. 94, p. 022 333, 2016.

[136] B. Chevallier-Mames, P.-A. Fouque, D. Pointcheval, J. Stern, and J. Traoré, "On some incompatible properties of voting schemes", in *Towards Trustworthy Elections. Lecture Notes in Computer Science*, vol. 6000, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 191–199.

[137] S. L. Braunstein and P. Van Loock, "Quantum information with continuous variables", *Reviews of modern physics*, vol. 77, no. 2, p. 513, 2005.

[138] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead", *Science*, vol. 362, no. 6412, 2018, ISSN: 0036-8075. DOI: 10.1126/science.aam9288. [Online]. Available: https://science.sciencemag.org/content/362/6412/eaam9288.

[139] M. Pant, H. Krovi, D. Towsley, *et al.*, "Routing entanglement in the quantum internet", *npj Quantum Information*, vol. 5, no. 1, p. 25, 2019. DOI: 10.1038/s41534-019-0139-x. [Online]. Available: https://doi.org/10.1038/s41534-019-0139-x.

[140] X. Guo, C. R. Breum, J. Borregaard, *et al.*, "Distributed quantum sensing in a continuous-variable entangled network", *Nature Physics*, vol. 16, no. 3, pp. 281–284, 2020. DOI: 10.1038/s41567-019-0743-x. [Online]. Available: https://doi.org/10.1038/s41567-019-0743-x.

[141] H. Leone, N. R. Miller, D. Singh, N. K. Langford, and P. P. Rohde, " QuNet: Cost vector analysis and multi-path entanglement routing in quantum networks ", arXiv:2105.00418. [Online]. Available: https://arxiv.org/abs/2105.00418.

[142] C. Meignant, D. Markham, and F. Grosshans, "Distributing graph states over arbitrary quantum networks", *Phys. Rev. A*, vol. 100, p. 052 333, 5 2019. DOI: 10.1103/PhysRevA.100.052333. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.100.052333.

[143] ——, " Classical-quantum network coding: a story about tensor ", arXiv:2104.04745. [Online]. Available: https://arxiv.org/abs/2104.04745.

[144] B. Zhang and Q. Zhuang, "Entanglement formation in continuous-variable random quantum networks", *npj Quantum Information*, vol. 7, no. 1, p. 33, 2021. DOI: 10.1038/s41534-021-00370-w. [Online]. Available: https://doi.org/10.1038/s41534-021-00370-w.

[145] F. Hahn, A. Pappa, and J. Eisert, "Quantum network routing and local complementation", *npj Quantum Information*, vol. 5, no. 1, p. 76, 2019.

[146] W. Asavanant, Y. Shiozawa, S. Yokoyama, *et al.*, "Generation of time-domain-multiplexed two-dimensional cluster state", *Science*, vol. 366, no. 6463, pp. 373–376, 2019.

[147] M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen, and U. L. Andersen, "Deterministic generation of a two-dimensional cluster state", *Science*, vol. 366, no. 6463, pp. 369–372, 2019, ISSN: 0036-8075. DOI: 10.1126/science.aay4354. eprint: https://science.sciencemag.org/content/366/6463/369.full.pdf. [Online]. Available: https://science.sciencemag.org/content/366/6463/369.

[148] M. Chen, N. C. Menicucci, and O. Pfister, "Experimental realization of multipartite entanglement of 60 modes of a quantum optical frequency comb", *Phys. Rev. Lett.*, vol. 112, p. 120 505, 12 2014. DOI: 10.1103/PhysRevLett.112.120505. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.112.120505.

[149] S. Yokoyama, R. Ukai, S. C. Armstrong, *et al.*, "Ultra-large-scale continuous-variable cluster states multiplexed in the time domain", *Nature Photonics*, vol. 7, no. 12, p. 982, 2013.

[150] J. Nokkala, F. Arzani, F. Galve, *et al.*, "Reconfigurable optical implementation of quantum complex networks", *New Journal of Physics*, vol. 20, no. 5, p. 053 024, 2018.

[151] H. Yonezawa, T. Aoki, and A. Furusawa, "Demonstration of a quantum teleportation network for continuous variables", *Nature*, vol. 431, no. 7007, pp. 430–433, 2004.

[152] N. C. Menicucci, P. van Loock, M. Gu, C. Weedbrook, T. C. Ralph, and M. A. Nielsen, "Universal quantum computation with continuous-variable cluster states", *Phys. Rev. Lett.*, vol. 97, p. 110 501, 11 2006. DOI: 10.1103/PhysRevLett.97.110501. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.97.110501.

[153] N. C. Menicucci, S. T. Flammia, and P. van Loock, "Graphical calculus for gaussian pure states", *Physical Review A*, vol. 83, no. 4, p. 042 335, 2011.

[154] M. Gu, C. Weedbrook, N. C. Menicucci, T. C. Ralph, and P. van Loock, "Quantum computing with continuous-variable clusters", *Physical Review A*, vol. 79, no. 6, p. 062 318, 2009.

[155] M. Walschaers, N. Treps, S. Bhuvanesh, L. D. Carr, and V. Parigi, " Emergent complex quantum networks in continuous-variables non-Gaussian states ", arXiv:2012.15608. [Online]. Available: https://arxiv.org/abs/2012.15608.

[156] F. Arzani, G. Ferrini, F. Grosshans, and D. Markham, "Random coding for sharing bosonic quantum secrets", *Phys. Rev. A*, vol. 100, p. 022 303, 2 2019. DOI: 10.1103/PhysRevA.100.022303. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.100.022303.

[157] O. Pinel, J. Fade, D. Braun, P. Jian, N. Treps, and C. Fabre, "Ultimate sensitivity of precision measurements with intense gaussian quantum light: A multimodal approach", *Phys. Rev. A*, vol. 85, p. 010 101, 1 2012. DOI: 10.1103/PhysRevA.85.010101. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.85.010101.

[158] M. Gessner, L. Pezzè, and A. Smerzi, "Sensitivity bounds for multiparameter quantum metrology", *Phys. Rev. Lett.*, vol. 121, p. 130 503, 13 2018. DOI: 10.1103/PhysRevLett.121.130503. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.121.130503.

[159] L. Lami, B. Regula, X. Wang, R. Nichols, A. Winter, and G. Adesso, "Gaussian quantum resource theories", *Physical Review A*, vol. 98, no. 2, p. 022 335, 2018.

[160] M. Idel, D. Lercher, and M. M. Wolf, "An operational measure for squeezing", *Journal of Physics A: Mathematical and Theoretical*, vol. 49, no. 44, p. 445 304, 2016.

[161] M. E. J. Newman, *Networks, second edition*. Oxford University Press, 2018.

[162] A. L. Barabási, *Networks science*. Cambridge University Press, 2016.

[163] P. van Loock and S. L. Braunstein, "Multipartite entanglement for continuous variables: A quantum teleportation network", *Physical Review Letters*, vol. 84, no. 15, p. 3482, 2000.

[164] S. Pirandola and S. Mancini, "Quantum teleportation with continuous variables: A survey", *Laser Physics*, vol. 16, no. 10, pp. 1418–1438, 2006.

[165] R. Simon, "Peres-horodecki separability criterion for continuous variable systems", *Physical Review Letters*, vol. 84, no. 12, p. 2726, 2000.

[166] C. Weedbrook, S. Pirandola, R. García-Patrón, *et al.*, "Gaussian quantum information", *Rev. Mod. Phys.*, vol. 84, pp. 621–669, 2 2012. DOI: 10.1103/RevModPhys.84.621. [Online]. Available: https://link.aps.org/doi/10.1103/RevModPhys.84.621.

[167] M. Ohliger, K. Kieling, and J. Eisert, "Limitations of quantum computing with gaussian cluster states", *Phys. Rev. A*, vol. 82, p. 042 336, 4 2010. DOI: 10.1103/PhysRevA.82.042336. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.82.042336.

[168] M. Van den Nest, A. Miyake, W. Dür, and H. J. Briegel, "Universal resources for measurement-based quantum computation", *Phys. Rev. Lett.*, vol. 97, p. 150 504, 15 2006. DOI: 10.1103/PhysRevLett.97.150504. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.97.150504.

[169] N. Jones, "How to stop data centres from gobbling up the world's electricity", *Nature*, vol. 561, no. 7722, pp. 163–167, 2018.

[170] F. Centrone, N. Kumar, E. Diamanti, and I. Kerenidis, "Experimental demonstration of quantum advantage for np verification with limited information", *Nature communications*, vol. 12, no. 1, pp. 1–11, 2021.

[171] A. W. Harrow and A. Montanaro, "Testing product states, quantum merlin-arthur games and tensor optimization", *Journal of the ACM (JACM)*, vol. 60, no. 1, pp. 1–43, 2013.

[172] F. Centrone, E. Diamanti, and I. Kerenidis, "Practical quantum electronic voting", *arXiv preprint arXiv:2107.14719*, 2021.

[173] F. Centrone, F. Grosshans, and V. Parigi, "Cost and routing of continuous variable quantum networks", *arXiv preprint arXiv:2107.14719*, 2021.

[174] G. B. Alliance, "A vision for a sustainable battery value chain in 2030: Unlocking the full potential to power sustainable development and climate change mitigation", in *Geneva, Switzerland: World Economic Forum*, 2019.

[175] F. Campaioli, F. A. Pollock, and S. Vinjanampathy, "Quantum batteries", in *Thermodynamics in the Quantum Regime*, Springer, 2018, pp. 207–225.

[176] F. Campaioli, F. A. Pollock, F. C. Binder, *et al.*, "Enhancing the charging power of quantum batteries", *Physical review letters*, vol. 118, no. 15, p. 150 601, 2017.

[177] D. Ferraro, M. Campisi, G. M. Andolina, V. Pellegrini, and M. Polini, "High-power collective charging of a solid-state quantum battery", *Physical review letters*, vol. 120, no. 11, p. 117 702, 2018.

[178] F. Caravelli, G. Coulter-De Wit, L. P. García-Pintos, and A. Hamma, "Random quantum batteries", *Physical Review Research*, vol. 2, no. 2, p. 023 095, 2020.

[179] N. Friis and M. Huber, "Precision and work fluctuations in gaussian battery charging", *Quantum*, vol. 2, p. 61, 2018.

[180] G. Manzano, F. Galve, R. Zambrini, and J. M. Parrondo, "Entropy production and thermodynamic power of the squeezed thermal reservoir", *Physical review E*, vol. 93, no. 5, p. 052 120, 2016.

[181] W. Pusz and S. L. Woronowicz, "Passive states and kms states for general quantum systems", *Communications in Mathematical Physics*, vol. 58, no. 3, pp. 273–290, 1978.

[182] M. G. Genoni, L. Lami, and A. Serafini, "Conditional and unconditional gaussian quantum dynamics", *Contemporary Physics*, vol. 57, no. 3, pp. 331–349, 2016.

[183] M. Mehboudi, J. M. Parrondo, and A. Acín, "Linear response theory for quantum gaussian processes", *New journal of physics*, vol. 21, no. 8, p. 083 036, 2019.

[184] A Hurwitz, R Bellman, and R Kalaba, "Selected papers on mathematical trends in control theory", *Dover*, 1964.

[185] E. X. DeJesus and C. Kaufman, "Routh-hurwitz criterion in the examination of eigenvalues of a system of nonlinear ordinary differential equations", *Physical Review A*, vol. 35, no. 12, p. 5288, 1987.

[186] S. Vinjanampathy and J. Anders, "Quantum thermodynamics", *Contemporary Physics*, vol. 57, no. 4, pp. 545–579, 2016.

[187] S. Deffner, "Geometric quantum speed limits: A case for wigner phase space", *New Journal of Physics*, vol. 19, no. 10, p. 103 018, 2017.

[188] L. Mancino, M. G. Genoni, M. Barbieri, and M. Paternostro, "Nonequilibrium readiness and precision of gaussian quantum thermometers", *Physical Review Research*, vol. 2, no. 3, p. 033 498, 2020.

[189] L. Banchi, S. L. Braunstein, and S. Pirandola, "Quantum fidelity for arbitrary gaussian states", *Physical review letters*, vol. 115, no. 26, p. 260 501, 2015.

Acknowledgements

Calling naives those believing that the accomplishment of this work is merit of a single person would be an euphemism, at the very least. During this long journey the author was helped in many ways by different people and this section is an attempt to credit them. Nonetheless, I decided to provide these contributors with the privilege of anonymity by hiding their surnames, so that they can deny their contribution in case this thesis revealed to be a complete failure.

First of all, I would like to thank my jury, who revised my thesis and joined my defence. The thesis reporters, Anthony and Norbert, have given a crucial preliminary feedback, that helped me to spot some errors in the calculations and to understand which parts of the manuscript were not clear. During the defence, the examiners, Pérola and Yasser, together with the reporters, asked me very relevant questions that helped me to improve the thesis and to identify the most significant directions to pursue my research. At the same time, I cannot forgive that I was named doctor in computer science. Firstly, I have never witnessed a defence in which the thesis specialization was specified out loud. Secondly, but most importantly, unless you believe that I have been programming photons in the last three years, my research field is physics and not informatics (despite what my doctoral school forced me to write in the front page).

A key acknowledgement is due to my supervisors Eleni and Iordanis. Working together with you taught me a lot, not only in an academic sense. You let me walk on my feet, allowing me to develop my interests and my collaborations autonomously, while always keeping an eye on me and being there in my time of need. To Eleni in particular, I want to say that your being a fun, genuine and nice person and a brilliant researcher at the same time, was for me inspirational and it is far from being a common trait. However, I hate the title of the thesis. It is not a big deal and you are still the best, but I had to tell you.

I cannot find the right words to express how lucky I feel for being part of such a unique research group as the Quantum Information group of LIP6 and I would like to thank you all for the marvellous experience it has been: Adrien, Alex, Alissa, Andrea, Anthia, Anupama, Armando, Beatrice, Clément, Damian, Dimitrios, Dominik, Elham, Francesco, Frédéric, Gözde, Ivan, Léo, Luis, Luka, Mina, Majid, Mathieu, Natansh, Niraj, Paolo, Paul and Paul, Pierre Emmanuel, Rawad, Rhea, Robert, Shradda, Shane, Shouvik, Simon, Ulysse, Uta, Valentina, Yao and all those that I might forget to mention. I learnt so much from all of you while having tons of fun and, despite the nominal prescription that splits us in admins, permanents, postdocs, PhD students and interns, I cannot help considering you true friends before colleagues. Among these, there are some that deserves a special note: Laura, Verena and Yoann, the three musketeers of the new PhD generation, Raja, the only Parisian I could ever bond with, Nathan, hero of the karaoke nights, Victor, Matteo and Andrea, my adventures fellows. A special tribute goes as well to some people outside LIP6: Valentina, Francesca and Beate, from LKB, Jonas and Daniel, from IRIF, Marco, Ilaria, Valeria and Luca, from

NEQO (you will always be NEQO to me).

Outside my lab, there were some people that really made my permanence in Paris extraordinary, with and without pandemics. Besides the ones I have already mentioned, there is obviously Virginia, the best neighbor I could ever wish for, Luca and Francesco, companions of delicious meals and nasty discussions, and the rest of the crew, Filippo, Federica, Denise, Laura and Mireia. You have all made these years the best adventure I have ever had. A deep thanks goes to my whole "extended" family who always supported me, in particular to Angelo and Maria Grazia, my parents, Margherita, my little sister, Maria, my grandma and Giuseppe, my grandpa, that could not be there, but who always wanted to see me as a doctor, Licia, Giovanni, Nicolò and Marco, for welcoming me when it started and sustaining me til the end. To all my friends that came to see my defence, Renato, Flavio, Giordano, Emilia and Miriam, and all my friends in Rome and around the world that could not come but always believed in me, I give you my warmest hug and my richest gratitude.

Finally, to Ester, the person that listened to me and walked with me through all these years, in joy and dark times, I don't even know how to thank you. I have no idea where the future will bring us, but I will always remember how we passed the last years: with love and a smile.