Towards Secure and Scalable Quantum Networks:

Enhancing Distance and Efficiency of Quantum Key Distribution and Quantum Repeaters

Özlem Erkiliç

A thesis submitted for the degree of
Doctor of Philosophy

Australian National University

Centre of Excellence for Quantum Computation and Communication technology,

Department of Quantum Science and Technology

January, 2025

Declaration

This thesis presents research conducted from February 2020 to January 2025 at the Department of Quantum Science, Research School of Physics, Faculty of Science, The Australian National University, Canberra. To the best of my knowledge, and except where appropriately acknowledged, the work herein is original and has not been submitted, in whole or in part, for any degree at another university.

Özlem Erkılıç
January, 2025

Acknowledgments

A PhD is never just one person's effort. Let's begin with this: how did I get here, to this point in my life? Why did I choose to do this? I mean, really, why would anyone ever do this to themselves?

It was another rainy day in Melbourne, driving my old 2006 Toyota Corolla down Sydney Road, with tram bells ringing in the background. I finally arrived at work and parked my car in the Ford Motor Company's car park, right next to shiny Ford Mustangs. I liked my colleagues, and the work environment was great, but I craved more Maths in my life, something technical. Yet there I was, working on Excel spreadsheets and feasibility reports. So, the first acknowledgment goes to my former career manager, Jason Smith (who will probably never read this), thank you for encouraging me to pursue research.

Next, I owe a huge thanks to Prof. Igor Bray, my old Physics lecturer, for always offering guidance and sparking my love for quantum mechanics. I also want to thank Prof. Phil Bland (yes, I know you wanted me to do a PhD in your group). While I chose a different path, your support meant a lot. Thank you for putting me in touch with Prof. Ping Koy Lam and encouraging me to follow my dreams in quantum communications.

To my ANU supervisors, I am deeply grateful. Prof. Ping Koy Lam, thank you for always offering guidance, being incredibly passionate about science, and finding time for us no matter how busy you are. Your dedication and enthusiasm have been truly inspiring. I also want to thank my supervisor, Dr. Syed Assad. I'm really grateful for your endless patience and for never judging my endless stream of questions, no matter how silly they might have been. Thank you for always taking the time to explain things clearly and for providing thoughtful, constructive feedback on my papers to help me improve. Your guidance has made a world of difference, and I think I finally learnt how to approach problems. Equally, I want to extend my heartfelt gratitude to my other supervisor, Dr. Sophie Zhao. Your guidance has been invaluable, not only in science but in life and my career as well. You encouraged me to apply for every opportunity that came my way, always pushing me to aim higher. Beyond the lab, you have been a mentor and a great friend, offering advice and support that extended far beyond research. Thank you for teaching me crucial experimental skills and completing the experimental paper would have been impossible without your expertise, and I am sincerely grateful for all your contributions.

To my collaborators outside of ANU, thank you for your support and contributions to

my research. It has been a privilege to work alongside such talented and passionate individuals. Dr. Yong-Su Kim, thank you for teaching me the basics of twin-field QKD. I really enjoyed learning about Korean culture and cuisine from you. I hope to visit you and KIST in Korea someday! Prof. Ulrik Lund Andersen and Prof. Jonas Schou Neergard-Nielsen, thank you for hosting me in Denmark and making me feel like part of your group. I would also like to thank Dr. Zhenghao Liu for being a great supervisor and teaching me fiber-optics in the lab. Thank you, Dr. Donghwa Lee and Dr. Ze-Yan Hao, for helping me troubleshoot the experiment when Zhenghao was away and for brainstorming solutions with me. Your support and insights made a real difference in the lab. Lastly, I want to thank the rest of the computing lab at DTU for welcoming me into the group. Thank you Romain, Óscar, Emil and Daniel for your support and the good times we shared. Best of luck with your PhDs!

I also want to express my gratitude to the rest of my ANU group. Thank you, Aaron for teaching me essential experimental skills and more importantly, for your friendship. Your emotional support, your willingness to listen, and the memorable adventures in Japan with Zac made this journey so much more enjoyable. I also want to thank Oliver for troubleshooting the experiment with me and for building the detectors we needed to make it all work. Your incredible electronics knowledge has been invaluable. Jiri, thank you for answering my EOM questions and levitating my experimental table again. Aritra, thank you for tackling quantum information problems with me. Your insights and approach to theory have always impressed me, I genuinely believe you already have an incredible understanding of the field. Beyond the science, thank you for being a true friend, for listening to my meltdowns, and for reminding me to stop spiraling when things got tough. Angus, thank you for aligning the EOMs with me, at least a hundred times! I would have banged my head against the wall without your help. I really enjoyed working in the lab with you, and I deeply admire your knowledge of physics. Arindam, thank you for the delicious curries you cooked for me and for always reminding me to chill. I will miss your calmness and ability to keep extending sentences you started. Simon and Jake, you represent the next generation of our quantum information team, and I have no doubt that you both will achieve incredible things during your PhDs. Thank you for your contributions to the team, and a special thanks to Jake for taking the time to proofread my thesis.

To those who were once part of the ANU team, thank you for making my time there truly memorable. Each of you has left a lasting impact on my journey, both professionally and personally. Spyros, thank you for being so enthusiastic about quantum information and teaching me the basics when I first joined ANU. Biveen, thank you for tackling QKD problems with me, patiently answering my endless cavity questions, and taking me on those amazing sightseeing adventures in Singapore. You have been more than just a colleague, you have been a great friend, always ready with advice when I needed it most. I just wish

you had not left ANU for your post-doc. Lorcan, thank you for leaving me your Born rule experiment, I deconstructed it to pieces and managed to turn it into a new paper. I admire how incredibly efficient you are at accomplishing tasks and your knowledge of quantum information. But more than that, thank you for being like a brother to me. When you left ANU, I did not realise just how much I would miss you and your Irish accent. I have never met anyone with your level of positivity, and it is something I always envy. Vijey, thank you for the books you gave me, your infectious enthusiasm for research, and, of course, your memes! My friend, you are a great scientist, and with your level of dedication, I have no doubt that you always will be. Angela, thank you for showing me around Singapore, exploring Berlin together, and sharing your room with me. I wish you had stayed at ANU for the remainder of my time there, I missed your laughter. Chenyue, thank you for joining me at the gym, always bringing me new types of coffee to try, and introducing me to great cafes. I am really amazed by how much ice-cream you can eat, your ability to fall asleep instantly and your love for opto-mechanics.

To the other people at DQST, thank you for making my time at ANU such a rewarding experience. From our lunches and coffee breaks to the occasional silly discussions, your company made the everyday moments enjoyable. Simon Haines, thank you for the little coffee cup you made for me (and for making a second one after I broke the first!). I also loved our shared moments roasting Yosri, it was always good fun. And thank you for going out of your way to send me post-doc ads. I really appreciate your thoughtfulness and efforts to help me along my next journey. Zain, thank you for teaching me to be firm and to voice my thoughts when I don't agree with people. I admire your unwavering principles and your courage to stand up for what you believe in. Thank you for listening to my problems and always offering thoughtful advice. Also, I guess I should thank you for being my "coat twin", I couldn't resist getting the same yellow Kathmandu jacket after seeing how good it looked on you. Ryan Husband, thank you for being such a joyful presence and for your dedication to crafting sentences with words that start with the same letter, depending on the day. I especially enjoyed your "F" day, it was fantastic fun! I also admire how hard-working and patient you are, and I have no doubt that you will achieve amazing results in your PhD. And to Yosri, thank you for everything... Thank you for being my best friend, a shoulder to cry on, your never-ending lectures, advices, our coffee dates almost every day, immature jokes, dinners you cooked for me and Zac, vacuuming our house, taking me on detour around Canberra to let Zac prepare a surprise birthday party for me, taking care of our lovely cats, Pippin and Merry. Thank you for always welcoming me in your life, you are a brother that I never had. I am sad that our paths will be in different cities or even countries, but I know you will always be on the other side of the phone for me.

I also want to express my gratitude to Luda from the HDR administration team. Luda,

your incredible responsiveness to my emails, ensuring my scholarship was always up to date so I received my payments on time, and even accommodating my last-minute changes to slides for the John Carver seminar, has not gone unnoticed. Thank you for your efficiency and support throughout my PhD journey. I also want to thank Belinda Barbour, our departmental administrator, for always being so helpful in organising my PhD-related travel and ensuring everything ran smoothly. I also really appreciated our chats in the kitchen, catching up about the weekend, and your warmth and friendliness that made the department feel more like a community.

To my friends outside of ANU, thank you for making my time in Canberra special. You have been a big part of my life outside the lab, bringing laughter, adventures, and much-needed support when I needed it the most. Meg, arigatou gozaimasu for being our interpreter in Japan and saving me from having to explain what I want. And thank you (and Aaron) for bringing the bundle of joy, Mayuka, into the world, she always brightens everyone's day. Hui, thank you for becoming Yosri's housemate, which gave me the chance to meet you and become your friend. I admire your determination to achieve every goal you set, your commitment to self-growth, and, most of all, your laughter that always brightens the room. Apoorva, thank you for all your dessert recommendations and for sending me Instagram posts about loukoumades (I promise to check out the new store in Canberra!). And of course, thank you for teaming up with Hui to roast Yosri, it was always good fun. Ridhima, thank you for bringing warmth and kindness to every gathering and always welcoming us in your house. I have always admired your impeccable sense of fashion, you are undoubtedly the most stylish person in our group. Taneesh, thank you for all the philosophical discussions, your unique view of life, and your endless positivity. I will never understand how you manage to have so many friends, it feels like you know the entire city of Canberra! Also, thank you for sharing your knowledge on better health habits and helping me achieve my gym goals. Max, thank you for starting off as Zac's friend and somehow ending up as mine too. I really appreciate you teaching me rock climbing tricks and cooking us amazing meals with John (though, just to be clear, I still hate Knower!). I admire your ridiculously diverse set of skills, seriously, why are you so good at everything? So jealous... John, I'm going to repeat the first sentence from Max's. Thank you for starting off as Zac's friend and somehow ending up as mine too. Thank you for cooking us delicious meals and being my gym partner. I will really miss our gym sessions, but more importantly, I will miss looking at you and thinking, "We're the same person." (Obviously not physically; I wish I had your level of muscle, but definitely mentally!). I admire your determination to achieve your goals and your dedication to continuous self-growth. I wish I had the same level of desire and drive to better myself. Max and John, honestly, I have been missing you both so much, especially having you just a five-minute walk away. Life isn't the same without those

quick catch-ups! Also, a big thank you to both of you for keeping Zac happy and entertained while I was buried in my PhD.

Tezimi Avustralya'da başlayıp, Danimarka'da yazıp ve düzeltmelerini Türkiye'de yaptım. Bu süreçte bana o kadar çok kişi yardımcı oldu ki. Danimarka'dayken beni ziyaret edip Danimarka turu attırdığın için teşekkür ederim Fırat abi ve tabii ki de bana Amsterdam'ı gezdirdiğın için. Canım Gülcan ablam, beni evinde ağırlayıp, güzel kurabiyelerinle beni şişmanlattığın için teşekkür ederim (ve tabii ki de Ege için). Ege'ciğim, ara ara Flemenkçe konuşup, tatlı tatlı gülümseyerek ve de durmadan beni koşturduğun için çok teşekkür ederim. Küçük cool adamım benim. Gökay abi, şenliğin ve şakacılığın için teşekkür ederim. Zeynel dayıcığım, bana ve Fırat abiye yemekler yaptığın için teşekkür ederim. Tezimin son dokunuşlarını canım İpek halamın ve Durak dedemin (aslında teyzem ve eniştem ama açıklaması uzun sürer) yanında yaptım. Bana bu süreçte ikinci annem gibi baktıkları için teşekkür ederim. Ve beni derslerimden ve arkadaşlarımdan alı koymaya çalışan ama benim en tatlı arkadaşım olan Emir'e, benimle sürekli oyun oynadığı için çok teşekkür ederim. Emir, çok şekersin. Aynı zamanda bana benim ergenliğimi hatırlattığı için Nehir'e ve benim peşimde koşuşturan Yeliz ablaya çok teşekkür ederim. Suzan halacığım ve Sultan ablacığım, beni evinizde ağırladığınız ve aynı zamanda istediğim her şeyi yaptığınız için teşekkür ederim. Küçük Çağın bey, ara ara beni sabotaj edip, bilgisayarımda tuşlara basmaya çalışsan da, gülücüklerinle beni mutlu ettiğin için teşekkür ederim. Anneanneciğim, beni Danimarka'dayken sürekli aradığın ve iyi dileklerin için çok teşekkür ederim. Ve en sonunda da tabii ki babaannemle, dedeme... Doktoram için son sunumlarımı yaparken evde sessizce dolaşıp, bana sürekli kahve alıp, ve Didim'de yürüyüşlere götürdüğünüz için teşekkür ederim. Hepinizi çok seviyorum, iyi ki varsınız.

Madem, Türkçe yazmaya başladım, şimdi de sıra sende. Cansu, canım arkadaşım, gerçekten aynı hayatları yaşadığımıza inanamıyorum. Sana bu süreçte, senin de aynı süreçten geçtiğin için teşekkür ediyorum, benim zeki ve olimpiyat şampiyonu arkadaşım. Ve tabii ki Gözde... Beni bu süreçte en iyi anlayanın sen olduğuna adım gibi eminim. İyi ki Quantum Sydney'de "Telefonunu kullanabilir miyim?" diye sormuşsun da iyi ki tanışmışız. Bana bu süreçte destek olup beni dinlediğin için çok teşekkür ederim ve unutma, sen de yolun sonuna geldin. Harika bir tez yazıp, mükemmel makalelerin olacağını unutma, benim süper zeki, en iyi fizikçi arkadaşım.

Ve ailem... Canım annem, beni bugünlere getirmek için verdiğin emeklerin, gösterdiğin sevgin ve bitmek bilmeyen fedakârlıkların için ne kadar teşükkür etsem az. Beni büyütürken karşılaştığın her zorluğa rağmen, bana her zaman destek oldun ve hayallerimi gerçekleştirmem için cesaret verdin. Her şey için minnettarım ve seni çok seviyorum. Beni benden daha iyi tanıyan, hissettiğim her duyguyu en derinden hisseden annem, dünyaya geri gelsem bir tek senin annem olmanı isterim, iyi ki varsın. Babam, zamanında aldığın

kararları anlamakta zorlandığım ve tam bir ergen gibi davrandığım için özür dilerim. Avustralya'ya geri dönmek gerçekten en doğru karar olmuş. Bugün doktorayı bitirmeye bir adım daha yaklaşıyorsam, bu senin sayende. Her şey için teşekkür ederim. Canım kardeşim, Öykü'm, bana her zaman destek verdin ve "Bunu yapabilirsin!" diye cesaretlendirdin. Ne zaman pes edecek gibi olsam, hep yanımda olup "You go girl!" diyen sendin, ve bunun için sana sonsuz teşekkür ederim. Ama aslında seninle ben gurur duyuyorum. Sen, cesaretinle, azminle ve disiplininle hayatında neyi hedeflersen hep başarıyorsun ve bunu defalarca kanıtladın. Deprem bölgesinde gönüllü çalışmalara katıldığında, zor koşullarda bile yılmadan insanların hayatlarına dokundun. Bu, her insanın yapabileceği bir şey değil. Kendinden emin, yardımsever ve çalışkan ruhunla her zaman etrafındakilere ilham veriyorsun. Yine de benim için her zaman, arkamdan "ABAAA!" diye koşturan o küçük çocuk olarak kalacaksın. Ve seni o hâlinle her zaman sarıp sarmalayacağım.

I also want to thank Cathy, Sean, and Emilya for being like a second family to me. Your support, encouragement, and genuine pride in my accomplishments have meant so much. I am especially grateful to Cathy and Sean for raising such an incredible son, Zac, my partner, who has been my constant source of strength and support throughout this journey.

To my two fur babies, Pippin and Merry, thank you for bringing so much joy and comfort into my life. My beautiful baby girl Pippin, thank you for always coming to cuddle me as soon as my alarm goes off in the morning, falling asleep by my side, and sabotaging my plans to get up and head to the university. Because of you, I often found myself snoozing longer than I should have, but those moments were always worth it, especially when you started purring. My little Merry, thank you for sabotaging my work. Every time I picked up my laptop or notebook, you decided it was time to cuddle. Your persistence and charm made it impossible to get anything done, but you always made me smile. I love both of you so, so much.

Finally, to my partner Zac, I don't even know where to begin. Sevgilim, no words could ever truly capture the depth of your support throughout this journey, and no amount of thanks could ever be enough. It feels like you did this PhD alongside me. Thank you for proof-reading all my papers, applications, and my thesis, and even trying to help me solve the problems in every project. Thank you for always believing in me, for encouraging me when I was ready to give up, for wiping away my tears, and for waking up in the middle of the night when I felt anxious and couldn't sleep. Let's be honest, if the roles were reversed, I probably would have just kept sleeping! Also, thank you so much for taking on the responsibility of cooking, cleaning, and managing the house chores when things got intense with my PhD. I couldn't have done this without you. I am so incredibly grateful that 9.5 years ago, my lab got cancelled, and I ended up in yours. We have grown up together, and through it all, you have changed me for the better. Thank you for touching my life and,

more importantly, for becoming my life. I am so, so proud of the person you have grown into over the years. We still have so much growing up to do, and I am so excited for the next adventure in our lives. Thank you, sevgilim, for always being here for me. I love you sooooo much...

Abstract

Quantum communications enable secure key transmission and entanglement distribution, but their rates and maximum transmission distances are limited due to the losses and noise introduced by quantum channels. Various techniques have been developed to address these limitations, tailored to the platform and the nature of the decoherence.

In this thesis, we explore ways to enhance the performance of quantum communications, with a particular focus on increasing the key rates and transmission distances in quantum key distribution (QKD), a method that leverages quantum mechanics to securely share keys between trusted parties. Additionally, we aim to improve the purity of entangled states shared between two parties, contributing to broader advancements in quantum communications. We begin by introducing a software-enhanced continuous-variable QKD (CV-QKD) protocol, where keys are encoded onto the phase and amplitude degrees of the optical field. This protocol enhances both transmission distance and key rates through a post-selection method employing arbitrary filters, experimentally demonstrated on two different platforms. Its adaptability makes it highly promising, as it can be implemented on existing CV-QKD platforms and dynamically optimises key rates for rapidly changing channels.

We then present a protocol for the pure-loss channel leveraging quantum repeaters to mitigate the channel losses by segmenting the total communication distance into smaller, more manageable intervals. This repeater-like protocol introduces a more efficient entanglement-swapping measurement at the repeater station than the state-of-the-art twin-field protocols. Instead of polarisation encoding, our protocol relies on encoding keys in the photon-number basis, optimising the states to achieve the highest key rates for each distance. Notably, this protocol shows strong potential for improving long-distance quantum communication by surpassing the capacity of the direct communication channel at a shorter distance than the existing repeater protocols such as twin-field QKD while achieving an overall higher transmission distance.

Finally, in this thesis, we demonstrate that for the Pauli-dephasing channel, placing a node in the middle of the quantum channel to perform a Bell-state measurement as an entanglement-swapping operation does not result in improved key rates, even with reduced decoherence. As a result, we propose an entanglement purification protocol that refines a larger set of noisy entangled states into a smaller set of high-fidelity ones using local operations and classical communication. This purification protocol builds upon earlier purification methods, extending their application from two Bell pairs to any number of Bell pairs

and thereby achieving the capacity of the dephasing channel. Through numerous recursive iterations, it produces near-perfect Bell pairs, making it well-suited for quantum repeaters and correcting dephasing errors in quantum computers.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Encryption has been an integral part of society since ancient times, serving as a tool to protect information and maintain secrecy. Among the earliest and most notable methods of encryption is the Caesar cipher, named after Julius Caesar, who famously used it to secure messages sent to his military. This technique, known as 'letter substitution', operates by shifting each letter in a message by a fixed number of positions, as determined by a key. While the Caesar cipher was effective in its time, its simplicity ultimately led to its downfall, as the limited number of possible shifts made it vulnerable to brute-force attacks. Moreover, its security depended on keeping the encryption method itself secret, a violation of Kerckhoffs' principle [1], which states that a cryptographic system should remain secure even if everything about the system is public knowledge [1–3].

As history progressed, encryption techniques became increasingly sophisticated, evolving from simple pen-and-paper methods to complex electromechanical devices. One notable example is the Enigma machine, used by the Germans during World War II to encode military messages. The Enigma employed a system of rotors and electrical circuits to transform a message into ciphertext [4]. Its settings changed daily, with operators referencing a codebook that specified the configuration for each day. Messages were typed into the machine letter by letter, lighting up corresponding encrypted letters on the keyboard. For instance, typing "A" would light up the letter "Y". The encrypted message was then announced via radio. While British forces intercepted these transmissions, deciphering them was nearly impossible without the settings of the machine, as the Enigma offered more than 158 quintillion possible configurations, making brute-force attacks infeasible. However, the Enigma code was eventually broken with the invention of Alan Turing's Bombe machine. By leveraging predictable parts of messages, known as "cribs," and exploiting reciprocal encryption properties of the Enigma machine (e.g., if "A" maps to "Y," then "Y" maps back to "A"), the Bombe systematically tested and eliminated incorrect configurations [4, 5]. This breakthrough changed the course of the war, leading to the defeat of the Nazis.

As cryptographic techniques evolved and cryptanalysts consistently discovered vulnerabilities in the existing codes, the focus shifted towards designing methods that are robust enough to resist the computational power of modern computers. This shift led to the development of encryption methods relying on mathematical algorithms such as RSA [6], im-

plemented by Rivest, Shamir and Adleman. RSA is an example of public-key cryptography, where two mathematically linked keys are used, one public and one private. In RSA, the public key is shared with everyone and the private key is kept secret. Messages are encrypted using the public key and can only be decrypted with the corresponding private key, ensuring secure communication over untrusted networks. The security of RSA lies in the mathematical challenge of factoring large numbers into their prime components. In RSA, the public and private keys are linked through the product of two large prime numbers. The public key includes this product, known as the modulus, and an exponent used for encryption. However, the private key is derived from the same prime numbers, which remains secret. Without knowing these prime numbers, it is computationally infeasible to reverse-engineer the private key from the public key, as factoring large numbers becomes exponentially harder as their size increases.

Therefore, RSA offers computational security, as its security relies on the assumed hardness of a mathematical problem. However, the discovery of quantum computers [7–13] poses a significant threat to RSA encryption [14]. Quantum computers use qubits which can exist in multiple states simultaneously, enabling them to perform certain calculations exponentially faster. Algorithms such as Shor's algorithm [15], can exploit this capability to factor large numbers efficiently. For instance, while brute-forcing the private key would take billions of years on a classical computer, an ideal quantum computer, in theory, could accomplish this task within a few hours [15–17].

In contrast, one-time pad (OTP) provides information-theoretic security as it remains secure even against adversaries with unlimited computational power. OTP is a symmetric-key scheme that requires a pre-shared key at least as long as the message itself [18]. As the name suggests, the key is discarded after single use and needs to be truly random. In OTP, each character of the message is combined with the corresponding character of the key through modular addition, allowing the recipient to decrypt the message using the same pre-distributed key. Despite its advantage, the key management and distribution is one of the limitations of OTP due to the requirement of single use of keys and storage of large-sized keys.

To address the key distribution challenges of the OTP and the vulnerabilities of RSA encryption, one of the proposed solutions is quantum key distribution (QKD) [19–22] which leverages quantum mechanics to securely distribute keys. In QKD, keys are encoded onto quantum states and transmitted through a quantum channel, where the receiver measures the states to extract the key. The security of QKD relies on the no-cloning theorem [23], which prevents an eavesdropper from copying an unknown quantum state. Any attempt to intercept the key introduces detectable errors by the trusted parties. However, the practical implementation of QKD is limited by the vulnerability of quantum states to loss and noise,

restricting the distance over which keys can be reliably distributed.

While QKD is one of the most widely studied applications of quantum communications, there are several other protocols that harness quantum mechanics to enable secure communication between distant parties. Unlike QKD, quantum secure direct communication (QSDC) [24–33] transmits the actual message directly by encoding it onto quantum states, eliminating the need for key distribution. Quantum secret sharing (QSS) [34–48] enables a secret, either a message or a key, to be distributed among multiple parties, such that it can only be reconstructed when an authorised subset of participants collaborates, making it well-suited for secure communication in distributed settings. Finally, quantum teleportation [49–61], perhaps the most widely recognised concept in quantum communications, allows a quantum state to be transferred between distant parties using shared entanglement and classical communication, without physically sending the state itself. Although these protocols are not the focus of this thesis, they represent essential components of the broader quantum communication landscape.

This thesis aims to improve the performance of QKD by developing and analysing new protocols to address its limitations. Additionally, it seeks to propose protocols that can serve as foundational building blocks for the quantum internet. The quantum internet [62, 63] is a future network designed to enable secure communication, distributed quantum computing, and other advanced quantum technologies. It achieves this by linking quantum devices through entanglement [64, 65], a phenomenon where the states of two or more particles are correlated. In entanglement, the state of one particle depends on the state of the others, regardless of the distance between them. In this thesis, we explore how these entangled quantum states can be utilised and manipulated within our protocols. The remainder of this thesis is organised as follows:

In Chapter 2, we introduce the theoretical tools used throughout this thesis, including matrix mechanics, discrete-variable (DV) and continuous-variable (CV) quantum states, Gaussian operations, and quantum measurement techniques.

In Chapter 3, we present the tools to experimentally implement the CV quantum states discussed in Chapter 2. To this end, we outline the implementation of quantum sideband modulations, Gaussian measurements using homodyne and heterodyne detection, and key optical locking methods such as cavity and phase locking.

In Chapter 4, we present the fundamental concepts of quantum communication theory. We begin with classical and quantum information measures, including entropy and the Holevo bound, followed by an overview of quantum channels such as pure-loss, thermal-loss, and Pauli dephasing. We then introduce key capacity measures and explore both discrete [19, 20] and continuous-variable [21, 22] QKD protocols, which are central to this thesis. The chapter concludes with a discussion of quantum repeaters as a strategy to over-

come channel limitations, and presents a comprehensive overview of state-of-the-art QKD demonstrations.

In Chapters 5, 6, and 7, we present the main results of this thesis. In Chapter 5, we present a CV-QKD protocol that we developed and implemented experimentally. Our protocol uses probabilistic filters at the sender and receiver stations which dynamically optimise the secret-key rate for rapidly changing channels such as terrestrial links and satellite-to-ground communications. Our protocol is able to extract keys even under channel conditions considered non-secure by parameter estimation. Although it improves key rates, the probabilistic nature of the protocol prevents it from reaching or exceeding the quantum channel capacity, which defines the maximum achievable key rate for a given channel.

In Chapter 6, we present a DV-based QKD protocol designed to reduce losses of the pure-loss channel by dividing the quantum channel into smaller segments, a technique known as quantum repeaters. In this approach, entanglement between the trusted parties is established through an untrusted party, referred to as the repeater station, using an entanglement swapping measurement. Our protocol introduces a more efficient entanglement swapping measurement and incorporates high-dimensional states, resulting in improved key rates and greater transmission distances compared to state-of-the-art protocols. Our protocol also surpasses the capacity of the repeaterless lossy channel at much shorter distances compared to existing protocols.

In Chapter 7, we demonstrate that for the Pauli-dephasing channel, a common channel type in quantum communications and quantum computing, a repeater protocol using simple entanglement swapping via a central node is insufficient to exceed the repeaterless capacity. This highlights the necessity of either error correction or purification of the distributed states to achieve better performance. We then propose an entanglement purification protocol that employs an iterative process to purify the states in each round. With repeated iterations, our protocol produces states with a fidelity approaching one and achieves the capacity of the channel.

Finally, in Chapter 8, we conclude this thesis and outline potential directions for future research. A large portion of the work presented in this thesis has been published in or submitted to peer-reviewed journals. Below is a list of related publications:

1. Enhanced Continuous-Variable Quantum Key Distribution Protocol via Adaptive Signal Processing
   Ö. Erkılıç, B. Shajilal, L.O. Conlon, A. Walsh, A. Das, S. Kish, T. Symul, P.K. Lam, S.M. Assad, J. Zhao
   arXiv:2507.18049 (2025), under review in *Communication Physics*.

2. Surpassing the Repeaterless Bound with a Photon-Number Encoded Measurement-

Device-Independent Quantum Key Distribution Protocol
Ö. Erkılıç, L.O. Conlon, B. Shajilal, S. Kish, S. Tserkis, Y.S. Kim, P.K. Lam, S.M. Assad
npj Quantum Information **9**, 29 (2023).

3. Capacity-Achieving Entanglement Purification Protocol for Pauli Dephasing Channel
Ö. Erkılıç, M.S. Winnel, A. Das, S. Kish, P.K. Lam, J. Zhao, S.M. Assad
arXiv:2411.14573 (2024), manuscript under review in *IOP Quantum Science and Technology*.

Below is a list of publications based on research conducted during my PhD that are not included in this thesis:

1. Multi-hop quantum repeater based on heralded teleportation
A.A. Baiju, Ö. Erkılıç, B. Shajilal, L. O. Conlon, P.K. Lam
Manuscript in preparation.

2. Machine Learning Assisted Quantum Communications
A.A. Baiju, Ö. Erkılıç, B. Shajilal, L. O. Conlon, P.K. Lam
Manuscript in preparation.

3. Securing Upstream Continuous-Variable Quantum Key Distribution Networks Against Reference Pulse Side-Channel Attacks
S. Kish, E. Villasenor, Ö. Erkılıç, M. Sayat, S. Camtepe
Manuscript in preparation.

4. Optimal Gaussian Probes for Lossy Phase Estimation
A. Walsh, B. Shajilal, L.O. Conlon, Ö. Erkılıç, O. Thearle, J. Janousek, P.K. Lam, S.M. Assad, J. Zhao
To be submitted to Physical Review Letters (2025).

5. All-Gaussian Binary State Discrimination Beyond the Coherent Helstrom Bound
A. Walsh, B. Shajilal, L.O. Conlon, Ö. Erkılıç, O. Thearle, J. Janousek, P.K. Lam, S.M. Assad, J. Zhao
Manuscript in preparation.

6. Precision bounds for characterising quantum measurement
A. Das, S. Yung, L.O. Conlon, Ö. Erkılıç, A. Walsh, P.K. Lam, S.M. Assad, J. Zhao
Submitted to Nature Communications (2025).

7. Generation of Squeezed-Cat States via Spontaneous Parametric Down-Conversion for GKP Encoding

Ö. Erkılıç, A. Das, B. Shajilal, P.K. Lam, S.M. Assad
Manuscript in preparation.

Chapter 2

Theoretical Quantum Optics Toolbox

This chapter introduces the key theoretical tools from quantum optics that underpin the protocols and analysis developed in later chapters. It begins with a brief overview of the matrix formalism used to represent quantum states, followed by a discussion of discrete-variable and continuous-variable states, the two main physical platforms used in quantum communication. The focus then narrows to Gaussian states, as they form the basis for many of the protocols analysed in this thesis, particularly in Chapters 3, 4 and 5. Their mathematical simplicity and experimental relevance make them an essential starting point for understanding more advanced quantum communication schemes.

2.1 Matrix Mechanics

Schrödinger's wavefunction [66] is the most well-known way to describe how a state evolves in quantum mechanics. However, in the context of quantum information, we use the matrix formalism developed by Heisenberg, Born, and Jordan [67, 68] to examine how states evolve under specific transformations, which is also the approach used in this thesis.

2.1.1 Density Matrices

The density matrix for a pure state, $|\psi\rangle$, is expressed as

$$\rho = |\psi\rangle\langle\psi| \,. \tag{2.1}$$

In experiments, however, the state is often mixed, and the density matrix is then written as a weighted sum of pure states

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \,, \tag{2.2}$$

where p_i is the probability associated with each pure state, and the probabilities satisfy $\sum_i p_i = 1$. The probability of measuring the i^{th} outcome is given by $\text{Tr}[\rho\Pi_i]$, where $\text{Tr}[\rho]$ denotes the trace operation on the matrix ρ and Π_i is the projector.

Density matrices, whether representing pure or mixed states, have several important properties:

- **Positivity**: $\rho \geq 0$. This means that the density matrix is positive semidefinite, with all its eigenvalues being non-negative, ensuring no negative probabilities.
- **Normalisation**: $\mathrm{Tr}[\rho] = 1$. This means that the trace of the density matrix ρ is equal to 1, which corresponds to the sum of all probabilities being 1. The trace of the density matrix is particularly useful, as it helps determine the probability of measurement outcomes based on a given measurement operator. Additionally, it can be used to distinguish between pure and mixed states: $\mathrm{Tr}[\rho^2] = 1$ for pure states, and $\mathrm{Tr}[\rho^2] < 1$ for mixed states.
- **Hermiticity**: $\rho = \rho^\dagger$. The density matrix, ρ, is Hermitian, meaning it is equal to its conjugate transpose, $\rho^\dagger$, a property required to ensure real, measurable probabilities.

2.1.2 Operator Matrices

As discussed in the previous section, physical measurements must yield real values, which is why the associated observable must be represented by a Hermitian operator. Unlike density matrices, however, observables are not required to satisfy the conditions of positivity or normalisation. For instance, in the case of an observable $\hat{O} = \sum_i \lambda_i |o_i\rangle\langle o_i|$, the eigenvalues λ_i are not required to be non-negative.

2.2 Discrete-Variable Quantum States

Discrete-variable (DV) quantum systems are represented by a two-dimensional Hilbert space and are widely used in quantum computing and communications. In these systems, the most common state is known as a qubit, which is often described in the computational basis with $|0\rangle$ and $|1\rangle$, where

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.3}$$

Any pure qubit state can be expressed as a linear combination of $|0\rangle$ and $|1\rangle$ by [69]

$$|\psi\rangle = \cos\big(\theta/2\big)\,|0\rangle + e^{i\phi}\sin\big(\theta/2\big)\,|1\rangle\,, \tag{2.4}$$

$0 \leq \theta \leq \pi$ represents the polar angle, and $0 \leq \phi \leq 2\pi$ denotes the azimuthal angle. Eq. (2.4) describes a qubit as a vector on the Bloch sphere, as shown in Fig. 2.1. When $\theta = 0$ or $\theta = \pi$, the qubit is located at the poles of the sphere, corresponding to the computational basis states $|0\rangle$ and $|1\rangle$. For $\theta = \pi/2$, the qubit lies on the equator of the sphere.

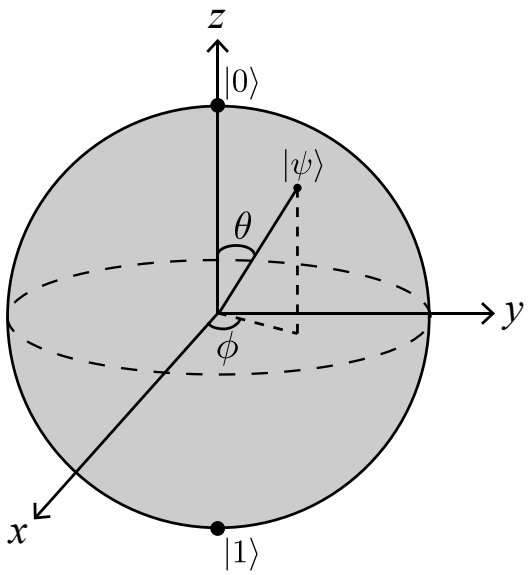

Figure 2.1: Bloch sphere representation of qubits. The angles θ and ϕ represent the polar and azimuthal angles, respectively. The state $|\psi\rangle$ corresponds to the expression in Eq. (2.4). The north pole of the sphere represents the computational state $|0\rangle$, while the south pole represents $|1\rangle$.

In addition to the computational basis states, there are four other key states relevant for quantum key distribution, which are as follows:

$$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}, \tag{2.5a}$$

$$|+i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \quad |-i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}. \tag{2.5b}$$

These six vectors correspond to the eigenvectors of the Pauli matrices, a fundamental class of 2×2 matrices in quantum mechanics. For example, the computational basis states shown in Eq. (2.3) are eigenvectors of the Pauli matrix, σ_z, while Eq. (2.5a) and Eq. (2.5b) are the eigenvectors of the Pauli matrices σ_x and σ_y, respectively. These matrices are also referred to as the Z, X, and Y bases and are expressed as

$$\sigma_z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}, \quad \sigma_x = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}, \quad \sigma_y = \begin{pmatrix}0 & -i\\i & 0\end{pmatrix}. \tag{2.6}$$

Therefore, using these Pauli matrices and the identity matrix, we can write any single qubit

density matrix in the following form

$$\rho = \frac{1}{2}\big(\mathbb{1}_2 + c \cdot \sigma\big), \tag{2.7}$$

where $\sigma = (\sigma_x, \sigma_y, \sigma_z)$ are the Pauli matrices while $c = (c_x, c_y, x_z)$ are the Bloch vectors where they must satisfy $|c| \leq 1$. For pure qubit states $|c| = 1$ and for mixed qubit states $|c| < 1$.

Experimentally, a qubit in the computational basis corresponds to the polarisation of light in a photonic system. For instance, the $|0\rangle$ state represents horizontally polarised light, while the $|1\rangle$ state corresponds to vertically polarised light.

2.2.1 Single Qubit Operations

Most quantum processors begin with the qubit in the $|0\rangle$ state. To create any desired single-qubit state, we need to apply certain operations to $|0\rangle$. Therefore, in this section, we outline the required transformation to generate the desired states.

U Gate

Before discussing specific gates, we introduce the U gate, which represents the most general unitary transformation for a single-qubit state.

$$U(\theta, \phi, \lambda) = \begin{pmatrix} \cos\big(\theta/2\big) & -e^{i\lambda}\sin\big(\theta/2\big) \\ e^{i\phi}\sin\big(\theta/2\big) & e^{i(\lambda+\phi)}\cos\big(\theta/2\big) \end{pmatrix}, \tag{2.8}$$

where $0 \leq \theta \leq \pi,\ 0 \leq \phi \leq 2\pi$ and $0 \leq \lambda \leq 2\pi$.

Standard Rotation Gates

There are three key rotation gates that define rotations around the x, y, and z axes of the Bloch sphere. The rotation around the x-axis is represented as

$$R_x(\theta) = \begin{pmatrix} \cos\big(\theta/2\big) & -i\sin\big(\theta/2\big) \\ -i\sin\big(\theta/2\big) & \cos\big(\theta/2\big) \end{pmatrix} = U(\theta, -\pi/2, \pi/2), \tag{2.9}$$

where, for $\theta = \pi$, the matrix corresponds to the Pauli-X gate, $X = \sigma_x$, as shown in Eq. (2.6). The Pauli-X gate functions as the quantum equivalent of the classical NOT gate, flipping the states $|0\rangle$ to $|1\rangle$ and vice versa (i.e., $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$).

In a similar fashion, a rotation around the y-axis is represented by

$$R_y(\theta) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix} = U(\theta, 0, 0), \tag{2.10}$$

and when $\theta = \pi$, it corresponds to the Pauli-Y gate, $Y = \sigma_y$, as seen in Eq. (2.6). Finally, the rotation around the z-axis is expressed as

$$R_z(\phi) = \begin{pmatrix} e^{-i\phi/2} & 0 \\ 0 & e^{i\phi/2} \end{pmatrix} = U(0, \phi, \lambda), \tag{2.11}$$

and when $\phi = \pi$, this gives the Pauli-Z gate, $Z = \sigma_z$, from Eq. (2.6).

Hadamard Gate

The Hadamard gate is defined as

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.12}$$

The Hadamard gate is essential for creating quantum superpositions, such as $H|0\rangle = |+\rangle$ and $H|1\rangle = |-\rangle$. It is also widely used for basis transformations. For example, the relation $HZH = X$ illustrates this.

2.2.2 Two-Qubit Operations

In a two-qubit system, the dimensionality increases to $2^2 = 4$. As a result, the basis vectors for this system are formed by taking the tensor products of the single-qubit basis vectors, such as $|0\rangle \otimes |0\rangle$. The most commonly used basis vectors for a two-qubit system are listed below

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{2.13}$$

While there are many two-qubit gates, this thesis focuses on the CNOT and SWAP gates. For other gates, refer to [69].

Table 2.1: Truth table of the CNOT gate. CNOT acts on two-qubit states with first and second qubits being control and target, respectively.

Input	Output
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

CNOT Gate

The most commonly used controlled Pauli gate is the CNOT gate, also referred to as the Controlled-X gate. This gate flips the target qubit when the control qubit is in the state $|1\rangle$, as shown in Table 2.1 and is given by

$$C_X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.14}$$

However, if the roles of the qubits are reversed, such that the first qubit becomes the target and the second qubit becomes the control, the equivalent C_X gate is expressed as

$$C_X = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}. \tag{2.15}$$

The CNOT gate is highly versatile, as it can be combined with the Hadamard gate to create entangled states, such as the Bell state $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

SWAP Gate

The SWAP gate is frequently used when working with multiple qubits, allowing operations to be applied between different qubits by reordering them. In a two-qubit system, as the name implies, it swaps the two qubits, as shown below

$$|00\rangle \to |00\rangle\,, \quad |01\rangle \to |10\rangle\,, \quad |10\rangle \to |01\rangle\,, \quad |11\rangle \to |11\rangle\,. \tag{2.16}$$

The matrix representation of this operation is expressed as

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.17}$$

2.3 Continuous-Variable Quantum Optics

Unlike DV quantum systems, continuous-variable (CV) systems operate within an infinite-dimensional Hilbert space, as the name suggests. To explore this, we begin with a quantum description of the electromagnetic (EM) field, followed by an introduction to important CV states that are used throughout this thesis.

2.3.1 Quantisation of the Electromagnetic Field

Quantising the electromagnetic field is essential for understanding light-matter interactions at the quantum level, as well as photon statistics and the behaviour of photons within a cavity. To explore this, consider an EM field confined within a finite volume. Solving Maxwell's equations with the boundary condition that the EM field goes to zero at the walls allows us to describe the EM field in the following way

$$\mathbf{E}(\mathbf{r},t) = i\sum_k \left(\frac{\hbar\omega_k}{2\varepsilon_0}\right)^{1/2} [\alpha_k \mathbf{u}_k(\mathbf{r}) e^{-i\omega_k t} + \alpha_k^* \mathbf{u}_k^*(\mathbf{r}) e^{i\omega_k t}], \tag{2.18}$$

where $\hbar$ is the reduced Planck's constant, ω_k refers to the angular frequency of the k^{th} mode of the electric field, ε_0 is the permittivity of free space, α_k and α_k^* are dimensionless amplitudes and $\mathbf{u}_k$ are the orthogonal mode functions, $\mathbf{r}$ is the position vector and t denotes time [70]. Similarly, the magnetic field can be expressed as

$$\mathbf{B}(\mathbf{r},t) = -i\sum_k \left(\frac{\hbar}{2\varepsilon_0}\right)^{1/2} [\alpha_k \mathbf{k}\times\mathbf{u}_k(\mathbf{r}) e^{-i\omega_k t} + \alpha_k^* \mathbf{k}\times\mathbf{u}_k^*(\mathbf{r}) e^{i\omega_k t}], \tag{2.19}$$

where $\mathbf{k}$ represents the propagation direction of the EM wave. The total energy of the EM field within a volume V is derived by adding the contributions from both the electric and magnetic field energies.

$$\begin{aligned} \mathcal{H} &= \frac{1}{2}\int_V (\varepsilon_0 |\mathbf{E}(\mathbf{r},t)|^2 + \mu_0 |\mathbf{B}(\mathbf{r},t)|^2) \\ &= \sum_k \hbar\omega_k (\alpha_k^*\alpha_k + \frac{1}{2}), \end{aligned} \tag{2.20}$$

where μ_0 is the permeability of free space. The quantisation of the EM field in Eq. (2.18) can be obtained by substituting the complex amplitudes α_k and α_k^* with annihilation and creation operators $\hat{a}_k$ and $\hat{a}_k^\dagger$, respectively [71]. These operators satisfy the bosonic commutation relations

$$[\hat{a}_k, \hat{a}_l] = [\hat{a}_k^\dagger, \hat{a}_l^\dagger] = 0, \quad [\hat{a}_k, \hat{a}_l^\dagger] = \delta_{kl}, \tag{2.21}$$

where δ_{kl} denotes the Dirac delta function. Therefore, the quantised EM field becomes

$$\mathbf{E}(t) = i \sum_k \left(\frac{\hbar \omega_k}{2\varepsilon_0} \right)^{1/2} [\hat{a}_k e^{i\omega_k t} + \hat{a}_k^\dagger e^{-i\omega_k t}]. \tag{2.22}$$

Using the quantised EM field in Eq. (2.22), the Hamiltonian becomes

$$\hat{\mathcal{H}} = \sum_k \hbar \omega_k (\hat{a}_k \hat{a}_k^\dagger + \frac{1}{2}). \tag{2.23}$$

This represents the total energy across the k modes, with each mode contributing an amount proportional to the number of photons present, along with the vacuum fluctuation energy, $\hbar\omega_k/2$. Vacuum fluctuations, arising from quantum mechanics, are unavoidable noise present in all measurements in our experiments, commonly referred to as the quantum shot noise limit.

The eigenstates of the Hamiltonian $\hat{\mathcal{H}}$ in Eq. (2.23) are known as Fock states, or photon number states, denoted by $|n_k\rangle$, where n_k indicates the number of photons in the k^{th} mode. These states form a complete orthonormal basis

$$\langle n_k | m_k \rangle = \delta_{nm}, \quad \sum_{n_k=0}^{\infty} |n_k\rangle\langle n_k| = \mathbb{1}, \tag{2.24}$$

where $|m_k\rangle$ is another Fock state in the k^{th} mode and δ_{nm} is the delta function. Fock states are particularly useful, as they can be used to represent other quantum states of light in the following form

$$|\psi\rangle = \sum_{n_k} c_k |n_k\rangle , \tag{2.25}$$

where c_k are the complex coefficients representing how much of each Fock state contributes to the overall state $|\psi\rangle$. Furthermore, Fock states also clarify the role of annihilation and creation operators. When applied to a Fock state, these operators remove or add a photon, respectively.

$$\hat{a}_k |n_k\rangle = \sqrt{n_k} |n_k - 1\rangle , \quad \hat{a}_k^\dagger |n_k\rangle = \sqrt{n_k + 1} |n_k + 1\rangle . \tag{2.26}$$

The mean photon number of each Fock state is then determined by the number operator,

defined as $\hat{n}_k |n_k\rangle = n_k |n_k\rangle$, where the operator is expressed as

$$\hat{n}_k = \hat{a}_k^\dagger \hat{a}_k. \tag{2.27}$$

Quadrature Operators

Since the annihilation and creation operators are not Hermitian and cannot be measured, we instead introduce the quadrature operators of the EM field, denoted as $\hat{x}$ and $\hat{p}$ [72].

$$\hat{x} = \hat{a}_k + \hat{a}_k^\dagger, \quad \hat{p} = i(\hat{a}_k^\dagger - \hat{a}_k). \tag{2.28}$$

Here, $\hat{x}$ and $\hat{p}$ correspond to the amplitude and phase quadratures of the EM field, respectively. Using these operators, a more general expression for any pair of conjugate quadratures can be written with a rotation angle θ as follows

$$\hat{x}^\theta = \hat{a}_k e^{-i\theta} + \hat{a}_k^\dagger e^{i\theta}. \tag{2.29}$$

Importantly, these quadrature operators do not commute, as can be shown by substituting Eq. (2.28) into Eq. (2.21).

$$[\hat{x}, \hat{p}] = 2i. \tag{2.30}$$

$\hat{x}$ and $\hat{p}$ can be viewed as the real and imaginary components of the annihilation and creation operators [73]. The eigenstates of the quadrature variables are obtained from

$$\hat{x} |x\rangle = x |x\rangle, \quad \hat{p} |p\rangle = p |p\rangle, \tag{2.31}$$

where $x \in \mathbb{R}$ and $p \in \mathbb{R}$ correspond to continuous variables. Additionally, the EM field can be expressed in terms of the quadrature operators by substituting them into Eq. (2.22)

$$\mathbf{E}(t) = \sum_k \left(\frac{\hbar\omega_k}{2\varepsilon_0}\right)^{1/2} [\hat{x} \sin(\omega_k t) - \hat{p} \cos(\omega_k t)]. \tag{2.32}$$

From Eq. (2.32), we can see that the quadratures correspond to the in-phase and out-of-phase components of the EM field.

Heisenberg's Uncertainty Relation

The Heisenberg uncertainty principle states that it is impossible to measure both quadratures of the EM field simultaneously with perfect precision. As a result, the product of the

quadrature operators must satisfy the following relation, with $\hbar$ set to 2,

$$\Delta\hat{x}^2\Delta\hat{p}^2 \geq 1, \tag{2.33}$$

where $\Delta\hat{x}^2 = \langle\hat{x}^2\rangle - \langle\hat{x}\rangle^2$ gives the variance of the measurement in the x quadrature which similarly applies to the p quadrature and $\langle\hat{x}\rangle$ represents the expectation value of x.

2.3.2 Gaussian States and Gaussian Operations

In this section, we present key Gaussian states and Gaussian operations that will be used throughout this thesis. Since the states discussed are either single or two-mode, we omit the mode subscript k for simplicity.

As both single and two-modes states are Gaussian they can be fully described by their first (mean) and second moments (variance). The mean and covariance matrix of a single-mode state is expressed as,

$$\mu = \begin{pmatrix} \langle\hat{x}\rangle \\ \langle\hat{p}\rangle \end{pmatrix}, \quad \sigma = \begin{pmatrix} \langle\hat{x}^2\rangle - \langle\hat{x}\rangle^2 & \frac{1}{2}\langle\hat{x}\hat{p} + \hat{p}\hat{x}\rangle - \langle\hat{x}\rangle\langle\hat{p}\rangle \\ \frac{1}{2}\langle\hat{x}\hat{p} + \hat{p}\hat{x}\rangle - \langle\hat{x}\rangle\langle\hat{p}\rangle & \langle\hat{p}^2\rangle - \langle\hat{p}\rangle^2 \end{pmatrix}. \tag{2.34}$$

Similarly, two-mode Gaussian states can be represented by a covariance matrix, which is particularly useful for describing entanglement or quantum correlations [74].

$$\sigma_{ij} = \frac{1}{2}\langle\hat{o}_i\hat{o}_j + \hat{o}_j\hat{o}_i\rangle - \langle\hat{o}_i\rangle\langle\hat{o}_j\rangle, \tag{2.35}$$

Here, we define $\hat{o} = (\hat{o}_1, \hat{o}_2, \hat{o}_3, \hat{o}_4) = (\hat{x}_1, \hat{p}_1, \hat{x}_2, \hat{p}_2)$, where $\hat{x}_1, \hat{p}_1$ and $\hat{x}_2, \hat{p}_2$ are the quadrature operators for the first and second modes, respectively. Throughout this thesis, the operators $\hat{a}, \hat{a}^\dagger$ and $\hat{b}, \hat{b}^\dagger$ will be used to represent the annihilation and creation operators for the first and second modes, respectively.

Vacuum States

The vacuum state is the zero-photon state of the quantum optical field, denoted as $|0\rangle$. Despite containing zero photons, the energy of this state is $\langle 0|\hat{\mathcal{H}}|0\rangle = \hbar\omega/2$. Notably, this corresponds to the energy of the vacuum fluctuations previously referred to as "quantum shot noise" [75] in Sec. 2.3.1. The vacuum state is the minimal uncertainty state, with both quadratures satisfying $\Delta\hat{x} = \Delta\hat{p} = 1$.

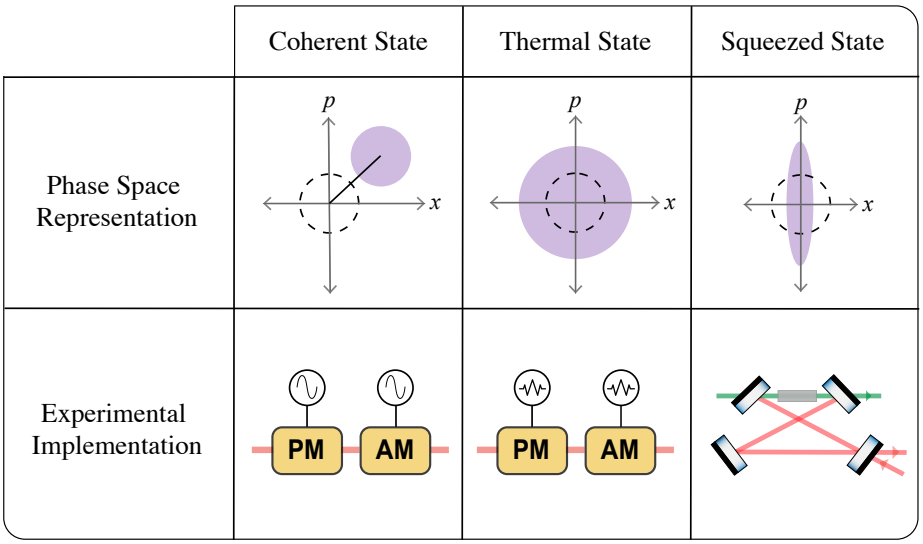

Figure 2.2: Comparison of coherent, thermal, and squeezed states. The first row illustrates the phase-space representation of each state, with the dashed circle representing the vacuum state. The second row shows the experimental setups for generating these states: coherent states are produced by feeding a sine wave into the phase and amplitude electro-optic modulators (EOM), denoted as PM and AM, respectively. Thermal states are generated by applying white noise to the EOMs, and squeezed states are created using a bowtie cavity with a Periodically Poled Potassium Titanyl Phosphate (PPKTP) crystal and four mirrors for optical parametric amplification.

Coherent States and Displacement Operator

Coherent states can be thought as the quantum mechanical states that approximate the output of a stable laser [76]. Similar to vacuum states, coherent states are also minimum-uncertainty states as the product of their uncertainty in amplitude and phase quadratures saturate the Heisenberg uncertainty principle given in Eq. (2.33). Coherent states are the eigenstates of the annihilation operator

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,, \tag{2.36}$$

and can be expanded in the Fock basis as

$$|\alpha\rangle = \sum_n |n\rangle\langle n|\alpha\rangle = e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,, \tag{2.37}$$

where $\alpha = (x + ip)/2$ is the complex amplitude and when $\alpha = 0$, the state simply becomes a vacuum state. Coherent states can be generated via a displacement operator acting on a vacuum state

$$|\alpha\rangle = \hat{D}(\alpha)\,|0\rangle = \exp\Big(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\Big), \tag{2.38}$$

where $\hat{D}(\alpha)$ denotes the displacement operator. These states are obtained by feeding a sine wave at the desired frequency to phase and amplitude electro-optic modulators as shown in Fig. 2.2. As coherent states are single-mode Gaussian states, they can be described by first and second moments which are given by

$$\mu = \begin{pmatrix} 2\mathrm{Re}(\alpha) \\ 2\mathrm{Im}(\alpha) \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.39}$$

The photon number distribution of coherent states follows a Poissonian distribution with the probability of finding a certain number of photons being

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n} e^{-|\alpha|^2}}{n!}. \tag{2.40}$$

The mean photon number and the variance in photon number for coherent states can be determined from

$$\langle \hat{n} \rangle = |\alpha|^2, \quad \Delta\hat{n}^2 = \langle \hat{n}^2 \rangle - \langle \hat{n} \rangle^2 = |\alpha|^2. \tag{2.41}$$

In contrast to Fock states, coherent states form an overcomplete basis meaning that instead of the completeness relation summing up to the identity, it follows

$$\int |\alpha\rangle\langle\alpha| \, d\alpha^2 = \pi \mathbb{1}. \tag{2.42}$$

Thermal States

Thermal states can be viewed as a coherent mixture of Fock states. The density matrix of a thermal state with a mean photon number, $\bar{n}$, is expressed as [74]

$$\rho(\bar{n}) = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(1+\bar{n})^{n+1}} |n\rangle\langle n| . \tag{2.43}$$

Alternatively, they can be also expressed as a Gaussian mixture of coherent states as [77]

$$\rho(\alpha) = \int \frac{1}{\pi\bar{n}} e^{-|\alpha|^2/\bar{n}} |\alpha\rangle\langle\alpha| \; d^2\alpha. \tag{2.44}$$

The covariance matrix of a thermal state is given by

$$\sigma = \begin{pmatrix} 2\bar{n}+1 & 0 \\ 0 & 2\bar{n}+1 \end{pmatrix}, \tag{2.45}$$

with zero mean. It is evident from the covariance matrix that thermal states are not minimum uncertainty states. In quantum key distribution, the key information is often encoded onto coherent states. However, the average state corresponds to a thermal state [78]. These states are experimentally generated by supplying white noise to the electro-optic modulators over a specific frequency range as shown in Fig. 2.2.

Squeezed States and Squeezing Operator

Squeezed states are another example of minimum uncertainty states. Unlike coherent states, which have equal uncertainty in both quadratures, squeezed states exhibit reduced uncertainty in one quadrature while the uncertainty in the other is correspondingly increased. The squeezing operator is expressed as [79]

$$\hat{S}(\varepsilon) = \exp\left(\frac{1}{2}(\varepsilon^* \hat{a}^2 - \varepsilon \hat{a}^{\dagger 2})\right) \quad \text{with} \quad \varepsilon = re^{2i\phi}, \tag{2.46}$$

where r denotes the squeezing parameter and ϕ represents the squeezing angle. Using Eq. (2.46), a squeezed vacuum state can be represented as follows

$$|\varepsilon\rangle = \frac{1}{\sqrt{\cosh(r)}} \sum_{n=0}^{\infty} \left(-e^{-i\phi}\tanh(r)\right)^n \frac{\sqrt{(2n)!}}{2^n n!} |2n\rangle\,. \tag{2.47}$$

The covariance matrix of a squeezed vacuum state with squeezing angle $\phi = 0$ and zero mean is given by [74]

$$\sigma = \begin{pmatrix} e^{-2r} & 0 \\ 0 & e^{2r} \end{pmatrix}. \tag{2.48}$$

This matrix is obtained by applying a single-mode squeezing operation to a vacuum state within the covariance matrix formalism. The squeezing operation in this representation is defined as [74]

$$S(r) = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix}. \tag{2.49}$$

Experimentally, squeezed states are generated via the use of optical parametric amplifier (refer to Refs. [79, 80] for further details) as shown in Fig. 2.2.

Two-Mode Squeezed Vacuum States and Two-Mode Squeezing

Two-mode squeezed vacuum (TMSV) states hold significant importance in continuous-variable quantum optics. Their non-classical nature and entanglement make them essential for various applications in quantum communications. A TMSV state can be generated by

interfering two orthogonal squeezed states on a beamsplitter. The unitary operator responsible for generating two-mode squeezing is expressed as [74]

$$\hat{S}_2(r) = \exp\left(\frac{r}{2}(\hat{a}\hat{b} - \hat{a}^\dagger\hat{b}^\dagger)\right), \tag{2.50}$$

where r corresponds to the two-mode squeezing parameter and $\hat{a}$, $\hat{b}$ are the annihilation operators and $\hat{a}^\dagger$, $\hat{b}^\dagger$ are the creation operators for the first and second modes, respectively. The squeezing operator acting on two-mode vacuum states gives a TMSV state in the Fock-basis as [74]

$$|\text{TMSV}\rangle = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}(-\lambda)^n |n\rangle_a |n\rangle_b , \tag{2.51}$$

where $\lambda = \tanh(r) \in [0, 1]$. In the covariance matrix picture, the squeezing operation can be given as [74]

$$S_2(r) = \begin{pmatrix} \cosh(r)\mathbb{1}_2 & \sinh(r)\sigma_z \\ \sinh(r)\sigma_z & \cosh(r)\mathbb{1}_2 \end{pmatrix} \quad \text{where} \quad \mathbb{1}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.52}$$

Thus, applying the squeezing operator to the covariance matrix of a two-mode vacuum state results in the following covariance matrix for a TMSV state [74]

$$\sigma_{\text{TMSV}} = \begin{pmatrix} V\mathbb{1}_2 & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & V\mathbb{1}_2 \end{pmatrix}, \tag{2.53}$$

where $V = \cosh(2r)$ denotes the thermal variance. Note that Eq. (2.53) is particularly useful for the security analysis of quantum key distribution and will be frequently referenced throughout this thesis.

Phase Rotation

Phase rotation is another example of a Gaussian transformation where its operator is expressed as [74]

$$\hat{R}(\theta) = \exp\left(-i\theta\hat{a}^\dagger\hat{a}\right), \tag{2.54}$$

with θ representing the angle of rotation. In the covariance matrix picture, this unitary matrix is given as [74]

$$R(\theta) = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}. \tag{2.55}$$

Beamsplitter

As the simplest example of an interferometer, the beamsplitter is one of the most important Gaussian transformations, which is defined by [74]

$$\hat{B}(\theta) = \exp\left(\theta(\hat{a}^\dagger \hat{b} - \hat{a}\hat{b}^\dagger)\right), \tag{2.56}$$

where $\theta = \cos^2\theta \in [0, 1]$ represents the beamsplitter transmissivity, τ. When $\tau = 1/2$, the beamsplitter is considered balanced. In the covariance matrix formalism, the beamsplitter transformation is given as

$$B(\tau) = \begin{pmatrix} \sqrt{\tau}\mathbb{1}_2 & \sqrt{1-\tau}\mathbb{1}_2 \\ -\sqrt{1-\tau}\mathbb{1}_2 & \sqrt{\tau}\mathbb{1}_2 \end{pmatrix}. \tag{2.57}$$

2.4 Measurements

In quantum mechanics, measurements are described by a set of linear operators, $\hat{M}_m$, acting on the observed state, where m represents the possible measurement outcomes. Assuming $|\psi\rangle$ is the state of the quantum system before the measurement, the probability of obtaining the outcome m is given by [69]

$$p(m) = \langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle\,. \tag{2.58}$$

This is also known as the Born rule and the state after the measurement can be expressed as

$$|\psi'\rangle = \frac{\hat{M}_m\,|\psi\rangle}{\sqrt{\langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle}}. \tag{2.59}$$

In quantum mechanics, measurement operators must satisfy the completeness criteria,

$$\sum_m = \hat{M}_m^\dagger \hat{M}_m = \mathbb{1}, \tag{2.60}$$

which ensures that the sum of probabilities for all possible outcomes equals one

$$\sum_m p(m) = \sum_m \langle\psi|\hat{M}_m^\dagger \hat{M}_m|\psi\rangle = 1. \tag{2.61}$$

2.4.1 Projective Measurements

Projective measurements are widely used in quantum computation and communication. These measurements are represented by a Hermitian observable, $\hat{M}$, which can be expressed

in its spectral decomposition as

$$\hat{M} = \sum_m m\hat{P}_m, \tag{2.62}$$

where $\hat{P}_m$ is the projector associated with the eigenvalue m. After measuring the state $|\psi\rangle$, the probability of getting the outcome m is given by

$$p(m) = \langle\psi|\hat{P}_m|\psi\rangle\,. \tag{2.63}$$

Therefore, for a given outcome m, the state after the measurement can be expressed as

$$|\psi'\rangle = \frac{\hat{P}_m\,|\psi\rangle}{\sqrt{p(m)}}. \tag{2.64}$$

Projective measurements are a special case of the measurements described in the previous section. In addition to satisfying the completeness condition, the projectors are mutually orthogonal, meaning each projector corresponds to a distinct, non-overlapping subspace [69].

2.4.2 Positive Operator-Valued Measure (POVM)

POVM operators represent the most general form of measurements in quantum mechanics and are described by a set of operators denoted as $\{\hat{E}_m\}$

$$\hat{E}_m = \hat{M}_m^\dagger \hat{M}_m, \tag{2.65}$$

where $\hat{M}_m$ is the measurement operator. E_m is a positive operator that follows $\sum_m \hat{E}_m = \mathbb{1}$ and the probability of an outcome is obtained from $p(m) = \langle\psi|\hat{E}_m|\psi\rangle$ [69]. These operators $\hat{E}_m$ are also known as the POVM elements, and the entire set $\hat{E}_m$ forms the POVM.

2.5 Concluding Remarks

This chapter presented the theoretical background relevant to this thesis and highlighted the key states and operations that will be used throughout. While a brief overview of experimental implementations for some quantum states was provided, the following chapters will explore those most central to this work in more detail. For readers interested in learning more about other quantum states and operations, we recommend the following references [72–74].

Chapter 3

Experimental Realisation of Continuous-Variable Quantum Optics

This chapter introduces the experimental tools that are essential for implementing our quantum key distribution protocol given in Chapter 5. These tools are critical for modulating, measuring, and stabilising quantum optical states in a practical laboratory setting. We begin with a discussion on linearised field operators, which are fundamental for understanding amplitude and phase modulations in quantum optics experiments. This leads naturally to the quantum sideband picture, which captures how quantum information is encoded around the carrier frequency. The chapter then explains how quantum states are measured using homodyne and heterodyne detection, and concludes with a description of the locking techniques used to stabilise the experiment over long durations.

3.1 The Quantum Sideband Modulations

In this section, we provide an explanation of how the state of light is described through the linearisation of field operators. We also explore the quantum sideband representation, using phasor diagrams to visualise quantum states more intuitively. We then explore classical modulation schemes, such as amplitude and phase modulation, and present their quantum counterparts.

3.1.1 Linearisation of Operators

Linearising the quadrature operators is crucial for understanding quantum optical experiments involving sideband modulations. In most quantum optics experiments, the electromagnetic fluctuations are small compared to the intensity of the laser beam, allowing operators representing the electromagnetic field to be approximated as a steady-state value, corresponding to the classical field amplitude, plus small quantum fluctuations. To simplify the analysis, only the linear terms in these fluctuations are considered. Therefore, the

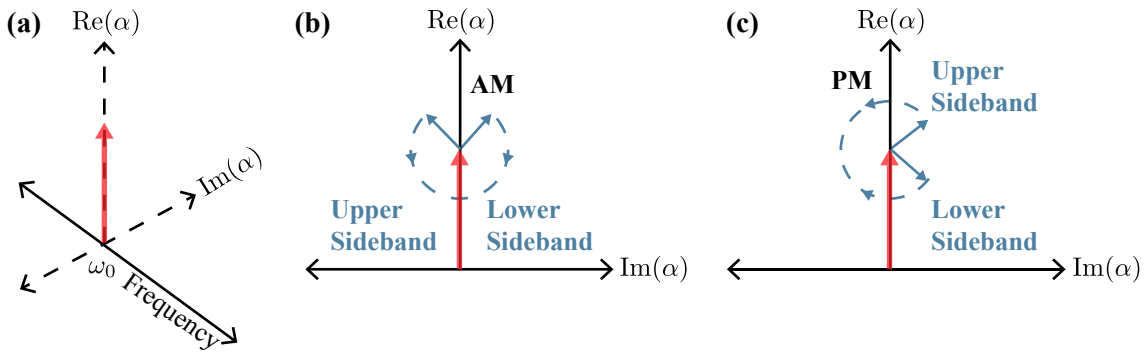

Figure 3.1: Phasor diagrams Phasor diagrams of **(a)** the carrier frequency of the laser **(b)** amplitude modulation and **(c)** phase modulation, respectively.

linearised annihilation and creation operators can be expressed as

$$\hat{a}_k = \alpha + \delta\hat{a}_k, \quad \hat{a}_k^\dagger = \alpha^* + \delta\hat{a}_k^\dagger, \tag{3.1}$$

where the time independent α term represents the steady-state expectation value of the operator $\hat{a}_k$, and $\delta\hat{a}_k$ denotes its time-varying fluctuation. This decomposition assumes the following conditions

$$\langle\delta\hat{a}_k(t)\rangle = \langle\delta\hat{a}_k^\dagger(t)\rangle = 0, \quad |\delta\hat{a}_k(t)| \ll \alpha. \tag{3.2}$$

These conditions imply that the fluctuation term has a zero mean and is significantly smaller than the steady-state amplitude α, allowing the higher-order fluctuation terms to be neglected. Using Eq. (2.28), the linearised quadrature operators then can be written as

$$\delta\hat{x}(t) = \delta\hat{a}_k(t) + \delta\hat{a}_k^\dagger(t), \quad \delta\hat{p}(t) = i(\delta\hat{a}_k^\dagger(t) - \delta\hat{a}_k(t)). \tag{3.3}$$

A more general linearised expression for an arbitrary quadrature is given by the following equation

$$\delta\hat{x}_k^\theta = \delta\hat{a}_k e^{-i\theta} + \delta\hat{a}_k^\dagger e^{i\theta}, \tag{3.4}$$

with a mean $\langle\delta\hat{x}_k^\theta\rangle = 0$ and a variance of $\Delta\hat{x}_k^{\theta\,2} = \langle(\delta\hat{x}_k^\theta)^2\rangle$.

3.1.2 Amplitude and Phase Modulations

A classical optical field with a frequency ω_0 can be expressed as

$$\alpha(t) = \alpha_0 e^{i\omega_0 t}, \tag{3.5}$$

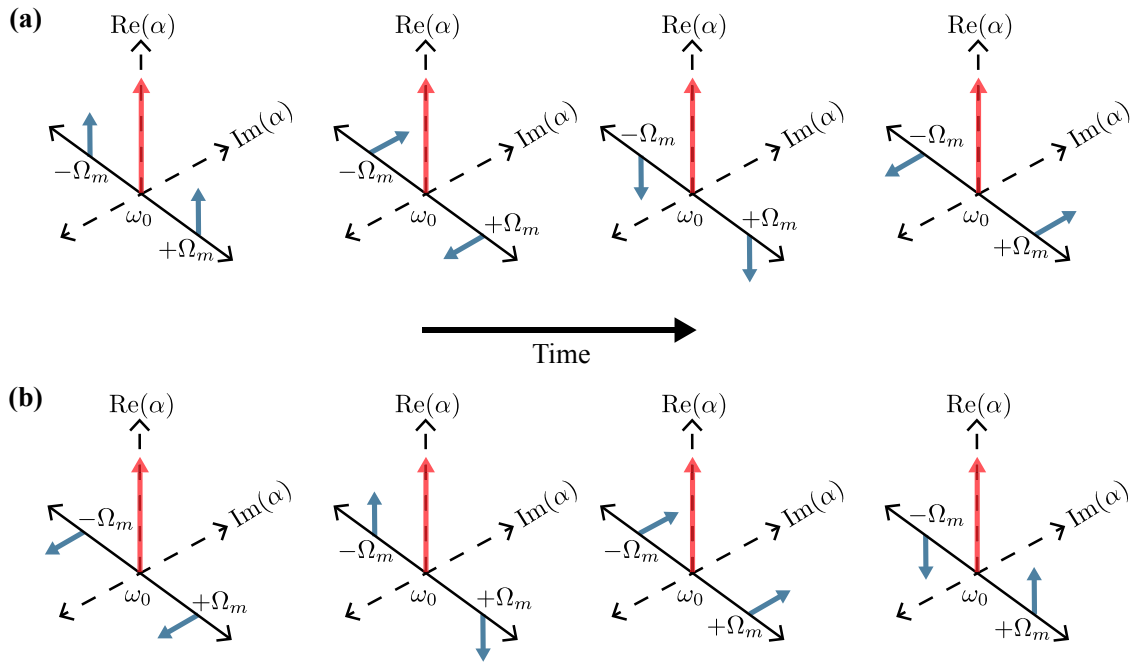

Figure 3.2: Phasor diagrams of the evolutions of the sidebands (a) in amplitude modulation, **(b)** phase modulation

which is also known as the *carrier*. The amplitude modulation of this carrier field at a frequency Ω_m is given by [79]

$$\begin{aligned}\alpha(t) &= \alpha_0 e^{i\omega_0 t}\big(1 - M\cos(\Omega_m t)\big)\\ &\approx \alpha_0\left[e^{i\omega_0 t} - \frac{M}{2}\big(e^{i(\omega_0-\Omega_m)t} + e^{i(\omega_0+\Omega_m)t}\big)\right],\end{aligned} \tag{3.6}$$

where M represents the modulation depth and Ω_m is the modulation frequency. From Eq. (3.6), it is clear that amplitude modulation generates two frequency components around the carrier frequency ω_0. These frequencies, $\omega_0+\Omega_m$ and $\omega_0-\Omega_m$, are referred to as the upper and lower sidebands which are shown as rotating phasors in Fig. 3.1(b). The sidebands have equal amplitudes and rotate in sync with the carrier, causing the imaginary components to cancel each other out, as shown in Fig. 3.2(a), and producing a real vector along the real axis. Similarly, the phase modulation with a frequency Ω_m can be expressed as [79]

$$\begin{aligned}\alpha(t) &= \alpha_0 e^{i\omega_0 t} e^{iM\cos(\Omega_m t)}\\ &\approx \alpha_0\left[e^{i\omega_0 t} + i\frac{M}{2}\big(e^{i(\omega_0-\Omega_m)t} + e^{i(\omega_0+\Omega_m)t}\big)\right].\end{aligned} \tag{3.7}$$

Unlike amplitude modulation, the sidebands produced by phase modulation rotate out of sync with the carrier. As a result, the real components are always opposite, while the imag-

inary components point in the same direction, as shown in Fig. 3.2(b). This causes the real components to cancel each other out. It is important to note that the rate of rotation of the phasors depend on the modulation frequency while their amplitude depends on the modulation depth.

3.1.3 Quantum Sidebands

In Sec. 3.1.1, we introduced the linearisation of the annihilation and creation operators, expressed in terms of the steady-state complex amplitude α and its conjugate α^*, along with the time-dependent fluctuation operators $\delta\hat{a}_k$ and $\delta\hat{a}_k^\dagger$. Here, α represents the carrier field at frequency ω_0, while the fluctuation terms $\delta\hat{a}_k$ and $\delta\hat{a}_k^\dagger$ can be viewed as the quantum counterparts of the upper and lower sidebands in a classical optical field [81, 82]. This implies that amplitude fluctuations at the modulation frequency Ω_m contribute to the fluctuations of the amplitude quadrature operator, expressed as $\delta\hat{x}(\Omega_m) = \delta\hat{a}(\Omega_m) + \delta\hat{a}^\dagger(\Omega_m)$. Likewise, phase fluctuations at the modulation frequency Ω_m affect the phase quadrature operator, given by $\delta\hat{p}(\Omega_m) = i(\delta\hat{a}^\dagger(\Omega_m) - \delta\hat{a}(\Omega_m))$.

3.1.4 Experimental Realisation of Amplitude and Phase Modulators

In our experiment, we employed free-space electro-optic modulators (EOMs) from Thorlabs, specifically the EO-AM-NR-C2 for amplitude modulation and the EO-PM-NR-C2 for phase modulation (refer to Ref. [79] for the experimental alignment of these modulators). Both modulators use MgO-doped lithium niobate birefringent crystals to employ the Pockels effect. Lithium niobate has two axes, referred to as the fast and slow axes, each with a different refractive index.

For phase modulation, the input light is aligned with the fast axis of the lithium niobate crystal, typically the z-axis. We use a vertically polarised beam to ensure that no component lies along the slow axis, preventing any unwanted polarisation changes during modulation. When an electric field is applied along the z-axis, it alters the refractive index of the fast axis, producing a sinusoidal phase shift in the beam and thereby modulating its phase which is depicted in Fig. 3.3(a).

In contrast to the phase modulator, the amplitude modulator consists of two crystals, each rotated by $45°$. The optical axes of the crystals are orthogonal to one another as shown in Fig. 3.3(b). While amplitude modulation could be achieved with a single crystal, the second crystal helps compensate for temperature-dependent polarisation drifts. When a vertically polarised beam enters the modulator, its polarisation is split into two orthogonal components aligned with the slow and fast axes of the crystals. Applying an electric field alters the refractive indices in both axes, inducing different phase shifts in each component.

This results in elliptically polarised light, which is then passed through a polarising beamsplitter to select the horizontally polarised component, achieving amplitude modulation.

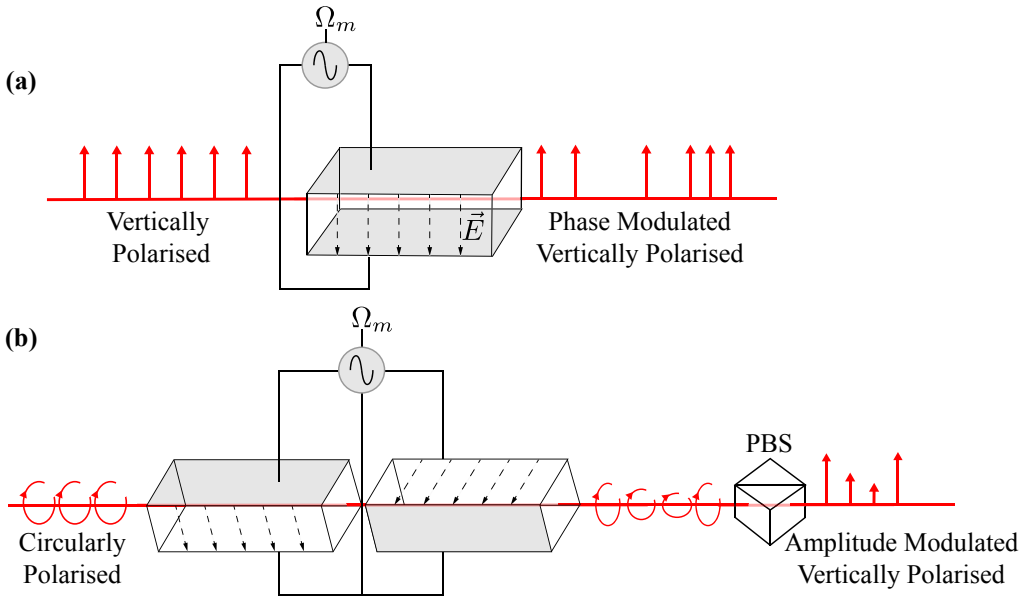

Figure 3.3: Schematic of phase and amplitude modulators. (a) and **(b)** illustrate the basic operating principles of phase and amplitude modulators, using birefringent crystals.

3.2 Gaussian Measurements

Direct detection with a single photodiode is commonly used to measure the intensity of the beam, as the photocurrent is directly proportional to the number of photons in the beam. However, this method does not provide any information about the amplitude or phase quadratures of the light. To access quadrature information, a reference beam is typically required in quantum optics experiments. This is achieved through either homodyne detection, which reveals information about a specific quadrature, or heterodyne detection, which simultaneously provides both amplitude and phase quadrature information.

3.2.1 Homodyne Detection

In our experiments, homodyne detection is commonly used to measure the amplitude (x) or phase (p) quadratures of CV quantum states. The quantum state $|\psi\rangle$ is typically mixed with a bright coherent state, known as the local oscillator (LO), on a beamsplitter with transmissivity T as shown in Fig. 3.4. If we denote the incoming signal as $\hat{a}_{in}$ and the local oscillator as $\hat{b}_{in}$, the input modes undergo a linear Bogoliubov transformation after the beamsplitter,

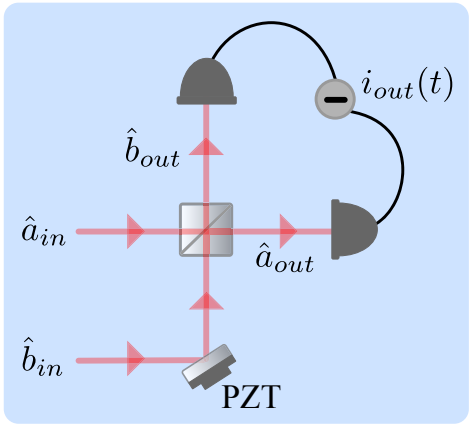

Figure 3.4: Homodyne detection: The input signal beam and local oscillator (LO) beam, denoted by $\hat{a}_{in}$ and $\hat{b}_{in}$, respectively, are directed into a beamsplitter. The output beams, $\hat{a}_{out}$ and $\hat{b}_{out}$, correspond to the input beams after passing through the beamsplitter. These output beams are detected by two photodetectors, and the resulting currents are subtracted. This subtracted current is proportional to the difference in the photon numbers between the signal and LO beams, which in turn is proportional to the quadrature operator. PZT denotes the piezo-electric mirror which is used to control the phase of the LO.

as follows

$$\begin{pmatrix} \hat{a}_{out} \\ \hat{b}_{out} \end{pmatrix} \rightarrow \begin{pmatrix} \sqrt{T} & \sqrt{1-T} \\ -\sqrt{1-T} & \sqrt{T} \end{pmatrix} \begin{pmatrix} \hat{a}_{in} \\ \hat{b}_{in} \end{pmatrix}. \tag{3.8}$$

For a balanced homodyne detector, where $T = 1/2$, the photocurrents of the detectors can be expressed as [83]

$$i_1(t) \propto g_D \langle \hat{a}^\dagger_{out} \hat{a}_{out} \rangle = \frac{g_D}{2} (\hat{a}^\dagger_{in} \hat{a}_{in} + \hat{b}^\dagger_{in} \hat{b}_{in} + \hat{a}^\dagger_{in} \hat{b}_{in} + \hat{b}^\dagger_{in} \hat{a}_{in}), \tag{3.9a}$$

$$i_2(t) \propto g_D \langle \hat{b}^\dagger_{out} \hat{b}_{out} \rangle = \frac{g_D}{2} (\hat{a}^\dagger_{in} \hat{a}_{in} + \hat{b}^\dagger_{in} \hat{b}_{in} - \hat{a}^\dagger_{in} \hat{b}_{in} - \hat{b}^\dagger_{in} \hat{a}_{in}). \tag{3.9b}$$

Here, $g_D = \frac{\eta_d e}{h v}$ [84] represents the detector gain, where η_d is the photodiode efficiency, e is the electronic charge, h is Planck's constant, and v is the optical frequency. Following Eq. (3.9), the difference in the photocurrents is given as

$$i_{out}(t) = i_1(t) - i_2(t) \propto g_D (\hat{a}^\dagger_{in} \hat{b}_{in} + \hat{b}^\dagger_{in} \hat{a}_{in}). \tag{3.10}$$

Substituting $\hat{a}_{in} = \alpha + \delta \hat{a}_{in}$ for the signal and $\hat{b}_{in} = \beta e^{i\theta}$ for the LO beams into Eq. (3.10), respectively, the subtracted photocurrents can be simplified to

$$i_{out}(t) = i_1(t) - i_2(t) \propto 2\alpha\beta \cos\theta + \beta \delta \hat{x}^\theta, \tag{3.11}$$

where $\delta \hat{x}^\theta$ is given in Eq. (3.4) and θ represents the phase difference between the signal

beam and the local oscillator, controlled by a piezoelectric transducer mirror. The difference in photocurrents, known as the output of a balanced homodyne detector, consists of a DC component and an AC component, with the latter containing the noise spectrum of the signal. A much brighter local oscillator is crucial in homodyne detection as it amplifies the weak quantum signal, making it measurable even in the presence of the electronic noise of the detector.

The overall efficiency of the homodyne detection process is determined by the photodiode efficiency and the mode-matching efficiency, also referred to as the visibility of the interference between the signal and LO beams.

$$\eta_{\text{HD}} = \eta_d \times \text{VIS}^2 = \eta_d \times \left(\frac{i_{max} - i_{min}}{i_{max} + i_{min}}\right)^2, \tag{3.12}$$

where η_d represents the photodiode efficiency, and VIS refers to the visibility of the interference fringes. In our experiments, VIS is typically less than 1 due to practical mismatches between the signal and LO, such as differences in spatial or polarisation modes.

3.2.2 Heterodyne Detection

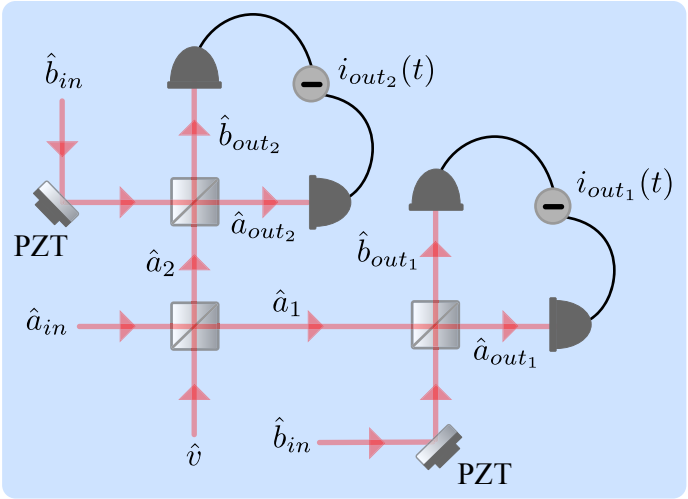

Figure 3.5: Heterodyne detection: The input signal beam and local oscillator beam, denoted by $\hat{a}_{in}$ and $\hat{b}_{in}$, respectively, are mixed on a 50/50 beamsplitter with a vacuum mode $\hat{v}$. The output beams, $\hat{a}_1$ and $\hat{a}_2$ are then sent to two separate homodyne detectors to measure x and p quadratures simultaneously. Two PZT mirrors are used to control phases of the local oscillator in each homodyne set-up.

An optical setup for heterodyne detection is illustrated in Fig. 3.5, where a pair of homodyne detectors measure both quadratures simultaneously. To achieve this, the signal beam is split into two paths using a 50/50 beamsplitter, which also introduces additional vacuum

noise in the process. For instance, if the input beam is denoted as $\hat{a}_{in}$, the output beams at each port are expressed as

$$\hat{a}_1 = \frac{1}{\sqrt{2}}(\hat{a}_{in} + \hat{v}), \quad \hat{a}_2 = \frac{1}{\sqrt{2}}(\hat{a}_{in} - \hat{v}), \tag{3.13}$$

where $\hat{v}$ represents the vacuum noise.

3.3 Locking Techniques

In quantum optics experiments, feedback control is commonly used to adjust and stabilise system performance in response to deviations. This is often achieved by feeding the current output of the system to a controller which compares it to the target value and calculates the error. The controller then modifies the inputs of the system to bring the output back to the desired level.

In our experiment, we apply feedback control through two different locking techniques to ensure optimal system performance. Pound-Drever-Hall locking is used to achieve a specific spatial mode, while relative phase locking is employed to preserve the phase relationship between two interfering signals.

3.3.1 Cavity Locking

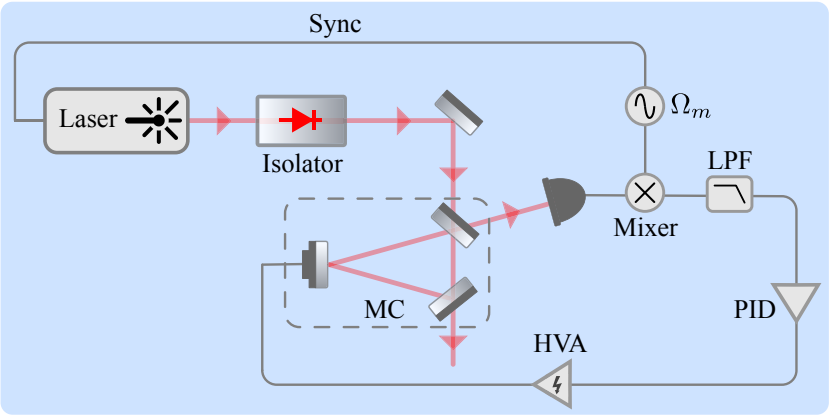

Figure 3.6: Pound-Drever-Hall locking scheme for the mode-cleaner cavity. The laser emits a signal beam, phase-modulated by its internal phase modulator. This beam is monitored at the reflected port of the mode-cleaning cavity by a detector. The detector's output is then mixed down with a sine wave at frequency Ω_m, generated by a signal generator to which the laser is also synchronised. The demodulated signal is then low-pass filtered to produce an error signal, controlled by a PID controller. The PID output is sent to a high-voltage amplifier that adjusts the mode cleaner to maintain the cavity lock. MC: Mode-cleaner, HVA: High-voltage amplifier, LPF: Low-pass filter, PID: Proportional-Integral-Derivative controller.

Pound-Drever-Hall (PDH) locking is a widely used technique for locking a cavity, commonly employed for stabilising laser frequencies [85]. This method examines how the reflected power responds to a frequency-modulated input based on its position relative to resonance. For instance, when the laser operates above resonance, increasing the laser frequency leads to an increase in the reflected power. Conversely, below resonance, an increase in the frequency results in a decrease in the reflected power. By monitoring these changes in the reflected power, an error signal is generated to track the fluctuations in the laser frequency, which is then fed back to stabilise the laser.

In our experiments, we use a mode-cleaning cavity (MC) to produce a beam with a specific spatial mode, specifically the fundamental Gaussian mode (TEM_{00}). A schematic of the setup for this locking scheme is shown in Fig. 3.6. After the laser beam is emitted, it first passes through a Faraday isolator to prevent any back-reflection into the laser. The beam is then directed into the MC and locked to the resonant frequency of the cavity. To achieve this, we use the PDH technique, which relies on phase modulation to determine the locking point. The laser we use has an internal phase modulation capability. The reflected signal from the cavity is detected, demodulated at the same frequency as the modulation, and the resulting error signal is low-pass filtered. This error signal is then processed by a PID (Proportional-Integral-Derivative) controller, with the output being fed back to the piezoelectric mirror of the cavity to maintain the lock.

To understand the locking scheme in more detail, we consider the measured power at the detector, P_{ref}, which is given by [85]

$$\begin{aligned} P_{ref} \propto 2\sqrt{P_c P_s}\big[&\text{Re}[F(\omega_0)F^*(\omega_0+\Omega_m) - F^*(\omega_0)F(\omega_0-\Omega_m)]\cos(\Omega_m t) \\ &+\text{Im}[F(\omega_0)F^*(\omega_0+\Omega_m) - F^*(\omega_0)F(\omega_0-\Omega_m)]\sin(\Omega_m t)\big], \end{aligned} \tag{3.14}$$

where ω_0 is the laser frequency (the carrier frequency), and Ω_m is the modulation frequency. P_c represents the power of the carrier, while P_s denotes the power of the sideband (modulation frequency). The reflection coefficient of the cavity, $F(\omega_0)$, is given by [85]

$$F(\omega_0) = \frac{r(e^{i\phi}-1)}{1-r^2e^{i\phi}}, \tag{3.15}$$

where r represents the reflectivity of the input coupler and ϕ is the phase accumulated by the beam during each round trip in the cavity which is given by

$$\phi = \frac{2\pi f}{v_{fsr}}. \tag{3.16}$$

Here, f is the laser frequency, and v_{fsr} represents the free spectral range of the cavity. In our

locking scheme, we use fast modulation operating in the MHz regime, causing the cosine term in Eq. 3.14 to vanish. As a result, the error signal is given by

$$\epsilon \approx -2\sqrt{P_c P_s}\mathrm{Im}[F(\omega_0)F^*(\omega_0+\Omega_m) - F^*(\omega_0)F(\omega_0-\Omega_m)]. \tag{3.17}$$

3.3.2 Relative Phase Locking

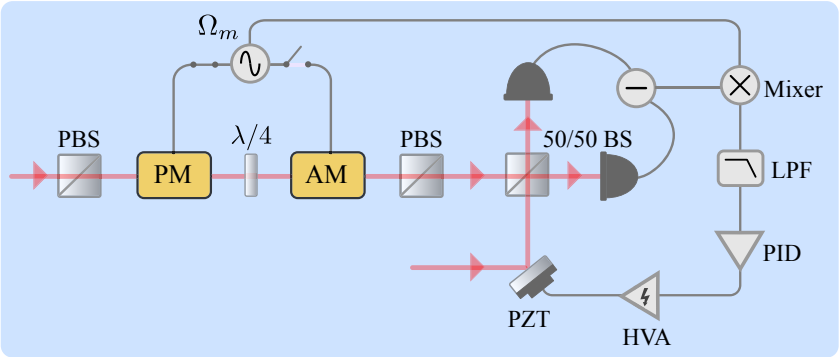

Figure 3.7: Schematic of relative phase locking. A modulation frequency of Ω_m is applied to either the phase or the amplitude modulator, depending on whether the amplitude or phase quadrature is being locked in the experiment. The modulated signal is detected by a homodyne detector, and the detector's output is demodulated at Ω_m. The demodulated signal is low-pass filtered to produce an error signal, which is fed to a PID controller. The PID output is then sent to a high-voltage amplifier, which drives the piezo-electric mirror, adjusting the phase of the local oscillator. PBS: Polarising beamsplitter, $\lambda/4$: Quarter wave-plate, PM: Phase modulator, AM: Amplitude modulator, BS: Beamsplitter, PZT: Piezo-electric mirror, HVA: High-voltage amplifier, PID: Proportional-Integral-Derivative controller, LPF: Low-pass filter.

In addition to the mode-cleaning cavity, we implement relative phase locking in our experiment. For phase locking, we apply phase modulation at a sideband frequency that differs from the signal frequency, and for quadrature locking (out of phase), we use amplitude modulation. A schematic of our locking setup is shown in Fig. 3.7, where the homodyne signal output is used to lock the local oscillator to the signal beam. For both phase and quadrature locking, we typically introduce an additional frequency to the modulators. For example, to lock in phase, a frequency Ω_m is applied to the modulator. The homodyne detector output is then demodulated at Ω_m and passed through a low-pass filter to isolate the DC component, which serves as the error signal. This error signal is subsequently fed to the piezoelectric mirror, adjusting the phase of the LO. The error signal is given by

$$\epsilon_P \propto \alpha_{in}\alpha_{LO}\sin\theta, \tag{3.18}$$

where θ is the relative phase between the signal beam and the LO, and α_{in} and α_{LO} represent the intensities of the signal and LO beams, respectively.

Similarly, for quadrature locking, we follow the same procedure as the phase locking, but now the modulation frequency, Ω_m, is applied to the amplitude modulator instead of the phase modulator. In this case, the error signal is given by

$$\epsilon_Q \propto \alpha_{in}\alpha_{LO}\cos\theta. \tag{3.19}$$

In our experiment, we utilise both quadratures. When sampling amplitude quadrature data, we lock the system using the phase modulator. On the other hand, to record phase data, we use the amplitude modulator to lock to the phase quadrature.

Chapter 4

Fundamentals of Quantum Communications

This chapter introduces key concepts in classical and quantum information theory that are extensively used throughout this thesis and are crucial for understanding its results presented in Chapters 5, 6, and 7. It begins with an exploration of classical and quantum entropy measures, which are employed to quantify the mutual information shared between Alice and Bob, as well as Eve's information in quantum communication tasks. Next, we describe how quantum channels, often attributed to Eve, are modelled and how they transform the distributed quantum states. The chapter then provides an overview of quantum key distribution and its variants, along with a basic security analysis of the primary protocol referenced in this thesis. Finally, we examine the fundamental limits that constrain the distribution of quantum states and explore the current techniques used to mitigate noise and losses in quantum communication which form the foundations of the protocols presented in Chapters 6 and 7. To contextualise these concepts, a brief summary of recent state-of-the-art QKD demonstrations is also included, highlighting the pace of experimental progress and global interest in quantum-secure communication.

4.1 Classical Information Theory

In this section, we introduce foundational concepts from classical information theory, which play a critical role in understanding information processing, transmission, and quantification. Key measures such as Shannon entropy [86], joint and conditional entropy, and mutual information are explored, each providing insight into the uncertainty and relationships between variables. We also discuss binary entropy, which is particularly relevant for systems with two possible outcomes. Together, these concepts establish a theoretical basis for quantifying key rates in quantum key distribution and evaluating the capacities of quantum communication channels in later sections of this thesis.

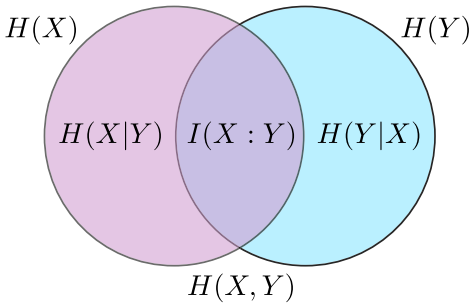

Figure 4.1: Entropy venn diagram for two random variables. The purple circle represents the entropy of variable X, denoted by $H(X)$, and the blue circle represents the entropy of variable Y, denoted by $H(Y)$. The overlapping area shows their mutual information, $I(X:Y)$, while the non-overlapping regions represent the conditional entropies $H(X|Y)$ and $H(Y|X)$, which quantify the uncertainty in X given Y, and in Y given X, respectively.

4.1.1 Shannon Entropy

Shannon entropy, or information entropy, was first introduced by Claude Shannon in Ref. [86] and is fundamental in understanding information transmission, storage, and processing. It provides a mathematical way to quantify the uncertainty in the information of a variable. Mathematically, the Shannon entropy of a random variable, X, is expressed as

$$H(X) = -\sum_x p(x) \log_2 p(x), \tag{4.1}$$

where $p(x)$ represents the probability of X having the outcome x and $\log_2$ denotes the logarithmic base 2 which allows entropy to be expressed in terms of bits. When there is no uncertainty in the variable, the Shannon entropy is 0, as there is no new information to gain when the outcome is certain. Conversely, entropy reaches its maximum value of 1 when the outcome is entirely random. For example, in a fair coin toss, where the probability of landing heads or tails is 0.5, the entropy is 1 bit.

Shannon entropy can also be extended beyond a single variable to multiple variables. For instance, the joint entropy of two variables, X and Y, is given by

$$H(X,Y) = -\sum_{x,y} p(x,y) \log_2 p(x,y), \tag{4.2}$$

where $p(x,y)$ represents the probability of obtaining outcomes x and y together. Notably, if X and Y are independent, their joint entropy simplifies to $H(X,Y) = H(X) + H(Y)$. Another important measure in information theory is the conditional entropy, which quantifies the information required to describe the outcome of X given that the value of Y is known.

This is given by

$$H(X|Y) = -\sum_{x,y} p(x|y) \log_2 p(x|y), \tag{4.3}$$

where $p(x|y) = p(x,y)/p(y)$ represents the conditional probability. The final entropy measure relevant to this thesis is mutual information, which quantifies the amount of information gained about one random variable by observing another. For example, the mutual information between variables X and Y is expressed as

$$H(X:Y) = I(X:Y) = -\sum_{x,y} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)}. \tag{4.4}$$

Mutual information is symmetric, meaning $I(X:Y) = I(Y:X)$ for Shannon entropies. It is maximised when X and Y are identical ($X = Y$) and minimised when X and Y are completely independent. Below are additional entropy relations commonly used in information theory

$$\begin{aligned} H(X|Y) &= H(X,Y) - H(Y) \\ H(Y|X) &= H(X,Y) - H(X) \\ I(X:Y) &= H(X) + H(Y) - H(X,Y) = H(X) - H(X|Y) = H(Y) - H(Y|X). \end{aligned} \tag{4.5}$$

These relations are visually represented by the Venn diagram shown in Fig. 4.1.

4.1.2 Binary Entropy

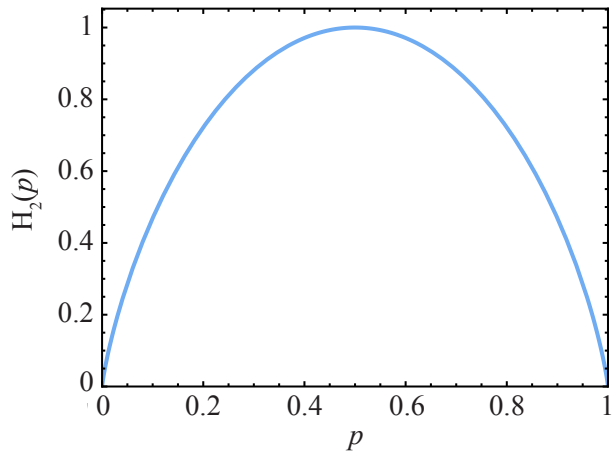

Figure 4.2: Plot of binary entropy. p represents the probability of the random variable, and $H(p)$ is its entropy, which reaches its maximum when $p = 0.5$.

Binary entropy is a specific case of the entropy function and is particularly useful for

quantifying information rates in certain channels such as symmetric channels [87], as will be discussed in the following sections of this thesis. Unlike general Shannon entropy, which measures the uncertainty in a random variable X with multiple possible outcomes, binary entropy applies to a random variable with only two possible outcomes, as its name suggests. Therefore, the binary entropy is given by

$$\mathrm{H}_2(p) = -p \log_2 p - (1-p) \log_2 (1-p), \tag{4.6}$$

where $p \in [0, 1]$ represents the probability associated with the variable X (refer to Fig. 4.2 for a plot of this function).

4.2 Quantum Information Theory

In this section, we introduce concepts in quantum information theory that serve as analogues to those in classical information theory for quantum systems. Key topics include von Neumann entropy [88], which measures the uncertainty in a quantum state, and the Holevo bound [89], which limits the amount of classical information extractable from a quantum channel. These concepts provide the foundation to quantify key rates, bound the information accessible to a malicious party, and calculate the information shared between entangled states.

4.2.1 Von Neumann Entropy

Von Neumann entropy [88] serves as the quantum analogue of Shannon entropy [86], measuring the information content of a quantum state. For a quantum state described by the density matrix ρ, the von Neumann entropy is defined as

$$S(\rho) = -\mathrm{Tr}[\rho \log_2 \rho]. \tag{4.7}$$

Alternatively, the von Neumann entropy can be calculated using the eigenvalues of the density matrix ρ as

$$S(\rho) = -\sum_i \lambda_i \log_2 \lambda_i, \tag{4.8}$$

where λ_i is the i^{th} eigenvalue of ρ. This approach is the most commonly used method for computing the entropy of a quantum state.

4.2.2 Von Neumann Entropy of Gaussian States

As discussed earlier in Sec. 2.3.2, a Gaussian quantum state is often represented by its covariance matrix. Consequently, for a Gaussian state, the von Neumann entropy can be determined from the covariance matrix using the symplectic eigenvalues of the state. Given a covariance matrix σ, it can be decomposed into a direct sum of thermal states through a symplectic transformation S as follows

$$\sigma = S\tilde{\sigma}S^T, \quad \tilde{\sigma} = \bigoplus_{i=1}^{N} \lambda_i \mathbb{1}, \tag{4.9}$$

where $\tilde{\sigma}$ is known as the Williamson form of the covariance matrix σ, and λ_i are the symplectic eigenvalues of σ [90]. Here, the symplectic eigenvalues are obtained from the matrix $|i\Omega\sigma|$ where Ω is given as

$$\Omega = \bigoplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{4.10}$$

Thus, the entropy of this Gaussian state is computed from

$$S(\sigma) = \sum_{i=1}^{N} g(\lambda_i), \tag{4.11}$$

where

$$g(x) = \left(\frac{x+1}{2}\right)\log_2\left(\frac{x+1}{2}\right) - \left(\frac{x-1}{2}\right)\log_2\left(\frac{x-1}{2}\right). \tag{4.12}$$

One-Mode Thermal Decomposition

For a single-mode state, the symplectic eigenvalue can be calculated as the square root of the determinant of its covariance matrix

$$\lambda_1 = \sqrt{\det(\sigma)}. \tag{4.13}$$

Two-Mode Thermal Decomposition

In this thesis, we frequently use two-mode Gaussian states to quantify the information shared between two trusted parties. The covariance matrix for a two-mode state is given by

$$\sigma = \begin{pmatrix} a\mathbb{1}_2 & c\sigma_z \\ c^T\sigma_z & b\mathbb{1}_2 \end{pmatrix}, \tag{4.14}$$

where $a = a^T$, $b = b^T$ and c are 2×2 real matrices and σ_z is defined in Eq. 2.6. In this case, the Williamson's decomposition of σ is simply given by $\tilde{\sigma} = \lambda_2\mathbb{1}_2 \oplus \lambda_1\mathbb{1}_2$, where the symplectic eigenvalues are

$$\lambda_{1,2} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4\det(\sigma)}}{2}}, \tag{4.15}$$

with $\Delta = \det(a) + \det(b) + 2\det(c\sigma_z)$ [91].

4.2.3 Holevo Bound

The Holevo bound describes the upper limit of classical information that can be obtained from a quantum channel [89]. In QKD, it provides an upper bound on the information accessible to an untrusted party, referred to as Eve.

Consider a case where Alice prepares an ensemble of quantum states, ρ_a, with probabilities, p_a. The amount of maximum extractable information is given by

$$\chi(a:B) = S(\rho_A) - \sum_a p_a S(\rho_a), \tag{4.16}$$

where ρ_A is Alice's average state of the ensembles she prepares and $S(.)$ denotes the von Neumann entropy given in Eq. (4.8).

4.3 Quantum Channels

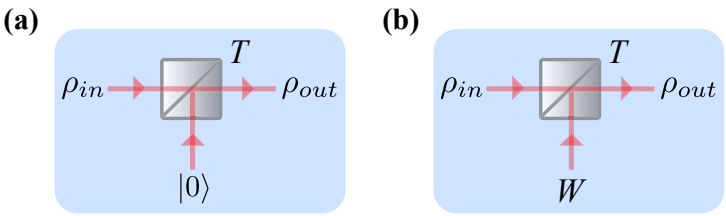

Figure 4.3: Modelling of pure-loss and thermal-loss channels. (a) and **(b)** illustrate the modeling of the pure-loss and thermal-loss channels, respectively, using a beamsplitter with transmissivity T. The input state interacts with a vacuum state in the pure-loss channel (a) and with a thermal state in the thermal-loss channel (b).

Quantum information is typically transmitted through quantum channels, which introduce decoherence, degrading the quality of quantum communication. Quantum channels are linear mappings that take the density matrix of a state and transform it into another density matrix. Accurately modelling these channels is essential for understanding the noise and loss affecting the transmitted states. In secure communications, quantum channels are often treated as environments controlled by an adversary, with any decoherence

attributed to this party. Therefore, precise channel modelling is critical for bounding the adversary's knowledge and ensuring secure information transfer. While numerous types of quantum channels exist, this thesis focuses specifically on pure-loss, thermal-loss, and dephasing channels. For more comprehensive information on quantum channels, refer to Refs. [69, 92–94].

4.3.1 Bosonic Pure-Loss Channel

The bosonic pure-loss channel is one of the most common lossy channels in quantum communications, typically modelled as a beamsplitter with transmissivity $T \in [0, 1]$ that mixes the incoming state with a vacuum mode, as shown in Fig. 4.3(a) for free-space channels. For a quantum channel with an optical fibre, we assume a loss of 0.2 dB per km, which corresponds to a transmissivity of $T = 10^{-0.02d}$, where d represents the distance in km.

Furthermore, the single-mode pure-loss channel can be represented using Kraus operators, which describe the transformation of the density matrix into its new form after passing through the channel. The Kraus-operator form is given by [95, 96]

$$\mathcal{E}(\rho) = \sum_{i=0}^{\infty} \hat{A}_i \rho \hat{A}_i^\dagger, \tag{4.17}$$

where the Kraus operator associated with losing i photons to the environment is $\hat{A}_i = \sqrt{\frac{(1-T)^i}{i!}} T^{\hat{n}/2} \hat{a}^i$. Here, $\hat{n}$ denotes the number operator, defined in Eq. (2.27), and $\hat{a}$ is the annihilation operator.

4.3.2 Thermal-Loss Channel

The thermal-loss channel is also modelled by a beamsplitter with transmissivity T, but here the incoming state is mixed with a thermal state of variance $W = 2\bar{n} + 1$ with a mean photon number $\bar{n}$, as shown in Fig. 4.3(b). In the context of quantum key distribution, this thermal state is often attributed to Eve, who adjusts her variance to simulate the transmission loss, T, and channel noise, ξ. In this case, Eve's variance in terms of the channel parameters is given by

$$W = \frac{\xi T}{1 - T} + 1. \tag{4.18}$$

Additionally, the thermal-loss channel can be decomposed into a pure-loss channel with transmissivity $\eta = T/G$ and a quantum-limited amplifier with gain $G = 1 + (1 - T)\bar{n} = T\xi/2 + 1$. The Kraus-operator representation for this decomposition is given by

$$\mathcal{E}(\rho) = \sum_{i,k=0}^{\infty} \hat{B}_k \hat{A}_i \rho \hat{A}_i^\dagger \hat{B}_k^\dagger, \tag{4.19}$$

where the Kraus operators for the pure-loss channel and the quantum-limited amplifier are given by

$$\hat{A}_i = \sqrt{\frac{(1-\eta)^i}{i!}} \eta^{\hat{n}/2} \hat{a}^i \tag{4.20a}$$

$$\hat{B}_k = \sqrt{\frac{1}{k!\, G} \left(\frac{G-1}{G}\right)^k} \hat{a}^{\dagger k} G^{-\hat{n}/2}, \tag{4.20b}$$

respectively.

4.3.3 Pauli Dephasing Channel

The Pauli dephasing channel models a type of noise in which qubits undergo phase flips, a common issue in quantum computers. In this thesis, we specifically examine the qubit dephasing channel, applicable to qubits in a two-dimensional Hilbert space. Consider a qubit initially in the state $\alpha |0\rangle + \beta |1\rangle$. After passing through a dephasing channel, the qubit will be in the state $\alpha |0\rangle - \beta |1\rangle$ with probability p or remain $\alpha |0\rangle + \beta |1\rangle$ with probability $1 - p$, where p represents the probability of a phase flip.

The dephasing channel can be mathematically described using the Kraus representation, where the action of the channel on a density matrix ρ is given by

$$\mathcal{E}(\rho) = \hat{A}_0 \rho \hat{A}_0^\dagger + \hat{A}_1 \rho \hat{A}_1^\dagger, \tag{4.21}$$

with the Kraus operators defined as

$$\hat{A}_0 = \sqrt{1-p}\, \mathbb{1}_2, \quad \hat{A}_1 = \sqrt{p}\, \sigma_z. \tag{4.22}$$

4.4 Quantum Key Distribution

Quantum key distribution (QKD), first introduced by Bennett and Brassard in 1984 [19], enables the secure distribution of a private key between two trusted parties, commonly referred to as Alice and Bob. QKD consists of two main steps: first, Alice encodes the key onto a quantum state and sends it through a quantum channel to Bob, who performs measurements on the received states. Then, using a classical channel, Alice and Bob apply a post-processing protocol to extract the final key from their correlated data. QKD protocols are generally classified into two categories, based on the degrees of freedom in the underlying quantum system. Discrete-variable (DV) protocols encode key information in discrete degrees of freedom, such as the polarisation of photonic states [19,20]. Continuous-variable (CV) protocols, on the other hand, use continuous degrees of freedom, such as the amplitude and phase quadratures of the optical field [21,22]. In this thesis, we will later introduce

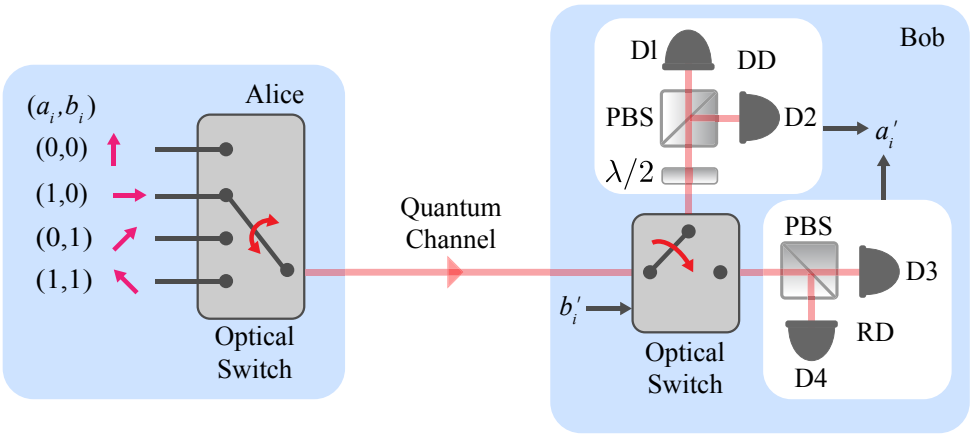

Figure 4.4: Diagram of the BB84 protocol. Alice randomly encodes the keys onto horizontally/vertically or diagonally/anti-diagonally polarised light according to the values of a_i and b_i. She sends the states to Bob, who measures them in either the computational or the diagonal basis based on his randomly generated value b_i' and records the outcomes as a_i'.

the protocols we designed, each employing one of these two schemes.

4.4.1 Discrete-Variable QKD

Table 4.1: All possible combinations of random bits a_i and b_i. Up and left arrows represent vertically and horizontally polarised light, respectively, while arrows at $45°$ and $135°$ indicate diagonally and anti-diagonally polarised light.

a_i	b_i	Encoded State	Polarisation
0	0	$\|0\rangle$	↑
1	0	$\|1\rangle$	→
0	1	$\|+\rangle$	↗
1	1	$\|-\rangle$	↖

The most well-known discrete-variable QKD (DV-QKD) protocol is the BB84 protocol, proposed by Bennett and Brassard [19]. In BB84, Alice generates two random bits a_i and b_i for each photon she sends to Bob. She uses a_i to create the secret key, while b_i determines the basis she will use to encode a_i. The basis choices in BB84 are the computational basis, $\{|0\rangle, |1\rangle\}$, and the diagonal (or X) basis, $\{|+\rangle, |-\rangle\}$, as described in Sec. 2.2 in Eqs. (2.3) and (2.5a), respectively. To encode the key information in the computational basis, Alice uses horizontally or vertically polarised light as shown in Fig. 4.4. Similarly, in the X basis, she encodes the key as a superposition of horizontally and vertically polarised light. The specific polarisation Alice uses depends on the combination of a_i and b_i. For example, if Alice generates $a_i = 0$ and $b_i = 0$, she encodes the state $|0\rangle$ using vertically polarised light. If instead $a_i = 0$ and $b_i = 1$, she encodes the state $|+\rangle$ with diagonally polarised light. All

possible combinations are summarised in Table 4.1.

Bob also randomly generates a variable b_i' to decide which basis to use for his measurements, with his measurement outcomes recorded as a_i'. Randomly switching between bases for both Alice and Bob is essential for ensuring security against a potential eavesdropper. If Alice were to use the same basis consistently, Eve could intercept and measure the quantum state in that basis, recreate it, and send it on to Bob, thus going undetected by Alice and Bob and compromising the purpose of quantum key distribution. However, when Alice encodes the key across different bases, Eve cannot simply clone the states, as the no-cloning theorem prevents perfect cloning of two non-orthogonal states [23], such as $|0\rangle$ and $|+\rangle$. For example, if Alice sends a bit 0 encoded as the state $|0\rangle$, Eve has to guess the encoding basis and randomly picks one to measure the state. If she chooses the diagonal basis, she might accidentally recreate the state $|+\rangle$, introducing an error that Alice and Bob can detect.

Once Alice finishes sending the quantum states, she and Bob proceed to the sifting procedure, where Alice announces b_i to Bob over an authenticated classical channel. Bob discards any measurement outcomes where $b_i \neq b_i'$. After sifting, Alice randomly selects a portion of her bits a_i and has Bob compare them against his measurement outcomes a_i'. If Eve has been intercepting the communication, some of Bob's measurements are likely to be incorrect. Alice and Bob then check whether the observed error rate exceeds an acceptable threshold. If it does, they terminate the protocol, as this indicates Eve has gained too much information. If the threshold is not exceeded, Alice and Bob proceed to reconcile any remaining discrepancies between a_i and a_i'. In BB84, the channel is typically considered insecure when the quantum bit error rate (QBER) exceeds a protocol-specific threshold of around 11% under collective attacks, beyond which no secret key can be distilled [97–99].

4.4.2 Continuous-Variable QKD

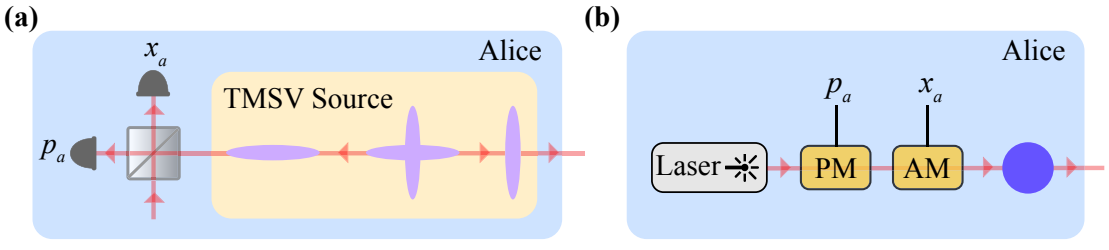

Figure 4.5: The equivalence between the entanglement-based and prepare-and-measure schemes. **(a)** illustrates the entanglement-based QKD scheme, where Alice prepares a TMSV state. She retains one arm of the TMSV state and performs a heterodyne measurement to obtain the outcomes x_a and p_a, while sending the other arm to Bob. This setup is equivalent to preparing a coherent state by encoding x_a and p_a directly in the lab, as shown in **(b)**.

In continuous-variable QKD (CV-QKD), unlike DV-QKD, keys are encoded in the amplitude and phase quadratures of the optical field and are measured using heterodyne or homodyne detection [21, 22]. CV-QKD protocols can be divided into two main types: those with Gaussian modulation (GM CV-QKD), where coherent states are modulated according to a Gaussian distribution [78, 100–109], and those with discrete modulation (DM CV-QKD) [110–117], which use a constellation of modulated coherent states. In this thesis, we focus on GM CV-QKD protocols; for information on DM CV-QKD protocols, refer to Refs. [87, 118].

Prepare-and-Measure and Entanglement-Based Schemes

QKD protocols (both DV and CV based protocols) can be expressed in either entanglement-based (EB) or prepare-and-measure (PM) schemes. Both of these models are mathematically equivalent [74, 119], however the entanglement-based representation is more convenient for the security analysis of a QKD protocol. In the conventional entanglement-based CV-QKD protocols, Alice sends one arm of a TMSV state to Bob while performing a heterodyne measurement on the other arm of the TMSV state she kept as shown in Fig. 4.5. This procedure is equivalent to Alice sending a coherent state in the prepare-and-measure scheme [119].

Gaussian Modulated Coherent State Protocol

The Gaussian modulated coherent state protocol, which uses either homodyne [78, 100, 103, 105–107] or heterodyne detection [101, 102, 108], is the simplest CV-QKD protocol. In this scheme, the key is encoded onto a coherent state that is randomly displaced in both quadratures, as shown in Fig. 4.5(b). The GG02 protocol, introduced by Grosshans and Grangier [78, 100], is the most widely used GM CV-QKD protocol, where the Gaussian modulation variance is optimised for each transmission distance to achieve optimal key rates. Although the original protocol employs homodyne detection, variants using heterodyne detection, such as the no-switching protocol [101], have also been developed.

A schematic of the coherent state protocol with homodyne detection is shown in Fig. 4.6(a), where Alice generates two random numbers, x_a and p_a, from a Gaussian distribution with zero mean and variance V_a. These values are encoded onto a coherent state using amplitude and phase modulators, respectively. Alice then transmits each state to Bob through a quantum channel. Bob measures either x or p, randomly switching between the two quadratures. He records his measurement outcomes as x_b and, once his measurements are complete, he reveals to Alice which quadrature he measured. Alice then discards either x_a or p_a based on Bob's chosen measurement basis.

While coherent state protocols are one type of GM CV-QKD protocol, other variants exist

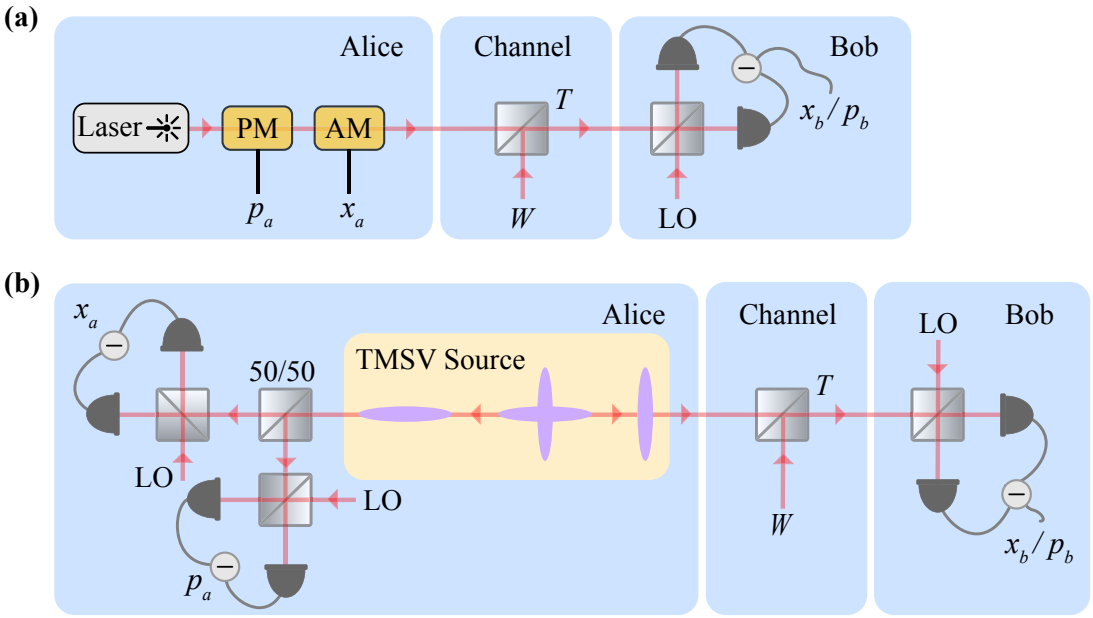

Figure 4.6: Coherent state protocol with homodyne detection. **(a)** Prepare-and-measure representation of the coherent state protocol with homodyne detection. **(b)** Entanglement-based version of the protocol, where Alice performs heterodyne detection on one arm of the TMSV state, projecting the other arm onto a coherent state.

where keys are encoded onto displaced squeezed states, with Bob performing either homodyne or heterodyne detection [22,104,120–123]. In this thesis, however, we focus exclusively on GM CV-QKD protocols that use coherent states. For a broader security analysis of GM CV-QKD protocols, refer to Ref. [124].

4.4.3 Security Analysis of the Coherent State Protocol with Homodyne Detections

As previously discussed in Sec. 4.4.2, the EB scheme is commonly employed to evaluate the security of QKD protocols. The EB-representation for the protocol using coherent states and homodyne detection is illustrated in Fig. 4.6(b). In this scheme, Alice generates a TMSV state instead of coherent states, with its covariance matrix represented in Eq. (2.53), where V denotes the thermal variance of the state. Alice keeps one arm of the TMSV state and transmits the other to Bob through a thermal channel, modelled as a beamsplitter with transmissivity T and thermal variance W, as shown in Fig. 4.3. It is worth noting that when $W = 1$, the quantum channel reduces to a pure-loss channel. After transmission through the channel,

the joint covariance matrix of Alice and Bob can then be expressed as follows

$$\sigma_{\mathrm{AB}} = \begin{pmatrix} V\mathbb{1}_2 & \sqrt{T(V^2-1)}\sigma_z \\ \sqrt{T(V^2-1)}\sigma_z & TV + (1-T)W\mathbb{1}_2 \end{pmatrix} = \begin{pmatrix} a\mathbb{1}_2 & c\sigma_z \\ c\sigma_z & b\mathbb{1}_2 \end{pmatrix}. \tag{4.23}$$

In QKD, Alice and Bob perform a reconciliation step, which involves error correction. This process can follow one of two approaches: direct reconciliation or reverse reconciliation. In direct reconciliation, Bob corrects errors in his bits keeping Alice's data as the reference, while in reverse reconciliation, Alice corrects errors in hers to match Bob's data. Early CV-QKD protocols relied on direct reconciliation [78, 121, 125] but were limited by the 3 dB loss threshold, beyond which a secure key could not be extracted. This limitation arises because, as channel loss increases, Bob's ability to accurately infer Alice's data degrades, while Eve gains relatively more information about Alice's states than Bob does. In CV-QKD, a protocol becomes insecure when Eve's knowledge about the key exceeds the mutual information shared between Alice and Bob. To overcome this limitation, reverse reconciliation was introduced [100, 119, 126], by using Bob's measurement outcomes as the reference and having Alice correct her data accordingly, it ensures that Eve, who only has access to what is lost in the channel, cannot gain an informational advantage. Additionally, modern error-correcting codes such as low-density parity check (LDPC) codes perform better in the low signal-to-noise regime [127–129], which aligns with the conditions experienced by Bob over long distances. This further supports the use of reverse reconciliation, where the decoding is applied to Bob's noisy data rather than Alice's stronger signals, enabling secure communication over longer distances [100, 119]. Consequently, the protocols discussed in this thesis assume reverse reconciliation.

While the direction of reconciliation does not alter Alice and Bob's mutual information, it directly impacts the amount of information accessible to Eve. In QKD, Eve is assumed to hold the purification of the joint state shared by Alice and Bob [124]. As a result, quantifying Eve's information requires only Alice and Bob's joint state, without the need to assume a specific attack strategy, since her information is bounded by the Holevo quantity. Eve's information can be expressed as

$$I_E = S(\sigma_{\mathrm{AB}}) - S(\sigma_{\mathrm{A|B}}), \tag{4.24}$$

where $S(\sigma_{\mathrm{AB}})$ and $S(\sigma_{\mathrm{A|B}})$ represent the von Neumann entropies of Alice and Bob's joint quantum state and Alice's covariance matrix conditioned on Bob's measurement outcome, respectively. The symplectic eigenvalues for these states can be derived from Eq. (4.15)

and (4.13). Alice's conditional covariance matrix is given by

$$\sigma_{\mathrm{A|B}} = \sigma_a - \frac{1}{V_{B_x}} \sigma_c \Pi_x \sigma_c^T, \tag{4.25}$$

where $\sigma_a = a\mathbb{1}_2$, $\sigma_c = c\sigma_z$ and $V_{B_x} = b$. Here, $\Pi_x = \mathrm{diag}(1,0)$ if Bob measures the x quadrature and $\Pi_p = \mathrm{diag}(0,1)$ for the p quadrature. Substituting these expressions, we obtain

$$\sigma_{\mathrm{A|B}} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} - \frac{1}{b} \begin{pmatrix} c^2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a - \frac{c^2}{b} & 0 \\ 0 & a \end{pmatrix}. \tag{4.26}$$

Alternatively, Eve's information can be derived directly from her covariance matrix. This approach, however, requires assuming a specific attack strategy for Eve. One such strategy is the entangling cloner attack, a Gaussian attack that is optimal for Gaussian encoding and channels [124, 130]. In this scenario, Eve prepares TMSV state with a variance designed to emulate the quantum channel [74]. She replaces the channel between Alice and Bob with a beamsplitter, sending one mode E_1 through the beamsplitter to interact with Alice's state while retaining the other mode E_2 [131]. Recalling that the thermal variance of the channel was previously denoted as W, the covariance matrix of Eve's TMSV state can be expressed as

$$\sigma_{\mathrm{E_1E_2}} = \begin{pmatrix} W\mathbb{1}_2 & \sqrt{W^2-1}\sigma_z \\ \sqrt{W^2-1}\sigma_z & W\mathbb{1}_2 \end{pmatrix}. \tag{4.27}$$

Thus, the overall covariance matrix of the system, including Alice, Bob, and Eve, before Alice sends one arm of her TMSV state through the quantum channel, is given as

$$\sigma_{\mathrm{ABE_1E_2}} = \begin{pmatrix} V\mathbb{1}_2 & \sqrt{V^2-1}\sigma_z & 0 & 0 \\ \sqrt{V^2-1}\sigma_z & V\mathbb{1}_2 & 0 & 0 \\ 0 & 0 & W\mathbb{1}_2 & \sqrt{W^2-1}\sigma_z \\ 0 & 0 & \sqrt{W^2-1}\sigma_z & W\mathbb{1}_2 \end{pmatrix}. \tag{4.28}$$

As mentioned previously, Eve now replaces the channel with a beamsplitter with a tranmissivity of T. The transformation acting on the arm that Alice sends to Bob, B, and one of Eve's mode E_1 can be written as

$$\mathrm{BS}_{\mathrm{BE_1}} = \begin{pmatrix} \mathbb{1}_2 & 0 & 0 & 0 \\ 0 & \sqrt{T}\mathbb{1}_2 & \sqrt{1-T}\mathbb{1}_2 & 0 \\ 0 & -\sqrt{1-T}\mathbb{1}_2 & \sqrt{T}\mathbb{1}_2 & 0 \\ 0 & 0 & 0 & \mathbb{1}_2 \end{pmatrix}. \tag{4.29}$$

Therefore, the joint state between Alice, Bob and Eve after the channel becomes

$$\sigma'_{\mathrm{ABE_1E_2}}=\begin{pmatrix} V\mathbb{1}_2 & \sqrt{T(V^2-1)}\sigma_z & -\sqrt{(1-T)(V^2-1)}\sigma_z & 0 \\ \sqrt{T(V^2-1)}\sigma_z & (TV+(1-T)W)\mathbb{1}_2 & \sqrt{T(1-T)}(W-V)\mathbb{1}_2 & \sqrt{(1-T)(W^2-1)}\sigma_z \\ -\sqrt{(1-T)(V^2-1)}\sigma_z & \sqrt{T(1-T)}(W-V)\mathbb{1}_2 & (TW+(1-T)V)\mathbb{1}_2 & \sqrt{T(W^2-1)}\sigma_z \\ 0 & \sqrt{(1-T)(W^2-1)}\sigma_z & \sqrt{T(W^2-1)}\sigma_z & W\mathbb{1}_2 \end{pmatrix}. \tag{4.30}$$

Tracing out Alice and Bob's modes, the covariance matrix of Eve's average state is

$$\sigma_{\mathrm{E_1E_2}} = \begin{pmatrix} (TW+(1-T)V)\mathbb{1}_2 & \sqrt{T(W^2-1)}\sigma_z \\ \sqrt{T(W^2-1)}\sigma_z & W\mathbb{1}_2 \end{pmatrix}. \tag{4.31}$$

Similar to Alice's conditional state, Bob's homodyne measurement transforms Eve's substate to

$$\sigma_{\mathrm{E_1E_2|B}} = \sigma_{\mathrm{E_1E_2}} - \frac{1}{V_{B_x}}\sigma_{c_{eb}}\Pi_x\sigma_{c_{eb}}, \tag{4.32}$$

where $\sigma_{\mathrm{E_1E_2}}$ is given in Eq. 4.31, $V_{B_x} = TV + (1-T)W$ and $\sigma_{c_{eb}}$ denotes the correlations matrix between Eve and Bob as

$$\sigma_{c_{eb}} = \begin{pmatrix} \sqrt{T(1-T)}(W-V)\mathbb{1}_2 \\ \sqrt{(1-T)(W^2-1)}\sigma_z \end{pmatrix}. \tag{4.33}$$

Therefore, Eve's conditional covariance matrix on Bob's measurement outcome is

$$\sigma_{\mathrm{E_1E_2|B}} = \begin{pmatrix} \frac{VW}{TV+(1-T)W} & 0 & \frac{\sqrt{T(W^2-1)}V}{TV+(1-T)W} & 0 \\ 0 & TW+(1-T)V & 0 & -\sqrt{T(W^2-1)} \\ \frac{\sqrt{T(W^2-1)}V}{TV+(1-T)W} & 0 & \frac{TVW-T+1}{TV+(1-T)W} & 0 \\ 0 & -\sqrt{T(W^2-1)} & 0 & W \end{pmatrix}. \tag{4.34}$$

Hence, Eve's information can be obtained from

$$I_E = S(\sigma_{\mathrm{E_1E_2}}) - S(\sigma_{\mathrm{E_1E_2|B}}). \tag{4.35}$$

by determining the symplectic eigenvalues of the matrices via Eq. (4.15) and substituting them into Eq. (4.11).

As a last step, Alice and Bob's mutual information is obtained from

$$I_{AB} = \frac{1}{2}\log_2\frac{V_{A_x}}{V_{A_x|B_x}}, \tag{4.36}$$

where V_{A_x} represents Alice's variance of the classical data in the EB-scheme where she

performs a heterodyne measurement on the mode she keeps. This variance is given by $V_{A_x} = (a+1)/2$ and $V_{A_x|B_x} = V_{A_x} - c^2/(2b)$ denotes Alice's variance conditioned on Bob's measurement outcomes. Using both Alice and Bob's mutual information and Eve's information, the key rate can be quantified as

$$K = \beta I_{AB} - I_E, \tag{4.37}$$

where β is the reconciliation efficiency. In CV-QKD, security depends not on a fixed error threshold but on the interplay between reconciliation efficiency β, mutual information I_{AB} and the Holevo bound I_E. A CV-QKD protocol becomes insecure when $\beta I_{AB} \leq I_E$, which varies with channel loss, excess noise and modulation parameters.

4.4.4 Security Analysis of the Coherent State Protocol with Heterodyne Detections

When Bob performs heterodyne detection, the covariance matrices of the joint quantum state shared by Alice and Bob, as well as Eve's average state, remain unchanged. However, the measurement alters the conditional states $\sigma_{\mathrm{A|B}}$ and $\sigma_{\mathrm{E_1E_2|B}}$. In this case $\sigma_{\mathrm{A|B}}$ is derived from

$$\sigma_{\mathrm{A|B}} = \sigma_a - \frac{1}{V_{B_x}+1}\sigma_c\sigma_c^T. \tag{4.38}$$

Using the same definitions as Eq. (4.25), this matrix becomes

$$\sigma_{\mathrm{A|B}} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} - \frac{1}{b+1}\begin{pmatrix} c^2 & 0 \\ 0 & c^2 \end{pmatrix} = \begin{pmatrix} a - \frac{c^2}{b+1} & 0 \\ 0 & a - \frac{c^2}{b+1} \end{pmatrix}. \tag{4.39}$$

Similarly, Eve's state conditioned on Bob's measurement outcome is represented by

$$\sigma_{\mathrm{E_1E_2|B}} = \begin{pmatrix} \frac{TW+(1-T)V+WV}{TV+(1-T)W+1} & 0 & \frac{\sqrt{T(W^2-1)}(V+1)}{TV+(1-T)W+1} & 0 \\ 0 & \frac{TW+(1-T)V+WV}{TV+(1-T)W+1} & 0 & -\frac{\sqrt{T(W^2-1)}(V+1)}{TV+(1-T)W+1} \\ \frac{\sqrt{T(W^2-1)}(V+1)}{TV+(1-T)W+1} & 0 & \frac{TVW-T+W+1}{TV+(1-T)W+1} & 0 \\ 0 & -\frac{\sqrt{T(W^2-1)}(V+1)}{TV+(1-T)W+1} & 0 & \frac{TVW-T+W+1}{TV+(1-T)W+1} \end{pmatrix}. \tag{4.40}$$

As in the previous section, the symplectic eigenvalues of $\sigma_{\mathrm{A|B}}$ and $\sigma_{\mathrm{E_1E_2|B}}$ can be obtained from from Eq. (4.13) and Eq. (4.15), respectively. Eve's information can then be obtained from either Eq. (4.24) or Eq. (4.35).

As Bob performs heterodyne measurement, Alice and Bob's mutual information be-

comes

$$I_{AB} = \log_2 \frac{V_A}{V_{A|B}}, \tag{4.41}$$

where $V_A = (a+1)/2$ and $V_{A|B} = V_A - c^2/(2(b+1))$. The key rate is then obtained from Eq. (4.37).

4.5 Channel Capacities

Quantum communications [132] guarantee the reliable transmission of quantum information, efficient distribution of entanglement [133, 134], and enable the establishment of secure secret keys [118, 135]. However, the achievable rates for these tasks are inherently constrained by the capacity of the quantum channels [93, 94, 126, 136].

The Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [93] establishes the fundamental limit on the maximum amount of private states that can be transmitted over a given quantum channel during point-to-point communication between Alice and Bob (see Ref. [136] for the strong converse property of the bound). Similar to the capacity of the point-to-point communications, commonly referred to as the repeaterless bound, there are also fundamental limits on achievable rates for end-to-end communications [94], that incorporate quantum repeaters. Quantum repeaters are devices which divide the quantum channel into smaller segments to make the decoherence of the channel more manageable [63, 137–139].

In this section, we specifically focus on the capacities of the pure-loss and Pauli dephasing channels. In the following section, we discuss how these capacities serve as benchmarks for evaluating the performance of quantum repeaters.

4.5.1 Reverse Coherent Information

Before discussing the specific capacities of the channels, it is important to first define how these capacities are quantified. The amount of distributed entanglement in a given channel is known as the entanglement flux which gives the upper bound of the channel capacity [93], whereas the reverse coherent information (RCI) [126, 140] is a lower bound that measures the amount of the distillable entanglement of a quantum state, which is achievable by an optimal protocol based on one-way classical communication. The RCI is defined as [140–143]

$$\mathrm{RCI}(\rho_{\mathrm{AB}}) = S(\rho_{\mathrm{A}}) - S(\rho_{\mathrm{AB}}), \tag{4.42}$$

where $S(\rho_{\mathrm{A}})$ denotes the von Neumann entropy of Alice's reduced state, obtained by tracing out Bob's subsystem ($\mathrm{Tr}_{\mathrm{B}}[\rho_{\mathrm{AB}}]$), and $S(\rho_{\mathrm{AB}})$ represents the von Neumann entropy of the joint state shared by Alice and Bob. Both entropies are calculated using Eq. (4.8).

For both the pure-loss and Pauli dephasing channels, the entanglement flux coincides with the RCI, indicating that the capacities of these channels are tight. Consequently, these channels are distillable [93].

4.5.2 Bosonic Pure-Loss Channel Capacity

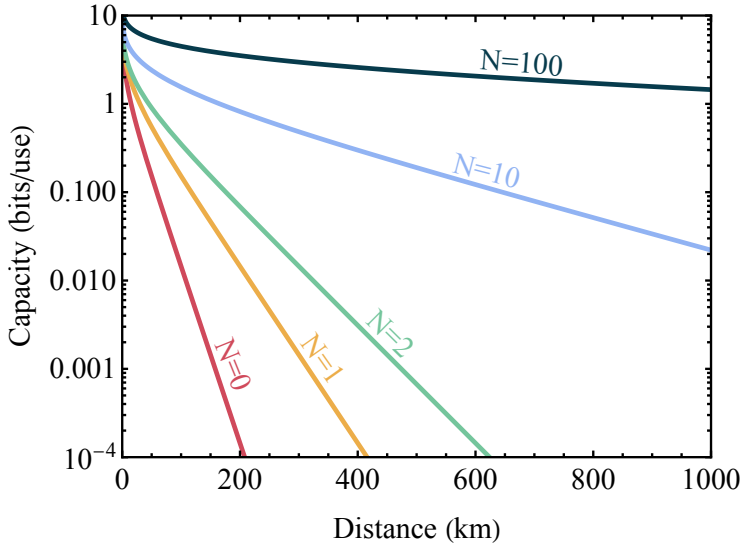

Figure 4.7: Channel capacities of the bosonic pure-loss channel with N repeaters. Obtained using Eq. (4.44) for a fibre-based pure-loss channel with 0.2 dB loss per km, where $\eta = 10^{-0.02d}$ with d indicating the distance in km.

The point-to-point channel capacity of the bosonic pure-loss channel is given by

$$C(\eta) = -\log_2(1-\eta), \tag{4.43}$$

where η is the channel transmissivity. For the pure-loss channel, the PLOB bound can be achieved using a squeezed-state protocol without requiring multiple copies of quantum states or collective measurements [118]. In the presence of a repeater chain, the end-to-end quantum capacity scales with the number of repeaters and is given by [94]

$$C(\eta) = -\log_2(1-\sqrt[N+1]{\eta}), \tag{4.44}$$

where N represents the number of repeaters in the channel. Fig.4.7 illustrates how the capacity evolves with increasing numbers of repeaters. Whether the repeater bounds can be saturated with a simple protocol remains an open question. Unlike the repeaterless bound, achieving these bounds likely requires multiple copies of quantum states and collective measurements, as shown in the works of García-Patrón et al. [140] and the protocol proposed by

Winnel et al. [144]. However, in Chapter 6, we introduce a repeater protocol that surpasses the repeaterless bound capacity while remaining below the single-repeater bound, using single copies of states and individual measurements. We also outline an experimentally feasible implementation of this protocol.

4.5.3 Pauli Dephasing Channel Capacity

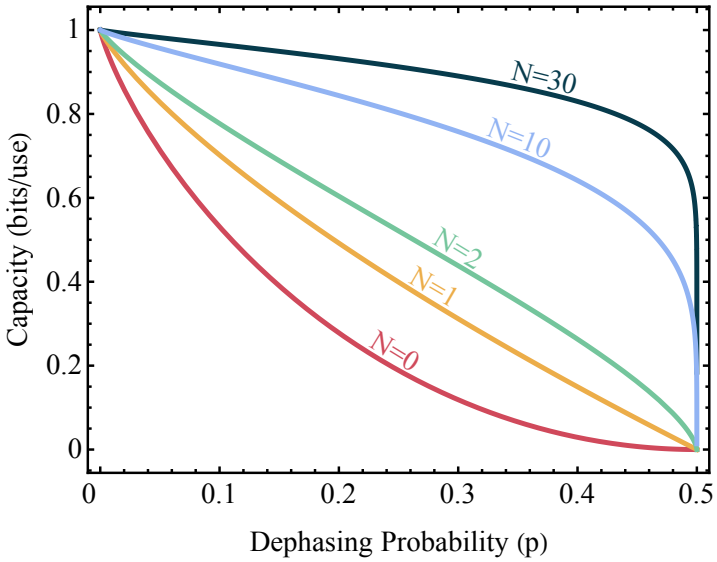

Figure 4.8: Channel capacities of the Pauli dephasing channel with N repeaters. Obtained using Eq. (4.47) for dephasing probabilities in the range $0 \leq p \leq 0.5$.

The channel capacity of the Pauli dephasing channel without repeaters is given by

$$C(p) = 1 - \mathrm{H}_2(p), \tag{4.45}$$

where H_2 represents the binary Shannon entropy, as defined in Eq.(4.6), and $p \in [0, 0.5]$ is the dephasing probability of the channel. This capacity is an achievable rate for key generation, two-way entanglement distribution, and two-way quantum communication [93]. The point-to-point capacity can be achieved when Alice distributes maximally entangled Bell states to Bob, and Bob performs measurements in the Hadamard basis to maximise the secret key rate.

Similar to the pure-loss channel, the capacity of the dephasing channel scales with the number of repeaters. In this case, the effective dephasing probability is given by

$$p_e(N) = \frac{1 - \sqrt[\frac{1}{N+1}]{1-2p}}{2}, \tag{4.46}$$

where N is the number of repeaters. Therefore, the end-to-end channel capacity in the presence of repeaters becomes

$$C(p) = 1 - \mathrm{H}_2\left(\frac{1 - \sqrt[\frac{1}{N+1}]{1-2p}}{2}\right). \tag{4.47}$$

Fig. 4.8 illustrates how the channel capacity scales with the number of repeaters, providing a comparison between the point-to-point capacity and the end-to-end capacity for various values of N.

While achieving the point-to-point channel capacity requires only a single state with individual measurements, reaching the channel capacities in the presence of repeaters is significantly more challenging for the Pauli dephasing channel. In Chapter 7, we will present our recent protocol, which can saturate the capacities of this channel.

4.6 Quantum Repeaters

As mentioned in Sec. 4.5, quantum repeaters are devices designed to divide the quantum channel into smaller segments, making the losses and noise in the channel more manageable [63, 137–139]. For example, in QKD protocols, repeaters can extend the transmission distance by breaking the total distance between the sender and receiver into shorter distances reducing the overall loss that quantum states experience [137–139, 145, 146]. However, it is important to note that a device supporting only QKD does not qualify as a quantum repeater, as quantum repeaters are designed to facilitate a broader range of quantum communication tasks and play a vital role in building scalable quantum networks.

To distribute entanglement across these segments, quantum repeaters rely on entanglement swapping [147–149], a process in which a repeater node shares entangled states with two distant parties and performs a quantum measurement to establish entanglement between them. This distribution is further improved by entanglement distillation [144, 150–156], where multiple copies of weakly entangled states are transformed into a smaller number of highly entangled states using local operations and classical communication to mitigate the effects of noise and loss in the channel.

Quantum repeaters are often classified into three generations based on the techniques they employ to mitigate loss and noise [139, 157]. The first and second generations rely on the techniques discussed earlier, such as entanglement swapping and distillation. The first-generation uses two-way classical communication for entanglement purification, which introduces significant latency. The second-generation improves on this by enabling one-way classical communication and employing quantum error detection to identify faults. However, it cannot fully correct errors, and failed attempts require restarting the proto-

col [137, 157]. In contrast, third-generation repeaters employ quantum error correction (QEC) [158–167], where quantum information is encoded into logical qubits using error-correcting codes. These codes distribute the information redundantly across multiple physical qubits, enabling the detection and correction of errors caused by noise or loss without disturbing the encoded quantum state. This approach ensures greater resilience and allows for robust communication over long distances (for a more detailed discussion of the different generations of quantum repeaters, see Sec. 6.1).

In Chapter 6, we propose a repeater protocol that builds on these principles: the EB version serves as a general repeater for entanglement distribution between two trusted parties via a central node, while the PM-based version is tailored specifically for QKD.

4.7 State-of-the-Art QKD Demonstrations

QKD protocols can also be classified based on the network architecture connecting the trusted parties. In point-to-point QKD, quantum states are transmitted directly from Alice to Bob without any intermediate nodes. In contrast, relay-based QKD involves a third party that facilitates key distribution between Alice and Bob, typically through intermediate measurements. This section highlights several state-of-the-art QKD demonstrations representative of both categories.

4.7.1 Point-to-Point QKD

Point-to-Point QKD represents the most direct form of QKD, where quantum states are prepared by Alice and transmitted over a quantum channel to Bob, who performs measurements to extract correlated outcomes. Many of the earliest and most well-known QKD experiments have been implemented in this point-to-point configuration, including some of the longest-distance demonstrations in optical fibre and free-space links.

DV-QKD Demonstrations

Table 4.2 summarises several state-of-the-art point-to-point DV-QKD experiments across various platforms, including optical fiber, satellite links, and free-space channels. These demonstrations showcase a range of protocols such as BB84 [19] and its variants such as:

- **3-state time-bin BB84:** This protocol is based on the BB84 scheme but simplifies the implementation by using only three quantum states instead of the standard four. [168, 169].
- **Decoy-state BB84:** introduces decoy intensity levels [168–171] to improve security against photon-number-splitting (PNS) attacks [172, 173]. In DV-QKD, weak coher-

ent pulses are often used as an approximation to single photons. However, since these pulses can occasionally contain multiple photons, they become vulnerable to PNS attacks, where Eve can intercept the pulse, extract one photon, and store it for later measurement.

- **Differential Phase Shift QKD (DPS-QKD):** encodes information in the relative phase between successive pulses of light [174, 175].
- **Reference-Frame-Independent QKD (RFI-QKD):** RFI-QKD is a quantum key distribution protocol specifically designed to eliminate the need for a shared reference frame between the sender and receiver [176, 177]. Unlike standard QKD protocols, which require precise alignment of measurement bases between Alice and Bob, RFI-QKD remains robust even in the presence of misalignments, which would otherwise introduce errors.
- **High-Dimensional Dispersive Optics QKD (HD-DO-QKD):** This protocol leverages high-dimensional encoding by using time-frequency modes shaped through dispersive optical elements [178, 179]. Information is encoded across multiple orthogonal temporal or spectral modes, allowing each photon to carry more than one bit of information.
- **BBM92:** is the entanglement-based version of the BB84 protocol where a source produces entangled photon pairs, typically in a Bell state, and sends one photon to Alice and the other to Bob [180].

Notably, some of the longest-distance QKD implementations have been realised via satellite-based links, which benefit from significantly lower channel loss compared to optical fibers. Once above the turbulent atmosphere, photons travel through near-vacuum with minimal attenuation, enabling secure key distribution at 1000 km.

CV-QKD Demonstrations

Table 4.3 presents a selection of state-of-the-art point-to-point CV-QKD experiments implementing various protocols. While the majority of demonstrations are based on the widely

[1] Pol.:Polarisation
[2] DPS: Differential Phase Shift
[3] RFI: Reference-Frame-Independent
[4] HD-DO: High-Dimensional Dispersive-Optics
[5] ent:Entanglement-Based
[6] In-Line LO: LO is generated by Alice and sent to Bob.
[7] 16-QAM: 16-Quadrature Amplitude Modulation
[8] LLO: stands for local-local oscillator where LO is generated locally by Bob.
[9] OFDM: Orthogonal Frequency-Division Multiplexing

Table 4.2: Experimental DV-QKD demonstrations

Reference	Protocol	Medium	Distance (km)	Key Rate (bps)	Year
Boaron *et al.* [168]	3-state BB84	Fiber	421	6.5 bps @405 km	2018
Li *et al.* [181]	Pol. BB84 [1]	Fiber	328	233	2023
Wang. *et al.* [175]	DPS-QKD [2]	Fiber	260	1.85	2012
Liu *et al.* [177]	RFI-QKD [3]	Fiber	250	0.65	2024
Liu *et al.* [179]	HD-DO-QKD [4]	Fiber	242	0.06	2023
Liu *et al.* [182]	BB84	Fiber	200	15	2010
Yin *et al.* [183]	BBM92 (ent.) [5]	Satellite	1000	3.5 (avg)	2017
Liao *et al.* [171]	Decoy BB84	Satellite	719	>100	2017
Ecker *et al.* [184]	BBM92 (ent.)	Free-space	143	300	2021

Table 4.3: Experimental CV-QKD demonstrations

Reference	Protocol	LO Scheme	Medium	Distance (km)	Key Rate	Year
Zhang *et al.* [107]	Gaussian (GG02)	In-line [6]	Fiber	202.81	6.5 bps	2020
Pan *et al.* [185]	Discrete (16-QAM) [7]	LLO [8]	Fiber	126.56	171.42 kbps	2025
Hajomer *et al.* [109]	Gaussian (GG02)	LLO	Fiber	100	25.4 kbps	2024
Wang *et al.* [186]	Gaussian (OFDM) [9]	LLO	Fiber	100	2.25 Mbps	2025
Pi *et al.* [187]	Gaussian (GG02)	LLO	Fiber	100	0.51 Mbps	2023
Jouguet *et al.* [105]	Gaussian (GG02)	In-line	Fiber	80	2.3 kbps	2013

used GG02 protocol [78, 100] discussed in Sec. 4.4.2, several experiments also explore alternative approaches.

- **16-QAM (Quadrature Amplitude Modulation):** is a discrete-modulation (DM) CV-QKD protocol that encodes quantum information into one of 16 distinct coherent states arranged in a two-dimensional lattice in phase space.

- **OFDM (Ortogonal Frequency-Division Multiplexing):** is a variant of Gaussian-modulated QKD protocols where the modulation is applied across multiple frequency channels (subcarriers) using orthogonal frequency-division multiplexing (OFDM). Each subcarrier is modulated with a Gaussian distribution of quadratures, and due to the orthogonality, the subcarriers do not interfere with each other.

Another notable distinction in Table 4.3 is how the local oscillator (LO) is implemented. A strong LO beam is essential for accurately measuring the encoded quantum information, as it enhances the signal-to-noise ratio during detection. In CV-QKD systems, there are two main approaches to generating the LO. For the in-line LO scheme, Alice generates the LO and transmits it alongside the quantum signal through the same channel. While this simplifies phase referencing and alignment, it also exposes the LO to potential side-channel attacks, as an eavesdropper could access both the signal and the LO, allowing her to extract

phase reference information and potentially compromise the key [188–192]. In contrast, the local local oscillator (LLO) approach generates the LO independently at Bob's receiver. This improves security by eliminating the need to transmit the LO, but introduces technical challenges such as phase drift and laser synchronisation between Alice and Bob. These issues can reduce the achievable transmission distance and increase system complexity.

As seen in Tables 4.2 and 4.3, DV-QKD demonstrations can achieve significantly longer distances, while CV-QKD implementations tend to be limited in range but offer much higher key rates, ranging from bps to Mbps. This highlights an inherent trade-off between distance and key rate, depending on the chosen platform. This trade-off primarily stems from differences in loss tolerance and noise resilience. DV-QKD is inherently more tolerant to loss as the key generation relies on the successful detection of individual photons, meaning that even low transmission can still yield a usable key. In contrast, CV-QKD encodes information in the quadratures of coherent states, which attenuate with distance and become increasingly difficult to measure accurately in low-SNR conditions. Additionally, CV-QKD is more sensitive to noise, particularly phase noise. In systems using a LLO, any misalignment between Alice's and Bob's lasers introduces phase drift, which appears as noise during measurement [193–195]. These factors collectively give DV-QKD a clear advantage for long-distance communication, where CV-QKD is more susceptible to loss and noise. However, CV-QKD offers significantly higher key rates at shorter distances and benefits from compatibility with standard telecommunication components.

4.7.2 Relay-Based and Network-Oriented QKD

Table 4.4 summarises several experimental demonstrations of relay-based or network-oriented QKD systems. These experiments extend beyond point-to-point links and demonstrate how secure keys can be distributed over multi-node architectures using either trusted or untrusted intermediate nodes.

In a trusted-relay network, intermediate nodes (relays) are assumed to be secure and honest parties. These nodes receive and decrypt the key from one party, then re-encrypt and send it to the next. This hop-by-hop method enables long-distance QKD by chaining together shorter segments. However, the overall end-to-end security of the system hinges on the integrity of every relay node. If even one node is compromised, the entire key path can be exposed. While this architecture simplifies implementation and supports high key rates, it is only suitable for environments where node security can be physically ensured.

In contrast, in an untrusted-relay network (or using untrusted nodes), intermediate stations are not assumed to be secure, and the system is designed such that the final key remains confidential even if some or all relay nodes are compromised or malicious. This is achieved through protocols that prevent any intermediate node from learning the key and

Table 4.4: Experimental network-oriented QKD demonstrations

Reference	Type	Medium	Relay Type	No of Modes	Distance (km)	Key Rate	Year
Chen *et al.* [196]	DV	Fiber	Trusted	46	18	49.5 kbps	2021
Chen *et al.* [197]	DV	Fiber + Free-Space	Trusted	109	4600	1.1 kbps @2043 km	2021
Stucki *et al.* [198]	DV	Fiber	Trusted	3	17.1	1 kbps	2011
Sasaki *et al.* [199]	DV	Fiber	Trusted	6	90	2.2 kbps	2011
Wang *et al.* [200]	DV	Fiber	Trusted	5		0.4 kbps @14.8 dB	2010
Chen *et al.* [201]	DV	Fiber	Trusted	5	130	0.2 kbps	2010
Peev *et al* [202]	CV+ DV	Fiber	Trusted	6	83	3.1 kbps @33 km	2009
Chen *et al.* [203]	DV	Fiber	Trusted	3	20	1.5 kbps	2009
Tang *et al.* [204]	DV	Fiber	Untrusted	4	55	16.5 bps	2016
Yan *et al.* [205]	DV	Fiber	Untrusted	5		164-407 bps @30 dB	2025
Wei *et al.* [206]	DV	Fiber	Untrusted	5	180	31 bps	2020
Hajomer *et al.* [207]	CV	Fiber	Untrusted	3	10	2.6 Mbps	2025
Pirandola *et al.* [208]	CV	Free-Space	Untrusted	3	150		2014
Minder *et al.* [209]	DV	Fiber	Untrusted	3	530		2019
Chen *et al.* [210]	DV	Fiber	Untrusted	3	509		2020
Chen *et al.* [211]	DV	Fiber	Untrusted	3	511		2021
Pittaluga *et al.* [212]	DV	Fiber	Untrusted	3	605		2021
Chen *et al.* [213]	DV	Fiber	Untrusted	3	658		2022
Liu *et al.* [214]	DV	Fiber	Untrusted	3	1002	9.53×10^{-12} per pulse	2023
Zhou *et al.* [215]	DV	Fiber	Untrusted	3	603	0.12 bps	2024
Huang *et al.* [216]	DV	Fiber	Untrusted	33		19.57 bps @30 dB	2025
Park *et al.* [217]	DV	Fiber	Untrusted		50	1.52 bps	2022

we discuss some of these protocols in detail in Chapter 6. In these schemes, the relays act only as passive measurement nodes, and security is guaranteed even if the relay is controlled by an adversary.

It is also important to note that the majority of existing network-oriented QKD demonstrations have been implemented using DV protocols. This trend reflects the relative maturity and practicality of DV approaches in multi-node configurations, especially where intermediate nodes are not fully trusted. In contrast, CV protocols, while advantageous in terms of high key rates and hardware compatibility, face greater challenges in such settings. This is largely because standard CV measurement techniques used by the untrusted node do not readily establish entanglement between adjacent modes in the way DV-based schemes can. As a result, CV-QKD still requires further development to support secure and scalable implementations in complex network topologies involving untrusted relays. One promising direction may lie in hybrid approaches, where quantum information is encoded in CV states, such as squeezed states, but decoded using DV measurement techniques.

Chapter 5

Software-Enhanced Continuous-Variable Quantum Key Distribution

In the previous chapter in Sec. 4.4.2, we introduced CV-QKD protocols, which are compatible with existing telecommunication infrastructure. Despite this advantage, CV-QKD faces challenges such as losses in terrestrial fibres and atmospheric scintillation in free-space channels. Studies in the literature have shown that probabilistic filters emulating physical quantum processes can enhance the performance of CV-QKD, but their effectiveness is inherently constrained by the characteristics of these physical processes.

In this chapter, we present a CV-QKD protocol that surpasses the optimal Gaussian-modulated CV-QKD (GG02) protocol by employing probabilistic filters with no physical representation, thereby overcoming the limitations imposed by physical processes. Our protocol incorporates distinct filters at Alice's and Bob's stations, each designed to serve a specific purpose, along with a refined security analysis that avoids overestimating Eve's information. Our protocol dynamically optimises the secret-key rate for rapidly changing channels, including terrestrial links and satellite-to-ground communications. It can extract keys even in regions considered non-secure by parameter estimation, as demonstrated both experimentally and theoretically. Implemented at software level, our protocol requires no hardware modifications and can be integrated into existing QKD systems.

This research is currently under review in Communication Physics.
Enhanced Continuous-Variable Quantum Key Distribution Protocol via Adaptive Signal Processing
Ö. Erkılıç, B. Shajilal, L.O. Conlon, A. Walsh, A. Das, S. Kish, T. Symul, P.K. Lam, S.M. Assad, J. Zhao
arXiv:2507.18049 (2025).

5.1 Introduction

A key step in QKD is parameter estimation, which is often performed after error reconciliation to assess channel noise and loss, helping to bound Eve's information [124]. This helps optimise experimental parameters, assuming the channel varies slowly. However, if parameter estimation falls within a non-secure region, key data must be discarded, and rapid variations like atmospheric scintillation can render these estimates ineffective.

In CV-QKD, passive methods that do not require feedback loops to optimise experimental parameters can enhance key rates by employing quantum processes such as noiseless linear amplifiers (NLAs) [218, 219], phase-sensitive amplifiers [220], photon subtraction [221,222], and photon catalysis [222–224]. While these techniques can increase key rates, they are challenging to implement. Recent post-selection protocols emulate such physical processes using digital filtering, where applying a quantum process becomes equivalent to first detecting the quantum state and then digitally filtering the measured outcomes. This approach is particularly useful for point-to-point applications like QKD. For example, measurement-based NLA (MB-NLA) replaces physical NLAs by employing Gaussian post-selection on detection outcomes. This approach extends the transmission distance of CV-QKD [225–227] and also provides overall performance enhancements in CV-based quantum communications [60, 228–230]. Similar approaches have been applied to photon subtraction and photon catalysis protocols, where physical processes are replaced with non-Gaussian virtual photon-subtraction [231, 232] and Gaussian zero-photon catalysis post-selection [233]. However, since these methods still emulate physical processes, the post-selection filters are constrained by the characteristics of those processes. Additionally, these protocols rely on Gaussian extremality, which states that Gaussian states maximise the von Neumann entropy for a given covariance matrix [234,235]. This results in an overestimation of Eve's information with non-Gaussian filters, leading to an underestimation of the key rate.

In this chapter, we present a new CV-QKD protocol using Gaussian modulations and homodyne or heterodyne detection followed by post-selection. The protocol introduces a paradigm shift by eliminating the need to simulate physical processes for filtering. It combines post-selection at both Alice's and Bob's stations: Alice's Gaussian filter optimises modulation variance to achieve key rates near the optimal GG02 performance, while Bob's non-Gaussian filter emulates a higher-performing channel, surpassing optimal GG02 key rates. Typically, protocols employing non-Gaussian post-selection rely on Gaussian extremality, which often leads to an underestimation of key rates [231, 232]. In contrast, our security analysis bypasses Gaussian extremality, providing a more accurate bound on Eve's information after Bob's filter. The protocol dynamically optimises key rates for rapidly changing

channels, such as satellite-to-ground links, where rapid channel changes render any parameter estimation unreliable. Moreover, it can extract keys even in regions where unfiltered channel parameters would not allow secure QKD under the GG02 protocol. Experimental results demonstrate a threefold increase in key rates compared to the optimal GG02 protocol, while simulations for Low Earth Orbit satellite quantum communications reveal up to a 400-fold improvement over the non-optimised approach.

5.2 The Protocol

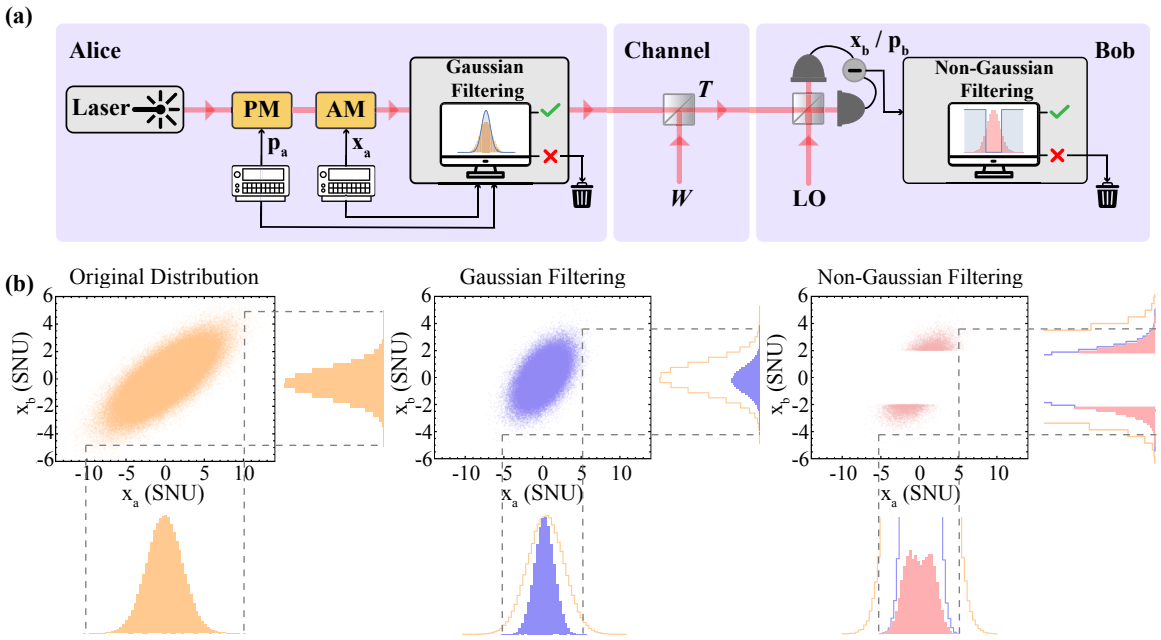

Figure 5.1: Experimental schematic and illustrative diagram of the filtering process. (a) Alice encodes coherent states $|(x_a + ip_a)/2\rangle$ from a Gausssian distribution with zero mean and variance V_{mod} using white noise generated by function generators. She samples x_a and p_a simultaneously, then sends the encoded states through a quantum channel with transmittivity T and thermal noise W. Bob performs homodyne detection to measure x_b and p_b, randomly switching between these two quadratures. After data acquisition and once the states have been sent to Bob, Alice applies a Gaussian filter to the measurement data kept on her computer, followed by Bob applying a non-Gaussian filter to his measurement outcomes. **(b)** Left: The correlation between Alice's variables x_a and Bob's measurement outcomes x_b before any post-selection. Middle: The correlation after Alice's Gaussian post-selection superimposed by the original distribution (orange), which reduces the variance of the Gaussian-modulated variables, effectively creating a thermal state with this variance. Right: The correlations after Bob's non-Gaussian post-selection, resulting in highly non-Gaussian distributions for x_a and x_b. PM/AM: Electro-optic phase/amplitude modulators and LO: Local oscillator.

The experimental setup is shown in Fig. 5.1(a), where Alice generates two variables, x_a and p_a, from zero-mean Gaussian distributions $\mathcal{N}(0, V_{mod})$ with variance V_{mod} in units of

vacuum noise using two independent function generators. These variables are imprinted onto a 1064 nm continuous-wave laser by modulating its sideband at $3-5$ MHz via electro-optical amplitude and phase modulators, generating a thermal state with quadrature variance $V_{mod}+1$. Alice keeps these variables to apply a Gaussian filter to both x_a and p_a after the states have been sent to Bob and measured. The encoded state is sent through a quantum channel with transmittance T and thermal noise W, simulated by a half-wave plate and polarising beamsplitter. Bob performs homodyne detection, randomly measuring the x or p quadrature. The homodyne signal is filtered by a $3-5$ MHz bandpass filter and then fed to the oscilloscope with a sampling rate of 25 MSamples/s, collecting 10 million samples. Both homodyne data and Alice's data were digitally filtered with a $3-3.5$ MHz bandpass filter.

While the experimental setup follows the well-known GG02 protocol [78, 100], which utilises Gaussian modulated coherent states and homodyne detection, our protocol diverges at the software level. This software-level protocol can be applied to any system with Gaussian modulated states and coherent detection. After the data acquisition, Alice's post-selection is applied on the samples x_a and p_a where Alice's Gaussian post-selection filter is defined by the following expression

$$F_A(x_a) = e^{-g_x^2 x_a^2}, \tag{5.1}$$

where x_a is the randomly generated variable and $g_x \geq 0$ represents the filter gain. Each symbol, x_a, is either kept or discarded based on the probability $F_A(x_a)$. The same function applies to p_a, replacing g_x with g_p. This post-selection on x_a and p_a imitates attenuating the modulation variance, as shown in Fig. 5.1(b). When $g_x = 0$, no filtering is applied, but as g_x increases significantly (e.g., $g_x = 10^5$), the modulation variance approaches zero, effectively turning the state into vacuum. In the GG02 protocol, there is an optimal modulation variance for each distance and noise combination to achieve the best key rates. While Alice's post-selection does not alter the channel parameters, it reduces the modulation variance to match the optimal GG02. Unlike GG02, which requires modulation variance optimisation, Alice's approach optimises both the variance and key rates without needing prior channel characterisation. The optimisation also inherently depends on the reconciliation efficiency, β, which quantifies how efficiently Alice and Bob can extract shared bits from their correlated data during classical post-processing (see Eq. (4.37)). Lower values of β reduce the mutual information between Alice and Bob, shifting the modulation variance that maximises the final key rate. Therefore, when comparing key rates or optimising filters, the effect of β must be taken into account.

The key rates can be further optimised by using a non-Gaussian post-selection per-

formed by Bob. Bob's post-selection filter can be expressed as

$$F_B(x_b) = \begin{cases} 0 & -c_x < x_b < c_x \\ 1 & \text{elsewhere,} \end{cases} \tag{5.2}$$

where x_b represents Bob's homodyne measurement outcome and c_x is the cut-off parameter of the filter which can take values from 0 to the largest measurement outcome of Bob. Bob's post-selection discards all the numbers within the cut-off, therefore, it creates a highly non-Gaussian distribution as shown in Fig. 5.1(b). This post-selection effectively simulates a channel with better performance than the original one used by Alice to send the quantum states.

As mentioned previously in Sec. 4.4.3, in QKD, Eve holds the purification of Alice and Bob's joint state σ_{AB}, meaning her von Neumann entropy matches that of the state shared by Alice and Bob. Therefore, Eve's information can be bounded by the Holevo bound [89] given in Eq. (4.24). Since Bob's post-selection is non-Gaussian, using the covariance matrices σ_{AB} and $\sigma_{\mathrm{A|B}}$ would overestimate Eve's information due to Gaussian extremality, leading to lower key rates. Instead, we directly calculate Eve's information from her density matrix, assuming that she performs a general Gaussian attack. In this attack, Eve prepares a two-mode squeezed vacuum (TMSV) state with a variance that mimics the quantum channel [74]. She replaces the channel between Alice and Bob with a beamsplitter, injecting one mode (E_1) into the beamsplitter to interact with Alice's state, while retaining the other mode (E_2) [131]. While the optimal strategy after post-selection is not known, our assumption follow from the intuition that Alice and Bob can verify (within some tolerance) that the channel remains Gaussian by computing higher-order moments from their measurement outcomes such as skewness and kurtosis, thereby restricting Eve to Gaussian attacks. Eve's information is then calculated as follows

$$I_E = S(\rho_{\mathrm{E_1E_2}}) - S(\rho_{\mathrm{E_1E_2|B}}(x_b)), \tag{5.3}$$

where $S(\rho_{\mathrm{E_1E_2}})$ represents the von Neumann entropy of Eve's average state, and $S(\rho_{\mathrm{E_1E_2|B}}(x_b))$ gives the von Neumann entropy of Eve's conditional state given Bob measures an outcome x_b. This equation saturates Eq. (4.24) when Bob performs no post-selection, and everything remains Gaussian. In that case, Eve's average state is the sum of all Gaussian conditional states measured by Bob. With non-Gaussian post-selection, the conditional states remain Gaussian, but Eve's average state becomes non-Gaussian. Since Bob can discard measurement outcomes within the filter cut-off, Eve's average state is no longer obtained by simply summing all the states, but is derived from the filtered results as

follows

$$\rho_{\mathrm{E_1E_2}} = \sum_{x_i=-n}^{n} p'_b(x_i)\rho_{\mathrm{E_1E_2|B}}(x_i), \tag{5.4}$$

where n is the maximum number that Bob measures and $p'_b(x_i)$ denotes Bob's probability of getting a given outcome, x_i. This method is particularly beneficial because it does not rely on Gaussian extremality to determine key rates. Previously, this reliance limited the performance of some protocols when non-Gaussian post-selection was used [231].

It is important to note that post-selection by both parties is not always required. Depending on the channel parameters, either Alice's post-selection or Bob's post-selection alone may be sufficient, while in some cases, both may be necessary. The advantage of our protocol lies in its ability to be augmented into existing CV-QKD setups without any hardware modifications, as it operates entirely at the software level.

5.2.1 Security Analysis of Alice's Gaussian Post-Selection

The random variables generated by Alice's function generator follow a Gaussian distribution as described below

$$p_a(x_a) = \frac{1}{\sqrt{2\pi V_{mod_x}}}\exp\left[\frac{-x_a^2}{2V_{mod_x}}\right], \tag{5.5}$$

where V_{mod_x} represents the modulation variance of Alice along the x quadrature with random variables x_a. The modulation variance of the x and p quadrature are not symmetric due to the experimental imperfections. However, as Bob performs a homodyne measurement, Alice's Gaussian distribution of the x and p quadrature variables can be expressed individually. In the following, we explicitly present the analysis for the x quadrature, which can be similarly applied to the p quadrature. When Alice applies the filter shown in Eq. (5.1), the probability of success is given by

$$P_{A_x} = \int_{-\infty}^{\infty} F_A(x_a)p_a(x_a)\,dx_a = \frac{1}{\sqrt{2g_x^2V_{mod_x}+1}}, \tag{5.6}$$

where g_x is the gain of the Gaussian filter for the x quadrature. Experimentally, Alice's filter, as described in Eq. (5.1), is implemented by generating a random number uniformly distributed between 0 and 1. The filter then retains the variables whose corresponding filter function values are greater than or equal to this random number. The probability of success is determined by the ratio of samples kept after filtering to the total number of samples. For our experiment, the gains were optimised for a transmission distance by numerically sweeping over possible gain values and selecting the configuration that maximised the secure key rate. This optimisation accounted for both the mutual information between Alice and Bob and the Holevo bound representing Eve's accessible information (refer to Eq. (5.14)). For a

distance of 29.1 km, we used $g_x = 0.213$ and $g_p = 0.259$, while for a distance of 39.1 km, the gains were $g_x = 0.178$ and $g_p = 0.213$.

After Alice's post-selection, the modulation variance of the effective thermal state is reduced. The equivalent modulation variance is expressed as follows

$$\tilde{V}_{mod_x} = \int_{-\infty}^{\infty} \frac{x_a^2 F_A(x_a) p_a(x_a)}{P_{A_x}} \, dx_a = \frac{V_{mod_x}}{2g_x^2 V_{mod_x} + 1}. \tag{5.7}$$

Alice's post-selection cannot modify the channel parameters. However, Bob's effective variance also reduces, as he must disregard the data that Alice discards. Therefore, Bob's variance, using Alice's new variance $V_x = \tilde{V}_{mod_x} + 1$, can be expressed as

$$V_{b_x} = T(V_x + \xi_x) + (1 - T)W_x, \tag{5.8}$$

where ξ_x is trusted excess noise coming from the state preparation, T is the channel transmittance which represents the channel loss and is introduced experimentally using a half-wave plate followed by a PBS. This loss is equivalent to a distance of $d = -\log_{10} T/0.02$ assuming a loss of 0.2 dB per km. W_x denotes the thermal noise from the quantum channel, attributed to Eve. Similarly, the covariance between Alice and Bob after Alice's post-selection scales to $T\tilde{V}_{mod_x}$ in the prepare-and-measure (PM) scheme. QKD protocols can be expressed in either entanglement-based (EB) or prepare-and-measure schemes. While mathematically equivalent [74, 119], the EB representation is more convenient for security analysis. Therefore, the new covariance between Alice and Bob in the equivalent EB scheme can be expressed as

$$C_x = \sqrt{T(V_x^2 - 1)}. \tag{5.9}$$

The EB-based covariance matrix of the quantum state between Alice and Bob can be written as [236] (refer to Appendix A.1 for the derivation of the PM covariance matrix and Appendix A.3 for derivation of the covariance matrices starting from the EB model)

$$\sigma_{\mathrm{AB}}^{\mathrm{EB}} = \begin{pmatrix} V_x & 0 & C_x & 0 \\ 0 & V_p & 0 & -C_p \\ C_x & 0 & V_{b_x} & 0 \\ 0 & -C_p & 0 & V_{b_p} \end{pmatrix}. \tag{5.10}$$

Note that C_p has the same form as C_x, but with a different variance, V_p. Similarly, Bob's variance V_{b_p} follows the same formula as Eq. (5.8), with the variance V_p, trusted noise ξ_p, and thermal noise W_p.

The mutual information between Alice and Bob can be calculated using the EB-based

covariance matrix shown in Eq. (5.10). In our protocol, we employ reverse reconciliation, meaning the direction of classical communication is from Bob to Alice [124]. As mentioned previously in Sec. 4.4.3, while the direction of reconciliation does not affect the mutual information between Alice and Bob, it influences how much information Eve can access. CV-QKD protocols with reverse reconciliation, unlike direct reconciliation, allow key distribution beyond the 3 dB loss limit [100, 237]. The mutual information between Alice and Bob is calculated using Eq. (4.36) with $V_{A_x} = (V_x + 1)/2$ and $V_{A_x|B_x} = V_{A_x} - C_x^2/(2V_{b_x})$.

Eve's average covariance matrix also scales after Alice's post-selection, as Alice and Bob keep fewer states than originally. As previously mentioned, Eve performs an entangling cloner attack, where she creates a TMSV state with modes E_1 and E_2. Mode E_1 interacts with incoming signal from Alice, while mode E_2 is kept by Eve. After Alice's post-selection, the variance of E_1 is updated as follows, while the variance of E_2 remains unchanged

$$V_{E_{1_x}} = TW_x + (1 - T)(V_x + \xi_x). \tag{5.11}$$

Note that the variance of the p quadrature for this mode follows the same formula, but with Alice's variance V_p, trusted excess noise ξ_p and a thermal noise of W_p. In practice, there exists a slight discrepancy between W_x and W_p due to the asymmetry in the experimental measurements. This implies that Eve introduces slightly different noise in the x and p quadratures, expressed as W_x and W_p, respectively. To achieve this, Eve must create two separate TMSV states [74] and combine them at a 50/50 beamsplitter before interacting with Alice's signal. Based on these, Eve's average covariance matrix can be expressed as

$$\sigma_{\mathrm{E_1E_2}} = \begin{pmatrix} V_{E_{1_x}} & 0 & C_{E_x} & 0 \\ 0 & V_{E_{1_p}} & 0 & C_{E_p} \\ C_{E_x} & 0 & W_x & 0 \\ 0 & C_{E_p} & 0 & W_p \end{pmatrix}, \tag{5.12}$$

where $C_{E_x} = 0.5(-\mathrm{e}^{2r_1} + \mathrm{e}^{2r_2})$ and $C_{E_p} = 0.5(-\mathrm{e}^{-2r_1} + \mathrm{e}^{-2r_2})$ where r_1 and r_2 are the squeezing parameters of the TMSV states of Eve which are given by $r_1 = 0.5\ln\left(W_x + \sqrt{W_x^2 - W_x/W_p}\right)$ and $r_2 = 0.5\ln(W_x/W_p) - 0.5\ln\left(W_x + \sqrt{W_x^2 - W_x/W_p}\right)$. Eve's information is calculated using the Holevo bound [89] given in Eq. (4.35) where her state conditioned on Bob's measurement outcome x_b is obtained from Eq. (4.32). In this case, the $\sigma_{c_{eb}}$ is given as

$$\sigma_{c_{eb}} = \begin{pmatrix} C_{E_1B_x} & 0 \\ 0 & C_{E_1B_p} \\ C_{E_2B_x} & 0 \\ 0 & C_{E_2B_p} \end{pmatrix}, \tag{5.13}$$

where $C_{E_1B_x} = \sqrt{T(1-T)}\big(W_x - (V_x + \xi_x)\big)$, $C_{E_1B_p} = \sqrt{T(1-T)}\big(W_p - (V_p + \xi_p)\big)$, $C_{E_2B_x} = \sqrt{(1-T)}C_{E_x}$ and $C_{E_2B_p} = \sqrt{(1-T)}C_{E_p}$.

The secret key rate is calculated using Eq. (4.37). In our experiment, we assume $\beta = 92\%$ when calculating the key rates. As Bob performs homodyne measurements on the x quadrature half of the time and on the p quadrature the other half, and since the variances and noise parameters differ between these quadratures due to experimental imperfections, Alice and Bob's mutual information, as well as Eve's information, must be averaged over both quadratures. This leads to $I_{AB} = 0.5P_{A_x} \times I_{AB_x} + 0.5P_{A_p} \times I_{AB_p}$ and $I_E = 0.5P_{A_x} \times I_{E_x} + 0.5P_{A_p} \times I_{E_p}$. Therefore, the overall key rate after Alice's post-selection is expressed as

$$K(g_x, g_p) = \max_{g_x, g_p} \left[\beta I_{AB}(g_x, g_p) - I_E(g_x, g_p)\right] \tag{5.14}$$

5.2.2 Security Analysis of Bob's Non-Gaussian Post-Selection

Bob's initial distribution before his post-selection can be expressed as

$$p_b(x_b) = \frac{1}{\sqrt{2\pi V_{b_x}}} \exp\left[\frac{-x_b^2}{2V_{b_x}}\right], \tag{5.15}$$

where x_b corresponds to Bob's measurement outcome. Following Alice's post-selection, Bob applies the filter shown in Eq. (5.2), which gives a probability of success of

$$P_{B_x} = \int_{-\infty}^{\infty} F_B(x_b) p_b(x_b)\, dx_b = 1 - \mathrm{erf}\left[\frac{c_x}{\sqrt{2V_{b_x}}}\right], \tag{5.16}$$

where c_x is the cut-off parameter of the filter function.

Following Bob's post-selection, his output probability distribution becomes

$$\tilde{p}_b(x_b) = \begin{cases} 0 & -c_x < x_b < c_x \\ \frac{p_b(x_b)}{P_{B_x}} & \text{elsewhere,} \end{cases} \tag{5.17}$$

As Bob's filter is non-Gaussian, we avoid using the Gaussian extremality as this approach underestimates the secret key rate due to overestimating Eve's information. Therefore, we propose calculating the absolute bound on Eve's information directly from her density matrix.

To express Eve's conditional state shown in Eq. (4.32) as a density matrix, we first use Williamson's decomposition, which provides a symplectic matrix s and a diagonal matrix ω, following $s\sigma_{\mathrm{E_1E_2|B}_x} s^T = \omega$ [90]. We then decompose the symplectic matrix, s, further using

the Bloch-Messiah decomposition [238], representing s as a series of beamsplitters, squeezers, and phase rotations: $s = s_u s_i s_v$ in the covariance matrix notation and $S = S_U S_I S_V$ in the density matrix notation. In our case, both s_u and s_v are expressed through phase rotations and beamsplitters: $S_U = R(\theta_1, \theta_2)B(\tau_U)R(\theta_3, \theta_4)$ and $S_V = R(\theta_5, \theta_6)B(\tau_V)R(\theta_7, \theta_8)$, where each parameter needs to be solved. The s_i component is expressed through two-mode squeezing operations, $S_I = S(r_1, r_2)$. Therefore, Eve's overall conditional density matrix is written in terms of the symplectic density matrix S and a mixed thermal state Λ

$$\rho_{\mathrm{E_1E_2|B}_x}(x_b = 0) = S\Lambda S^\dagger, \tag{5.18}$$

where $\Lambda = \rho_1 \otimes \rho_2$, with ρ_1 and ρ_2 being thermal states given by $\sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle\langle n|$, having mean photon numbers $\bar{n}_1$ and $\bar{n}_2$, respectively. Note that $\bar{n}_i = (\lambda_i - 1)/2$, where λ_i represents the i^{th} diagonal terms of the diagonal matrix ω. In our case, ω has two unique diagonal terms, λ_1 and λ_2, which are used to calculate the mean photon numbers $\bar{n}_1$ and $\bar{n}_2$.

To calculate Eve's information, we need to determine her average density matrix, which is the sum of her all conditional matrices over Bob's measurement outcomes weighted by the probability density for the respective outcome. Given that Bob measures an outcome x_b, Eve's conditional state is

$$\rho_{\mathrm{E_1E_2|B}_x}(x_b) = D(\alpha_1(x_b), \alpha_2(x_b))\rho_{\mathrm{E_1E_2|B}_x}(x_b = 0)D^\dagger(\alpha_1(x_b), \alpha_2(x_b)), \tag{5.19}$$

where $D(\alpha_1(x_b), \alpha_2(x_b))$ represents the displacement operator for Eve's modes 1 and 2 in the form of

$$D(\alpha_1(x_b), \alpha_2(x_b)) = \exp\Big(\alpha_1(x_b)a^\dagger - \alpha_1(x_b)a\Big) \otimes \exp\Big(\alpha_2(x_b)a^\dagger - \alpha_2(x_b)a\Big),$$

where α_1 and α_2 are functions of Eve's conditional means based on Bob's measurement outcomes, x_b. The matrix of Eve's conditional means is calculated from

$$\mu_{E_1E_2}(x_b, p_b) = \sigma_{c_{eb}} \begin{pmatrix} V_{b_x} & 0 \\ 0 & V_{b_p} \end{pmatrix}^{-1} \begin{pmatrix} x_b \\ p_b \end{pmatrix}, \tag{5.20}$$

where $p_b = 0$ for homodyne detection when x_b is measured and $x_b = 0$ when p_b is measured. Therefore $\alpha_1(x_b) = \mu_{\mathrm{E}_1}(x_b)/2$ and $\alpha_2(x_b) = \mu_{\mathrm{E}_2}(x_b)/2$ where $\mu_{\mathrm{E}_1}(x_b)$ and $\mu_{\mathrm{E}_2}(x_b)$ are obtained from the entries of the $\mu_{\mathrm{E_1E_2}}(x_b, 0)$ matrix as follows: $\mu_{\mathrm{E}_1}(x_b) = \mu_{\mathrm{E_1E_2}}(x_b, 0)[1]$ and $\mu_{\mathrm{E}_2}(x_b) = \mu_{\mathrm{E_1E_2}}(x_b, 0)[3]$.

Although each conditional state has the same entropy, they contribute differently to Eve's average state due to the varying probabilities of obtaining each conditional state.

Therefore, we determine Eve's average density matrix by multiplying each conditional state with their corresponding probabilities from Bob's post-selected probability distribution followed by summing them all up. Note that Bob's probability of getting a given outcome is obtained from

$$p'_b(x_i) = \int_{x_i-\Delta}^{x_i+\Delta} \tilde{p}_b(x_i)\, dx_b. \tag{5.21}$$

To calculate the key rates after the non-Gaussian post-selection, we discretise Eve's information to determine the conditional states for each of Bob's measurement outcomes. Therefore, Δ in Eq. (5.21) is the width of the discretised bins and in our results $\Delta = 0.1$. Consequently, Eve's average state can be calculated from Eq. (5.4). Eve's information is then calculated using the Holevo bound which is

$$I_{E_x} = S(\rho_{\mathrm{E_1E_2}}) - S(\rho_{\mathrm{E_1E_2|B}_x}(0)), \tag{5.22}$$

where $S(\rho_{\mathrm{E_1E_2}})$ represents the von Neumann entropy for Eve's average state while $S(\rho_{\mathrm{E_1E_2|B}_x}(0))$ gives the von Neumann entropy of Eve's conditional state which remains the same irrespective of Bob's measurement outcome x_b.

In order to find Alice and Bob's mutual information, the new bivariate Gaussian distribution between Alice and Bob following Alice's post-selection is fitted to the following function

$$f_{AB}(x_a, x_b) = \frac{1}{2\pi\sigma_a\sigma_b\sqrt{1-\rho^2}} \exp\left[-\frac{1}{2(1-\rho^2)}\left(\frac{x_a^2}{\sigma_a^2} - \frac{2\rho x_a x_b}{\sigma_a\sigma_b} + \frac{x_b^2}{\sigma_b^2}\right)\right], \tag{5.23}$$

where $\sigma_a = \sqrt{(V_x+1)/2}$ and $\sigma_b = \sqrt{V_{b_x}}$ are the standard deviations of Alice and Bob, respectively, and $\rho = C_x/\sqrt{2\sigma_a\sigma_b}$ represents the correlation term between them.

Using Eq. (5.23), we generate a probability table between Alice and Bob for each values of x_a and x_b where $x_a = -15, -15+\Delta, \cdots, 15$ and $x_b = -9, -9+\Delta, \cdots, 9$. The mutual information then is calculated from

$$I_{AB_x} = H_{A_x} + H_{B_x} - H_{AB_x}, \tag{5.24}$$

where H_{A_x}, H_{B_x}, and H_{AB_x} represent the Shannon entropy of Alice's classical variable, Bob's classical variable, and the joint entropy of Alice and Bob's classical variables, respectively.

After Bob's post-selection H_{AB_x} can be computed from

$$H_{AB_x} = -\sum_{x_a=-n_a}^{n_a}\sum_{x_b=-n_b}^{-c_x-\Delta/2}\frac{f_{AB}(x_a,x_b)}{P_{B_x}}\log_2\left[\frac{f_{AB}(x_a,x_b)}{P_{B_x}}\right]- \sum_{x_a=-n_a}^{n_a}\sum_{x_b=c_x+\Delta/2}^{n_b}\frac{f_{AB}(x_a,x_b)}{P_{B_x}}\log_2\left[\frac{f_{AB}(x_a,x_b)}{P_{B_x}}\right], \tag{5.25}$$

where c_x is the cut-off parameter of Bob's filter function in Eq. (5.2); where n_a and n_b represent the maximum number that Alice prepares and Bob measures, respectively.

Alice's probabilities after Bob's post-selection can be found from

$$f_A(x_a) = \sum_{x_b=-n_b}^{-c_x-\Delta/2}\frac{f_{AB}(x_a,x_b)}{P_{B_x}} + \sum_{x_b=c_x+\Delta/2}^{n_b}\frac{f_{AB}(x_a,x_b)}{P_{B_x}}, \tag{5.26}$$

which is used to compute H_{A_x}

$$H_{A_x} = -\sum_{x_a=-n_a}^{n_a} f_A(x_a)\log_2\left[f_A(x_a)\right]. \tag{5.27}$$

Similarly, Bob's probabilities from the probability table after his post-selection can be found from

$$f_B(x_b) = \sum_{x_a=-n_a}^{n_a}\frac{f_{AB}(x_a,x_b)}{P_{B_x}}, \tag{5.28}$$

which is used to calculate H_{B_x} as

$$H_{B_x} = -\sum_{x_b=-n_b}^{-c_x-\Delta/2} f_B(x_b)\log_2\left[f_B(x_b)\right] - \sum_{x_b=c_x+\Delta/2}^{n_b} f_B(x_b)\log_2\left[f_B(x_b)\right]. \tag{5.29}$$

5.2.3 Calculation of the Final Key Rate

Since both Alice and Bob perform post-selection, we need to consider the probabilities of success and average the key rates over the x and p quadratures. Following Bob's filtering process, the average mutual information between Alice and Bob becomes $I_{AB} = 0.5P_{B_x}P_{A_x}I_{AB_x} + 0.5P_{B_p}P_{A_p}I_{AB_p}$. Eve's information is averaged in the same manner as the mutual information. Finally, the key rate is calculated using Eq. (4.37).

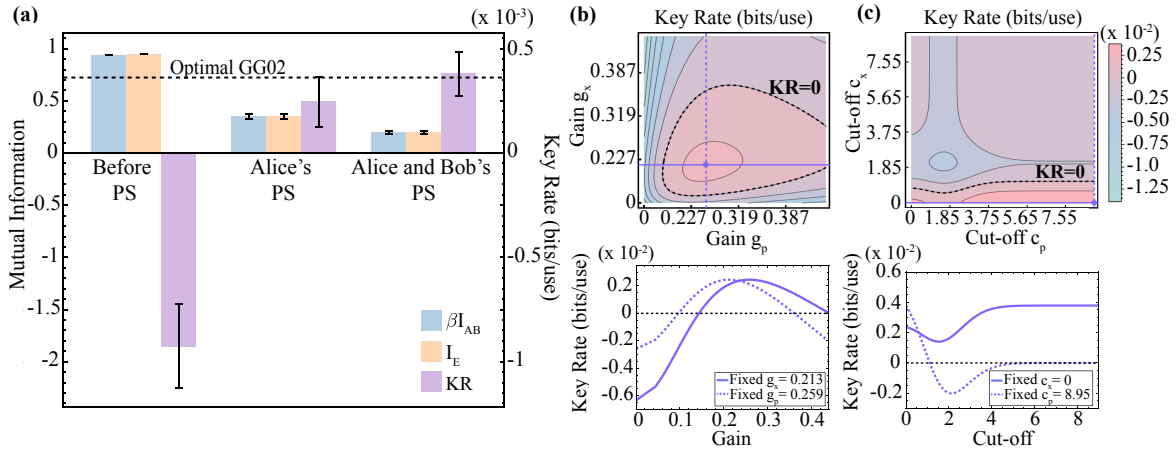

Figure 5.2: Experimental results of a quantum channel with a transmission of $T = 0.26$. This is equivalent to a fibre distance of 29.1 km (assuming 0.2 dB loss per km), and the thermal noise for the x and p quadratures are $W_x = 1.02 \pm 0.001$ and $W_p = 1.01 \pm 0.001$ in shot noise units (SNU), respectively. **(a)** From left to right, we give the mutual information between Alice and Bob (blue boxes), Eve's information (orange boxes) and the key rates of the protocol (purple boxes) before any post-selection, after Alice's post-selection and after Alice and Bob's post-selection combined, respectively. The key rate is initially negative, indicating that Eve's information exceeds the mutual information of Alice and Bob, making it a non-secure region. After Alice's post-selection, the key rate becomes positive but remains below the optimal GG02 rate for that distance. The key rate is further optimised by applying a post-selection on Bob's side where the key rate achieves the optimal GG02 line. **(b)** The top figure shows the contour plot of the key rates after Alice's post-selection along the x and p quadratures, with gains ranging from 0 to 0.436. The bottom figure illustrates the key rate slices at optimal performance after Alice's post-selection with fixed gains g_x and g_p. The solid line represents fixed g_x while varying g_p, and the dashed line represents fixed g_p while varying g_x. **(c)** Top figure demonstrates the contour plot of the key-rates after Bob's post-selection with the cut-off parameters ranging from 0 to 8.95, while the bottom figure shows the key rates after Bob's post-selection with fixed optimal cut-offs in the x (solid line) and p (dashed line) quadratures. The solid line varies the cut-off in the p quadrature while keeping the x cut-off fixed, and the dashed line varies the cut-off in the x quadrature while keeping the p cut-off fixed. KR: Key rate, $\mathrm{I_{AB}}$: Mutual information between Alice and Bob, $\mathrm{I_E}$: Eve's information and β: Reconciliation efficiency. The reconciliation efficiency is set to 92%. The error bars indicate the statistical uncertainties in the data. For details on how they are calculated, refer to the Methods section.

5.3 Results

Figure 5.2 shows the experimental results for a loss of $T = 0.26$ with thermal noise values of $W_x = 1.02$ SNU and $W_p = 1.01$ SNU for the x and p quadratures, respectively. This loss corresponds to an equivalent fibre distance of 29.1 km assuming a fibre loss of 0.2 dB per km. The key rate extracted from the raw data is initially negative, as illustrated in Fig. 5.2(a). This is because the modulation variance used in the experiment is not optimal for the 29.1 km distance with the given noise parameters, leading to Eve receiving more information than Alice and Bob, and thus a negative key rate as defined in Eq. 4.37. The

experimental modulation variances for the x and p quadratures were $V_{mod_x} = 12.73$ SNU and $V_{mod_p} = 13.52$ SNU, while the optimal GG02 modulation variances required for this regime are $V_{mod_x} = 6.14$ SNU and $V_{mod_p} = 5.97$ SNU. The asymmetry in the variances is due to asymmetric noise in the state preparation stage. A portion of this preparation noise, primarily due to modulator electronics, is considered trusted in our security analysis. Alice applies a Gaussian filter with gains of $g_x = 0.213$ and $g_p = 0.259$ to reduce the modulation variances. These gains yield the optimal key rate, as indicated in Fig. 5.2(b). Although the key rate becomes positive after Alice's post-selection, it does not reach the optimal GG02 key rate due to the success probability penalty of the post-selection process ($P_{A_x} = 0.68$ and $P_{A_p} = 0.60$ are the probability of success of Alice's post-selection on the x and p quadratures, respectively, giving a total probability of success of 0.41) as shown in Fig. 5.2(a).

To further optimise the key rate, Bob applies a non-Gaussian filter with cut-off parameters of $c_x = 0$ and $c_p = 8.95$ which is shown in Fig. 5.2(c). Bob keeps the x quadrature unchanged as it is already optimal but discards most measurements in the p quadrature where the maximum value is $p_b = 9$. The key rate increases and saturates at 0.0038 ± 0.001 bits/use, surpassing the optimal GG02 key rate of 0.0036 bits/use. Our protocol turned regions with negative key rates, deemed insecure by the GG02 protocol, into regions with positive key rates. In these regions, we achieved key rates close to the optimal GG02 rates that are only achievable using optimal modulation which requires accurate channel estimations.

Next, we investigate distinct regimes where the system benefits from varying post-selection strategies. Figures 5.3(a) and (b) show that at 6 km and 15.1 km (transmission of $T = 0.76$ and $T = 0.50$, respectively), the key rates with Alice's Gaussian filter match those without post-selection, as the system parameters were already optimal. In this protocol, Alice's Gaussian filter attenuates the quantum signal by reducing the modulation variance, which is useful at long distances where photon losses require smaller optimal variances for the GG02 protocol. For shorter distances, where higher modulation variances are preferred, an inverted Gaussian filter can be used to increase the effective variance and optimise key rates. In contrast to the 6 km and 15.1 km regimes, Alice and Bob's post-selection improves the key rate when experimental parameters are sub-optimal. For example, without post-selection, the chosen parameters yield no positive key rate (solid line, Fig. 5.3(c)), but Alice's post-selection makes the key rate positive, surpassing the optimal GG02 rate when Bob also applies post-selection. Similarly, at 39.1 km (transmission of $T = 0.17$), Alice's post-selection increased the key rate by 1.7 times (Fig. 5.3(d)), but Bob's post-selection did not lead to further improvement, as it is more effective in extreme loss regimes where the GG02 protocol approaches negative key rates.

[1] Experimental imperfections cause asymmetry in the x and p quadratures. The first row shows the experimental values for x, while the second row shows the values for p.

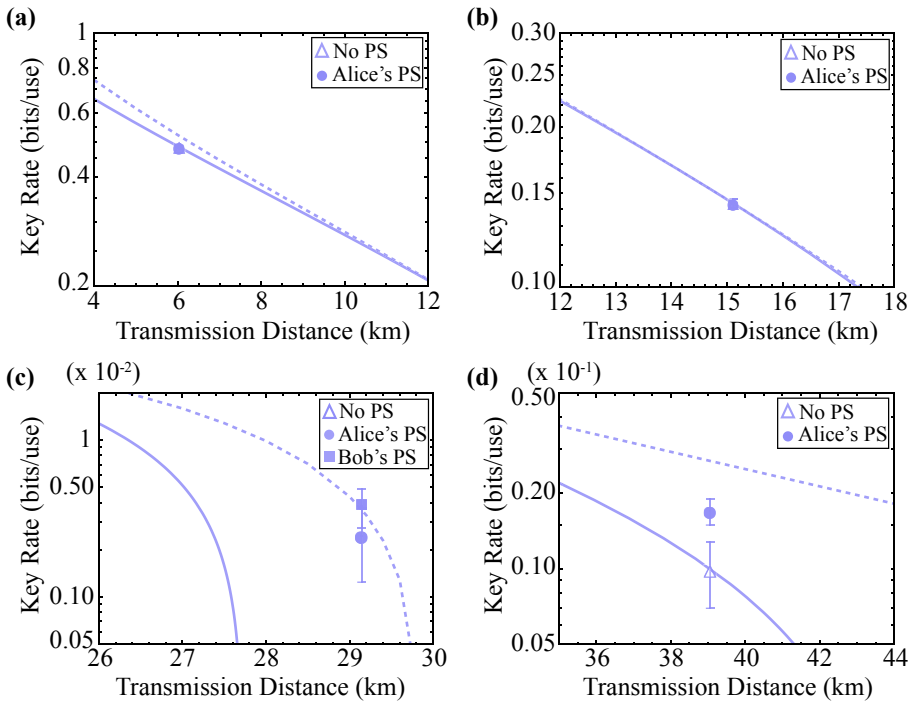

Figure 5.3: Experimental key rates for various channel parameters, assuming a fibre loss of 0.2 dB per km. The reconciliation efficiency is set to $\beta = 92\%$. Solid lines represent theoretical key rates of the GG02 protocol with fixed modulation variance, while dashed lines show theoretical key rates with optimal variances. Triangle markers indicate raw key rates before post-selection, circles show key rates after Alice's post-selection, and the square marker represents results after Bob's post-selection. **(a)** and **(b)** show the experimental results at $d = 6$ km ($T = 0.76$) and $d = 15.1$ km ($T = 0.50$), respectively. For $d = 6$ km, thermal noise is $W_x = 1.02 \pm 0.004$ and $W_p = 1.04 \pm 0.004$; for $d = 15.1$ km, $W_x = 1.02 \pm 0.002$ and $W_p = 1.03 \pm 0.002$. Key rates before and after Alice's post-selection overlap, indicating optimal operations. **(c)** Key rates at $d = 29.1$ km ($T = 0.26$) with thermal noise $W_x = 1.02 \pm 0.001$ and $W_p = 1.01 \pm 0.001$. The post-selections enhance the key rate which is otherwise negative; as a result, the data without post-selection (triangular marker) does not appear on the logarithmic scale. **(d)** Key rates at $d = 39.1$ km ($T = 0.17$) with thermal noise $W_x = 1.00 \pm 0.001$ and $W_p = 1.00 \pm 0.001$, where only Alice's post-selection was applied, as Bob's post-selection did not lead to any further improvements in this region.

Furthermore, we applied our protocol to state-of-the-art CV-QKD experimental demonstrations and showed improved performance (see Fig. 5.4(a)). Our protocol increased the key rates of the experimental results of Wang *et al.* [106] and Hajomer *et al.* [109], while doubling the key rate of Zhang *et al.* [107] and achieving a fivefold improvement for Li *et al.* [239] using Alice's post-selection where the percentage improvements are shown in Table 5.1. We projected their experimental demonstrations to larger distances by simulating their protocols using the parameters listed in Table 5.1, assuming these parameters remain constant across all distances. Under these conditions, our protocol extended the effective transmission distance by 42 km for Wang *et al.* [106] and Zhang *et al.* [107], while also en-

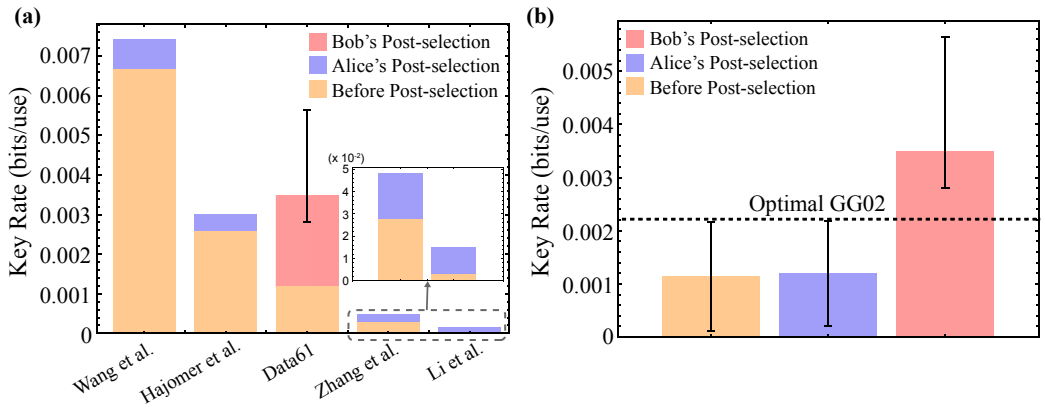

Figure 5.4: Key rates of existing experiments after applying our protocol, based on their original experimental parameters which are shown in Table 5.1. (a) Key rates from various experiments [106, 107, 109, 239] and the experimental data from Data61 using the CV-QKD setup from Quintessence Labs. Orange boxes represent the key rates before post-selection, purple boxes denote the results after Alice's post-selection, and the pink box shows the key rate after Bob's post-selection. **(b)** Key rates of Data61 at each step, with a reconciliation efficiency of $\beta = 92.5\%$ (refer to Appendix A.2 for the derivation of the key rate with heterodyne detection). The error bars for Bob's post-selection are based on worst and best-case estimates.

Table 5.1: Experimental parameters of the state-of-the-art CV-QKD demonstrations. d: Distance, V_{mod}: Modulation variance in shot noise units, ξ_{ch}: Channel noise, ξ_d: Dark noise, ξ_t: Trusted noise attributed to state preparation, η: Detection efficiency, β: Reconciliation efficiency, Hom: Homodyne, Het: Heterodyne, KR: Key rate, Inc: Increase.

Experiment	Detection	V_{mod} (SNU)	d (km)	Loss (dB)	ξ_{ch} (mSNU)	ξ_d (SNU)	ξ_t (SNU)	η (%)	β (%)	KR Inc. (%)	d Inc. (km)
Wang *et al.* [106]	Hom.	15	50	10	70	0.05	-	60.141	96.7	11.3	42
Hajomer *et al.* [109]	Het.	8.41	100	15.52	0.212	0.06272	-	68	92.5	16.4	19
Data61 CSIRO[1]	Het.	4.06 4.21	41.71	7.92	43.7 65.4	0.4401 0.4459	0.0867 0.0933	20.6	92.5	206.2	1
Zhang *et al.* [107]	Hom.	14.23	140.52	23.46	21.9	0.2717	-	61.34	96	74.5	42
Li *et al.* [239]	Het.	10	100	18.96	69.2	0.18	-	42	96.7	401.5	23

hancing the transmission distance for Hajomer *et al.* [109] and Li *et al.* [239] by 19 km and 23 km, respectively as shown in Fig. 5.5.

Our protocol was also implemented on the Quintessence Labs qOptica system at Data61, CSIRO Sydney, for a fibre distance of 41.71 km, using heterodyne detection with a modulation variance of approximately 4 SNU. Since this variance is close to the optimal value, Alice's post-selection offered little improvement. However, Bob's post-selection tripled the original key rate, surpassing the optimal GG02 rate by emulating a better performing channel as shown in Fig. 5.4. This improvement can be explained by considering an

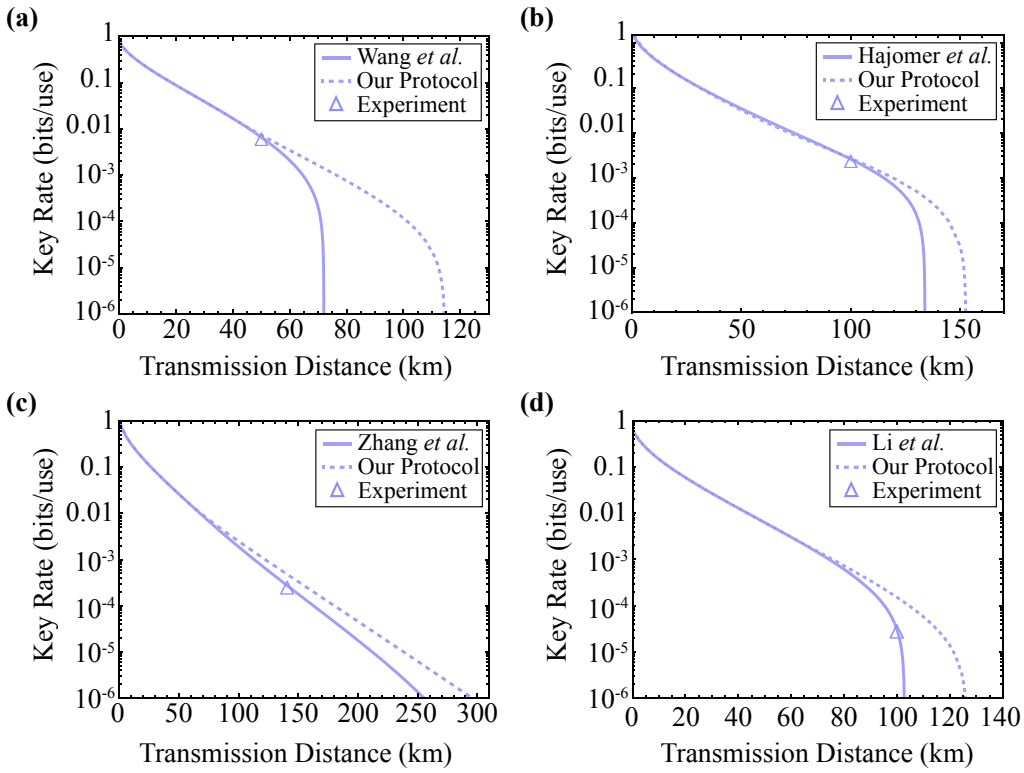

Figure 5.5: Simulated key rates for state-of-the-art experiments extended beyond their original demonstration distances. Solid lines indicate the projected key rates using the experimental parameters, while dashed lines show the key rates when applying our protocol with these same parameters. Simulation results are presented for Wang *et al.* [106] (42 km improvement), Hajomer *et al.* [109] (19 km improvement), Zhang *et al.* [107] (42 km improvement), and Li *et al.* [239] (23 km improvement) in **(a)**, **(b)**, **(c)**, and **(d)**, respectively. Refer to Table 5.1 for the experimental parameters.

entanglement-based experiment where Alice creates a two-mode squeezed vacuum state, sending one arm to Bob and measuring the other. With a Gaussian filter, the best achievable key rate is the optimal GG02 rate, as Gaussian operations cannot distill entanglement [240]. Non-Gaussian operations, however, enable entanglement distillation, allowing Bob to outperform the GG02 key rate. This was also observed in Hosseinidehaj *et al.* [227] when the MB-NLA filter was made slightly non-Gaussian. However, since their approach emulates a physical filter, it cannot be made highly non-Gaussian without deviating from its intended function as a noiseless amplifier. In contrast, our protocol offers the flexibility to choose any filter cut-off.

Our protocol's applicability extends beyond terrestrial setups and can be applied to improve satellite-to-ground communication links for CV-QKD. Figure 5.6(a) and (b) show how our protocol expands the communication window between the ground station and satellite under varying weather conditions, using the satellite-to-ground link model of Sayat *et al.* [129]. Assuming the satellite is in Low Earth orbit at 500 km altitude, the orange lines rep-

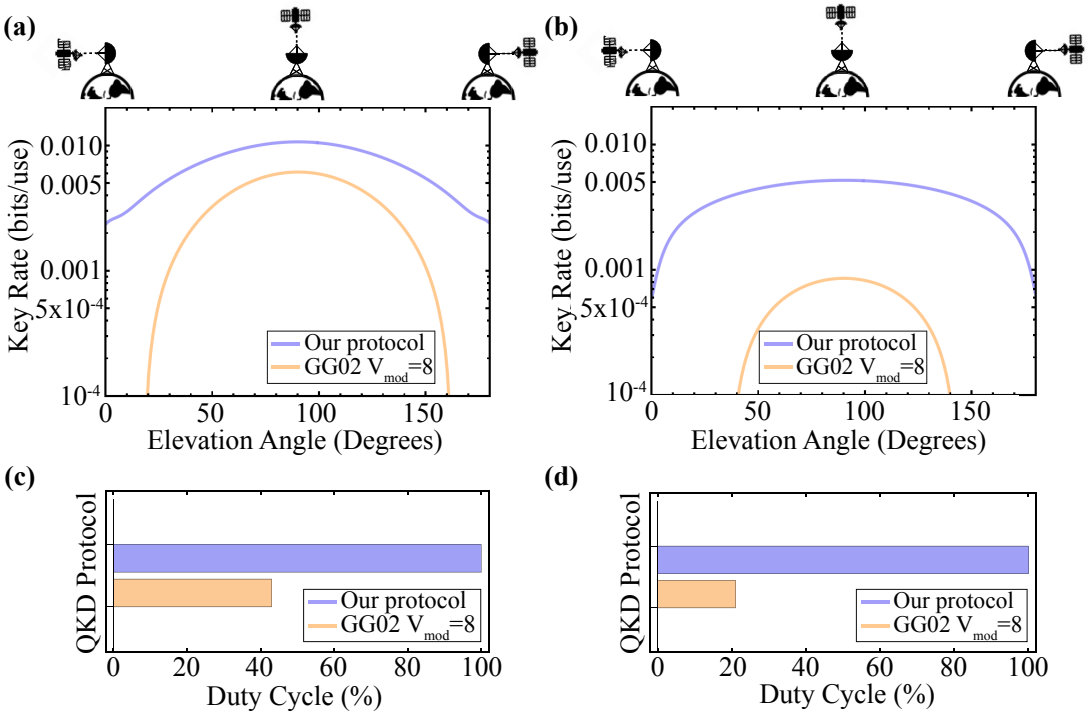

Figure 5.6: Key rates for satellite-to-ground communication as a function of elevation angle, using our protocol applied to the GG02 scheme with homodyne detection. The satellite is assumed to be orbiting at an altitude of 500 km in low-Earth orbit and the optical ground station is at an elevation of 0 km. We used the model and parameters from Sayat *et al.* [129] with a reconciliation efficiency of $\beta = 90\%$ (refer to the Appendix A.4 for the parameters). **(a)** The orange lines represent key rates with a fixed modulation variance of $V_{mod} = 8$, while the purple lines show key rates using our protocol with Alice's post-selection only. This simulation assumes good weather conditions with a visibility of $V = 200$ km and low turbulence corresponding to $C_n^2 = 10^{-16}$ m$^{-2/3}$. At each elevation angle, the post-selection gain was optimised to achieve the best key rates. **(b)** Key rates under bad weather conditions with a visibility of $V = 20$ km and high turbulence where $C_n^2 = 10^{-13}$ m$^{-2/3}$. **(c)** The duty cycle of our protocol and the GG02 protocol in good weather conditions using a key rate threshold of 10^{-4} from (a). **(d)** The duty cycle of our protocol and the GG02 protocol in bad weather conditions using a key rate threshold of 10^{-4} from (b).

resent the conventional GG02 protocol with a modulation variance of $V_{mod} = 8$, while the purple lines show the results of our protocol with Alice's post-selection. In good weather (Fig. 5.6(a)), the GG02 protocol supports communication between the optical ground station (OGS) and satellite at angles from 20° to 160°. In contrast, Alice's post-selection enables communication at all angles, boosting key rates by up to 40 times at the extremes where GG02 achieves the lowest key rates. In poor weather (Fig. 5.6(b)), our protocol further expands the communication window by 76°, achieving a 400-fold improvement in key rates under extreme conditions. In addition to higher key rates, our protocol offers a longer active communication window, defined as the time during which a positive key rate above 10^{-4} bits/use is maintained. Traditional CV-QKD protocols using LEO satellites allow for win-

dows of 1.28 hours in favourable weather and 38 minutes in poor conditions. In contrast, our protocol extends this window to 3 hours in any weather, maintaining a minimum key rate of 10^{-4} bits/use. If a higher key rate threshold were used, the GG02 protocol would have even smaller windows, while our protocol would still provide significantly longer active times (for more details, refer to Appendix A.4). This showcases that our protocol can be particularly useful in free-space channels, such as satellite-to-ground communication links, where rapid changes in the quantum channel are common.

5.4 Discussion

QKD plays a crucial role in securing communications against potential eavesdropping in the quantum era. However, challenges such as limited key rates and vulnerability to environmental factors have impeded its practical deployment.

Addressing these issues, we introduced a new protocol, which enhances CV-QKD by combining post-selection at both Alice and Bob's stations. This protocol utilises a Gaussian filter at Alice's end and a non-Gaussian box-like filter at Bob's end to optimise key rates even under non-ideal conditions. Our approach dynamically adjusts to varying quantum channel conditions, making it particularly effective in free-space channels such as ground-to-satellite communication links.

Experimental results demonstrated significant improvements in key rates when applying our protocol to state-of-the-art CV-QKD systems. We observed up to a five-fold increase in key rates using Alice's post-selection and tripling of the original key rate with Bob's post-selection on different systems. Additionally, our protocol extended the communication window between ground stations and satellites, showing robustness under both good and adverse weather conditions. Specifically, under poor weather conditions, our protocol expanded the communication window to all elevation angles and achieved a 400-fold improvement in key rates under extreme conditions.

The ability of our protocol to achieve secure key distribution even in rapidly changing quantum channels highlights its potential for practical implementation in challenging environments. By leveraging software-level modifications without the need for hardware changes, our approach provides a flexible and efficient solution for advancing CV-QKD technology.

Our current work focuses on asymptotic key rates which assumes an infinitely long key, with potential extensions to account for finite-size effects and composable security. In practical applications, data sizes are finite, and smaller block sizes can adversely affect key rates. Nevertheless, our protocol can be effective in scenarios where block sizes degrade key rate quality, however, a full composable security analysis remains an important direction for

future work. As Bob's post-selection involves a non-Gaussian filter, the security analysis cannot follow the Gaussian extremality. Instead, Eve's information is bounded by representing her state as a density matrix with some finite truncation in the Fock-number basis. This is computationally demanding and can be challenging if Alice's variance is too high. A recent paper by Denys *et al.* [241] provides an analytical lower bound on the asymptotic secret key rate for CV-QKD with arbitrary modulation schemes. Extending this to include Bob's post-selection could bypass the need for density matrices, making the security analysis less time consuming. In this work, we restrict Eve to Gaussian attacks. However, the optimal eavesdropping strategy in the presence of non-Gaussian post-selection remains an open question. Future studies should consider whether Eve could perform a non-Gaussian attack to compromise the key.

Our protocol could potentially be applied to CV-QKD protocols with discrete modulation (DM CV-QKD) [111,115,117], which utilise a constellation of modulated coherent states. In particular, Bob's non-Gaussian post-selection could enable dynamic switching between different types of DM CV-QKD protocols by selectively combining states from the constellation of modulated coherent states. While Bob's post-selection filter is similar in shape to those used in the DM CV-QKD protocol proposed by Kanitschar and Pacher [242], which demonstrated switching between formats like 8PSK and QPSK, our approach differs in that Alice sends Gaussian-modulated states. This allows Bob to emulate a wider range of modulation formats (e.g., BPSK, QPSK, or multiring) through flexible filter design, enabling more general DM or GM CV-QKD switching.

Chapter 6

Photon-Number Encoded Measurement-Device-Independent QKD Protocol

Decoherence poses a significant challenge to QKD over large distances. In the previous chapter, we examined the use of post-selection, a probabilistic technique, to enhance the key rates of QKD in direct communication between Alice and Bob. While this approach offers improvements, it cannot surpass the capacity of the repeaterless channel outlined in Sec. 4.5.2 due to the inherent probability of success of the protocol as well as the overall losses in the quantum channel. However, there are alternative approaches with the potential to overcome this bound.

As mentioned in Sec. 4.6, one of the proposed solutions is to use quantum repeaters, which divide the total distance between the users into smaller segments to minimise the effects of the losses in the channel. In this chapter, we introduce a repeater-like protocol which uses high-dimensional states prepared by two distant trusted parties and a more efficient entanglement swapping measurement at the repeater station. As this protocol requires Fock-number states (introduced in Sec. 2.3.1) which are hard to implement, we present an experimentally feasible protocol that can be implemented with current technology. We show that our protocol outperforms the existing measurement-device-independent and twin-field QKD (TF-QKD) protocols by achieving better key rates in general and higher transmission distance in total when experimental imperfections are considered. It also surpasses the fundamental limit of the repeaterless bound mentioned in Sec. 4.5.2 at a much shorter transmission distance in comparison to the existing TF-QKD protocols.

This research has been published in
Surpassing the Repeaterless Bound with a Photon-Number Encoded Measurement-Device-Independent Quantum Key Distribution Protocol
Ö. Erkılıç, L.O. Conlon, B. Shajilal, S. Kish, S. Tserkis, Y.S. Kim, P.K. Lam, S.M. Assad
npj Quantum Information **9**, 29 (2023).

6.1 Introduction

As discussed in Chapter 4, Sec. 4.6, quantum repeaters are commonly classified into three generations based on the techniques they employ to overcome loss and noise. The first-generation of quantum repeaters relies on entanglement swapping and purification using two-way classical communication [157, 243]. First-generation quantum repeaters [137, 145, 146] begin by distributing entangled states between neighbouring nodes. At each link (e.g., between nodes 1–2 and 2–3), entanglement purification is applied to multiple entangled pairs, where one pair is sacrificed to increase the fidelity of the other. During entanglement purification, both nodes (e.g., node 1 and node 2) perform local operations and share their measurement outcomes via two-way classical communication; if their results match, the corresponding entangled state is kept, otherwise it is discarded [137, 150–152]. Once high-fidelity entangled pairs are established across adjacent links, entanglement swapping is performed at intermediate nodes (e.g., node 2), enabling the creation of entanglement between non-adjacent nodes (e.g., nodes 1 and 3). This process is repeated over multiple segments to extend entanglement across longer distances. The entanglement swapping operation depends on how the entangled states are generated. In photonic implementations common to quantum communications, entangled states are typically encoded in photon pairs, often Bell states. At the intermediate node (e.g., node 2), one photon from each neighbouring Bell pair is interfered on a 50:50 beamsplitter, and a joint measurement, commonly referred to as a Bell-state measurement, is performed [145, 244]. Successful detection events herald the establishment of entanglement between the distant nodes (e.g., nodes 1 and 3), even though those photons never directly interacted. This procedure forms the backbone of repeater-based long-distance quantum communications.

Second-generation quantum repeaters [245–248] build upon the first generation by introducing quantum error correction (QEC) [160] to address operational errors, while still relying on probabilistic methods such as heralded entanglement generation (HEG) and entanglement purification to combat photon loss. In HEG, two nodes (e.g., node 1 and node 3) send photons to a central station (e.g., node 2), where a joint measurement is performed. If the measurement is successful, a heralding signal is sent back to both nodes, confirming the presence of entanglement across the link, this step is the same as entanglement swapping. This step requires two-way classical communication to coordinate and confirm the success of entanglement generation before moving forward. Once entanglement is established across neighboring links, QEC-based techniques, such as teleportation-based nonlocal CNOT gates [245, 249], are used to create encoded Bell pairs between the nodes. These operations mitigate gate errors, measurement imperfections, and other operational noise in a deterministic manner. Unlike purification, QEC does not discard failed trials but instead

actively corrects errors within an encoded logical qubit. However, since the initial entanglement generation is still probabilistic, two-way signaling remains necessary to confirm successful events before applying QEC operations. This hybrid approach allows second-generation repeaters to improve fidelity and extend entanglement across longer distances more efficiently than the first generation.

Third-generation quantum repeaters [250–252] take a fundamentally different approach by relying entirely on deterministic error correction techniques such as QEC codes [35, 253–265], to address both photon loss and operational errors. In this model, quantum information is not encoded in individual qubits but rather in logical qubits which are encoded across multiple physical qubits using QEC codes. These physical qubits collectively form a redundancy-protected block that can be transmitted through a lossy channel. If the loss and error rates remain below a certain threshold, the logical qubit can be recovered from the received block without the need for classical feedback or post-selection. This makes third-generation repeaters inherently one-way, enabling significantly higher communication rates compared to earlier generations. The use of QEC not only removes the reliance on entanglement swapping or purification but also allows for continuous and fault-tolerant quantum communication across long distances.

Quantum repeaters typically require the use of quantum memories [146, 266–268]. In the context of quantum communications, the most relevant photon-compatible quantum memories are either rare-earth-ion-doped crystals (REIDCs) or cold atomic ensembles, typically using Rubidium-87 [269] or Caesium-133 atoms [270, 271] trapped in magneto-optical traps [268]. Among these, REIDCs currently hold the record for the longest storage times, with storage of optical quantum states demonstrated for up to one hour [272]. Although the efficiency at one hour is not explicitly reported, the total memory efficiency for a 5-minute storage time was measured to be below 1%. A more recent demonstration at the single-photon level achieved a storage time of one second with an efficiency of 12.7% [273], while the highest efficiency reported for the REIDCs remains as 69% for a storage time of 1.3 μs [274]. Despite their long coherence times and telecommunication compatibility, REIDCs often suffer from low overall efficiencies [272, 273, 275–277]. In contrast, cold-atom quantum memories currently offer the highest efficiencies, albeit with shorter storage times [269, 271]. For instance, an efficiency of 87% was achieved using cold Rubidium atoms for short storage durations [269], while 50% efficiency was maintained for storage times up to 0.6 ms. Similarly, cold Caesium atoms have demonstrated 85% efficiency at the single-photon level [270], with the highest reported efficiency reaching 92% for storage times on the order of microseconds [271]. Despite these impressive efficiencies, cold-atom memories operate outside of telecommunication wavelengths. As a result, frequency conversion is required to interface with standard communication infrastructure, which introduces addi-

tional losses and limits the practical performance of quantum repeaters [278, 279].

While quantum repeaters are essential for long-distance quantum networks, their practical implementation remains challenging due to limitations in current quantum memory technologies. As a result, alternative approaches that circumvent the need for quantum memories have gained significant attention. Measurement-device-independent QKD (MDI-QKD) protocols are a type of repeater-like protocols in which the secret keys are established via the measurement of an untrusted third party [280, 281]. These protocols are called 'measurement-device-independent' as Alice and Bob do not perform a measurement in their stations, but the measurement is performed by an untrusted party, called Charlie. These protocols have been explored experimentally in Refs. [281–286]. Twin-field QKD (TF-QKD) [287] is a DV based MDI protocol which utilises weak identical coherent states sent by both Alice and Bob to Charlie, who performs entanglement swapping via a probabilistic photon detection measurement. The TF-QKD protocol is the first repeater protocol without a quantum memory that is able to surpass the PLOB bound [210, 287–292] as it scales proportionally to the single-repeater bound [94]. CV based MDI (CV-MDI) QKD protocols work in a similar fashion where Alice and Bob both send a distribution of either coherent or squeezed states to Charlie, where he performs a heterodyne measurement [281, 293, 294]. In order to achieve a positive key rate in these CV-MDI protocols, the relay is positioned very close to Alice resulting in a very asymmetric set-up. As the relay is not placed right in the middle between Alice and Bob, the protocols scale like the repeaterless bound instead of the single-repeater bound [193]. Hence, these protocols always sit below the PLOB bound.

In this chapter, we present a photon-number encoded MDI repeater protocol that surpasses the PLOB bound without the use of quantum memories through an entanglement swapping measurement. Unlike the TF-QKD protocol, the entanglement swapping is obtained by a coherent total photon number measurement performed by Charlie who measures the total number of photons coming from Alice and Bob without knowing the individual contributions. Even though the photon-number encoded states are vulnerable to losses, we show that in the short distance regime, the secret key rates are much higher than the ones of the single-photon encoded states. We also propose an experimentally feasible protocol using single-photons as these high dimensional states reduce down to the single-photon level over large distances. This protocol performs better than the existing MDI and TF-QKD protocols as it attains higher key rates for the same transmission distances.

6.2 The Protocol

First, we introduce our MDI protocol illustrated in Fig. 6.1, providing the details of the states that Alice and Bob use for key generation and estimating Eve's information followed

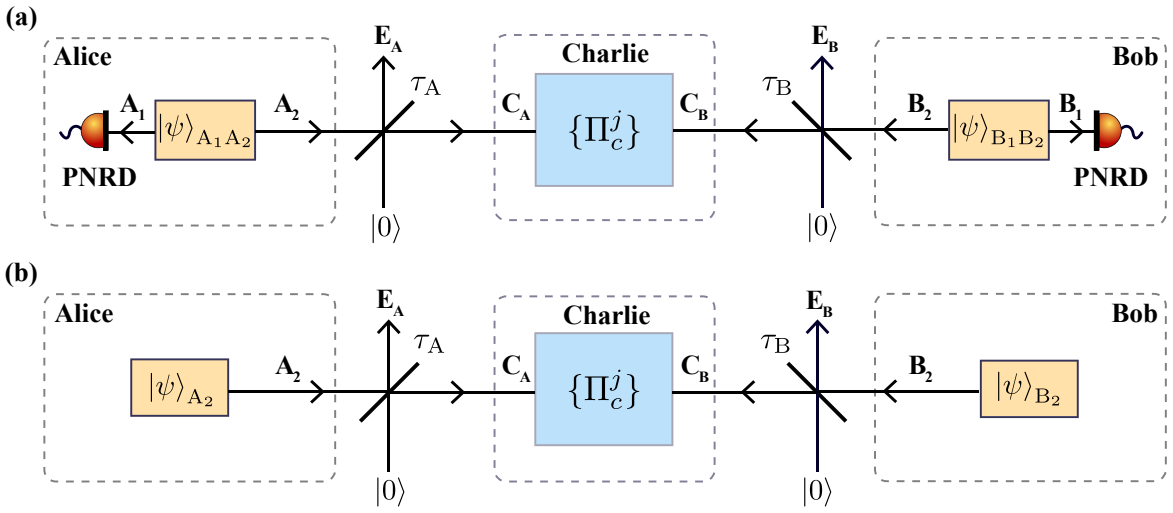

Figure 6.1: Equivalent representations of the protocol. (a) Entanglement-based scheme where both Alice and Bob send optimised states with $n_{\max} = 7$ to Charlie while keeping one arm of their states to themselves denoted as modes A_1 and B_1, respectively, and measure the number of photons using photon-number resolving detectors (PNRDs). Charlie interferes modes A_2 and B_2 coming from Alice and Bob and performs a coherent total photon number measurement. **(b)** Prepare-and-measure scheme where Alice and Bob send single-mode states to Charlie where they encode the key information on the single mode Fock state one at a time. Charlie then performs a total photon number measurement in his station on the modes that Alice and Bob send.

by Charlie's entanglement swapping measurement. We then derive the asymptotic key rate formula for the computation of the secret key rate. Finally, we present the results of the high-dimensional protocol followed by the experimentally feasible version of the MDI protocol using single-photons.

6.2.1 Alice and Bob's States for Generating a Key

Let us assume that both Alice and Bob generate two-mode entangled states in their stations where they keep one arm of the entangled states to themselves and send the other to Charlie. Charlie then performs a joint entanglement swapping measurement on the states that Alice and Bob send. This entangled two-mode state in Fock basis is expressed as

$$|\Psi\rangle_{A_1A_2} = \frac{1}{\sqrt{N}}\sqrt{1-\gamma^2}\sum_{n=0}^{n_{\max}}\gamma^n\,|nn\rangle_{A_1A_2}\,, \tag{6.1}$$

where $\gamma \in [0,1)$ is the squeezing parameter and N is the normalisation coefficient given by $\sum_{n=0}^{n_{\max}}(1-\gamma^2)\gamma^{2n}$. $n_{\max}$ is the maximum number of photons that Alice and Bob send individually where each party encodes the key information on the n-photon Fock states denoted as $|n\rangle$. Note that a TMSV state shown in Eq. 2.51 is retrieved when $n_{\max} \to \infty$ [74].

Here, we use the entanglement-based version, shown in Fig. 6.1(a), for the security anal-

ysis of the prepare-and-measure method, shown in Fig. 6.1(b). We express Alice's and Bob's states as follows

$$|\Psi\rangle_{\mathrm{A_1A_2}} = \sum_{n=0}^{n_{\max}} \sqrt{a_n}\,|nn\rangle_{\mathrm{A_1A_2}}\,, \tag{6.2}$$

$$|\Psi\rangle_{\mathrm{B_1B_2}} = \sum_{n=0}^{n_{\max}} \sqrt{b_n}\,|nn\rangle_{\mathrm{B_1B_2}}\,, \tag{6.3}$$

where $\sum_{n=0}^{n_{\max}} a_n = 1$ and $\sum_{n=0}^{n_{\max}} b_n = 1$. Here, a_n and b_n represent real coefficients of each Fock-number state $|nn\rangle$ for Alice and Bob, respectively. These coefficients are the same for both Alice and Bob and optimised to achieve an optimal key rate explained in more detail in Sec. 6.2.4.

In the entanglement-based scheme, Alice and Bob keep one arm of the entangled states to measure the number of photons using a photon-number resolving detector (PNRD) to establish a key while sending the other arm to Charlie. Charlie performs a coherent total photon number measurement on the incoming modes from Alice and Bob, and announces the outcome of his measurement (described in detail in Sec. 6.2.2). Alice and Bob's measurement in their own stations is represented as

$$\Pi_n = |n\rangle\langle n|\,, \tag{6.4}$$

where n denotes the number of photons being measured. In the prepare-and-measure scheme, this corresponds to preparing the Fock state $|n\rangle$ with probability a_n or b_n for Alice and Bob, respectively. The states in the prepare-and-measure scheme can be engineered experimentally with several different methods such as conditional teleportation [295], coherent displacements and photon subtraction [296], and repeated parametric-down conversion [297]. Alternatively, these states can be created by extending the work presented in Ref. [298] to higher photon levels where spontaneous parametric down-conversion (SPDC) generates entangled signal and idler photons, and conditional photon-number-resolving detection on the idler channel heralds the preparation of Fock states in the signal channel.

6.2.2 Charlie's Measurement

The states are sent to Charlie via a channel with a total transmissivity of $\tau \in [0, 1]$, which is split into smaller channels between Alice and Charlie and Charlie and Bob represented as τ_{A} and τ_{B}, respectively. Single-repeater protocols can be benchmarked based on the PLOB bound, which is given by $-\log_2(1-\tau)$ [93, 94]. In order to surpass this bound, the protocol needs to scale like the single-repeater bound [94], which is expressed as $-\log_2(1-\sqrt{\tau})$ (refer to Eq. (4.44) for a more generalised formula for N repeaters). This requires Charlie to be positioned in the middle of Alice and Bob such that the key-rate scales with the square root

of the transmission probability, $O(\sqrt{\tau})$. In this protocol, Charlie performs a collective photon number measurement on the incoming modes from Alice, A_2, and Bob, B_2. If Alice and Bob send a maximum of n photons each, denoted as $n_{\max}$, Charlie can measure from 0 to $2n_{\max}$ photons. Charlie's measurement can be realised by projecting the modes A_2 and B_2 onto the following states [299–301]

$$|\phi_c^j\rangle = \sum_{n=0}^{c} \frac{\omega^{nj}\,|n\rangle|c-n\rangle}{\sqrt{c+1}}, \tag{6.5}$$

where $c \in \{0, 1, \cdots, 2n_{\max}\}$ represents the total number of photons Charlie receives from the two modes, and $j \in \{0, 1, \cdots, c\}$ denotes the different states in the c-photon subspace states while ω is given by $\omega = \mathrm{e}^{\frac{2\pi\mathrm{i}}{c+1}}$.

For example, when $c = 2$, Charlie's three possible outcomes are

$$|\phi_2^0\rangle = \frac{1}{\sqrt{3}}(|02\rangle + |11\rangle + |20\rangle), \tag{6.6}$$

$$|\phi_2^1\rangle = \frac{1}{\sqrt{3}}(|02\rangle + \mathrm{e}^{\frac{2\pi\mathrm{i}}{3}}\,|11\rangle + \mathrm{e}^{-\frac{2\pi\mathrm{i}}{3}}\,|20\rangle), \tag{6.7}$$

$$|\phi_2^2\rangle = \frac{1}{\sqrt{3}}(|02\rangle + \mathrm{e}^{-\frac{2\pi\mathrm{i}}{3}}\,|11\rangle + \mathrm{e}^{\frac{2\pi\mathrm{i}}{3}}\,|20\rangle). \tag{6.8}$$

These measurements are designed such that even though Charlie knows the total number of photons between Alice and Bob, he does not know the number of photons in each mode separately.

The outcomes of Charlie's measurement form a valid positive operator value measurement (POVM) for a given outcome

$$\Pi_c^j = \left|\phi_c^j\right\rangle\!\left\langle\phi_c^j\right|, \tag{6.9}$$

with all the possible outcomes satisfying the identity resolution with $c \in \{0, 1, \cdots, 2n_{\max}\}$ and $j \in \{0, 1, \cdots, c\}$, i.e.,

$$\sum_{c=0}^{2n_{\max}} \sum_{j=0}^{c} \Pi_c^j = \mathbb{1}. \tag{6.10}$$

The measurement performed by Charlie establishes correlations between Alice and Bob. In the lossless channel, when Charlie detects two photons with his POVM element $|\phi_2^0\rangle$, Alice and Bob's state becomes $|\psi\rangle_{\mathrm{A_1B_1}|_{c=2}^{j=0}} = \sqrt{a_0 a_2}\,|02\rangle + a_1\,|11\rangle + \sqrt{a_2 a_0}\,|20\rangle$. Therefore, Charlie swaps the entanglement between Alice and Bob via the measurement he performs, similar to many MDI protocols [280, 287].

6.2.3 Alice and Bob's Check States for Security

A possible security issue is that Charlie can potentially lie to Alice and Bob about his measurement outcome, as he can perform separable measurements on Alice and Bob's modes individually or announce a different photon number from the one he actually measured. When the latter occurs, Alice and Bob can tell that Charlie is not telling the truth as the probabilities of measuring different number of photons are not equal. However, when the former happens, Alice and Bob cannot distinguish whether Charlie is performing a total photon number measurement or a separable measurement on the two modes. Even though the separable measurement does not yield an entangled state between Alice and Bob, it still establishes classical correlations between the parties. The probability of Charlie measuring a given number of photons when he performs a separable measurement ends up being the same as his joint measurement described in Sec. 6.2.2.

We address this security issue by Alice and Bob randomly switching from their key states and sending some check states to Charlie to detect any abnormalities in the system. One of the possible check states they send consists of a superposition of the photon number states, and are analogous to the original DV diagonal states in the following form

$$|+\rangle = \sum_{n=0}^{n_{\max}} \sqrt{\epsilon_n}\,|n\rangle\,, \tag{6.11}$$

where ϵ_n represents the coefficients a_n and b_n in Eqs. (6.2) and (6.3) for Alice and Bob, respectively.

The untrusted party, Charlie, is required to announce the total number of photons he measured as well as the outcome index (c, j). Table 6.1 shows Charlie's probability of measuring $c = 2$ photons as Alice and Bob send a mixture of key states and check states. Whenever both parties send $|{+}{+}\rangle_{\mathrm{AB}}$, the probability of Charlie measuring $c = 2$ photons is different for the non-separable and separable measurements. This is due to the nature of Charlie's POVM. For $c = 2$, Charlie has three different outcomes in this set labelled as $|\phi_2^0\rangle$, $|\phi_2^1\rangle$, and $|\phi_2^2\rangle$. If Alice and Bob send $|{+}{+}\rangle_{\mathrm{AB}}$, the probability of measuring $|\phi_2^0\rangle$ is $1/3$ whereas the other two outcomes return 0. In the case of separable measurements, the probability of measuring a two-photon event is equal, allowing Alice and Bob to determine whether Charlie is being dishonest or not.

The separable measurement is not the only possible measurement that Charlie can make. Ideally, Alice and Bob should not rely on Charlie's announcement of his measurement basis to determine if Charlie was being reliable or estimate how much information is leaked to another malicious party, called Eve. For security purposes, it is essential to utilise two or more non-orthogonal bases in QKD. For example, in BB84 [19] and the six-state protocol [302],

Table 6.1: Charlie's measurement probability for both non-separable and separable measurements for $c = 2$. Alice and Bob send a combination of their check states, $(+)$, $|+\rangle = \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle)$, and key states, (K), $\rho_{A_2} = \frac{1}{3}(|0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2|)$, in the prepare-and-measure representation with $n_{\max} = 2$ photons.

	Non-separable			**Separable**		
AB	$\mathbf{\Pi_2^0}$	$\mathbf{\Pi_2^1}$	$\mathbf{\Pi_2^2}$	**02**	**11**	**20**
KK	1/9	1/9	1/9	1/9	1/9	1/9
$K+$	1/9	1/9	1/9	1/9	1/9	1/9
$+K$	1/9	1/9	1/9	1/9	1/9	1/9
$++$	1/3	0	0	1/9	1/9	1/9

Alice sends states in two and three different orthogonal bases to Bob, respectively. By calculating the bit-error rates in these bases, Alice and Bob can estimate Eve's information. However, these protocols use only the probabilities of the matched measurement outcomes, which overestimates Eve's information resulting in a lower key rate [303]. Refs. [303, 304] showed that full tomography of the quantum state between Alice and Bob can enhance the secret key rate due to bounding Eve's information more accurately. Instead of using the statistics of the matched bases only, Alice and Bob can estimate their joint state from both the matched and unmatched bases. This joint state then can be used to calculate the Holevo bound on Eve's information.

Our protocol requires a similar approach to the protocols discussed above [303, 304], where Alice and Bob measure their joint state in mutually unbiased bases to perform a full tomography of their joint state in the entanglement-based scheme. Two bases $\{|e_i\rangle\}_{i=0}^{m-1}$ and $\{|h_i\rangle\}_{i=0}^{m-1}$ are called mutually unbiased when $|\langle e_i|h_j\rangle|^2 = 1/m$ for any i and j [305], where m is the dimension of the Hilbert space. If the dimension of the Hilbert space, m, is a power of a prime number, there exists $m+1$ mutually unbiased bases which form a complete set [306]. In Appendix B.1, we show how to estimate Eve's information by reconstructing Alice and Bob's joint state through full tomography when Alice and Bob send single-photon states, i.e., $n_{\max} = 1$. In the entanglement-based scheme, Alice and Bob measure the modes they keep in their stations using the eigenvectors of the X, Y and Z bases which are expressed as

$$|\pm x\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}, \tag{6.12a}$$

$$|\pm y\rangle = \frac{|0\rangle \pm i\,|1\rangle}{\sqrt{2}}, \tag{6.12b}$$

$$|+z\rangle = |0\rangle\,,\ |-z\rangle = |1\rangle\,. \tag{6.12c}$$

Note that these equations are equivalent to Eqs. (2.3), (2.5a), and (2.5b). These bases form a complete set of mutually unbiased bases for $m = 2$. In the equivalent prepare-

and-measure scheme, Alice and Bob's measurement on the two mode entangled states, $|\Psi\rangle_{A_1A_2} = \sqrt{a_0}\,|00\rangle + \sqrt{a_1}\,|11\rangle$ and $|\Psi\rangle_{B_1B_2} = \sqrt{b_0}\,|00\rangle + \sqrt{b_1}\,|11\rangle$ in the Z basis corresponds to them preparing the following states

$$|\psi_{+z}\rangle = |0\rangle\,, \tag{6.13a}$$

$$|\psi_{-z}\rangle = |1\rangle\,, \tag{6.13b}$$

with probability a_0 and b_0, and a_1 and b_1, respectively. Their measurement in the X basis is equivalent to them preparing the following states with equal probability

$$|\psi_{\pm x}\rangle = \sqrt{\epsilon_0}\,|0\rangle \pm \sqrt{\epsilon_1}\,|1\rangle\,, \tag{6.14}$$

i.e., they prepare $|\psi_{+x}\rangle$ and $|\psi_{-x}\rangle$ with a probability of 0.5, where ϵ_0 and ϵ_1 represent the coefficients a_0 and b_0, and a_1 and b_1, respectively. Similarly, their measurement in the Y bases corresponds to them preparing the following states with equal probability

$$|\psi_{\pm y}\rangle = \sqrt{\epsilon_0}\,|0\rangle \mp \mathrm{i}\sqrt{\epsilon_1}\,|1\rangle\,. \tag{6.15}$$

We present the detailed results of this protocol in Sec. 6.3.2.

When Alice and Bob wish to encode the key onto the higher dimensional states, i.e., $n_{\text{max}} > 1$, the number of check states they need to send increases. However, determining the existence of a complete set of mutually unbiased bases in an arbitrary dimensional Hilbert space is still an open problem in quantum information [307]. In this protocol, if Alice and Bob send states with n_{max} photons with a dimension of $m = n_{\text{max}} + 1$, they need to send check states using all the eigenvectors of $m + 1$ mutually unbiased bases to estimate Eve's Holevo bound provided that m is a power of a prime number. These check states can be determined by following the method discussed in Ref. [306]. They can also be implemented experimentally using the methods discussed in Refs. [295–297] and scaling the experiment performed by Bimbard et al. [298] from two-photon level to higher dimensions similar to the key states in the prepare-and-measure scheme. We show the key rates of these higher dimensional states later in detail in Sec. 6.3.1 with $n_{\text{max}} = 7$ photons.

6.2.4 Calculation of the Secret Key Rate

In the entanglement-based protocol, the global state before Charlie's measurement is a four-mode state. The dimension to simulate this protocol scales as m^4. Therefore, the coefficients of Alice and Bob's states in Eqs. (6.2) and (6.3) are optimised by considering a classical protocol where Eve and Charlie perform a photon number measurement on their modes. We

optimise the difference between the classical mutual information between Alice and Bob, and, Eve and Alice. We call this protocol the 'classical protocol' and an explicit method for the implementation of this protocol is shown in Appendix B.2. The reason for doing this is to avoid having to optimise a high dimensional four mode joint state with a total dimension of m^4. However, when computing the secret key rates, we do not assume any type of attacks for Eve and calculate Eve's Holevo bound instead and Charlie performs his collective photon number measurement. It is also important to note that the optimisation problem is not convex for the high-dimensional states and the solution provided for the coefficients a_n and b_n in this paper is one possible solution.

The states that Alice and Bob prepare were previously shown in Eqs. (6.2) and (6.3), respectively. They send these states through a pure-loss channel with a transmissivity τ_{A} and τ_{B} for the channel between Alice and Charlie and Charlie and Bob, respectively. The pure-loss channel is modelled with a beamsplitter with a transmissivity τ, where the beamsplitter mixes the input mode with the vacuum as shown in Fig. 4.3. Here, τ can be written as a function of the fibre distance, d, with a loss of 0.2 dB per km with $\tau = 10^{-0.02d}$.

In this protocol, we assume that Eve has full access to the channel between Alice and Charlie and Charlie and Bob including Charlie's measurements. Eve is modelled as mixing vacuum with the incoming modes, effectively simulating a pure-loss channel where photons are lost to the environment, losses that Eve is assumed to collect. Thus, we can express the state between Alice and Charlie and Charlie and Bob after Eve's attack as

$$\rho_{\mathrm{A}_1\mathrm{C}_\mathrm{A}} = \mathrm{Tr}_3\big[\{\mathbb{1}_m \otimes B(\tau_{\mathrm{A}})\}\{\rho_{\mathrm{A}_1\mathrm{A}_2} \otimes |0\rangle\langle 0|\}\{\mathbb{1}_m \otimes B(\tau_{\mathrm{A}})\}^\dagger\big], \tag{6.16a}$$

$$\rho_{\mathrm{C}_\mathrm{B}\mathrm{B}_1} = \mathrm{Tr}_1\big[\{B(\tau_{\mathrm{B}}) \otimes \mathbb{1}_m\}\{|0\rangle\langle 0| \otimes \rho_{\mathrm{B}_2\mathrm{B}_1}\}\{B(\tau_{\mathrm{B}}) \otimes \mathbb{1}_m\}^\dagger\big], \tag{6.16b}$$

where $\mathrm{Tr}_i[\rho]$ stands for tracing out the i-th mode of the state ρ.

After Charlie's measurement and tracing out his modes, the subnormalised state between Alice and Bob becomes

$$\tilde{\rho}_{\mathrm{AB}|_c^j} = \mathrm{Tr}_{23}\big[\big(\mathbb{1}_m \otimes \Pi_c^j \otimes \mathbb{1}_m\big)\big(\rho_{\mathrm{A}_1\mathrm{C}_\mathrm{A}} \otimes \rho_{\mathrm{C}_\mathrm{B}\mathrm{B}_1}\big)\big(\mathbb{1}_m \otimes \Pi_c^j \otimes \mathbb{1}_m\big)^\dagger\big]. \tag{6.17}$$

We can calculate Charlie's probability of obtaining outcomes (c, j) from the following expression

$$P_{_c^j} = \mathrm{Tr}\big[\tilde{\rho}_{\mathrm{AB}|_c^j}\big]. \tag{6.18}$$

Normalising Alice and Bob's joint state by Charlie's probability of measuring c photons

for his measurement j gives us the final conditional state between them as

$$\rho_{\mathrm{AB}|_c^j} = \frac{\tilde{\rho}_{\mathrm{AB}|_c^j}}{P_c^j}. \tag{6.19}$$

However, for the key states that Alice and Bob send, the probability of Charlie measuring c photons, Alice and Bob's conditional mutual information and Eve's conditional information do not change for each j ranging from 0 to c. As such, there is no need to calculate Alice and Bob's conditional joint state for each value of j. Therefore, we omit j from the following equations and set it to zero.

We then calculate Charlie's total probability of measuring c photons from

$$P_c = \sum_{j=0}^{c} \mathrm{Tr}\left[\tilde{\rho}_{\mathrm{AB}|_c^j}\right] = (c+1)\mathrm{Tr}\left[\tilde{\rho}_{\mathrm{AB}|_c^{j=0}}\right], \tag{6.20}$$

since there are $c+1$ POVM outcomes with a total photon number c.

In order to calculate Alice and Bob's mutual information, we first generate Alice and Bob's probability table as follows

$$P(n_a, n_b|c) = \langle n_a, n_b|\rho_{\mathrm{AB}|_c}|n_a, n_b\rangle\,, \tag{6.21}$$

where each term in Alice and Bob's mutual information is given by the conditional Shannon's entropy as expressed below

$$H(A|c) = -\sum_{n_a=0}^{n_{\max}} P(n_a|c)\log_2 P(n_a|c), \tag{6.22a}$$

$$H(B|c) = -\sum_{n_b=0}^{n_{\max}} P(n_b|c)\log_2 P(n_b|c), \tag{6.22b}$$

$$H(AB|c) = -\sum_{n_a=0}^{n_{\max}}\sum_{n_b=0}^{n_{\max}} P(n_a, n_b|c)\log_2 P(n_a, n_b|c). \tag{6.22c}$$

Using the equations above, we evaluate Alice and Bob's mutual information conditioned on Charlie's measurement outcome from $I_{AB|c} = H(A|c) + H(B|c) - H(AB|c)$.

Eve's information is calculated from Alice and Bob's conditional state after Bob's measurement outcome on this joint state using

$$I_{E|c} = S(\rho_{\mathrm{AB}|c}) - \sum_{b=0}^{n_{\max}} P_b S(\rho_{\mathrm{A}|cb}), \tag{6.23}$$

where Bob's POVM is shown in Eq. (6.4) in Sec. 6.2.1. b represents the number of photons

that Bob measures while P_b corresponds to Bob's probability of measuring b photons. The subnormalised state $\tilde{\rho}_{\mathrm{A}|cb}$ is obtained from

$$\tilde{\rho}_{\mathrm{A}|cb} = \mathrm{Tr}_2[(\mathbb{1}_m \otimes \Pi_b)\rho_{\mathrm{AB}|_c}(\mathbb{1}_m \otimes \Pi_b)^\dagger], \tag{6.24}$$

where Bob's probability of measuring b photons is given by

$$P_b = \mathrm{Tr}[\tilde{\rho}_{\mathrm{A}|cb}]. \tag{6.25}$$

Alice's subnormalised state conditioned on Bob's and Charlie's measurement outcomes, $\tilde{\rho}_{\mathrm{A}|cb}$ is then normalised by Bob's measurement probability by

$$\rho_{\mathrm{A}|cb} = \frac{\tilde{\rho}_{\mathrm{A}|cb}}{P_b}. \tag{6.26}$$

The asymptotic key rate of this protocol requires the combination of all the possible outcomes of Charlie's POVM since Alice and Bob are sending states with n photons each with a possibility of measuring 0 to $2n$ photons by Charlie. However, we discard events where Eve's conditional information is greater than Alice and Bob's conditional mutual information. For example, when a zero-photon event occurs, Eve gets more information than Alice and Bob due to all the photons being lost to Eve. As such we exclude the case when $c = 0$. Similarly, when Charlie measures $c = 2n_{\mathrm{max}}$ photons, the key rate conditioned on this measurement outcome is zero even though Eve's conditional information is zero. Therefore, the resulting asymptotic key rate can be expressed as

$$K = \sum_{c=0}^{2n_{\mathrm{max}}} P_c \mathrm{max}\left[0, I_{AB|c} - I_{E|c}\right]. \tag{6.27}$$

6.3 Results

6.3.1 The Results of the High-dimensional States

Our simulation results are shown in Fig. 6.2(a) for the pure-loss channel with 0.2dB loss per km. We compare our results with the existing MDI protocols such as the CV-MDI protocol from Pirandola et al. [281] and one of the best-performing TF-QKD protocols known as TF-QKD without phase post-selection (NPP-TF-QKD) from Cui et al. [308] and Lu et al. [309].

We first show the case where Alice and Bob send the states shown in Eq. (6.1) with a squeezing coefficient of $\gamma = 0.26$ for each distance with $n_{\mathrm{max}} = 7$ photons. The squeezing level of $\gamma = 0.26$ was determined based on the shortest distance that the protocol exceeds the

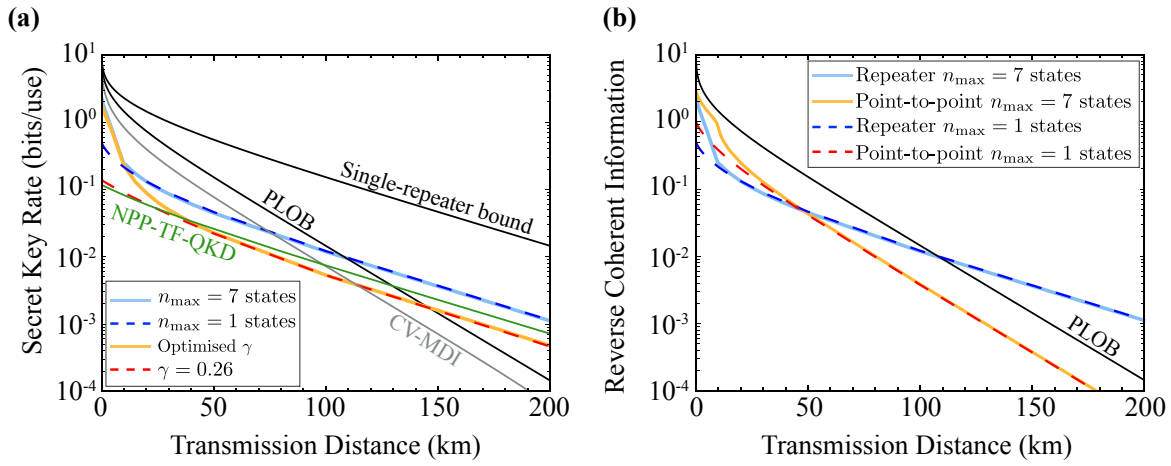

Figure 6.2: Simulation results of our repeater protocol for a pure-loss channel with a loss of 0.2 dB/km. (a) Solid orange and red dashed lines show the key rates of our protocol using the states shown in Eq. (6.1) with $n_{\max} = 7$ photons with optimised squeezing coefficients and a squeezing coefficient of $\gamma = 0.26$, respectively. Blue dashed line shows the results of the optimised states with $n_{\max} = 1$ photon given in Eqs. (6.2) and (6.3) and using Charlie's POVM with an outcome of 1 and 2 photons. The solid blue line shows our protocol using the optimised states with $n_{\max} = 7$ photons given in Eqs. (6.2) and (6.3). Black solid lines show the single-repeater and repeaterless bounds. Solid grey line represents the CV-MDI protocol [281] with a variance of 1000 and relay positioned at 0.01m away from Alice, while the solid green line shows the TF-QKD protocol with no phase post-selection (NPP-TF-QKD) [309] using optimised coherent states and infinite decoy states. **(b)** The comparison of the reverse coherent information of the optimised states with $n_{\max} = 7$ and $n_{\max} = 1$ photons in the form of Eqs. (6.2) and (6.3) in point-to-point communications between Alice and Bob and with a single-repeater. The faint blue and orange lines represent the RCI of the single-repeater and point-to-point communications of the optimised states with $n_{\max} = 7$ photons correspondingly, while the blue and red dashed lines show the RCI of the single-repeater and point-to-point communications of the optimised states with $n_{\max} = 1$ photon. The black solid line shows the reverse coherent information of an infinitely squeezed TMSV state denoted as PLOB.

PLOB bound (refer to Appendix B.4 Table B.3 for the details). With these states, the PLOB bound and the CV-MDI protocol are surpassed at 144 km and 114 km, respectively, while the protocol is performing worse than the TF-QKD protocol. We also demonstrate the key rates of the same states where the values of γ are optimised to give the maximum secret key rate at the corresponding distance. For distances greater than 50 km, there is not much difference compared to the states with $\gamma = 0.26$ and the PLOB bound is still surpassed at the same distance as the case of $\gamma = 0.26$. However, the key rates are now higher at short distances below 50 km. This indicates that in the short distance regime, the contribution of the higher order photons to the key rate is significant while at larger distances, the main contribution comes from the the first few photons of the state as the majority of the photons are lost to the environment at such distances. This can also be seen from the optimal squeezing level given in Table B.3 in Appendix B.4, which is higher for short distances and lower for larger

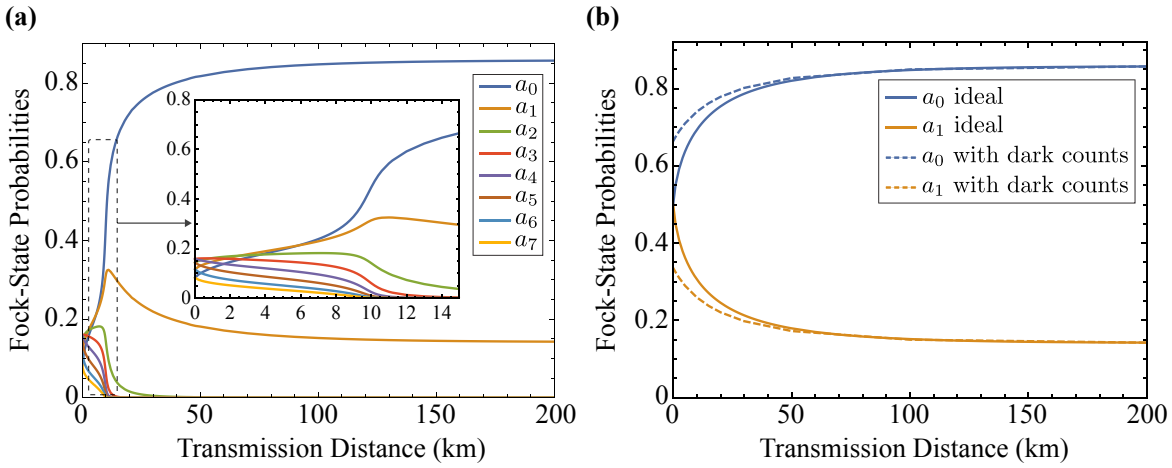

Figure 6.3: Simulation results of the optimised coefficients. (a) The optimised coefficients of the states shown in Eqs. (6.2) and (6.3) with $n_{\max} = 7$ photons, where the coefficients are explicitly shown in Table B.1 in Appendix B.4. **(b)** The optimised coefficients of the states shown in Eqs. (6.2) and (6.3) with $n_{\max} = 1$ photon (refer to Table B.2 given in Appendix. B.4 for the optimised coefficients for each distance).

distances.

When Alice and Bob send the optimised states shown in Eqs. (6.2) and (6.3), these states outperform the results of the states with optimised γ by surpassing the repeaterless bound and the CV-MDI protocol at 108 km and 75 km, respectively. These states also do considerably better than the TF-QKD protocol as the TF-QKD protocol exceeds the PLOB bound at only 130 km and its key rates are lower than our protocol at each distance. It is important to note that this result can also be achieved by using the optimised states with $n_{\max} = 1$ photon in the form of $\sqrt{a_0}\,|00\rangle + \sqrt{a_1}\,|11\rangle$ as shown in Fig. 6.2(a) since both states reach the PLOB bound at the same distance and the key-rates converge beyond 10 km. In Fig. 6.2(a), both high-dimensional and single-photons states have the same gradient, scaling like the single-repeater bound with $O(\sqrt{\tau})$. The probability of receiving n-photons in this case is given by $(\sqrt{\tau})^n$. Therefore, the main scaling of the key rates comes from the single-photon level, while the remaining photons help the key rate incrementally. As the loss gets higher, the probability of receiving higher photons drops. Therefore, beyond 10 km, we are only interested in 1 or 2 photons. This is further emphasised in Fig. 6.3(a) where we show the probability of sending each Fock-number state of the optimised states given in Eqs. (6.2) and (6.3) for each transmission distance. At short distances, the high-dimensional states have contribution from each photon number. It is important to note that at 0 km, the probability of sending each Fock-number state is not equal, despite the absence of loss. This is because when Charlie receives either 0 or 14 photons in total, the key rate drops to zero. In the former case, Eve obtains all the photons; in the latter, Charlie's announcement reveals

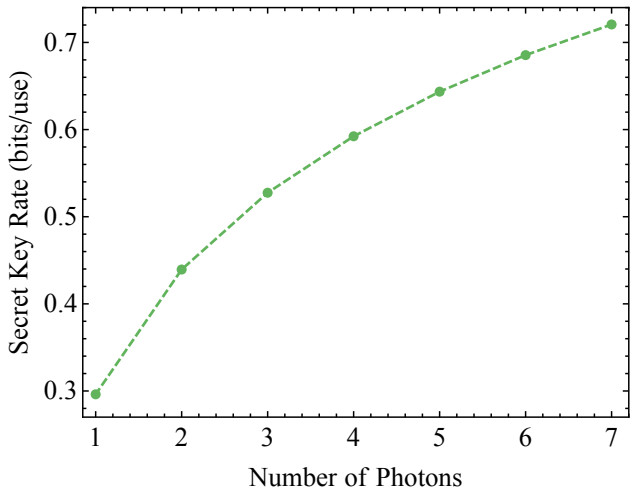

Figure 6.4: Simulation results of the secret key rate when the number of encoded photons varies from 1 to 7 photons at 5 km. The states are in the form of Eqs. (6.2) and (6.3) where the coefficients of each state are optimised.

that Alice and Bob must have sent 7 photons each, fully exposing their states. Since these outcomes are excluded from key generation, the optimiser reduces the weights of $|0\rangle$ and $|7\rangle$ resulting in a non-uniform probability distribution even at short distances. As the distance increases, the high-dimensional states reduce down to the single-photon level as the coefficients of the Fock states above one photon approach zero. The probabilities of sending zero and one photon, denoted as a_0 and a_1, of these high-dimensional states shown in Fig. 6.3(a) converge to the coefficients of the optimised states with $n_{\max} = 1$ photon shown in Fig. 6.3(b) beyond approximately 50 km. However, the main advantage of using the optimised states with $n_{\max} = 7$ is the ability of obtaining higher key rates at shorter distances. This is shown in Fig. 6.4, as the secret key rate increases when the number of encoded photons changes from 1 to 7 photons.

As the key rates of the optimised states with $n_{\max} = 7$ converge with the results of the states with optimised γ below 10 km and with the optimised states with $n_{\max} = 1$ photon, one can use the combination of the states with optimised γ and optimised states with $n_{\max} = 1$ photon beyond this distance to achieve the same results of the states given in Eqs. (6.2) and (6.3).

As mentioned previously, the maximum key rate achievable by QKD for the point-to-point and single-repeater communication is bounded by the PLOB and single-repeater bounds, respectively [93, 94]. These bounds are determined by the maximum amount of entanglement that a channel can sustain, also known as the entanglement flux, which coincides with reverse coherent information (RCI) of a maximally entangled TMSV state for the pure-loss channel [93, 126, 140]. The RCI is used to lower-bound the distillable entangle-

ment of a given channel [140] and is a measure of the transmission of quantum information. While the key rates above demonstrate that our protocol surpasses the PLOB bound and acts as a repeater, the secret key rate is a measure of the transmission of classical information. The key rates are also bounded by the amount of entanglement that Alice and Bob can distill. Therefore, we also compute the RCI of our quantum states to verify the distillable entanglement between Alice and Bob after Charlie's measurement using

$$\mathrm{RCI} = \sum_{c=0}^{2n_{\max}} P_c \max\left[0, S(\rho_{\mathrm{A}|c}) - S(\rho_{\mathrm{AB}|c})\right], \tag{6.28}$$

where $S(\rho_{\mathrm{AB}|c})$ and $S(\rho_{\mathrm{A}|c})$ are the von Neumann entropies of the joint state between Alice and Bob $\rho_{\mathrm{AB}|c}$ and Alice's state $\mathrm{Tr}_2[\rho_{\mathrm{AB}|c}]$, respectively.

In Fig. 6.2(b), we show the RCI of the optimised states with $n_{\max} = 7$ and $n_{\max} = 1$ when Alice and Bob perform point-to-point and single-repeater communications. We compare these results with the PLOB bound as it coincides with the RCI of a maximally entangled TMSV state in the pure-loss channel. Note that when Alice and Bob communicate directly using the optimised states with $n_{\max} = 7$, they cannot saturate the PLOB bound due to sending states with a limited number of photons. However, they can reach the PLOB bound if they send infinitely squeezed TMSV states with an infinite number of photons [118]. In Fig. 6.2(b), when Alice and Bob perform point-to-point communication, they can distill more entanglement at short distances. However, with the use of a repeater, they are able to distill more entanglement beyond 47 km and surpass the RCI of an infinitely squeezed TMSV state at 108 km. Note that they also surpass the PLOB bound at this distance when we calculate their secret key rate as shown in Fig. 6.2(a) and the key rates coincide with the reverse coherent information of Alice and Bob's conditional joint state on Charlie's measurement outcome. This indicates that after Charlie's measurement, Alice and Bob's PNRD measurement is optimal as Alice and Bob achieve the same key rates as the distillable entanglement of their joint state.

6.3.2 Realistic Implementation of the MDI Protocol with Single-Photon States

The experimental realisation of the higher dimensional optimised states and Charlie's measurement is quite challenging with state of the art technology. In this section, we present an experimentally feasible implementation of our protocol, shown in Fig. 6.5, by using single-photon states which can be performed with existing technology. Fig. 6.2(a) demonstrates that beyond 10 km, the single-photon states achieve the same key rates as the higher dimensional states and the high-dimensional states reduce down to the single-photon level as demonstrated in Fig. 6.3(a) and Fig. 6.3(b).

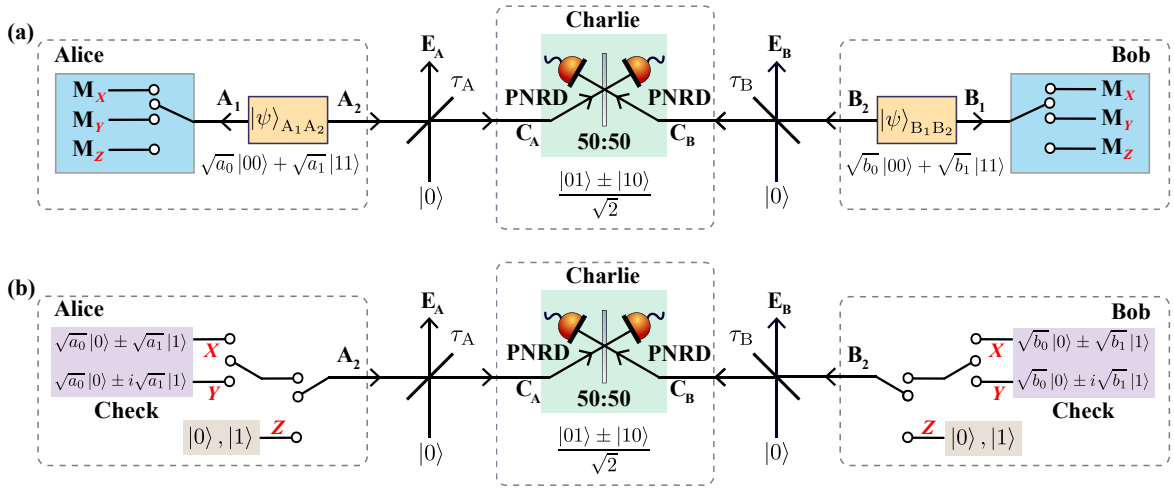

Figure 6.5: Equivalent representations of the protocol with single photons. **(a)** Entanglement-based scheme where both Alice and Bob send the optimised states in the form of $\sqrt{a_0}\,|00\rangle + \sqrt{a_1}\,|11\rangle$ and $\sqrt{b_0}\,|00\rangle + \sqrt{b_1}\,|11\rangle$ to Charlie while keeping one arm of their states to themselves denoted as modes A_1 and B_1. They perform a measurement in the X, Y and Z bases to compute the statistics of their matched and unmatched results. This measurement also projects the arm they sent to Charlie onto a single-mode state in the corresponding basis as shown in panel (b). Charlie interferes modes A_2 and B_2 coming from Alice and Bob, respectively, at a 50:50 beamsplitter and performs single-photon detection with PNRDs. A successful outcome occurs when Charlie's left (10 event) or right detector (01 event) registers a single click only. Alice and Bob ignore the instances of 02, 20 and 11 photon events. **(b)** Prepare-and-measure scheme where Alice and Bob send single-mode states to Charlie where they encode the key information in the Z basis. They send the states $|0\rangle$ and $|1\rangle$ with probabilities a_0, b_0 and a_1, b_1, respectively. They randomly switch to X and Y bases to send check states to estimate Eve's information (refer to Sec. 6.2.3 for the details of the check states). Charlie's measurement is the same as the one in the entanglement-based scheme shown in panel (a).

When Alice and Bob send single-photon states, Charlie can measure from 0 to 2 photons. However, as mentioned previously in Sec. 6.2.4, when Charlie measures 2 photons, the conditional secret key rate is zero as such the contribution to the key rate comes from only the single-photon detection events. This eliminates Charlie having to distinguish between $c = 2$ photon outcomes, i.e., $|\phi_2^0\rangle$, $|\phi_2^1\rangle$ and $|\phi_2^2\rangle$ and requires him to only distinguish between the single-photon outcomes. Therefore, we can simplify our protocol to Fig. 6.5, where Charlie interferes the single photons coming from Alice and Bob at a 50:50 beamsplitter and uses two photon-number resolving detectors up to the two-photon level. After Charlie's measurement, Alice and Bob can estimate their joint state to bound Eve's information using the statistics of their matched and unmatched data of X, Y and Z bases as mentioned in Sec. 6.2.4. This protocol is conceptually similar to Protocol 1 and Protocol 2 of Curty et al. [310]. One of the main differences is that our single-photon protocol uses PNRDs at Charlie's station which helps Alice and Bob to disregard any measurement that is a two-photon click (i.e. Charlie receives no clicks at one detector and two clicks on the other), resulting in

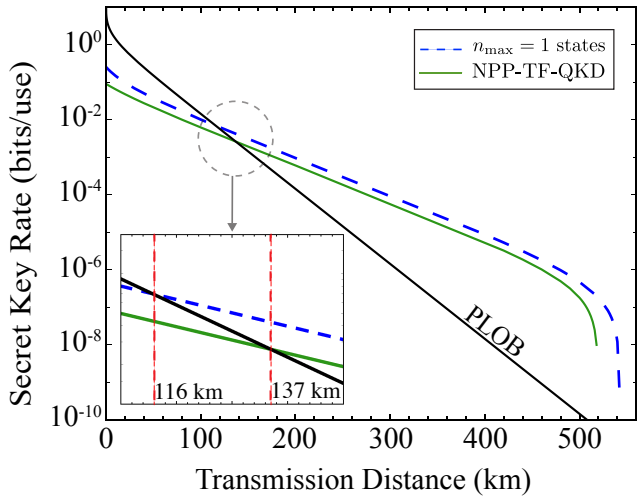

Figure 6.6: Simulation results of our repeater protocol using single-photon states with experimental parameters. The blue dashed line shows our protocol using the single-photon states in the form of $\sqrt{a_0}\,|00\rangle + \sqrt{a_1}\,|11\rangle$ and $\sqrt{b_0}\,|00\rangle + \sqrt{b_1}\,|11\rangle$ with optimised coefficients and perfect single-photon sources. The solid green line and black lines are the NPP-TF-QKD protocol [309] with infinite decoy states and the PLOB bound, respectively. We assume a dark count rate of 5×10^{-8} with a detector efficiency of 0.85 for both protocols.

a lower bit-error rate. Our protocol also estimates Eve's information more tightly as Alice and Bob perform a full tomography of their joint state using the eigenvectors of the X, Y and Z bases, whereas Ref. [310] only uses the measurement results of the X and Z bases. These two differences yield a higher key rate than the results of Ref. [310].

Additionally, we consider the detrimental effects of the detector inefficiency and dark counts to the key rates (see Appendix B.3 for the detector model). The single-photon states are optimised for a detector with an efficiency of 85% and a dark count rate of 5×10^{-8}, where the coefficients of the zero and single photons are shown in Table B.4 in Appendix B.4 and in Fig. 6.3(b). In a lossless channel, the probability of sending a single-photon initially is half. However, as the channel becomes more lossy, it is likely that the single-photon will be lost during transmission. When Charlie receives no photons, this corresponds to a large bit-error rate reducing the key rates. This is compensated by reducing the probability of sending single-photons to decrease the bit-error rates and increase the key rates [311]. With realistic dark count rates and detector efficiencies, our protocol using perfect single-photon sources surpasses the PLOB bound at 116 km while the NPP-TF-QKD with infinite decoy states surpasses at 137 km as shown in Fig. 6.6. The NPP-TF-QKD protocol drops to zero beyond 518 km whereas our protocol drops to zero beyond 542 km showing a 24 km advancement in the transmission distance.

To account for a more practical scenario, we simulate our protocol with imperfect single-photon sources and compare it with the NPP-TF-QKD protocol [309] with a finite number

of decoy states. When the single-photon sources used by Alice and Bob are heralded with imperfect detectors with a dark count rate of 5×10^{-8} and a detector efficiency of 0.85 for state preparation, the single-photon protocol achieves a total transmission distance of 480 km assuming 0.2 dB loss per km. When NPP-TF-QKD protocol [309] uses finite decoy states with two decoy modes with four intensities and the same dark count rates and detector efficiencies, the protocol achieves a total transmission distance of 470 km. Using a more realistic experimental set-up our protocol still performs better. However, as the heralding detectors used by Alice and Bob for the state preparation get more lossy, our protocol is likely to start performing worse than the TF-QKD protocols as these protocols use coherent states. Current superconducting nanowire single-photon detectors can achieve detector efficiencies up to 90% with dark count rates as low as 10^{-9} as demonstrated previously in Ref. [290].

The improvements made to the total transmission distance in our protocol are a result of several factors. Even though both the single-photon and NPP-TF-QKD [309] protocols use optimised states, our protocol has more freedom over optimising the coefficients of the single-photon state while the TF-QKD protocols need to ensure that the intensities of the coherent states are still weak enough while optimising the key rates. This is also one of the key differences between our protocol and the Sending-or-Not-Sending TF-QKD (SNS-TF-QKD) protocol [312], where Alice and Bob send weak coherent states and no states with a probability of ϵ and $1-\epsilon$, respectively. However, the probability of the single-photon detection is still determined by the intensity of the weak coherent states in the SNS-TF-QKD protocol whereas in this protocol, Alice and Bob send single-photon states with a probability of ϵ which determines the probability of detection at Charlie's detectors. Our protocol also has the ability to distinguish two-photon events occurring at a single detector at Charlie. For example, if Charlie receives no photons on one detector and two photons on the other, these events can be disregarded and do not contribute to bit-error rates. However, in TF-QKD protocols with single-photon detectors, this event would register as one click, causing an increase in the bit-error rate. Therefore, the use of PNRDs in Charlie's station improves the bit-error rates. Furthermore, our protocol can estimate Eve's information more accurately due to the use of the probabilities of the matched and unmatched bases. These are the main factors that distinguish our protocol from the existing MDI and TF-QKD protocols.

6.4 Discussion

In this chapter, we introduced an MDI protocol using higher dimensional states that surpasses the repeaterless bound without the need of quantum memories as it scales like the single-repeater bound. However, for large distances, the states required in this protocol reduce down to the single-photon level due to the losses in the channel. Based on this, we pro-

posed an experimentally feasible implementation of this protocol just using single-photons and photon-number resolving detectors which performs better than the existing protocols such as NPP-TF-QKD protocol [308, 309].

Furthermore, we investigated whether the single-repeater bound can be saturated with a simple protocol by using only single copies of the states sent by Alice and Bob and without collective measurements performed by Charlie. Our results show that unlike the repeaterless bound, this is probably not possible with single copies of the states and likely to require many copies of the states sent by Alice and Bob and collective measurements as previously shown by García-Patrón et al. [140] and a protocol proposed by Winnel et al. [144].

The results presented in this chapter refer to the asymptotic key rates, and the security of this protocol with finite-size effects needs to be considered in the future. In this protocol, there are no misalignment errors in the Z basis due to sending single-photons. However, the misalignment errors are likely to impact the statistics of the check states in the X and Y bases which can be investigated in future work. The feasibility of extending this protocol to a network of multiple users can also be studied. Additionally, it would be valuable to explore practical implementations of the required single-photon sources such as using SPDC or attenuated lasers, and evaluate their impact on key rates and error performance within this photon-number-based framework.

Note that there are two challenges in our protocol which are the implementation of the states that Alice and Bob prepare and Charlie's coherent total photon number measurement. Ref. [298] managed to implement the states we require for this protocol up to the two-photon level. We would like to motivate the community with a possible extension of the work presented in Ref. [298] to higher dimensions for state preparation and exploring ways to implement Charlie's measurement as they are likely to contribute to many areas in quantum information not only QKD, but also quantum metrology, entanglement swapping, entanglement distillation, optical quantum computing and error correction.

Chapter 7

Capacity-Achieving Entanglement Purification Protocol for Pauli Dephasing Channel

Quantum communication facilitates the secure transmission of information and the distribution of entanglement, but the rates at which these tasks can be achieved are fundamentally constrained by the capacities of quantum channels as explained previously in Sec. 4.5. Quantum repeaters typically enhance these rates by mitigating losses and noise, often by dividing the quantum channel into more manageable portions. In the previous chapter, we introduced a repeater-like protocol that surpassed the repeaterless capacity of the pure-loss channel by employing a more efficient entanglement swapping measurement at the repeater station. However, a simple entanglement swapping protocol via a central node is not effective against the Pauli dephasing channel due to the additional degradation introduced by Bell-state measurements. This highlights the importance of purifying distributed Bell states before performing entanglement swapping.

In this chapter, we introduce an entanglement purification protocol assisted by two-way classical communication that not only purifies the states but also achieves the channel capacities. Entanglement purification is a process by which two or more parties distill a smaller number of high-fidelity entangled states from a larger set of noisy or mixed entangled states using only local operations and classical communication (LOCC). Our protocol uses an iterative process involving CNOT gates and Hadamard basis measurements, progressively increasing the fidelity of Bell states with each iteration. This process ensures that the resulting Bell pairs are perfect in the limit of many recursive iterations, making them ideal for use in quantum repeaters and for correcting dephasing errors in quantum computers. The explicit circuit we propose is versatile and applicable to any number of Bell pairs, offering a practical solution for mitigating decoherence in quantum networks and distributed quantum computing.

This research has been submitted to IOP Quantum Science and Technology and is currently under review.

Capacity-Achieving Entanglement Purification Protocol for Pauli Dephasing Channel
Ö. Erkılıç, M.S. Winnel, A. Das, S. Kish, P.K. Lam, J. Zhao, S.M. Assad
arXiv:2411.14573 (2024).

7.1 Introduction

As outlined in Sec. 4.3.3, the Pauli dephasing channel primarily experiences decoherence due to phase flips [69]. This channel is considered distillable [93] because the upper bound on its capacity, known as the entanglement flux [93], is equal to the lower bound, the RCI [126, 140], as previously introduced in Sec. 4.5.1. The capacity of this channel can be achieved by Alice distributing maximally entangled Bell states to Bob, with Bob performing measurements in the Hadamard basis to maximise the secret key rate. As noted in the previous chapter, introducing a node to split the channel into two often helps surpass the direct communication capacity in other lossy channels [267, 287, 308, 312–314]. However, in the case of the dephasing channel, adding a node does not result in higher key rates compared to direct communication between Alice and Bob. For example, if Alice and Bob send maximally entangled Bell states to a quantum node, which then performs a Bell-state measurement to establish entanglement between them, the resulting RCI remains unchanged. This is true even though the effective decoherence before the entanglement swapping measurement is reduced. This outcome highlights the need for the state to be purified, either through entanglement purification or error correction, before the node performs the entanglement swapping measurement.

Entanglement purification [144, 150–153, 315–319] is used to concentrate the total entanglement of a large of number of noisy entangled states into a fewer number of states with higher purity using local operations and measurements by the parties sharing the states. Entanglement purification protocols can be classified into the following categories [320]:

- **Filtering protocols:** These protocols utilise a single copy of a mixed state and apply some local filtering measurements such as weak measurements to yield a state with better entanglement [321]. However, the achievable fidelity of the output state is limited by the probability of success and these protocols have limited capabilities for general mixed states [320].

- **Recurrence protocols:** These protocols operate on two copies of mixed states at a time by performing some local operations on both states and measuring one [150–152, 322]. This procedure is repeated until the desired fidelity is achieved. Even though these protocols can produce a maximally entangled pure state given enough iterations, the rates of these protocols cannot saturate the ultimate two-way capacities due to mea-

suring half of the states in each purification step.

- ***N*→*M* protocols:** These protocols use many copies of mixed states at a time where $N - M$ states out of N states are measured [323]. They are further classified into hashing and breeding protocols:

  - **Hashing protocols:** They are a special case of $N \to M$ protocols where they operate on a large number of mixed states. Here, both parties sharing the entangled states apply CNOT gates and other local unitary operations on their own pairs and measure some of the entangled states to get information about the remaining entangled pairs [151].
  - **Breeding protocols:** They work in a similar fashion, however, they also use pre-purified entangled states that are utilised to gain information about the unmeasured states.

It is known that the hashing protocols assisted with one-way classical communication [142, 151] can achieve the distillable entanglement capacity. While one-way communication is a subset of two-way classical communication, no protocol leveraging the additional features of two-way communication has been shown to reach this bound [320].

Quantum error correction (QEC) is an alternative method for purifying entangled states in noisy quantum channels by detecting and correcting errors without disturbing the quantum states [324]. Various QEC codes exist, such as repetition codes [167], quantum low-density parity-check (QLDPC) codes [163, 164, 166], and stabiliser codes [158–162]. Repetition codes are simple but less efficient, mainly correcting bit-flip errors. QLDPC codes offer efficient error correction with high tolerance using a sparse parity-check matrix. Stabiliser codes, like Shor's [158], Steane's [159] and CSS codes [160], encode quantum information into a larger Hilbert space, using a stabiliser group to detect and correct various errors. QEC has been shown to be equivalent to entanglement purification protocols using one-way classical communication [151, 320]. Specifically, CSS codes for Pauli-diagonal channels can be adapted for entanglement purification with one-way or two-way communication [325–327]. Two-way protocols are particularly effective as they allow for selectively discarding certain entangled pairs, resulting in higher fidelity. In contrast, one-way protocols do not permit discarding of pairs without losing information, making two-way purification protocols derived from CSS codes more effective [320].

While it is already known that the Pauli dephasing channel can be saturated using entanglement purification codes assisted by one-way classical communication, as it is a distillable channel [93, 320], a protocol leveraging two-way classical communication has yet to be established. In this chapter, we propose a two-way entanglement purification protocol with

an explicit circuit that achieves the dephasing channel capacity in the asymptotic limit. Alice prepares m pairs and sends one half of each pair to Bob. Both parties then apply CNOT gates locally on their dephased qubits, with the m^{th} qubit being the control and the others being the targets. After applying the CNOT gates, the control qubit is measured in the Hadamard basis. This recursive protocol involves Alice and Bob purifying the states in multiple stages, resulting in the remaining Bell pairs becoming purer with each iteration. By the final round of the protocol, the Bell pairs will have a fidelity close to one with respect to $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, making them suitable for use in a repeater protocol to distribute entanglement at the channel capacity. Although the capacity-achieving behaviour requires asymptotically large m, the protocol remains effective and competitive even for moderate m, making it relevant for realistic quantum network scenarios. This circuit can also be applied to any number of Bell pairs to correct dephasing errors accumulated in quantum computers. Furthermore, this protocol can serve as a foundational framework for addressing noise and mitigating decoherence in non-distillable channels, such as thermal-noise and depolarising channels, where two-way classical communication could be more advantageous, but would need to be tailored to suit the specific characteristics of those channels.

7.2 The Protocol

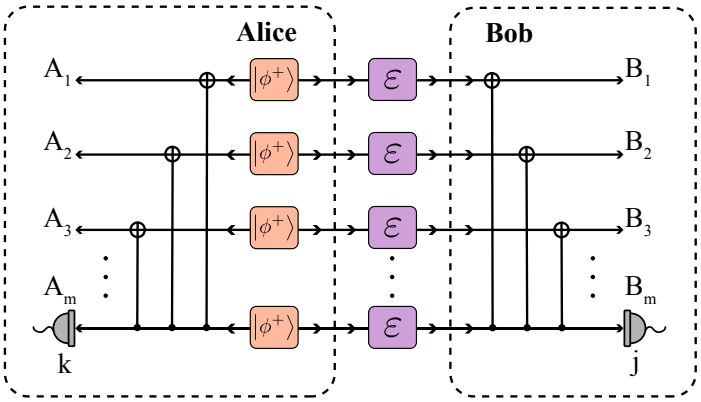

Figure 7.1: First stage of the protocol. Alice prepares m copies of $|\phi^+\rangle$ Bell states and sends them to Bob via a Pauli dephasing channel. Both apply CNOT gates on their qubits, with $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_\mathrm{m}$ and $\mathrm{B}_1, \mathrm{B}_2, \ldots, \mathrm{B}_\mathrm{m}$ representing their respective modes. After the CNOTs, A_m and B_m are measured in the Hadamard basis.

Assume we have a maximally entangled Bell state $|\phi^+\rangle$ in the form

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{7.1}$$

In the dephasing channel without a repeater, this pure state becomes a mixture of $|\phi^+\rangle$ and

$|\phi^-\rangle$ given by

$$\rho_{\text{AB}} = (1-p)\left|\phi^+\right\rangle\!\left\langle\phi^+\right| + p\left|\phi^-\right\rangle\!\left\langle\phi^-\right|, \tag{7.2}$$

where $|\phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$ and p is the dephasing probability, also known as the probability of a phase-flip with $0 \leq p \leq 1/2$. Note that when $p = 1/2$, the state becomes completely dephased. If there is a node in the mid-point splitting the channel into two, the effective state between the sender (Alice) and the node (Charlie) is given by

$$\rho_{\text{AC}} = \left(1 - \frac{1-\sqrt{1-2p}}{2}\right)\left|\phi^+\right\rangle\!\left\langle\phi^+\right| + \left(\frac{1-\sqrt{1-2p}}{2}\right)\left|\phi^-\right\rangle\!\left\langle\phi^-\right|. \tag{7.3}$$

Even though the state dephases less due to having a node, when Bell-state measurements (BSM) are used to swap entanglement, the resulting state between Alice and Bob is the same as Eq. (7.2) (refer to Appendix C.1 for the details). This indicates the necessity of purifying state before performing entanglement swapping.

7.2.1 The First Stage of the Protocol

In this protocol, Alice prepares m copies of Bell pairs and distributes them to Bob via a quantum channel as shown in Fig. 7.1. One half of each Bell pair undergoes dephasing with a probability of p during transmission. To mitigate the dephasing effects and enhance the purity of the Bell pairs, Alice and Bob apply CNOT gates between their respective m^{th} qubit and all other qubits. They then measure the m^{th} qubits, where the measured qubit acts as the control and the remaining qubits serve as the targets. Alice and Bob's measurement is performed using the eigenvectors of the X basis given as

$$|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}. \tag{7.4}$$

When Alice's and Bob's measurement outcomes, denoted as j and k respectively, match as either $(++)$ or $(--)$, they successfully distill entanglement, resulting in a slightly purified state. However, if the outcomes differ, resulting in $(+-)$ or $(-+)$, the distillation process fails. To determine this, Alice and Bob exchange their measurement results via two-way classical communication. This step ensures that both parties agree on whether the purification was successful or failed. As previously mentioned, this protocol is a recursive purification process. Regardless of whether the distillation is successful, Alice and Bob move on to the next stage to further purify the Bell pairs, as explained in the following section.

In the first stage, Alice and Bob apply CNOT gates, leaving the target qubits unchanged. The measured Bell pair (the control qubit) switches to $|\phi^-\rangle$ if there are an odd number of phase flips, and to $|\phi^+\rangle$ if there are an even number. For example, with three Bell pairs, as

Table 7.1: Truth table of the first stage of the protocol where Alice distributes three Bell pairs. T and C denote target and control Bell pairs, respectively, with the control being measured. The first and second columns show the state before and after applying the CNOT gates, where only the control qubit is affected. The third column presents the probability of dephasing noise occurring after distributing three Bell pairs. Pink entries indicate the accepted outcomes when Alice and Bob get a matching measurement outcome.

T,T,C	T,T,C	Probability
ϕ^+,ϕ^+,ϕ^+	ϕ^+,ϕ^+,ϕ^+	$(1-p)^3$
ϕ^+,ϕ^+,ϕ^-	ϕ^+,ϕ^+,ϕ^-	$p(1-p)^2$
ϕ^+,ϕ^-,ϕ^+	ϕ^+,ϕ^-,ϕ^-	$p(1-p)^2$
ϕ^+,ϕ^-,ϕ^-	ϕ^+,ϕ^-,ϕ^+	$p^2(1-p)$
ϕ^-,ϕ^+,ϕ^+	ϕ^-,ϕ^+,ϕ^-	$p(1-p)^2$
ϕ^-,ϕ^+,ϕ^-	ϕ^-,ϕ^+,ϕ^+	$p^2(1-p)$
ϕ^-,ϕ^-,ϕ^+	ϕ^-,ϕ^-,ϕ^+	$p^2(1-p)$
ϕ^-,ϕ^-,ϕ^-	ϕ^-,ϕ^-,ϕ^-	p^3

shown in Table 7.1, an even number of bit-flips results in a $|\phi^+\rangle$ state. A successful outcome is indicated when Alice and Bob both measure $(++)$ or $(--)$, ensuring the measured Bell pair is always $|\phi^+\rangle$. This measurement selects states with $0, 2, \cdots$ bit flips thus removing first-order dephasing errors. The unnormalised eigenvalues of the joint state of the remaining pairs are then based on the probabilities of even bit-flips,

$$\tilde{\lambda}_{s_1}(j) = (1-p)^{m-j}p^j, \tag{7.5}$$

where j represents the number transmission errors with $j = 0, 2, \ldots, m$ and each eigenvalue has a multiplicity of $\binom{m}{j}$. The normalised eigenvalues are given by

$$\lambda_{s_1}(j) = \frac{\tilde{\lambda}_{s_1}(j)}{P_{s_1}(m)}, \tag{7.6}$$

where the normalisation factor

$$P_{s_1}(m) = \frac{1}{2}\left(1 + (1-2p)^m\right), \tag{7.7}$$

is the probability of success for this round.

For the mismatched outcomes $(+-)$ or $(-+)$, the eigenvalues of the conditional state are derived from an odd number of phase-flips, calculated using Eq. (7.5) with $j = 1, 3, \ldots, m$ and denoted as $\lambda_{f_1}(j)$. Each eigenvalue has a multiplicity of $\binom{m}{j}$. The probability of failure is given by

$$P_{f_1}(m) = 1 - P_{s_1}(m) = \frac{1}{2}(1 - (1-2p)^m). \tag{7.8}$$

This protocol maps individually distributed Bell pairs to a higher-dimensional state. For

instance, if Alice and Bob share $m = 3$ dephased Bell pairs, after the first round, the remaining state between them becomes a diagonal state in the Bell basis, as shown below

$$\begin{aligned}\rho_{\mathrm{A_1B_1A_2B_2}} =&\lambda_{s_1}(0)\left|\phi^+\phi^+\right\rangle\!\left\langle\phi^+\phi^+\right| + \lambda_{s_1}(1)\left|\phi^+\phi^-\right\rangle\!\left\langle\phi^+\phi^-\right| + \\ &\lambda_{s_1}(1)\left|\phi^-\phi^+\right\rangle\!\left\langle\phi^-\phi^+\right| + \lambda_{s_1}(2)\left|\phi^-\phi^-\right\rangle\!\left\langle\phi^-\phi^-\right|. \end{aligned} \tag{7.9}$$

Here, $\lambda_{s_1}(0)$, $\lambda_{s_1}(1)$, and $\lambda_{s_1}(2)$ are the eigenvalues of this state. As seen in Eq. (7.9), the remaining state now consists of a mixture of 2 Bell pairs between Alice and Bob, with each eigenvalue indicating the number of errors left after measuring the third Bell pair. Specifically, $\lambda_{s_1}(0)$ corresponds to no errors, while $\lambda_{s_1}(1)$ and $\lambda_{s_1}(2)$ represent 1 and 2 errors, respectively.

After the first round of the protocol, we can calculate the RCI. Since the Pauli dephasing channel is distillable, RCI serves as a tight bound, indicating the amount of distillable entanglement. To saturate the capacity of the dephasing channel, we also need to keep the unsuccessful states (i.e., states corresponding to mismatched measurement outcomes), as these states still contain useful entanglement between Alice and Bob, consistent with findings in [328]. Unlike conventional entanglement purification protocols that focus on reaching a target fidelity with minimal rounds or input resources, our objective here is to develop a protocol that asymptotically achieves the dephasing channel capacity. As this capacity is defined by the RCI and is fundamentally difficult to saturate, requiring asymptotically large numbers of Bell pairs and recursive operations, we adopt the RCI of the output state as our primary figure of merit. Therefore, after the first stage of the protocol, the RCI between Alice and Bob can be expressed as

$$\mathrm{RCI}_1 = \frac{1}{m}\big(P_{s_1}(m)\mathrm{RCI}(\rho_{\mathrm{AB}_{s_1}}) + P_{f_1}(m)\mathrm{RCI}(\rho_{\mathrm{AB}_{f_1}})\big), \tag{7.10}$$

where $P_{s_1}(m)$ and $P_{f_1}(m)$ represent the probabilities of success and failure of Alice and Bob's measurements, respectively, while $\rho_{\mathrm{AB}_{s_1}}$ and $\rho_{\mathrm{AB}_{f_1}}$ are the joint states between Alice and Bob corresponding to successful and failed measurements. Note that the overall RCI needs to be divided by m, the number of Bell pairs used, as the channel capacity is expressed as per channel use (refer to Eq. (4.42) for the definition of RCI). This normalisation by m, together with the inclusion of both successful and failed states weighted by their respective probabilities, ensures that the RCI expressions we derive (e.g., equations (7.10), (7.12) and (7.19)) reflect both the probabilistic nature of the protocol and the total resource cost. As such, the RCI serves as an effective entanglement rate per channel use, analogous to the conventional output-to-input ratio of purified Bell states required to reach a target fidelity.

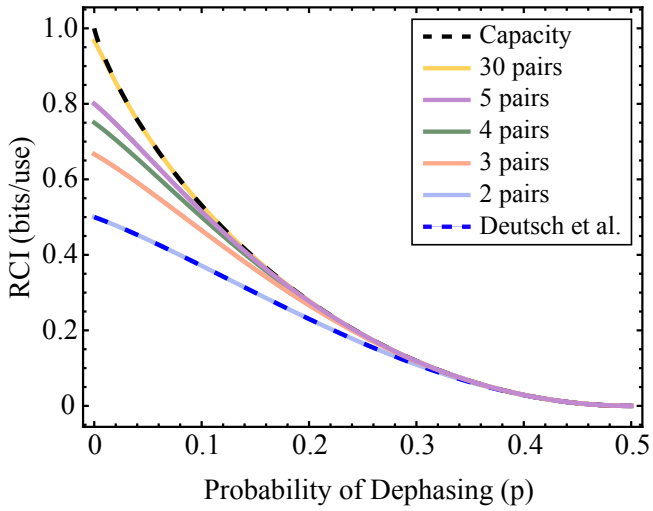

Figure 7.2: Simulation results of the first round of the protocol with increasing number of Bell pairs m shared between Alice and Bob. The black dashed line represents the dephasing channel capacity, while the blue dashed line shows results from Deutsch *et al.* [152].

The von Neumann entropy of Alice's qubit, $S(\rho_{\mathrm{A}})$ in Eq. (4.42), is always equal to 1 when Alice and Bob share a single Bell pair. However, when they share m Bell pairs and measure one out of the m pairs, $S(\rho_{\mathrm{A}}) = \log_2(2^{m-1}) = m-1$. The von Neumann entropy of Alice and Bob's joint state, $S(\rho_{\mathrm{AB}})$, in Eq. (4.42) is determined by

$$S(\rho_{\mathrm{AB}_{s_1}}) = -\sum_{j=0,2,\cdots}^{m} \binom{m}{j} \lambda_{s_1}(j) \log_2 \lambda_{s_1}(j), \tag{7.11a}$$

$$S(\rho_{\mathrm{AB}_{f_1}}) = -\sum_{j=1,3,\cdots}^{m} \binom{m}{j} \lambda_{f_1}(j) \log_2 \lambda_{f_1}(j), \tag{7.11b}$$

where $\binom{m}{j}$ denotes the multiplicity of each eigenvalue $\lambda_{s_1}(j)$ and $\lambda_{f_1}(j)$. Eq. (7.11a) presents the joint entropy of the successful state, while Eq. (7.11b) provides the entropy of the failed state. Therefore, the overall RCI of the first stage becomes

$$\mathrm{RCI}_1 = \frac{1}{m}\left[(m-1) + P_{s_1}(m) \sum_{j=0,2,\cdots}^{m} \binom{m}{j} \lambda_{s_1}(j) \log_2 \lambda_{s_1}(j) + P_{f_1}(m) \sum_{j=1,3,\cdots}^{m} \binom{m}{j} \lambda_{f_1}(j) \log_2 \lambda_{f_1}(j)\right]. \tag{7.12}$$

Note that the term $(m-1)$ comes from $P_{s_1}(m) S(\rho_{\mathrm{A}_{s_1}}) + P_{f_1}(m) S(\rho_{\mathrm{A}_{f_1}})$ where $S(\rho_{\mathrm{A}_{s_1}}) = S(\rho_{\mathrm{A}_{f_1}}) = m-1$ and $P_{s_1}(m) + P_{f_1}(m) = 1$.

Figure 7.2 presents the results of the first stage of the protocol. For $m = 2$, the RCI, success probability, and fidelity of the output state in our protocol match the results of Deutsch's protocol [152], despite the differing circuits. However, as the number of input Bell pairs increases, our protocol approaches the channel capacity, nearly saturating it at $m = 30$. Our

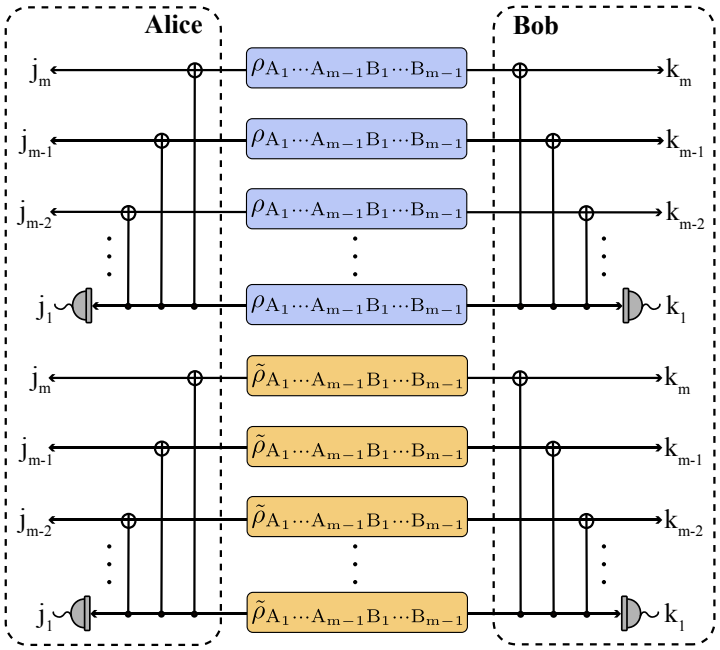

Figure 7.3: Second stage of the purification protocol. The blue and yellow boxes represent successful and failed states, respectively. The top half further purifies m copies of the successfully purified states from the first round, while the bottom half purifies m copies of the states that failed in the first round. The last rail serves as the control, with CNOTs applied and the last rail measured. If $j_1 = k_1$, further purification is achieved.

protocol extends Deutsch's recurrence protocol to the $N \to M$ regime providing an explicit circuit for the purification of any number of Bell pairs. It's important to note that Deutsch's protocol [152] cannot saturate the channel capacity while purifying the Bell pairs, as each round results in half of the Bell pairs being discarded, corresponding to a ratio of $1/2^n$ of the capacity at each round n. This necessitates using more Bell pairs to reach the capacity while purifying. For instance, in our protocol, we discard only one Bell pair out of every m pairs. Consequently, after each round of purification, we retain $(m-1)^n/m^n$ of the capacity, rather than $1/2^n$. However, as the number of Bell pairs increases, the rate of purification decreases, requiring additional rounds to achieve the desired purification level.

7.2.2 The Second Stage of the Protocol

To further purify the Bell states at the dephasing channel capacity, we use m copies of both the successfully purified high-dimensional states and the failed states from the first round, treating them separately. All the successful states are grouped together, and all the failed states are grouped with the other failed states as shown in Fig. 7.3. CNOT gates are then applied between the last rail and each individual state, with the last rail serving as the control. The last rail is then measured and if $j_1 = k_1$, further purification is achieved.

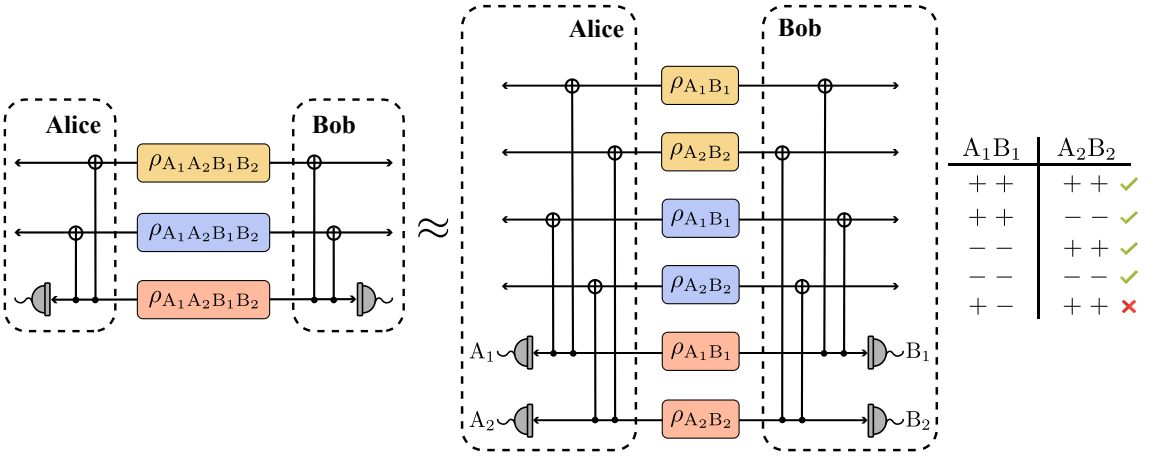

Figure 7.4: Schematic representation of measuring a high-dimensional state in terms of individual Bell pairs in the second round of the protocol, with $m = 3$ carried over from the first round. In the second round, there are $m = 3$ high-dimensional states $\rho_{A_1A_2B_1B_2}$. CNOTs are applied between Bell pairs that are not entangled with each other. Each high-dimensional state contains two Bell pairs, so measuring one high-dimensional state corresponds to measuring the two Bell pairs within it, $\rho_{A_1B_1}$ and $\rho_{A_2B_2}$. Alice and Bob achieve further purification when A_1 and B_1 agree and A_2 and B_2 agree, corresponding to outcomes $(++, ++), (++, --), (--, ++)$ and $(--, --)$.

Figure 7.4 demonstrates the application of CNOTs to the high-dimensional states for $m = 3$. The equivalent circuit is depicted in the center of Fig. 7.4. Following the first round of the protocol, the qubits within the high-dimensional state become entangled, with A_1 entangled with A_2 and B_1 entangled with B_2 in the state $\rho_{A_1A_2B_1B_2}$. In the second round, CNOTs are applied between the control qubits and the qubits that are not entangled with each other. For instance, if $\rho_{A_1A_2B_1B_2}$ is the control state, CNOTs are applied between qubit A_1 of the control state and all the other A_1 qubits, and similarly between qubit A_2 of the control state and all the other A_2 qubits. This avoids concentrating entanglement between the rails and instead focuses on enhancing the entanglement between Alice and Bob.

The CNOTs applied in the second round function the same as in the first round. Suppose Alice distributes 9 Bell pairs to Bob, intending to perform purification over 2 rounds. Some Bell pairs may experience phase-flips from $|\phi^+\rangle$ to $|\phi^-\rangle$. For instance, with 4 transmission errors after the first stage, Alice and Bob share states $\phi^+\phi^+\phi^+$ and two $\phi^-\phi^+\phi^-$ with a probability of $(1-p)^5p^4$ in the first stage. Alice and Bob group these Bell pairs into three blocks of three and apply the circuit shown in Fig. 7.4 (left). The first group $\phi^+\phi^+\phi^+$ has no errors, so the last Bell pair remains ϕ^+ and is measured. The other two blocks $\phi^-\phi^+\phi^-$ each have 2 errors, converting the last Bell pair from ϕ^- to ϕ^+ upon measurement, yielding a successful event. This is demonstrated in Fig. 7.5. In the second stage, Alice and Bob apply the circuit shown in Fig. 7.4 (center) with three blocks of two Bell pairs each: $\phi^+\phi^+$, $\phi^-\phi^+$, and $\phi^-\phi^+$. They regroup their qubits, combining all first pairs of each block into $\phi^+\phi^-\phi^-$

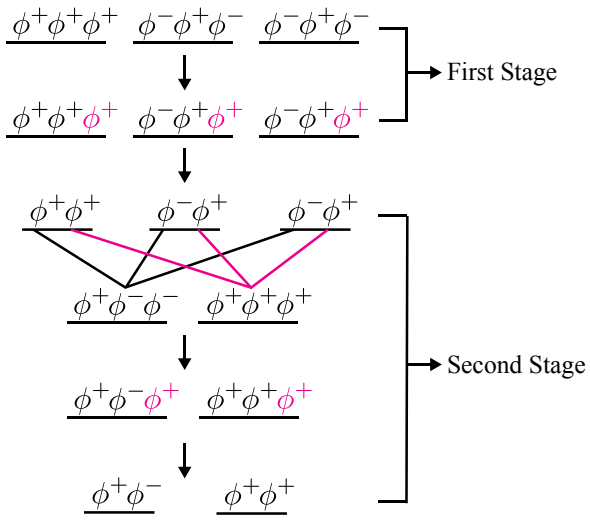

Figure 7.5: Illustration of the rearrangement of Bell pairs using a CNOT gate in the second stage of the protocol. Black and pink lines indicate how the Bell pairs are grouped together for the CNOT application in the second round.

and $\phi^+\phi^+\phi^+$ as shown in Fig. 7.5. The first block, with 2 errors, flips the last ϕ^- to ϕ^+. The second block, with no errors, keeps ϕ^+ as ϕ^+. When both blocks have an even number of errors, the event is considered successful.

As the state dimensions increase with each round of the protocol, simulating beyond $m = 4$ in the second round becomes computationally demanding. Therefore, we simulate this round classically using truth tables and tracking errors in each block for Alice and Bob. The eigenvalues of the successful state of the second round, given success in the first round, are determined by

$$\tilde{\lambda}_{s_1 s_2}(j) = (1-p)^{m^2-j} p^j, \tag{7.13}$$

where $j = 0, 4, 6, \ldots, m(m-1)$ for odd m and $j = 0, 4, 6, \ldots, m^2-4, m^2$ for even m. For example, with $m = 3$, the maximum number of errors per block to yield a successful event is 2, allowing up to 6 transmission errors out of 9 Bell pairs to still result in successful blocks. Similarly, for $m = 4$, 16 Bell pairs are needed for two rounds of purification, with up to 16 errors permissible in the first stage across 4 blocks. However, note that for even m, the second highest number of transmission errors in the second stage is $j = m^2 - 4$ errors, as $j = m^2 - 2$ errors in the first stage can lead to odd errors in some blocks in the second stage. For instance, with $m = 4$, one possible combination that $j = m^2 - 2 = 14$ transmission errors can occur in the first round is $\phi^-\phi^-\phi^-\phi^-$, $\phi^-\phi^-\phi^-\phi^-$, $\phi^-\phi^-\phi^-\phi^-$, and $\phi^-\phi^-\phi^+\phi^+$. Since each block has an even number of errors, this leads to success in the first round. However, when rearranged for the second round, new blocks become $\phi^-\phi^-\phi^-\phi^-$, $\phi^-\phi^-\phi^-\phi^-$, and $\phi^-\phi^-\phi^-\phi^+$. While the first two blocks have even errors, the last block has odd errors,

leading to failure.

Generalising the success probability of the second round as a function of m and p given the states were successful in the first round of the protocol is more challenging than Eq. (7.7) as the the qubits are rearranged in the second round to concentrate the entanglement between Alice and Bob rather than the unwanted entanglement between the rails. However, the probability of success of the second round given that the states were also successful in the first round is given by

$$P_{s_1 s_2}(m) = \sum_{j=4,6,\cdots,j_{m-1}}^{j_m} M \frac{\tilde{\lambda}_{s_1 s_2}(j)}{P_{s_1}^m(m)}, \tag{7.14}$$

where $j_m = m(m-1)$ and $j_{m-1} = m(m-1) - 2$ if m is odd or $j_m = m^2$ and $j_{m-1} = m^2 - 4$ if m is even. M represents the multiplicity of each eigenvalue $\tilde{\lambda}_{s_1 s_2}(j)$ and each eigenvalue needs to be normalised by $P_{s_1}^m(m)$ as the second stage of the protocol requires m copies of the successful high-dimensional states from the first round of the protocol (see Appendix C.2 for a more generalised expression for the probability of success of the second round). Finally, the eigenvalues also need to be normalised by the probability of success of the second round to get the coefficients of various Bell state combinations in the final state as

$$\lambda_{s_1 s_2}(j) = \frac{\tilde{\lambda}_{s_1 s_2}(j)}{P_{s_1}^m(m) P_{s_1 s_2}(m)}. \tag{7.15}$$

Similar to the first stage, we need to keep conditional states that do not result in a successful event in this round, as they still contain useful entanglement. Discarding them would prevent us from saturating the channel capacity. Therefore, we need to compute the RCI of the failed states in the second stage, given that they succeeded in the first round. The eigenvalues of the failed state can be derived from the eigenvalues of the succeeding states in the first and second rounds. Specifically, for the dephasing channel, the average state in the second round, comprising both the successful and failed states given success in the first round, is equal to $m-1$ copies of the successful state from the first stage. This ensures that when combined, the overall state retains the same purity as $m-1$ copies of the original state from the first stage, matching its eigenvalues. This occurs because, after the first round, we obtain m copies of a successful high-dimensional state, and measuring one of these copies does not alter the overall purity in the second round. However, among the conditional states, the successful state becomes purer while the failed state is less pure. The relationship between the average state from the second round of the protocol and $m-1$ copies of the successful state from the second round can be given as

$$\rho_{\mathrm{AB}_{s_1}}^{\otimes(m-1)} = P_{s_1 s_2}(m) \times \rho_{\mathrm{AB}_{s_1 s_2}} + P_{s_1 f_2}(m) \times \rho_{\mathrm{AB}_{s_1 f_2}}, \tag{7.16}$$

where $\rho_{\mathrm{AB}_{s_1}}$ represents the successful state from the first stage of the protocol. $P_{s_1s_2}(m)$ (given in Eq. (7.14)) and $P_{s_1f_2}(m)$ are the probabilities of success and failure, respectively, in the second round given the state was successful in the first round. $P_{s_1f_2}(m)$ is equal to $1 - P_{s_1s_2}(m)$. $\rho_{\mathrm{AB}_{s_1s_2}}$ and $\rho_{\mathrm{AB}_{s_1f_2}}$ are the successful and failed conditional states of the second round, respectively, given they succeeded in the first round. Using Eq. (7.16), the eigenvalues of the failed state can be expressed as

$$\lambda_{s_1f_2}(j_1, j_2) = \frac{1}{P_{s_1f_2}(m)}\left[\frac{(1-p)^{m(m-1)-j_1}p^{j_1}}{P_{s_1}^{m-1}(m)} - \frac{(1-p)^{m^2-j_2}p^{j_2}}{P_{s_1}^{m}(m)}\right], \tag{7.17}$$

where j_2 is the total number of transmission errors while j_1 is the number of remaining transmission errors after measuring some of the Bell pairs in the first round. The relationship between j_1 and j_2 is expressed as

$$m\text{=even}\begin{cases} j_2 = 0 & j_1 = 0 \\ j_2 = 4 & j_1 = 2 \\ j_2 = j_1, j_1+2, j_1+4 & 4 \leq j_1 < m(m-1)-2 \\ j_2 = j_1, j_1+2 & j_1 = m(m-1)-2 \\ j_2 = m^2 & j_1 = m(m-1), \end{cases} \tag{7.18a}$$

$$m\text{=odd}\begin{cases} j_2 = 0 & j_1 = 0 \\ j_2 = 4 & j_1 = 2 \\ j_2 = j_1, j_1+2, j_1+4 & 4 \leq j_1 < (m-1)^2 \\ j_2 = j_1 : m(m-1) : 2 & j_1 = (m-1)^2. \end{cases} \tag{7.18b}$$

Note that we do not discard the conditional failed states from the first round. Instead, we take m copies of these high-dimensional failed states and attempt to purify them further in the second round. As mentioned earlier, to saturate the capacity, we need to keep all conditional states regardless of success or failure as they contain useful entanglement. Therefore, we compute the RCI of both successful and failed states in the second round, given they failed in the first round. To do this, we first compute their eigenvalues which are given in Appendix C.3. Then using all the conditional states, the RCI of the second round of the protocol can be written as

$$\begin{aligned} \mathrm{RCI}_2 =& \frac{1}{m^2}\big[P_{s_1}(m)\big(P_{s_1s_2}(m) \times \mathrm{RCI}(\rho_{\mathrm{AB}_{s_1s_2}}) + P_{s_1f_2}(m) \times \mathrm{RCI}(\rho_{\mathrm{AB}_{s_1f_2}})\big) \\ &+ P_{f_1}(m)\big(P_{f_1s_2}(m) \times \mathrm{RCI}(\rho_{\mathrm{AB}_{f_1s_2}}) + P_{f_1f_2}(m) \times \mathrm{RCI}(\rho_{\mathrm{AB}_{f_1f_2}})\big)\big], \end{aligned} \tag{7.19}$$

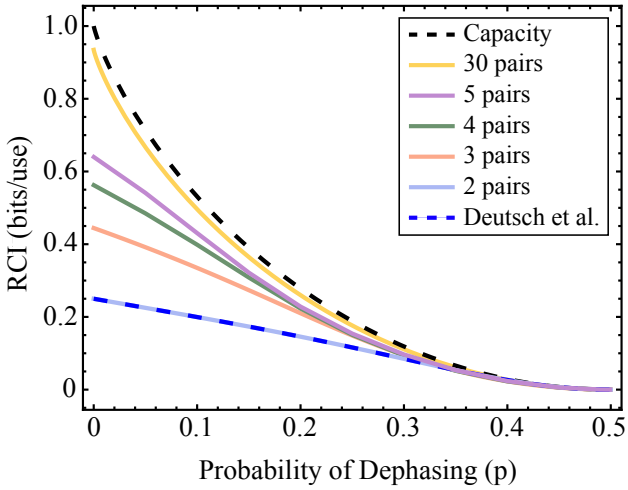

Figure 7.6: Simulation results of the second round of the protocol with increasing number of Bell pairs m shared between Alice and Bob. The black dashed line represents the dephasing channel capacity, while the blue dashed line shows results from Deutsch *et al.* [152]. The yellow line for $m = 30$ is simulated using $(m-1)^2/m^2 \times C$ where C represents the channel capacity.

where $\rho_{\mathrm{AB}_{f_1 s_2}}$ and $\rho_{\mathrm{AB}_{f_1 f_2}}$ represent the conditional states in the second round that succeeded and failed, respectively, given failure in the first round. The probabilities of success and failure in the second round, given first-round failure, are denoted by $P_{f_1 s_2}(m)$ and $P_{f_1 f_2}(m)$ (refer to Appendix C.3 for how to obtain the eigenvalues and the probabilities). Note that the average RCI is normalised by m^2 because distributing m^2 Bell pairs through the channel is required to proceed to the second round. The RCI of each conditional state is computed using Eq. (4.42), where $S(\rho_{\mathrm{A}})$ for each conditional state is $\log_2(2^{(m-1)^2}) = (m-1)^2$, and $S(\rho_{\mathrm{AB}})$ is calculated by summing the eigenvalues, substituting each into $-\tilde{\lambda}\log_2\tilde{\lambda}$.

Figure 7.6 illustrates the RCI during the second round of the protocol as m increases. For a fixed value of m, each line shows an expected decrease in performance compared to the first stage of the protocol, due to the normalisation of the average RCI by $1/m^2$. However, as m increases, the average RCI converges towards the capacity of the dephasing channel. Notably, compared to the previous round, the fidelity of the successful reduced states improve as shown in Fig. 7.7. For $m = 3$, the fidelity of the reduced two-mode state with $|\phi^+\rangle$ increases from 0.9 to 0.9762 in the first round of the protocol, reaching a fidelity of 0.9994 after the second round, as shown in Fig. 7.7(a). Similarly, for $m = 4$, the fidelity starts at 0.9654 in the first round and improves to 0.9986 in the second round, demonstrating the protocol's capability to purify with an increasing number of rounds, as proven in the following section. It is important to note that as m increases, the fidelity in each round will be slightly lower compared to that for a smaller value of m, since we only sacrifice one (high-dimensional) state each time each time. For example, measuring one state out of three contributes more to the remaining two than measuring one out of four. When the probability of dephasing

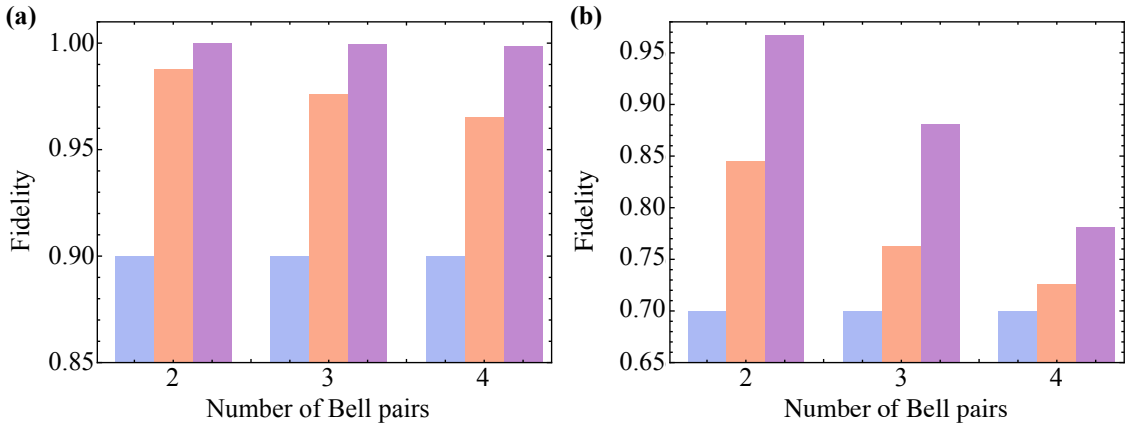

Figure 7.7: Comparison of the fidelity of the reduced successful states with the $|\phi^+\rangle$ state without purification and after the first and second rounds of the purification protocol. **(a)** presents the fidelity of the reduced states using $m = 2$, $m = 3$, and $m = 4$ Bell pairs, with a dephasing probability of $p = 0.1$, corresponding to an initial fidelity of $F = 0.9$ before purification. Blue boxes indicate the fidelity prior to purification, while pink and purple boxes represent the fidelities after the first and second rounds, respectively. **(b)** shows the fidelity of the reduced states for an initial dephasing probability of $p = 0.3$, corresponding to an initial fidelity of $F = 0.7$.

increases from $p = 0.1$ to $p = 0.3$, corresponding to higher decoherence, our protocol still enhances the fidelities, as shown in Fig. 7.7(b), albeit more gradually. This slower increase is expected due to the higher decoherence. However, when decoherence is high, fewer Bell pairs between Alice and Bob are needed to reach the channel capacity. Therefore, a smaller number of m already saturates the channel capacity, as observed in both Figs. 7.2 and 7.6.

7.3 Optimality of the Protocol

For the protocol to be optimal, it needs to achieve the channel capacity in each round while purifying the states. In this section, we demonstrate that our protocol can asymptotically achieve the capacity in the first and second rounds while purifying the states in each round, attaining a fidelity of 1 with a small number of qubits. Finally, we prove that the protocol remains optimal for each round of the purification step.

7.3.1 Achieving the Capacity

As the dephasing channel is a distillable channel, we use RCI [126, 140] shown in Eq. (4.42) as a benchmark to test the quality of our purification protocol. The RCI serves to quantify the amount of distillable entanglement between Alice and Bob to infer the secret key rate.

In this section, we show no entanglement is lost between the rounds of the purification process as $m \to \infty$. If we add the successful and failed states up after the first round, they

give the state of $m-1$ copies of the noisy Bell pairs as shown below

$$\frac{1}{m}\mathrm{RCI}(\rho_{\mathrm{AB}}^{\otimes(m-1)})=\frac{1}{m}\mathrm{RCI}(P_{s_1}(m)\times\rho_{\mathrm{AB}_{s_1}}+P_{f_1}(m)\times\rho_{\mathrm{AB}_{f_1}}), \tag{7.20}$$

where $\rho_{\mathrm{AB}}^{\otimes(m-1)}$ is $m-1$ copies of the initial state shown in Eq. (7.2). The intuition behind the RHS of Eq. (7.20) is that when combining the successful and failed states after the first round of the protocol, the overall state has the same entanglement as the state from the first stage with up to $m-1$ copies, since one copy was measured during the process.

Note that the RCI of ρ_{AB} is equal to $1-\mathrm{H}_2(p)$ which is the capacity, C of the dephasing channel. As there is no entanglement between each copy of ρ_{AB} before the purification process, we can use $S(\rho^{\otimes n})=n\,S(\rho)$. Therefore the LHS of Eq. (7.20) becomes

$$\begin{aligned}\frac{1}{m}\mathrm{RCI}(\rho_{\mathrm{AB}}^{\otimes(m-1)}) &=\frac{1}{m}\left(S(\rho_{\mathrm{A}}^{\otimes(m-1)})-S(\rho_{\mathrm{AB}}^{\otimes(m-1)})\right)\\ &=\frac{m-1}{m}\big(S(\rho_{\mathrm{A}})-S(\rho_{\mathrm{AB}})\big)\\ &=\frac{m-1}{m}(1-\mathrm{H}_2(p))\\ &=\frac{m-1}{m}C.\end{aligned} \tag{7.21}$$

This implies that after the first round of the protocol, the average state has the same RCI as $m-1$ copies from the previous round (see Appendix C.4 and Appendix C.5 for the proof of the RHS of Eq. (7.20) and the capacity proof for the second stage, respectively). Additionally, as $m\to\infty$,

$$\lim_{m\to\infty}\frac{m-1}{m}C=C. \tag{7.22}$$

For the n^{th} round of the protocol, the RCI of the average state between Alice and Bob can be expressed as

$$\mathrm{RCI}(\rho_{\mathrm{AB}_n})=\frac{1}{m^n}\mathrm{RCI}(\rho_{\mathrm{AB}_{n-1}}), \tag{7.23}$$

where $\mathrm{RCI}(\rho_{\mathrm{AB}_n})$ denotes the RCI of the average state of the current round, while $\mathrm{RCI}(\rho_{\mathrm{AB}_{n-1}})$ represents the RCI of $m-1$ copies of the average state from the previous round. The overall RCI needs to be normalised by the total number of Bell pairs used throughout the purification proceess. Since the RCI of the current round is equal to the previous round, the RCI of the n^{th} can be related to the first round by

$$\mathrm{RCI}(\rho_{\mathrm{AB}_n})=\frac{1}{m^n}\mathrm{RCI}(\rho_{\mathrm{AB}}^{\otimes(m-1)^n}). \tag{7.24}$$

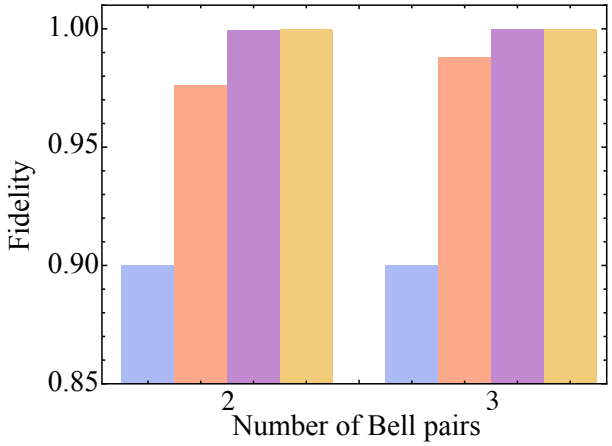

Figure 7.8: Comparison of the fidelity of the reduced states with the $|\phi^+\rangle$ state without purification and after the first, second and third rounds of the purification protocol. The left boxes are for $m = 2$ while the right shows the results of $m = 3$ for a dephasing value of $p = 0.1$. Blue boxes indicate the fidelity prior to purification, while pink, purple and yellow boxes represent the fidelity after the first, second and third rounds, respectively.

Using the same relations as Eq. (7.21), Eq. (7.24) becomes

$$\begin{aligned} \mathrm{RCI}(\rho_{\mathrm{AB}_n}) &= \left(\frac{m-1}{m}\right)^n \mathrm{RCI}(\rho_{\mathrm{AB}}) \\ &= \left(\frac{m-1}{m}\right)^n C. \end{aligned} \tag{7.25}$$

If $n = m$, the limit as $m \to \infty$ approaches C/e, which would result in the lower bound being less than the capacity. However, in each round, the effective dephasing is reduced compared to the previous round, leading to higher distillable entanglement. This might suggest a violation of the capacity. Nonetheless, this is prevented by the coefficient $\left(\frac{m-1}{m}\right)^n$ that appears before the capacity. Therefore, as long as $n \ll m$, we have

$$\lim_{m\to\infty} \left(\frac{m-1}{m}\right)^n C = C. \tag{7.26}$$

For $p = 0.1$ and $m = 2$ and $m = 3$, a fidelity very close to 1 is achieved within 3 rounds for both cases, as illustrated in Fig. 7.8. Although it is not immediately obvious in the figure, both fidelities approach 1 by the third round, starting from $F_2 = 0.9998$ for $m = 2$ and $F_2 = 0.9994$ for $m = 3$. This suggests that the rate at which the number of rounds needs to increase as m grows may not scale as quickly as m itself to purify while achieving the capacity.

For more rigorous proofs on achieving the channel capacity, we show in Appendix C.4 that the right-hand side of Eq. (7.20) equals the left-hand side in the first round of the pro-

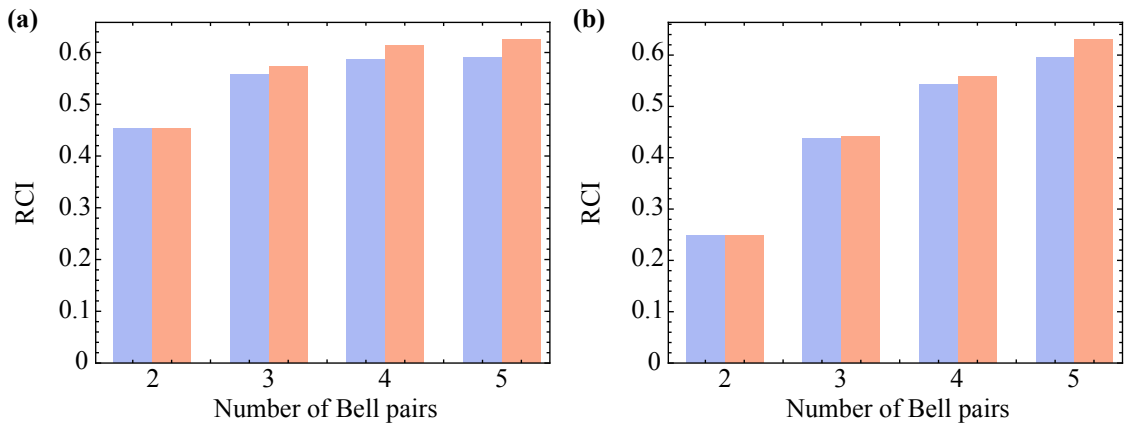

Figure 7.9: Comparison of the RCI between $m-1$ copies of the reduced successful states in the alternative protocol and the high-dimensional states in the actual protocol for a dephasing probability of $p = 0.1$. Blue boxes represent the alternative protocol, while pink boxes show the actual protocol. **(a)** illustrates the RCI of the states after the first round with an increasing number of Bell pairs, and **(b)** presents the results after the second round.

tocol, with an alternative proof provided by lower bounding the RCI in Eq. (7.10). This is further used in Appendix C.5, where we lower bound the RCI in the second round using Eq. (7.19) to confirm that it achieves the capacity. Finally, in Appendix C.6, we extend the proof to show that the protocol can achieve the channel capacity in any round of the purification process.

7.3.2 Purifying the States

While our protocol purifies the dephased Bell states, it also generates entanglement between Alice's and Bob's respective modes. For instance, for $m = 3$, after the first round we obtain the high-dimensional state $\rho_{\mathrm{A_1B_1A_2B_2}}$ with reduced states $\rho_{\mathrm{A_1B_1}}$ and $\rho_{\mathrm{A_2B_2}}$ which are both individually purer and identical. However, $\mathrm{A_1}$ and $\mathrm{A_2}$ now exhibit correlations that cannot be disregarded, as this entanglement contributes to attaining the channel capacity and further purification of the Bell pairs in subsequent rounds.

To prove that our protocol achieves the required fidelity of $F = 1$ and fully purifies the states, we can derive a lower bound. To this end, we propose an alternative protocol in which the correlations between Alice's and Bob's own modes are disregarded. In this alternative approach, instead of using m copies of $\rho_{\mathrm{A_1B_1A_2B_2}}$, we consider m copies of the reduced state $\rho_{\mathrm{A_1B_1}}$ and assume that the protocol is restarted from the first round with these fresh copies using the circuit in Fig. 7.1, which are purer than the initial ρ_{AB}. Proving that the alternative protocol serves as a lower bound to the actual protocol is challenging because finding a general expression for any number of copies, m, and rounds, n, is intractable due to the complexity of the eigenvalue multiplicities. However, Fig. 7.9 provides numerical

evidence that the RCI of the successful states in the alternative protocol is consistently lower than that of the actual protocol. Recall that RCI quantifies the distillable entanglement. As shown in Fig. 7.9(a), the RCI of $m-1$ copies of the reduced state is lower than that of the high-dimensional state obtained after the first round of the protocol, indicating that some useful entanglement between the rails is discarded. This effect is similarly observed in Fig. 7.9(b) after the second round.

The relationship between the fidelities of the two protocols can be further understood through the quantum data processing inequality (DPI), a key principle in quantum information theory. The DPI states that applying a completely positive trace-preserving (CPTP) map such as a local operation, lossy transformation, or quantum channel, to a quantum state cannot increase its fidelity with respect to a reference state [329–332]. In the alternative protocol, the process of tracing out certain modes can be regarded as a lossy operation that discards useful correlations between subsystems. Therefore, this can be expressed as

$$F^A(\rho_{\mathrm{AB}_{s_1}}, |\phi^+\rangle) \leq F^R(\rho_{\mathrm{AB}_{s_1}}, |\phi^+\rangle), \tag{7.27}$$

where F^A and F^R denote the fidelities of the alternative and the original protocols with respect to the $|\phi^+\rangle$ state, respectively.

It is worth noting that DPI is often discussed in contexts where the fidelity between two quantum states increases after processing because the operation "blurs" their differences. However, in this work, fidelity is measured with respect to a fixed reference state ($|\phi^+\rangle$). The partial trace operation, as a CPTP map, degrades the state relative to this fixed reference, rather than increasing fidelity as seen in other DPI contexts. This fidelity degradation can be intuitively understood by considering the discarded subsystems as an additional "processing step" that weakens the entanglement in the remaining state. An analogy to image compression illustrates this: removing certain details during compression results in an image that remains recognisable but lacks the full fidelity of the original.

To quantify this effect, we examine the reduced states after the first round of the protocol

$$\tilde{\rho}_{\mathrm{AB}} = \begin{pmatrix} 0.5 & 0 & 0 & b/2a \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ b/2a & 0 & 0 & 0.5 \end{pmatrix}, \tag{7.28}$$

where before the purification protocol, the off-diagonal term is $b/2a = (1-2p)/2$. However, after the purification process, the new value of a and b becomes

$$a(p) = 2^{m-2}\left[\left(\frac{1-2p}{2}\right)^m + \left(\frac{1}{2}\right)^m\right], \tag{7.29a}$$

Table 7.2: Comparison of fidelity across rounds for the alternative and original protocols. The initial dephasing probability is set to $p = 0.1$.

Round	Alternative Protocol	Original Protocol
F_0	0.9	0.9
F_1	0.97619	0.97619
F_2	0.998812	0.999384
F_3	0.999997	1

$$b(p) = 2^{m-2}\left[\left(\frac{1-2p}{2}\right)^{m-1}\left(\frac{1}{2}\right) + \left(\frac{1-2p}{2}\right)\left(\frac{1}{2}\right)^{m-1}\right]. \tag{7.29b}$$

Using Eqs. (7.29a) and (7.29b), the new dephasing probability becomes

$$\tilde{p}(p) = \frac{1}{2}\left(1 - \frac{b(p)}{a(p)}\right), \tag{7.30}$$

and the fidelity of the new states is given by $F = 1 - \tilde{p}$. It is important to note that the fidelities of the alternative protocol are always lower than those of the actual protocol but are still an improvement over the original states as depicted in Table 7.2.

As this alternative protocol has slightly worse fidelity due to ignoring the useful entanglement between the respective modes, the relationship between the fidelities can be expressed as

$$1 - p \leq F^A \leq F^R \leq 1, \tag{7.31a}$$

$$0 \leq p^R \leq p^A \leq p \leq \frac{1}{2}, \tag{7.31b}$$

where p^A and p^R denote the probabilities, of the alternative and the original protocols, respectively.

To demonstrate that our protocol fully purifies the states, we use an iterative map proof, establishing that $\tilde{p}^A \leq p \leq 1/2$ after the first round of the alternative protocol for any m. Following the second round, the relationship $\tilde{p}^{A'} \leq \tilde{p}^A \leq p$ holds, where $\tilde{p}^{A'}$ and $\tilde{p}^A$ represent the new probabilities after the second and first rounds of the alternative protocol, respectively. This indicates that with each repetition of the protocol, the probability of dephasing continually decreases, resulting in further purification of the states. The details of this proof are provided in Appendix C.7. Additionally, we present numerical evidence in Fig. 7.10 showing that the approximate protocol closely mirrors our original protocol, achieving complete purification of the states over multiple rounds for any number of Bell pairs, m. The key difference between the two protocols is that the approximate protocol, by ignoring some useful entanglement, purifies the states slower than the original protocol.

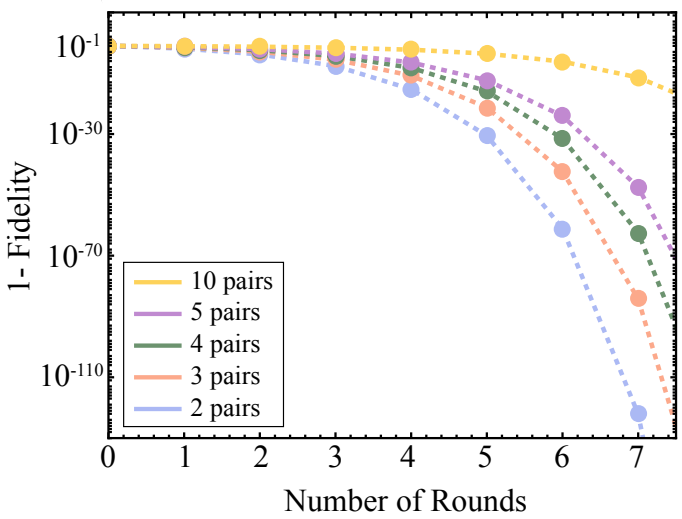

Figure 7.10: Dephasing probability of the alternative protocol (also corresponding to 1-fidelity) as a function of rounds with increasing number of Bell pairs. The initial dephasing probability is $p = 0.1$ corresponding to an initial fidelity $F = 0.9$ with respect to $|\phi^+\rangle$ state.

7.4 Discussion

Quantum communications enable secure information transfer and entanglement distribution but are limited by channel capacity and decoherence. Developing protocols that mitigate these challenges is key to realising quantum networks.

The Pauli dephasing channel exemplifies how decoherence can be particularly detrimental. While quantum repeaters can help mitigate losses and improve secret key rates beyond those of point-to-point communications, they fail to surpass the capacity of a repeaterless channel in the case of dephasing noise. This is because the Bell state measurements in repeaters further degrade the quantum states. To overcome this problem, we presented a purification protocol assisted with two-way classical communications designed to reach the dephasing channel capacity in the asymptotic limit. Through a recursive process, where Alice and Bob apply CNOT gates and measure in the Hadamard basis, the protocol purifies Bell pairs, improving their fidelity by correcting higher-order dephasing errors with each round. Ultimately, this method ensures the Bell pairs are nearly perfect, making them ideal for use in quantum repeaters before entanglement swapping with the respective nodes. Additionally, our protocol can also be applied to dephasing errors in quantum computers or to purify Bell states in distributed quantum computing. While achieving the dephasing channel capacity requires multiple Bell pairs, our protocol offers an explicit circuit that can be adapted to any number of pairs, with the repetition rate adjustable to the user's requirements. Importantly, our protocol remains relevant even outside the asymptotic limit. When implemented with small values of m, it naturally reduces to well-known schemes such as

Deutsch's protocol [152] and can be practically adapted into pumping [138] or banding-style [333] purification strategies. Pumping protocols repeatedly distill a slightly purified state using fresh noisy states, while banding protocols group intermediate states by fidelity and apply tailored purification steps within each group. Due to our protocol's optimisation for the dephasing channel, the same fixed circuit can be reused across rounds, providing a simple and scalable approach that performs well even under realistic resource constraints.

Although our circuit is specifically designed for the dephasing channel, it provides a framework for addressing noise and mitigating decoherence. As such, it can serve as a guide for adapting circuits to other noisy channels, such as depolarising, erasure, and thermal noise channels, where customised designs are required. Future work should also evaluate the protoocol's performance under more realistic conditions, including gate errors, memory decoherence, and compound noise, and explore extensions through circuit refinements.

Chapter 8

Conclusions and Outlook

In this thesis, we investigated ways to improve the performance of quantum communications, particularly focusing on quantum key distribution. As quantum states are fragile, this limits the distance they can be distributed and significantly reduces the key rate. Here, we focused on how both distance and key rates can be improved in quantum communications. To this end, we proposed three different protocols, each employing a different technique for distinct quantum channels, which were detailed in Chapters 5, 6, and 7. In the following subsections, we provide a summary of these chapters and outline potential directions for future research.

8.1 Summary of the CV-QKD Protocol with Post-Selection Filters

In Chapter 5, we focused on the question: "How can key rates between Alice and Bob be improved in a basic CV-QKD system using Gaussian modulated states and homodyne detection" when Alice and Bob communicate directly with each other. Previous studies showed that key rates and transmission distances can be improved by using probabilistic filters to mimic physical quantum operations [225–227, 231–233]. However, these improvements remained limited because the filters were constrained by the need to emulate these processes. In this chapter, the protocol we introduced and implemented experimentally eliminated the need to simulate physical processes when filtering. The protocol incorporated post-selection in both Alice and Bob's stations. The post-selection employed in Alice's station was a Gaussian filter, which optimised the modulation variance required for the estimated quantum channel. On the other hand, the filter used in Bob's station was a non-Gaussian filter which emulated a better performing quantum channel. As the filter is non-Gaussian, we provided an alternative security analysis which improved the key rates by not using the Gaussian extremality. This protocol is compatible with the existing CV-QKD setups using coherent states and enables dynamic optimisation of key rates for rapidly changing channels. Experimentally, our protocol achieved key extraction in regions previously considered insecure by parameter estimation, demonstrating up to a threefold improvement in key rates experimentally compared to the optimal GG02 protocol [78, 100]. Additionally, simulations for LEO satellite-to-ground quantum communications links showed key rate improvements of

up to 400-fold.

Our protocol considered the asymptotic limit. However, extending this to finite-size effects would be useful as in practical applications, data sizes are finite. Additionally, the security analysis after Bob's post-selection requires the calculation of Eve's density matrix to infer her information. This method is computationally demanding and is likely to be infeasible if the modulation variance is high. A recent paper by Denys *et al.* [241] provided an analytical lower bound on the asymptotic secret key rate for CV-QKD with arbitrary modulation schemes. Extending this to include Bob's post-selection could simplify the security analysis and reduce computational demands. Additionally, Alice and Bob's post-selection in our protocol can be interpreted as dynamically determining which states to keep. For this reason, our protocol could allow a dynamic switch between Gaussian-modulated and discrete modulated CV-QKD schemes with coherent states. Such an approach could be particularly advantageous for operation in scintillating channels.

8.2 Summary of the Repeater-Like MDI Protocol

While the CV-QKD protocol introduced in Chapter 5 improved key rates in a scintillating channel, it could not surpass or reach the channel capacity. This limitation arose from the absence of a repeater station to divide the channel. In Chapter 6, we investigated whether the single-repeater bound of the pure-loss channel could be achieved using a simple repeater protocol without quantum memories or collective measurements, as it is known that the repeaterless bound can be saturated with the squeezed-state protocol without requiring multiple states or collective measurements.

To address this, we proposed a protocol that employs high-dimensional states and introduced a new entanglement swapping measurement at the repeater station. In this protocol, keys were encoded onto photon number states and entanglement between Alice and Bob was established through Charlie's total photon-number counting measurement. Since Charlie is untrusted, he could only determine the total number of photons sent by Alice and Bob, without distinguishing their individual contributions. Alice and Bob's states were also optimised to maximise the key rates, showing that at short distances, higher photon numbers resulted in better key rates, while at larger distances, the optimal states dropped to the single-photon level. For this reason, we proposed a more experimentally practical protocol that uses single photons and photon-number resolving detectors capable of detecting up to two photons. Our protocol surpassed the repeaterless bound capacity at a shorter distance than the existing MDI protocols and extended the achievable QKD distance beyond their limits. However, our protocol could not reach the single-repeater capacity, as achieving this likely requires multiple copies of the states and the use of collective measurements.

The security analysis of our protocol was limited to the asymptotic limit, but studying the finite-size effects is necessary for a more practical scenario. Additionally, to verify that Charlie performs the correct measurements in our protocol, Alice and Bob switch bases and send check states in the X and Y bases, which are prone to misalignment errors. Incorporating these errors into the key rate calculations would make the analysis more applicable to realistic experimental setups. Furthermore, extending our protocol to a network of users could pave the way for its integration into the quantum internet, enabling secure communication on a larger scale. Finally, advancing state preparation from $n = 2$ photons [298] to higher dimensions and implementing Charlie's measurement could benefit not only QKD but also other areas of quantum information, such as quantum metrology, entanglement swapping, and optical quantum computing.

8.3 Summary of the Purification Protocol

In Chapter 7, we demonstrated that introducing a repeater splitting the Pauli-dephasing channel into two segments cannot surpass the repeaterless capacity of the dephasing channel, unlike the repeater protocol introduced for the pure-loss channel in Chapter 6. This is because the Bell-state measurements introduce additional decoherence to the distributed Bell states, resulting in the same amount of distillable entanglement as direct communication between Alice and Bob, without a node splitting the channel. To address this, we proposed a purification protocol that applies simple gates to distributed Bell pairs and measures one pair out of m pairs. With each iteration, the protocol maps the states to a higher-dimensional space, progressively increasing the purity of the individual Bell pairs. Furthermore, we demonstrated that our protocol achieves the capacity of the Pauli-dephasing channel, with the resulting states attaining a fidelity of 1 relative to the $|\phi^+\rangle$ state given enough iterations of the purification process.

Although the explicit circuit proposed in this protocol is versatile and applicable to any number of Bell pairs, it has not yet been tested on a real hardware. Observing how effectively the protocol mitigates dephasing errors in practice would be valuable. Additionally, we believe this protocol could be adapted for other noisy channels, such as thermal loss or depolarising channels, to explore strategies for achieving their capacities.

8.4 Closing Remarks and Outlook

Encryption has been evolving since ancient times, with codebreakers consistently finding ways to expose its flaws. As we enter the quantum era, it is clear that our current encryption methods must be improved, transitioning from traditional approaches to more innovative

solutions. While QKD offers information-theoretic security, there is ongoing debate within the cryptographic community regarding its practicality and necessity in the post-quantum era. Post-quantum cryptography (PQC) [334,335], which is based on classical mathematical problems believed to be hard even for quantum computers, presents a compelling alternative. PQC protocols are generally easier to deploy with existing infrastructure, however, their long-term security cannot be guaranteed until universal quantum computers are realised and their full capabilities are understood. In contrast, QKD provides provable security independent of computational assumptions, making it an attractive choice for highly sensitive applications such as governmental, military, and financial communications. Ultimately, no single solution is likely to fit all scenarios. A layered approach combining both QKD and PQC, using PQC for general-purpose encryption and QKD for critical secure links may offer the most robust path forward.

Although QKD offers information-theoretic security, its effectiveness is limited by the constraints on transmission distance. In this thesis, we introduced several protocols using both CV and DV platforms, which not only improve QKD distances and key rates but also contribute to advancements in other areas of quantum communications. The protocol presented in Chapter 5 provides a near-term solution for QKD that can be implemented on existing CV platforms with coherent states. Notably, this CV-QKD protocol has been implemented experimentally and integrated as a proof-of-principle into a commercial QKD platform with promising performance increase. The techniques introduced in this protocol for optimising states based on channel parameters can also be applied to other CV-QKD protocols, including those that use squeezed states.

The protocols outlined in Chapters 6 and 7 offer more efficient methods for entanglement distribution, serving as potential stepping stones toward the quantum internet [62,63] with applications extending beyond QKD. The DV-based protocol in Chapter 6 is more experimentally demanding, particularly in its entanglement-swapping step due to requiring higher-dimensional Fock states, but it can feasibly be demonstrated using single-photon encoding and PNRDs. The MDI nature of this protocol also makes it a strong candidate for secure, untrusted-relay QKD networks.

The entanglement purification protocol presented in Chapter 7 contributes to the long-term goal of achieving quantum communication at channel capacity. While its full experimental realisation remains challenging, given that capacity is reached only in the asymptotic limit, the scheme could still prove useful in practical scenarios where the generation of high-fidelity entangled states is prioritised over optimal key rates. In such cases, it may be implemented experimentally using a limited number of noisy Bell pairs. The primary challenge lies in the requirement for quantum memories to store and selectively process these states; however, for the development of future quantum networks, such demonstrations will be an

essential step forward.

Looking ahead, an important question is which physical platform DV or CV is best suited to meet the evolving demands of quantum communications. Each approach offers distinct advantages: DV-QKD has demonstrated superior performance over long distances and shows greater resilience to loss, while CV-QKD benefits from higher key rates at short distances and seamless integration with conventional telecommunications infrastructure. However, the choice of platform may ultimately depend on the specific application, network architecture and available technologies. In my view, DV-QKD is the stronger candidate for long-distance communication, particularly because entanglement-swapping measurements are more effective in DV implementations [210, 211, 287–289, 292, 312]. For instance, CV equivalents of MDI-QKD [281] have not demonstrated comparable success in repeater-like scenarios, largely due to their limited effectiveness over long distances. On the other hand, CV-QKD remains highly promising for short-distance applications making it well suited for scenarios such as establishing keys between multiple parties within a local network.

While QKD appears to be the most mature and promising application of quantum communications at present, the long-term goal should extend beyond point-to-point key distribution. Numerous large-scale initiatives are already underway to bring QKD into practical use, including OPENQKD in Europe, the UK Quantum Communications Hub, the Italian Quantum Backbone, national testbeds in Germany as well as large-scale efforts in South Korea and China. These projects aim to demonstrate the feasibility of QKD in applications ranging from secure government communications to financial services and smart grids. These efforts reflect growing international momentum toward operationalising QKD for everyday use. An excellent overview of these deployments and the broader standardisation landscape can be found in Stanley *et al.* [336].

However, to truly scale secure quantum communications, the next step must be the development of a fully connected quantum internet, one that supports not only key distribution but also quantum networking functions such as entanglement distribution, remote state preparation, and access to distributed quantum computing resources. Achieving this vision requires significant advances in hardware, especially quantum memories as they are essential for enabling entanglement-based quantum repeaters. Most current quantum memories operate outside the telecommunications band, requiring frequency conversion of the quantum signal before storage and this process introduces significant loss and limits efficiency. Moreover, increasing the coherence time of memories is still critical to synchronising entanglement across distant nodes. Overcoming these technological bottlenecks will be just as crucial as improving QKD protocol performance. The future of secure quantum communication will likely be shaped not only by protocols, but by the practical engineering of robust, scalable quantum hardware.

Appendix A

Software Enhanced CV-QKD Background

A.1 Detailed Description of the Experimental Parameters

In this section, we outline the procedure to implement data analysis in our experiments. Table A.1 summarises the experimental parameters for the operational regimes shown in Fig. 5.3. For each regime, the reconciliation efficiency is set to $\beta = 92\%$.

Table A.1: Experimental parameters for each regime. V_{mod}: Modulation variance in shot noise units, W: Eve's variance denoted as W_x and W_p for x and p quadratures, respectively. KR: Key rate

Distance (km)	Transmission	V_{mod} (SNU)[1]	$W_{x/p}$ (SNU)	KR	KR after Alice	KR after Bob
6.03±0.006	0.757±0.0002	12.62±0.009 13.52±0.009	1.02±0.004 1.04±0.004	0.4839±0.005	-	-
15.11±0.007	0.499±0.0002	12.65±0.009 13.63±0.01	1.02±0.002 1.03±0.002	0.1433±0.0028	-	-
29.14±0.008	0.261±0.0001	12.74±0.009 13.52±0.009	1.02±0.001 1.01±0.001	-0.0093 ± 0.0029	0.0025±0.0012	0.0038±0.0011
39.06±0.01	0.166±0.0001	12.58±0.008 13.40±0.009	1.00±0.001 1.00±0.001	0.0099±0.0029	0.0169±0.0020	-

Key to the data analysis is converting from the prepare-and-measure (PM) scheme to the entanglement-based (EB) scheme. This conversion enables the estimation of Eve's information, which in turn allows for calculating the final key rates. To this end, we begin by expressing Bob's raw data after detection, following the experimental setup illustrated in Fig. 5.1

$$x_b^r = \sqrt{T}(g_{e_x} x_a^r + x_t^r + x_{SN}^r) + \sqrt{1-T} x_{E_1}^r, \tag{A.1}$$

where g_{e_x} is the electronic gain of the system and x_a^r represents Alice's raw data, generated by sampling the output of function generators, while x_{SN}^r, $x_{E_1}^r$, and x_t^r correspond to shot

[1] Experimental imperfections cause asymmetry in the x and p quadratures. The first row shows the experimental values for x, while the second row shows the values for p. Empty cells indicate that post-selection was not required. The distance is calculated by assuming a fibre loss of 0.2 dB per kilometre.

noise, channel noise (introduced by Eve), and trusted excess noise, respectively. Alice and Bob's raw data are then calibrated to shot noise units as follows

$$x_a = \frac{x_a^r}{\sqrt{V_{SN} - V_{DN}}}, \tag{A.2a}$$

$$x_b = \frac{x_b^r}{\sqrt{V_{SN} - V_{DN}}}, \tag{A.2b}$$

where V_{SN} and V_{DN} represent the variances of the shot noise and dark noise respectively. After the calibration, Bob's data becomes

$$x_b = \sqrt{T}(g_{e_x} x_a + x_t + x_{SN}) + \sqrt{1-T}x_{E_1}. \tag{A.3}$$

Typically, dark noise is subtracted from the variance of the raw samples. However, given our high dark noise clearance of 20 dB, this correction was not applied. After calibrating the shot noise, the initial PM covariance matrix between Alice and Bob for the x quadrature can be calculated as follows

$$\sigma_{\mathrm{AB}_x}^{\mathrm{PM}} = \begin{pmatrix} V_{a_x} & C_{ab_x} \\ C_{ab_x} & V_{b_x} \end{pmatrix}, \tag{A.4}$$

where V_{a_x} represents Alice's variance $\langle \Delta x_a \Delta x_a \rangle$, C_{ab_x} denotes the covariance between Alice and Bob $\langle \Delta x_a \Delta x_b \rangle = g_{e_x}\sqrt{T}V_{a_x}$, and V_{b_x} is Bob's variance of the homodyne measurement for the x quadrature $\langle \Delta x_b \Delta x_b \rangle$.

After the shot noise calibration, Alice renormalises her data by the electronic gain of the system, g_{e_x}, to reveal the physical states she prepared. The gain is determined by setting the channel transmission to 1, corresponding to no loss, as

$$g_{e_x} = \frac{C_{ab_x}}{V_{a_x}}. \tag{A.5}$$

Notably, this gain also accounts for Bob's homodyne detection efficiencies ($\sim 97.6\%$), where we have taken into account the quantum efficiency of the photodiodes ($\sim 99\%$), mode-matching visibility ($\sim 99.3\%$). The calculated gains for our experiment are $g_{e_x} = 8.33 \pm 0.01$ and $g_{e_p} = 19.59 \pm 0.02$ for the amplitude and phase quadratures, respectively. Using these gains, rescaled covariance matrix for the x quadrature in the PM scheme becomes

$$\sigma_{\mathrm{AB}_x}^{\mathrm{PM}'} = \begin{pmatrix} g_{e_x}^2 V_{a_x} & g_{e_x} C_{ab_x} \\ g_{e_x} C_{ab_x} & V_{b_x} \end{pmatrix} = \begin{pmatrix} V_{mod_x} & C'_{ab_x} \\ C'_{ab_x} & V_{b_x} \end{pmatrix}, \tag{A.6}$$

where $C'_{ab_x} = g_{e_x}^2\sqrt{T}V_{a_x} = \sqrt{T}V_{mod_x}$ and V_{mod_x} represents the rescaled modulation variance of the x quadrature. Similarly, $\sigma_{\mathrm{AB}_p}^{\mathrm{PM}'}$ is also obtained from the expression above for the phase

quadrature. Note that Bob's homodyne variance, V_{b_x}, does not need to be scaled as it already includes the system gain when the measurement is performed. Therefore, Bob's variance becomes

$$\langle \Delta x_b \Delta x_b \rangle = T(g_{e_x}^2 V_{a_x} + \xi_x + 1) + (1-T)W_x = T(V_{mod_x} + \xi_x + 1) + (1-T)W_x. \tag{A.7}$$

Here, W_x denotes Eve's variance while ξ_x represents the variance of the trusted excess noise. In an ideal scenario with no system loss, Bob's variance should be $V_{b_x} = V_{mod_x} + 1$. However, due to noise in the state preparation during our experiment, the variance after the modulators becomes $V_{mod_x} + \xi_x$. Therefore, we model Bob's variance as $V_{b_x} = T(V_{mod_x} + 1 + \xi_x) + (1-T)W_x$ and when $T = 1$, the trusted excess noise, ξ_x and ξ_p for the x and p quadratures can be estimated from

$$\xi_x = V_{b_x} - V_{mod_x} - 1, \tag{A.8a}$$

$$\xi_p = V_{b_p} - V_{mod_p} - 1. \tag{A.8b}$$

The experimental values obtained for these trusted noises are $\xi_x = 0.28 \pm 0.003$ and $\xi_p = 0.40 \pm 0.002$.

For the security analysis, we use the EB scheme [74,119]. For each regime, the EB covariance matrix is obtained by rescaling the PM matrix given in Eq. (A.6) following the method described in Laudenbach *et al.* [236] as below

$$\begin{aligned}\sigma_{\mathrm{AB}}^{\mathrm{EB}} &= \begin{pmatrix} V_{mod_x}+1 & 0 & \sqrt{\frac{V_{mod_x}+2}{V_{mod_x}}}C'_{ab_x} & 0 \\ 0 & V_{mod_p}+1 & 0 & -\sqrt{\frac{V_{mod_p}+2}{V_{mod_p}}}C'_{ab_p} \\ \sqrt{\frac{V_{mod_x}+2}{V_{mod_x}}}C'_{ab_x} & 0 & V_{b_x} & 0 \\ 0 & -\sqrt{\frac{V_{mod_p}+2}{V_{mod_p}}}C'_{ab_p} & 0 & V_{b_p} \end{pmatrix} \\ &= \begin{pmatrix} V_x & 0 & C_x & 0 \\ 0 & V_p & 0 & -C_p \\ C_x & 0 & V_{b_x} & 0 \\ 0 & -C_p & 0 & V_{b_p} \end{pmatrix},\end{aligned} \tag{A.9}$$

where C'_{ab_x} and C'_{ab_p} are equal to $\sqrt{T}V_{mod_x}$ and $\sqrt{T}V_{mod_p}$, respectively [236]. As mentioned in Sec. 5.2.1, $V_x = V_{mod_x} + 1$ and $C_x = \sqrt{T(V_x^2 - 1)}$. For the phase quadrature, the same equations apply with V_{mod_x}, W_x and ξ_x replaced by V_{mod_p}, W_p and ξ_p, respectively. Additionally, when post-selection is applied, V_{mod_x} and V_{mod_p} must be replaced with $\tilde{V}_{mod_x}$ and $\tilde{V}_{mod_p}$, respectively.

A.2 Theoretical Model of Post-selection with Heterodyne Detection

In this section, we present the theoretical model of our protocol when heterodyne measurement is implemented at Bob's station.

A.2.1 Alice's Post-selection

In this case, Alice's data and her post-selection remains unchanged. Therefore, Eqs. (5.5) to (5.7) still hold. However, Bob's data, and therefore the calculation of the secret key, are different. Because Bob performs heterodyne detection, there is an added vacuum noise. Additionally, our theory model also accounts for detector noise and efficiency, necessary to analyse the data collected from Data61 that is presented in Fig. 5.4. Bob's measured variance can be expressed as

$$V_{b_x}^m = \frac{\eta T(V_{mod_x} + 1 + \xi_x) + \eta(1-T)W_x + (1-\eta) + 1}{2} + \xi_d. \tag{A.10}$$

Here, ξ_x is the trusted excess noise attributed to the state preparation, while W_x is Eve's thermal variance in the x quadrature. η represents the detector efficiency and ξ_d is the electronic noise of the detector. Bob's variance in the p quadrature is the same except variables V_{mod_x}, ξ_x and W_x are now replaced with V_{mod_p}, ξ_p and W_p. Note that variance of the quantum state received by Bob is $V_{b_x} = 2V_{b_x}^m - 1$ given by

$$V_{b_x} = \eta T(V_{mod_x} + 1 + \xi_x) + \eta(1-T)W_x + (1-\eta) + 2\xi_d. \tag{A.11}$$

Similarly, the covariance between Alice and Bob going from PM scheme to EB scheme needs to be scaled, where the initial PM covariance matrix (already normalised to the shot noise units) for the heterodyne detection is expressed as

$$\sigma_{\mathrm{AB}_x}^{\mathrm{PM}} = \begin{pmatrix} V_{mod_x} & C'_{ab_x} \\ C'_{ab_x} & V_{b_x}^m \end{pmatrix}, \tag{A.12}$$

where the covariance term C'_{ab_x} is given by $C'_{ab_x} = \sqrt{\eta T/2}V_{mod_x}$. Then the EB representation of the covariance matrix becomes

$$\sigma_{\mathrm{AB}}^{\mathrm{EB}} = \begin{pmatrix} V_{mod_x}+1 & 0 & \sqrt{\frac{2(V_{mod_x}+2)}{V_{mod_x}}}C'_{ab_x} & 0 \\ 0 & V_{mod_p}+1 & 0 & -\sqrt{\frac{2(V_{mod_p}+2)}{V_{mod_p}}}C'_{ab_p} \\ \sqrt{\frac{2(V_{mod_x}+2)}{V_{mod_x}}}C'_{ab_x} & 0 & 2V_{b_x}^m-1 & 0 \\ 0 & -\sqrt{\frac{2(V_{mod_p}+2)}{V_{mod_p}}}C'_{ab_p} & 0 & 2V_{b_p}^m-1 \end{pmatrix}$$
$$= \begin{pmatrix} V_x & 0 & C_x & 0 \\ 0 & V_p & 0 & -C_p \\ C_x & 0 & V_{b_x} & 0 \\ 0 & -C_p & 0 & V_{b_p} \end{pmatrix}. \tag{A.13}$$

When Alice performs post-selection, all instances of V_{mod_x} are replaced by the effective modulation variance $\tilde{V}_{mod_x}$, as calculated using Eq. (5.7). Additionally, $C_x = \sqrt{\eta T(V_x^2-1)}$, where $V_x = V_{mod_x}+1$ without post-selection, and $V_x = \tilde{V}_{mod_x}+1$ when Alice performs Gaussian post-selection.

As Bob performs heterodyne detection, the mutual information is different from the homodyne case. Given that Alice prepares a two-mode squeezed vacuum state in the equivalent EB scenario and sends one arm to Bob [119, 124] while measuring the other with heterodyne detection, her variance of the classical data is $V_{A_x} = (V_x+1)/2$. Bob's heterodyne variance is also $V_{b_x}^m = (V_{b_x}+1)/2$. Since both Bob and Alice perform heterodyne detection in the equivalent EB representation, the covariance terms scales by $1/2$ and becomes $C_x/2$. Therefore, $V_{A_x|B_x} = V_{A_x} - C_x^2/(4V_{b_x}^m)$. The mutual information is then calculated using Eq. (4.36) for x and p quadrature separately and averaged over both quadratures with $I_{AB} = 0.5I_{AB_x} + 0.5I_{AB_p}$.

Similar to the homodyne case, when Alice performs a post-selection, Eve's average and conditional covariance matrices need to scale as the effective modulation variance changes. Eve's average covariance matrix follow Eqs. (5.11) and (5.12). However, her conditional covariance matrix now depends on measurement outcomes of both quadratures instead of one. Therefore, the conditional covariance matrix can be calculated from [236]

$$\sigma_{\mathrm{E_1E_2|B}} = \sigma_{\mathrm{E_1E_2}} - \frac{1}{V_{b_x}+1}\sigma_{c_{eb}}\sigma_{c_{eb}}^T, \tag{A.14}$$

where $\sigma_{E_1E_2}$ is Eve's average covariance matrix from Eq. (5.12) and $\sigma_{c_{eb}}$ is the matrix de-

scribing the covariance terms between Eve and Bob given as

$$\sigma_{c_{eb}} = \begin{pmatrix} \sqrt{\eta T(1-T)}\big(W_x - (V_x + \xi_x)\big) & 0 \\ 0 & \sqrt{\eta T(1-T)}\big(W_p - (V_p + \xi_p)\big) \\ \sqrt{\eta(1-T)}C_{E_x} & 0 \\ 0 & \sqrt{\eta(1-T)}C_{E_p} \end{pmatrix}, \tag{A.15}$$

where C_{E_x} and C_{E_p} are expressed in Sec. 5.2.1. For full derivation of the matrix $\sigma_{c_{eb}}$, refer to Laudenbach *et al.* [236].

Eve's information is bounded by the Holevo bound [89] using Eq. (4.35). The secret key rate is then calculated using

$$K = P_{A_x} P_{A_p} (\beta I_{AB} - I_E), \tag{A.16}$$

where P_{A_x} where P_{A_p} are the probability of success of Alice's post-selection calculated using Eq. (5.6). Note that the total probability of success in the heterodyne case is $P_{A_t} = P_{A_x} \times P_{A_p}$.

A.2.2 Bob's Post-selection

The filter function that Bob uses for heterodyne measurements is given as

$$F_B(x_b, p_b) = \begin{cases} 0 & -c^2 < x_b^2 + p_b^2 < c^2 \\ 1 & \text{elsewhere,} \end{cases} \tag{A.17}$$

where c represents the cut-off parameter of the filter which can take the values from 0 to the largest measurement outcome of Bob. Bob's distribution before the post-selection can be expressed as

$$p_b(x_b, p_b) = \frac{1}{\pi\sqrt{(V_{b_x}+1)(V_{b_p}+1)}} \exp\left[-\frac{x_b^2}{(V_{b_x}+1)} - \frac{p_b^2}{(V_{b_p}+1)} \right]. \tag{A.18}$$

After Bob's post-selection process, the probability of success for a given cut-off can be found from

$$P_B(c) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} F_B(x_b, p_b) p_b(x_b, p_b)\, dx_b dp_b. \tag{A.19}$$

Notably, if $V_{b_x} = V_{b_p}$, the probability of success simplifies to $P_B(c) = \exp\left[-\frac{c^2}{V_{b_x}+1} \right]$. Bob's output distribution after the post-selection process becomes

$$\tilde{p}_b(x_b, p_b) = \begin{cases} 0 & -c^2 < x_b^2 + p_b^2 < c^2 \\ \frac{p_b(x_b, p_b)}{P_B(c)} & \text{elsewhere.} \end{cases} \tag{A.20}$$

Similar to the homodyne case, we avoid using the Gaussian extremality and instead bound Eve's information directly from her density matrices. As described in Sec. 5.2.2, we use Williamson's decomposition [90] to obtain a symplectic matrix, s, and a diagonal matrix, ω. We then further decompose the symplectic matrix, s using Bloch-Messiah decomposition [238] to express s as a series of beamsplitters, squeezers and phase rotations: $s = s_u s_i s_v$ in the covariance matrix notation and $S = S_U S_I S_V$ in the density matrix notation. In our case for Data61's results, both s_u and s_v are both expressed through phase rotations and beamsplitters: $S_U = R(\theta_1, \theta_2)B(\tau_U)R(\theta_3, \theta_4)$ and $S_V = R(\theta_5, \theta_6)B(\tau_V)R(\theta_7, \theta_8)$, where each parameter needs to be solved. The s_i component is expressed through two-mode squeezing operations, $S_I = S(r_1, r_2)$. Therefore, Eve's overall conditional density matrix is written in terms of the symplectic density matrix S and a mixed thermal state Λ

$$\rho_{\mathrm{E_1E_2|B}} = S\Lambda S^\dagger. \tag{A.21}$$

Note that $\rho_{\mathrm{E_1E_2|B}}$ in Eq. (A.21) does not provide any information about Bob's measurement outcomes, therefore, we assume that the conditional matrix is centred at zero. We then apply a displacement operator on the conditional matrix centred at zero to determine Eve's conditional density matrix for each measurement outcome Bob gets.

$$\rho_{\mathrm{E_1E_2|B}}(x_b, p_b) = D(\alpha_1(x_b, p_b), \alpha_2(x_b, p_b))\rho_{\mathrm{E_1E_2|B}}(x_b = 0, p_b = 0)D^\dagger(\alpha_1(x_b, p_b), \alpha_2(x_b, p_b)), \tag{A.22}$$

where $D(\alpha_1(x_b, p_b), \alpha_2(x_b, p_b))$ represents the displacement operator for Eve's modes 1 and 2 in the form of

$$D(\alpha_1(x_b, p_b), \alpha_2(x_b, p_b)) = \exp\Big(\alpha_1(x_b, p_b)a^\dagger - \alpha_1(x_b, p_b)a\Big) \otimes \exp\Big(\alpha_2(x_b, p_b)a^\dagger - \alpha_2(x_b, p_b)a\Big), \tag{A.23}$$

where α_1 and α_2 are functions of Eve's conditional means based on Bob's measurement outcomes, x_b and p_b. These conditional means for Eve are calculated from

$$\mu_{\mathrm{E_1E_2}}(x_b, p_b) = \frac{\sigma_c}{\sqrt{2}} \begin{pmatrix} V_{b_x}^m & 0 \\ 0 & V_{b_p}^m \end{pmatrix}^{-1} \begin{pmatrix} x_b \\ p_b \end{pmatrix}. \tag{A.24}$$

The values of α_1 and α_2 are calculated from $\alpha_1(x_b, p_b) = (\mu_{\mathrm{E_1}}(x_b) + i\mu_{\mathrm{E_1}}(p_b))/2$ and $\alpha_2(x_b, p_b) = (\mu_{\mathrm{E_2}}(x_b) + i\mu_{\mathrm{E_2}}(p_b))/2$ where $\mu_{\mathrm{E_1}}(x_b)$, $\mu_{\mathrm{E_1}}(p_b)$, $\mu_{\mathrm{E_2}}(x_b)$ and $\mu_{\mathrm{E_2}}(p_b)$ correspond to rows 1 to 4 of $\mu_{\mathrm{E_1E_2}}(x_b, p_b)$, respectively.

Even though each conditional state has the same entropy, they contribute differently to Eve's average state due to the varying probabilities of obtaining each conditional state. To determine Eve's average density matrix, we multiply each conditional state by its corre-

sponding probability from Bob's post-selected probability distribution and then sum them all. Bob's probability of obtaining a given outcome is calculated from

$$p'_b(x_i, p_j) = \int_{p_j-\Delta}^{p_j+\Delta} \int_{x_i-\Delta}^{x_i+\Delta} \tilde{p}_b(x_i, p_j)\, dx_b dp_b, \tag{A.25}$$

where Δ is the width of the bins and in our results $\Delta = 0.25$ for the heterodyne detection data. Summing over all the possible outcomes of Bob, Eve's average state becomes

$$\rho_{\mathrm{E_1E_2}} = \sum_{p_j=-n_p}^{n_p} \sum_{x_i=-n_x}^{n_x} p'_b(x_i, p_j) \rho_{\mathrm{E_1E_2|B}}(x_i, p_j), \tag{A.26}$$

where n_x and n_p are the maximum number that Bob measures and $p'_b(x_i, p_j)$ denotes Bob's probability of getting a given outcome, x_i and p_j. Eve's information then can be calculated from

$$I_E = S(\rho_{\mathrm{E_1E_2}}) - S(\rho_{\mathrm{E_1E_2|B}}(0,0)), \tag{A.27}$$

where $S(\rho_{\mathrm{E_1E_2}})$ represents the von Neumann entropy for Eve's average state while $S(\rho_{\mathrm{E_1E_2|B}}(0,0))$ gives the von Neumann entropy of Eve's conditional state given Bob measures $x_b = 0$ and $p_b = 0$.

In order to calculate Alice and Bob's mutual information after Bob's post-selection, we fit Alice and Bob's data to the following multivariate Gaussian distribution

$$f_{AB}(x_a, p_a, x_b, p_b) = \frac{1}{\sqrt{(2\pi)^k |\sigma^C_{\mathrm{AB}}|}} \exp\left[-\frac{1}{2} v^T (\sigma^C_{\mathrm{AB}})^{-1} v \right], \tag{A.28}$$

where $|\sigma^C_{\mathrm{AB}}|$ represents the determinant of the joint covariance matrix between Alice and Bob's classical variables. v is a k-dimensional column vector given as $v = (x_a, p_a, x_b, p_b)$ and therefore, $k = 4$. The classical covariance matrix between Alice and Bob is given as

$$\sigma^C_{\mathrm{AB}} = \begin{pmatrix} (V_x+1)/2 & 0 & C_x/2 & 0 \\ 0 & (V_x+1)/2 & 0 & -C_p/2 \\ C_x/2 & 0 & (V_{b_x}+1)/2 & 0 \\ 0 & -C_p/2 & 0 & (V_{b_p}+1)/2 \end{pmatrix}. \tag{A.29}$$

Using Eq. (A.28), we generate a probability table between Alice and Bob for each values of x_a, x_b, p_a and p_b where x_a and p_a range from -14 to 14 with increments of $\Delta = 0.25$, while x_b and p_b range from -8 to 8 with increments of the same width. The mutual information is then calculated using

$$I_{AB} = H_A + H_B - H_{AB}, \tag{A.30}$$

where the joint entropy between Alice and Bob, H_{AB} is computed from

$$H_{AB} = -\sum_{x_a=-n_a}^{n_a}\sum_{p_a=-n_a}^{n_a}\sum_{x_b=-c}^{c}\sum_{p_b=-\sqrt{c^2-x_b^2}}^{\sqrt{c^2-x_b^2}} \frac{f_{AB}(x_a,p_a,x_b,p_b)}{P_B(c)} \log_2\left[\frac{f_{AB}(x_a,p_a,x_b,p_b)}{P_B(c)}\right], \tag{A.31}$$

where n_a represents the maximum number that Alice prepares. In order to compute H_A, we need to obtain Alice's probabilities after Bob's post-selection

$$f_A(x_a,p_a) = \frac{1}{P_B(c)}\sum_{x_b=-c}^{c}\sum_{p_b=-\sqrt{c^2-x_b^2}}^{\sqrt{c^2-x_b^2}} f_{AB}(x_a,p_a,x_b,p_b). \tag{A.32}$$

H_A is then expressed as

$$H_A = -\sum_{x_a=-n_a}^{n_a}\sum_{p_a=-n_a}^{n_a} f_A(x_a,p_a)\log_2[f_A(x_a,p_a)]. \tag{A.33}$$

Similarly, Bob's probability from the probability table after his post-selection becomes

$$f_B(x_b,p_b) = \frac{1}{P_B(c)}\sum_{x_a=-n_a}^{n_a}\sum_{p_a=-n_a}^{n_a} f_{AB}(x_a,p_a,x_b,p_b). \tag{A.34}$$

Using Eq. (A.34), Bob's entropy is computed as

$$H_B = -\sum_{x_b=-c}^{c}\sum_{p_b=-\sqrt{c^2-x_b^2}}^{\sqrt{c^2-x_b^2}} f_B(x_b,p_b)\log_2[f_B(x_b,p_b)]. \tag{A.35}$$

A.2.3 Calculation of the Secret Key Rate

When both Alice and Bob perform post-selection, the key rate is computed from

$$K = P_B P_{A_x} P_{A_p}(\beta I_{AB} - I_E), \tag{A.36}$$

where P_B denotes probability of success of Bob's post-selection and, P_{A_x} and P_{A_p} are the probability of success of Alice's post-selection for the x and p quadratures, respectively.

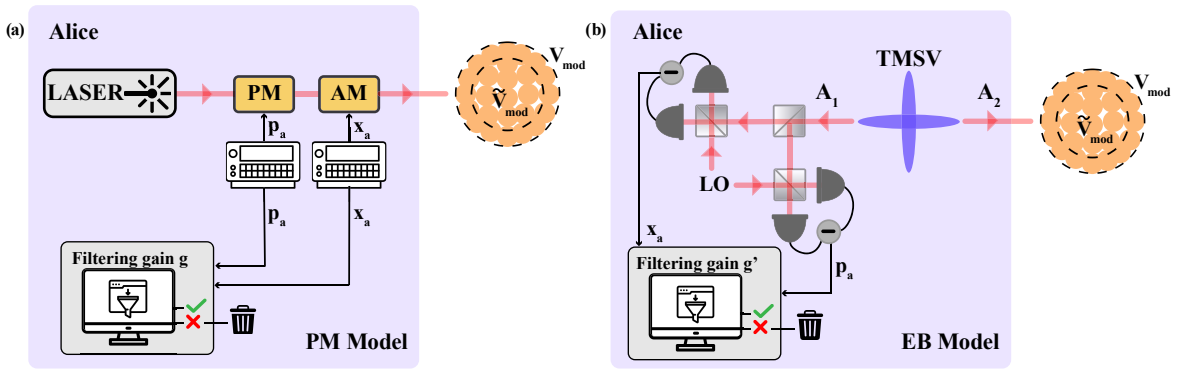

Figure A.1: The equivalence between the prepare-and-measure and entanglement-based models for Alice's post-selection. (a) Alice encodes coherent states $|(x_a + ip_a)/2\rangle$ from a Gaussian distribution with zero mean and variance, V_{mod}, using white noise generated by function generators. She samples x_a and p_a simultaneously. After data acquisition and once the states have been sent to Bob, Alice applies a Gaussian filter to her measurement outcomes with a filter gain, g. This shrinks the initial thermal state with a modulation variance of V_{mod} to $\tilde{V}_{mod}$. **(b)** Alice prepares a two-mode squeezed vacuum (TMSV) state with initial variance $V = V_{mod} + 1$ and zero mean. She performs heterodyne detection on mode A_1, followed by a Gaussian filter with gain g'. As a result, mode A_2 is projected onto a thermal state with zero mean and an effective modulation variance $\tilde{V}_{mod}$.

A.3 The Equivalence between the Entanglement-Based and Prepare-and-Measure Schemes

In this section, we derive the EB representation corresponding to Alice's post-selection in the PM scheme as shown in Fig. A.1(a). Alternatively, one can begin with the EB model to construct an equivalent experimental description of Alice's post-selection process. In Fig. A.1(b), Alice prepares a TMSV state and performs a heterodyne measurement on one mode, labeled A_1, while sending the other mode, A_2, to Bob. This measurement projects mode A_2 onto a thermal state with zero mean and variance V. The resulting covariance matrix after Alice's measurement is given by

$$\sigma^{EB}_{A_1A_2}(V) = \begin{pmatrix} \frac{V+1}{2}\mathbb{I}_2 & \sqrt{\frac{V^2-1}{2}}\sigma_z \\ \sqrt{\frac{V^2-1}{2}}\sigma_z & V\mathbb{I}_2. \end{pmatrix} \tag{A.37}$$

For simplicity, we initially assume symmetric variance in both quadratures. The model is later extended to incorporate asymmetric quadrature variances. The joint Gaussian distri-

bution corresponding to $\sigma^{\mathrm{EB}}_{A_1A_2}$ is given by

$$P_{A_1A_2}(V,x_a,p_a,x_b,p_b)=\frac{1}{\sqrt{4\pi^2|\sigma^{EB}_{A_1A_2}(V)|}}\exp\left[-\frac{1}{2}(x_a,p_a,x_b,p_b)\sigma^{EB^{-1}}_{A_1A_2}(V)(x_a,p_a,x_b,p_b)^T\right]. \tag{A.38}$$

When the quadratures are symmetric, Alice applies the following filter with an effective gain g'. This gain must be chosen to ensure consistency with the PM model derivation presented in Sec. 5.2.1. Therefore, Alice's filter is given by

$$F_A(x_a,p_a,g')=e^{-g'^2(x_a^2+p_a^2)}. \tag{A.39}$$

Applying the filter on A_1, gives the following probability of success

$$P_{A_t}(V,g')=\iiiint F_A(x_a,p_a,g')P_{A_1A_2}(V,x_a,p_a,x_b,p_b)\,d_{x_a}d_{p_a}d_{x_b}d_{p_b}=\frac{1}{g'^2(V+1)+1}, \tag{A.40}$$

where setting $g'=g\sqrt{\frac{2(V-1)}{(V+1)}}$ and $V-1=V_{mod}$ gives

$$P_{A_t}(V_{mod},g)=\frac{1}{2g^2V_{mod}+1}. \tag{A.41}$$

Recall that in the case of asymmetric quadratures, Alice's total success probability is given by $P_t=P_{A_x}\times P_{A_p}$, where P_{A_x} and P_{A_p} are defined in Eq. (5.6).

$$\begin{aligned}P_t(V_{mod_x},V_{mod_p},g_x,g_p)&=P_{A_x}(V_{mod_x},g_x)\times P_{A_p}(V_{mod_p},g_p)\\&=\frac{1}{\sqrt{2g_x^2V_{mod_x}+1}}\times\frac{1}{\sqrt{2g_p^2V_{mod_p}+1}},\end{aligned} \tag{A.42}$$

Setting $V_{mod_x}=V_{mod_p}=V_{mod}$ and $g_x=g_p=g$ gives the total probability of success as

$$P_t(V_{mod},g)=\frac{1}{2g^2V_{mod}+1}, \tag{A.43}$$

which matches Eq. (A.41). After Alice's post-selection the output joint distribution is expressed as

$$\tilde{P}_{A_1A_2}(V,x_a,p_a,x_b,p_b,g')=\frac{F_A(x_a,p_a,g')\times P_{A_1A_2}(V,x_a,p_a,x_b,p_b)}{P_{A_t}(V,g')}. \tag{A.44}$$

Integrating over mode A_1 gives the distribution of A_2 as

$$\tilde{P}_{A_2}(V,x_b,p_b,g')=\iint\tilde{P}_{A_1A_2}(V,x_a,p_a,x_b,p_b,g')\,d_{x_a}d_{p_a}, \tag{A.45}$$

which is used to determine the new thermal variance of A_2 after Alice's post-selection as

$$\tilde{V}(V,g') = \iint xb^2 \tilde{P}_{A_2}(V,x_b,p_b,g')d_{x_b}d_{p_b} = \frac{V+g'^2(V+1)}{g'^2(V+1)+1}. \tag{A.46}$$

As $\tilde{V}_{mod} = \tilde{V} - 1$ and $g' = g\sqrt{\frac{2(V-1)}{(V+1)}}$, the new modulation variance becomes

$$\begin{aligned} \tilde{V}_{mod}(V,g') &= \tilde{V}(V,g') - 1 \\ &= \frac{V-1}{g'^2(V+1)+1}, \\ \tilde{V}_{mod}(V_{mod},g) &= \frac{V_{mod}}{2g^2V_{mod}+1}, \end{aligned} \tag{A.47}$$

which is exactly the same as the modulation variance we derived in Eq. (5.7).

When the modulation variances are asymmetric due to experimental imperfections, this corresponds to Alice preparing a TMSV-like state in the EB scheme with unequal quadrature variances. Specifically, she generates two squeezed states with squeezing parameters r_1 and r_2 in the x and p quadratures, respectively. Upon performing a measurement on mode A_1, mode A_2 is projected into a thermal state with zero mean and variances V_x and V_p along the x and p quadratures. The effective covariance matrix then becomes

$$\sigma^{EB}_{A_1A_2}(V_x,V_p) = \begin{pmatrix} \frac{V_x+1}{2} & 0 & \sqrt{\frac{V_x^2-1}{2}} & 0 \\ 0 & \frac{V_p+1}{2} & 0 & -\sqrt{\frac{V_p^2-1}{2}} \\ \sqrt{\frac{V_x^2-1}{2}} & 0 & V_x & 0 \\ 0 & -\sqrt{\frac{V_p^2-1}{2}} & 0 & V_p \end{pmatrix}, \tag{A.48}$$

where the joint distribution now depends on the variances V_x and V_p, and has the same functional form as Eq. (A.38). We denote the asymmetric distribution as $P_{A_1A_2}(V_x,V_p,x_a,p_a,x_b,p_b)$. Alice's filter, modified to accommodate this asymmetry, can be written as

$$F_A(x_a,p_a,g'_x,g'_p) = e^{-(g'^2_x x_a^2 + g'^2_p p_a^2)}, \tag{A.49}$$

where g'_x and g'_p correspond to the effective gains applied to the x and p quadratures, respectively, in the asymmetric filtering scheme. The probability of success when Alice applies this filter to her measurement outcomes x_a and p_a becomes

$$\begin{aligned} P_{A_t}(V_x,V_p,g'_x,g'_p) &= \iiiint F_A(x_a,p_a,g'_x,g'_p)P_{A_1A_2}(V_x,V_p,x_a,p_a,x_b,p_b) \\ &= \frac{1}{\sqrt{(g'^2_x(V_x+1)+1)(g'^2_p(V_p+1)+1)}}. \end{aligned} \tag{A.50}$$

By setting $g'_x = g_x\sqrt{\frac{2(V_x-1)}{(V_x+1)}}$, $g'_p = g_p\sqrt{\frac{2(V_p-1)}{(V_p+1)}}$, and defining the modulation variances as $V_{mod_x} = V_x - 1$ and $V_{mod_p} = V_p - 1$, the probability of success becomes

$$\begin{aligned} P_{A_t}(V_x, V_p, g_x, g_p) &= \frac{1}{\sqrt{(2g_x^2(V_x-1)+1)(2g_p^2(V_p-1)+1)}} \\ P_{A_t}(V_{mod_x}, V_{mod_p}, g_x, g_p) &= \frac{1}{\sqrt{(2g_x^2 V_{mod_x}+1)(2g_p^2 V_{mod_p}+1)}}, \end{aligned} \tag{A.51}$$

which is exactly the same as the PM model and Eq. (A.42). After the post-selection process, the distribution of A_2 becomes

$$\tilde{P}_{A_2}(V_x, V_p, x_b, p_b, g'_x, g'_p) = \iint \tilde{P}_{A_1A_2}(V_x, V_p, x_a, p_a, x_b, p_b, g'_x, g'_p)\, d_{x_a} d_{p_a}, \tag{A.52}$$

then the thermal variance of A_2 is given by

$$\tilde{V_x}(V_x, g'_x) = \iint x b^2 \tilde{P}_{A_2}(V_x, V_p, x_b, p_b, g'_x, g'_p) d_{x_b} d_{p_b} = \frac{V_x + g_x'^2(V_x+1)}{g_x'^2(V_x+1)+1}. \tag{A.53}$$

As $\tilde{V}_{mod_x} = \tilde{V_x} - 1$ and $g'_x = g_x\sqrt{\frac{2(V_x-1)}{(V_x+1)}}$, the new modulation variance for the x quadrature becomes

$$\tilde{V}_{mod_x}(V_x, g'_x) = \frac{V_x - 1}{2g_x^2(V_x-1)+1} = \frac{V_{mod_x}}{2g_x^2 V_{mod_x}+1}, \tag{A.54}$$

which is equal to the modulation variance given in Eq. (5.7).

A.4 Parameters of the Satellite-to-Ground Simulation and duty cycle estimation

The results presented in Fig. 5.6 is calculated using the model described by Sayat *et al.* [129] where the parameters used in the model are described in Table A.2. For an optical ground state elevation of 0 km, the system can be visualized as illustrated in Fig. A.2. A satellite in Low Earth Orbit (LEO), traveling at an average speed of 7.6 km/s [337], typically completes 15 orbits around the Earth in a single day. During this period, the satellite is visible from the ground station for approximately 3 hours. Consequently, 100% duty cycle of secret key rate (SKR) delivery corresponds to 3 hours, irrespective of the tolerable minimum SKR. In the results shown in Fig. 5.6, we assume the minimum tolerable secret key rate (or threshold SKR) to be 10^{-4} bits per use. The duty cycle is determined by calculating the ratio of two arc lengths: the first from the zenith to the satellite at the altitude where the secret key rate exceeds the 10^{-4} bits/use threshold, and the second from the zenith to the horizon. Upon

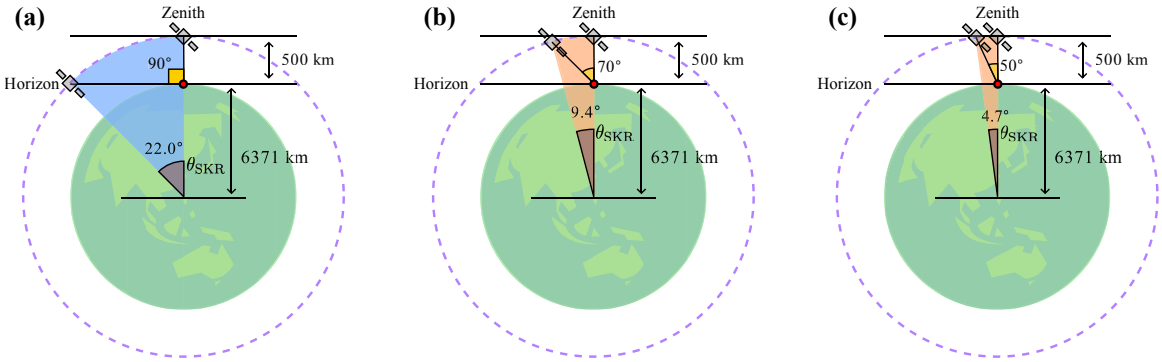

Figure A.2: Satellite to ground model used in calculating the results presented in Fig. 5.6. The satellite orbit is indicated by the purple dashed line and the red dot represents the optical ground station. **(a)** shows the geometric setting used to compute the duty cycle of our protocol. Regardless of weather conditions, the maximum zenith angle (shaded in yellow) where the secure key rate (SKR) exceeds 10^{-4} bits/use is $90°$. Notably, our protocol achieves SKR delivery throughout the entire 3-hour window, which represents the maximum possible transmission window for any QKD protocol (CV-QKD or DV-QKD) in this scenario, resulting in a 100% duty cycle. Figures **(b)** and **(c)** illustrate the model used to assess the duty cycle of a conventional GG02 protocol under good and bad weather conditions, respectively. In favorable weather, GG02 attains maximum zenith angles of approximately $70°$, yielding a duty cycle of approximately 43%. This drops to 21% in adverse weather due to a reduced maximum zenith angle of $50°$. The model incorporates the parameters outlined in Table A.2. It is important to emphasize that the aspect ratio between element dimensions and lengths depicted in the figure are not precise. The representation has been adjusted to represent the model succinctly. As a consequence the zenith angles look inaccurate. However, the stated values are accurate and employed in the duty cycle calculations.

simplification, the duty cycle is given by

$$\text{Duty cycle} = \frac{\theta_{\text{SKR}}}{22°} \times 100\%, \tag{A.55}$$

where the angle θ_{SKR} is the angle made between the satellite and the zenith with respect to the centre of the Earth. θ_{SKR} can be calculated from the elevation angle ϵ (= $90°-$ zenith angle) when the SKR crosses 10^{-4} bits per use and is given by

$$\theta_{\text{SKR}} = [90 - \epsilon] - \sin^{-1}\left[\cos[\epsilon]\frac{R_E}{R_E + L_{zen}}\right]. \tag{A.56}$$

Table A.2: Parameters of the Satellite-to-ground communication model in Fig. 5.6.

Radius of the Earth, R_E (km)	6371
Satellite Altitude at Zenith, L_{zen} (km)	500
Optical Ground Station Elevation, L_{OGS} (km)	0
Transmitter Aperture Diameter, D_t (m)	0.3
Receiver Aperture Diameter, D_r (m)	1
Transmitter Optics Efficiency, T_t	0.9
Receiver Optics Efficiency, T_r	0.9
Pointing Loss Efficiency, L_p	0.1
Atmosphere Thickness, L_{atm} (km)	20
Visibility, V (km)	20 km for bad weather conditions 200 km for good weather conditions
Refractive Index Structure Parameter, C_n^2 ($m^{-2/3}$)	10^{-13} for bad weather conditions 10^{-16} for good weather conditions
Probability Threshold, p_{th}	10^{-6}
Wavelength, λ (nm)	1550
Modulation Variance, V_{mod} (SNU)	8
Detector Efficiency, η (%)	90%
Detector Noise, ϵ_{det} (SNU)	0.0135
Excess Channel Noise, ϵ_{ch} (SNU)	0.0186
Detection Type	Homodyne
Reconciliation Efficiency, β (%)	90%

Appendix B

Photon-Number Encoded Measurement-Device-Independent QKD Protocol Background

B.1 Estimating Eve's Information Using Quantum Tomography with Single-Photon States

In this section, we show how Alice and Bob can estimate their joint state conditioned on Charlie's measurement outcome to bound Eve's information.

Alice and Bob measure their joint state in the X, Y and Z bases in the entanglement-based scheme as introduced in Sec. 6.2.3 to construct the statistics of their matched and unmatched results. From the probabilities measured in these bases, Alice and Bob can estimate their joint state. Writing their joint state as

$$\hat{\rho}_{\mathrm{AB}|c=1} = \frac{1}{4}\big(\mathbb{1}_4 + \vec{s}_a \cdot \vec{\sigma}_a + \vec{s}_b \cdot \vec{\sigma}_b + \sum_{j,k} r_{jk}(\sigma_j \otimes \sigma_k)\big), \tag{B.1}$$

where $\vec{s}_a \cdot \vec{\sigma}_a$ and $\vec{s}_b \cdot \vec{\sigma}_b$ describe Alice and Bob's reduced states calculated from their local measurements, while $r_{jk}(\sigma_j \otimes \sigma_k)$ gives the correlations between Alice and Bob determined from their measurements performed in the bases $j = \{X, Y, Z\}$ and $k = \{X, Y, Z\}$, where r_{jk} is the correlation coefficient and σ_j and σ_k are the standard Pauli matrices σ_X, σ_Y and σ_Z. The terms $\vec{s}_a \cdot \vec{\sigma}_a$ and $\vec{s}_b \cdot \vec{\sigma}_b$ can be expressed as

$$\vec{s}_a \cdot \vec{\sigma}_a = a_X(\sigma_X \otimes \mathbb{1}_2) + a_Y(\sigma_Y \otimes \mathbb{1}_2) + a_Z(\sigma_Z \otimes \mathbb{1}_2), \tag{B.2}$$

$$\vec{s}_b \cdot \vec{\sigma}_b = b_X(\mathbb{1}_2 \otimes \sigma_X) + b_Y(\mathbb{1}_2 \otimes \sigma_Y) + b_Z(\mathbb{1}_2 \otimes \sigma_Z), \tag{B.3}$$

where $\{a_X, a_Y, a_Z\}$ and $\{b_X, b_Y, b_Z\}$ represent the coefficients given in Eq. (B.7) and (B.8) when Alice and Bob measure in the bases $j = \{X, Y, Z\}$.

When Alice and Bob measure their own qubits in any basis $j = \{X, Y, Z\}$, their measure-

ment outcomes can be expressed as

$$\Pi_{\pm j} = |\pm j\rangle\langle\pm j|\,, \tag{B.4}$$

which can be calculated using the eigenvectors of the X, Y and Z bases as defined previously in Eq. (6.12a), (6.12b) and (6.12c). The probability of their measurement then can be calculated from

$$P_a(\pm j) = \mathrm{Tr}\big[(\Pi_{\pm j}\otimes\mathbb{1}_2)\rho_{\mathrm{AB}|c=1}(\Pi_{\pm j}\otimes\mathbb{1}_2)^\dagger\big], \tag{B.5}$$

$$P_b(\pm j) = \mathrm{Tr}\big[(\mathbb{1}_2\otimes\Pi_{\pm j})\rho_{\mathrm{AB}|c=1}(\mathbb{1}_2\otimes\Pi_{\pm j})^\dagger\big], \tag{B.6}$$

where $\rho_{AB|c=1}$ is determined from Eq. (6.19).

The coefficients in Eq. (B.2) and (B.3) can computed from Eq. (B.5) and (B.6) where

$$a_j = P_a(+j) - P_a(-j), \tag{B.7}$$

$$b_j = P_b(+j) - P_b(-j). \tag{B.8}$$

In order to determine the correlation coefficients r_{jk}, Alice and Bob construct a joint probability table of their measurements in all the bases where these probabilities are calculated from

$$P(a{=}\pm j, b{=}\pm k){=}\mathrm{Tr}\big[(\Pi_{\pm j}\otimes\Pi_{\pm k})\rho_{\mathrm{AB}|c=1}(\Pi_{\pm j}\otimes\Pi_{\pm k})^\dagger\big]. \tag{B.9}$$

Using Eq. (B.9), the correlation coefficients become

$$r_{jk} = P(a{=}{+}j, b{=}{+}k) + P(a{=}{-}j, b{=}{-}k) - P(a{=}{+}j, b{=}{-}k) - P(a{=}{-}j, b{=}{+}k). \tag{B.10}$$

After Alice and Bob reconstruct their estimated joint matrix $\hat{\rho}_{\mathrm{AB}|c=1}$, they can estimate Eve's information using the Holevo bound as given in Eq. (6.23).

B.2 Classical Protocol Used to Optimise the Coefficients of the High Dimensional States

This section describes how the states that Alice and Bob prepare are chosen. The coefficients of these states are determined based on the following classical protocol. We assume Eve taps off the signal sent by Alice and Bob, and measures the number of photons denoted as n_{e_a} and n_{e_b}. Then we maximise the average difference in mutual information

$$\max_{\{P(n_a),P(n_b)\}}\left[\sum_{c=0}^{2n_{\max}} P_c(n_c)\big(I_{AB|c} - I_{AE|c}\big)\right], \tag{B.11}$$

where $I_{AB|c}$ and $I_{AE|c}$ are Alice and Bob's mutual information and mutual information between Alice and Eve conditioned on Charlie's measurement outcome, respectively. $P(n_c)$ represents the probability of Charlie measuring n_c photons in total. Note that $P(n_a)$ and $P(n_b)$ are related to the optimised coefficients from Eq. (6.2) and (6.3) as they are the probability of sending n photons for the corresponding Fock-number state $|n\rangle$, also expressed as a_n and b_n throughout Chapter 6.

In the classical protocol, Charlie measures the number of photons coming from Alice and Bob individually with two separate PNRDs. In Fock basis, both classical and quantum simulations yield the same probabilities for Charlie's measurement outcome. The probability of Charlie measuring n_{c_a} or n_{c_b} photons on Alice's and Bob's mode individually can be computed as

$$P_{c_a}(n_{c_a}) = \sum_{n_a=0}^{n_{\max}} \binom{n_a}{n_{c_a}} \tau_{\mathrm{A}}^{n_{ca}} (1-\tau_{\mathrm{A}})^{n_a - n_{ca}} P(n_a), \tag{B.12}$$

where $n_{\max}$ refers to the maximum number of photons Alice and Bob are sending individually. τ_{A} is the probability of a photon arriving at Charlie from Alice or Bob as a function of the fibre distance with $\tau_{\mathrm{A}} = 10^{-0.02d}$. $(1-\tau_{\mathrm{A}})^{n_a - n_{ca}}$ is the probability of losing $n_a - n_{c_a}$ photons to Eve. The probability of the collective photon number measurement performed by Charlie for a given number of photons n_c can be calculated using Eq. (B.12) as shown below

$$P_c(n_c) = \sum_{n_{ca}=0}^{n_c} P_{c_a}(n_{c_a}) P_{c_b}(n_c - n_{c_a}), \tag{B.13}$$

where $n_c - n_{c_a}$ gives the number of photons measured on Bob's mode.

Alice and Bob's mutual information conditioned on Charlie's measurement outcome is obtained from the probability table between Alice and Bob which is as follows

$$P(n_a, n_b|n_c) = \binom{n_a + n_b}{n_c} \frac{\tau^{n_c}(1-\tau)^{n_a+n_b-n_c} P(n_a) P(n_b)}{P_c(n_c)}, \tag{B.14}$$

where $n_a + n_b$ is equal to the total number of photons in the system and τ in the equation above corresponds to the transmission probability in one channel only. We evaluate Alice and Bob's mutual information conditioned on Charlie's measurement outcome from the same approach shown in Sec. 6.2.4 using $I_{AB|c} = H(A|c) + H(B|c) - H(AB|c)$ and Eq. (6.22a), (6.22b) and (6.22c).

We quantify Eve's information conditioned on each photon measurement in a similar fashion to Alice and Bob's mutual information using $I_{E|c} = H(A|c) + H(E|c) - H(AE|c)$. Since Eve has access to both channels between Alice and Charlie and Charlie and Bob, we need to consider events where each party loses photons to Eve. We compute the probability table between Alice, Bob and the two modes of Eve conditioned on Charlie's outcome as

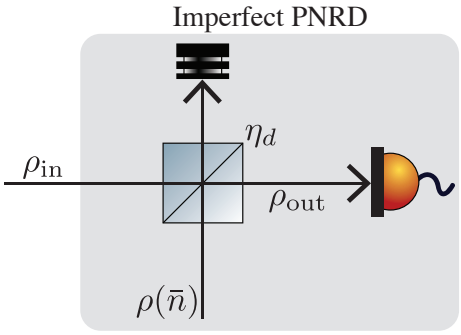

Figure B.1: Diagram of the method used to simulate the effect of dark counts in the PNRDs. ρ_{in} is the density matrix of the input state. The grey box represents a realistic photon number resolving detector with efficiency η_d and dark noise $(1-\eta_d)\bar{n}$.

follows

$$P(n_a, n_b, n_{e_a}, n_{e_b}|n_c) = \frac{1}{P_c(n_c)} \binom{n_a}{n_{e_a}} \binom{n_b}{n_{e_b}} \tau^{n_a+n_b-(n_{e_a}+n_{e_b})} (1-\tau)^{n_{e_a}+n_{e_b}} P(n_a) P(n_b), \tag{B.15}$$

provided $n_a + n_b - (n_{e_a} + n_{e_b}) = n_c$, where n_{e_a} and n_{e_b} are the photons lost to Eve by Alice and Bob, respectively, and $n_a + n_b - (n_{e_a} + n_{e_b})$ corresponds to the total number of photons measured by Charlie. Therefore, using the probability table between Alice, Bob and Eve, we can calculate the entropies below to compute Eve's information

$$H(E_{\text{A}}E_{\text{B}}|c) = -\sum_{n_{e_a}=0}^{n_{\max}} \sum_{n_{e_b}=0}^{n_{\max}} P(n_{e_a}, n_{e_b}|c) \log_2 P(n_{e_a}, n_{e_b}|c), \tag{B.16a}$$

$$H(AE_{\text{A}}E_{\text{B}}|c) = -\sum_{n_a=0}^{n_{\max}} \sum_{n_{e_a}=0}^{n_{\max}} \sum_{n_{e_b}=0}^{n_{\max}} P(n_a, n_{e_a}, n_{e_b}|c) \log_2 P(n_a, n_{e_a}, n_{e_b}|c). \tag{B.16b}$$

B.3 Modelling Dark Noise and Detector Efficiency

This section describes how to model the dark noise and detector efficiency at Charlie's photon number resolving detectors to achieve the results of Fig. 6.6 and the single-photon sources heralded by these detectors. The effects of dark noise is modelled by interacting the incoming state with a thermal state at a beamsplitter as in Fig. B.1.

The efficiency of the single photon detection in this framework is the transmissivity of the beamsplitter (τ), i.e., $\eta_d = \tau$. The density matrix of the state to be detected can be written down as

$$\rho_{\text{out}} = B(\eta_d)(\rho_{\text{in}} \otimes \rho(\bar{n}))B(\eta_d)^\dagger, \tag{B.17}$$

where $\rho(\bar{n})$ is the density matrix of the thermal state. The beamsplitter transformation is

shown in Eq. (2.56). The density matrix of the thermal state is given by

$$\rho(\bar{n}) = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(1+\bar{n})^{n+1}} |n\rangle\langle n| \,, \tag{B.18}$$

where $\bar{n} = \mathrm{Tr}[\rho(\bar{n})a^\dagger a]$ is the mean photon number of the thermal state. Consequently, the dark count is given by $(1-\eta_d)\bar{n}$. For low dark counts, the summation in Eq. (B.18) can be truncated accordingly.

B.4 Coefficients of the Optimised States

In this section, we present some of the coefficients of the optimised states with $n_{\max} = 7$ and $n_{\max} = 1$ photons used in Fig. 6.2(a) and (b) for each distance in Tables B.1 and B.2, correspondingly. These coefficients represent the probability of sending the corresponding Fock-number state. We give the values of the optimised squeezing parameters of the states given in Eq. (6.1) with $n_{\max} = 7$ photons for each distance used in Fig. 6.2(a) in Table B.3. In Table B.4, we present the coefficients of the optimised single-photon states shown in Fig. 6.6.

Table B.1: The coefficients of the optimised states with $n_{\max} = 7$ photons.

Distance (km)	a_0 b_0	a_1 b_1	a_2 b_2	a_3 b_3	a_4 b_4	a_5 b_5	a_6 b_6	a_7 b_7
0	0.0823	0.1162	0.1432	0.1582	0.1582	0.1432	0.1162	0.0823
0.5	0.1073	0.1359	0.1557	0.1603	0.1496	0.1267	0.0968	0.0676
1	0.1226	0.1472	0.1616	0.1600	0.1438	0.1174	0.0868	0.0605
2.5	0.1550	0.1705	0.1710	0.1567	0.1307	0.0994	0.0691	0.0477
5	0.1967	0.2012	0.1786	0.1483	0.1129	0.0787	0.0508	0.0329
10	0.4468	0.3137	0.1410	0.0601	0.0245	9.4433×10^{-3}	3.3895×10^{-3}	1.1308×10^{-3}
15	0.6654	0.2955	0.0366	2.4273×10^{-3}	1.1213×10^{-4}	3.9036×10^{-6}	9.8873×10^{-8}	0
20	0.7230	0.2608	0.0160	2.8606×10^{-4}	2.1895×10^{-6}	3.2584×10^{-9}	0	0
25	0.7548	0.2366	8.5496×10^{-3}	4.9545×10^{-5}	6.2159×10^{-8}	0	0	0
30	0.7760	0.2189	5.0283×10^{-3}	1.0464×10^{-5}	0	0	0	0
50	0.8176	0.1811	1.3468×10^{-3}	1.2642×10^{-7}	0	0	0	0
100	0.8477	0.1520	3.3582×10^{-4}	0	0	0	0	0
200	0.8571	0.1427	1.9467×10^{-4}	0	0	0	0	0

Table B.2: The coefficients of the optimised states with $n_{\max} = 1$ photon.

Distance (km)	a_0 b_0	a_1 b_1
0	0.5	0.5
0.5	0.5308	0.4692
1	0.5505	0.4495
2.5	0.5918	0.4082
5	0.6371	0.3629
10	0.6935	0.3065
15	0.7292	0.2708
20	0.7542	0.2458
30	0.7869	0.2131
50	0.8205	0.1795
100	0.8483	0.1517
200	0.8575	0.1425

Table B.3: The optimised squeezing parameters (γ) of the states shown in Eq. (6.1) with $n_{\max} = 7$ photons.

Distance (km)	Squeezing Parameter (γ)
0	0.84
0.5	0.83
1	0.83
2.5	0.82
5	0.81
10	0.71
15	0.52
20	0.44
25	0.40
30	0.37
40	0.33
50	0.30
100	0.26
200	0.25

Table B.4: The coefficients of the single-photon states when experimental imperfections are considered. The detector dark count rate is 5×10^{-8} and the detector efficiency is 0.85.

Distance (km)	a_0 b_0	a_1 b_1
0.5	0.6697	0.3303
1	0.6751	0.3249
2.5	0.6896	0.3104
5	0.7100	0.2900
10	0.7405	0.2595
15	0.7624	0.2376
20	0.7790	0.2210
30	0.8020	0.1980
50	0.8275	0.1725
100	0.8499	0.1501
200	0.8576	0.1424
400	0.8588	0.1412
420	0.8591	0.1409
440	0.8598	0.1402
460	0.8609	0.1391
480	0.8630	0.1370
490	0.8647	0.1353
500	0.8669	0.1331
516	0.8721	0.1279
518	0.8730	0.1270
520	0.8739	0.1261
522	0.8749	0.1251
524	0.8760	0.1240
530	0.8796	0.1204
532	0.8810	0.1190
534	0.8825	0.1175
536	0.8841	0.1159
538	0.8859	0.1141
540	0.8878	0.1122
542	0.8898	0.1102

Appendix C

Proofs of the Entanglement Purification Protocol

C.1 Proof of the Ineffectiveness of Bell-State Measurements in Pauli Dephasing Channel

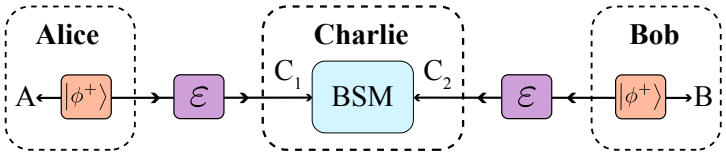

Figure C.1: Entanglement swapping measurement performed by Charlie using Bell-state measurements in the dephasing channel. Alice and Bob each prepare a $|\phi^+\rangle$ state, keeping one qubit and sending the other to Charlie. Charlie then interferes with the two incoming qubits and performs a Bell-state measurement, establishing entanglement between Alice and Bob.

In this section, we demonstrate that, even with the inclusion of a node between the trusted parties, an entanglement swapping process using Bell-state measurements results in a state identical to that of a repeaterless channel. The state in Eq. (7.3) represents the states shared between Alice and Charlie, and Charlie and Bob, after both Alice and Bob send a state to Charlie. When the original dephasing channel is divided into two by introducing a node, the Kraus operators for the channel with a node are given as

$$K_0 = \sqrt{1-p_e}\mathbb{1}_2 \tag{C.1a}$$

$$K_1 = \sqrt{p_e}\sigma_z, \tag{C.1b}$$

where $p_e = (1-\sqrt{1-2p})/2$ represents the probability of a phase-flip in the presence of a single node, and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. For n channels, the effective dephasing probability between each node is given by $p_e(n) = (1-(1-2p)^{\frac{1}{n}})/2$, which can be used to compute the channel capacity of $(n-1)$ repeaters using $C(n) = 1 - \mathrm{H}_2(p_e(n))$.

When Alice and Bob each prepare a $|\phi^+\rangle$ Bell state and send one arm to Charlie, the

resulting state, as described in Eq. (7.3), is obtained through the application of the Kraus operators as follows

$$\rho_{\mathrm{AC}} = (\mathbb{1}_2 \otimes K_0) \left|\phi^+\right\rangle\!\left\langle\phi^+\right| (\mathbb{1}_2 \otimes K_0)^\dagger + (\mathbb{1}_2 \otimes K_1) \left|\phi^+\right\rangle\!\left\langle\phi^+\right| (\mathbb{1}_2 \otimes K_1)^\dagger. \tag{C.2}$$

This state can be expressed in the computational basis as

$$\begin{aligned}\rho_{\mathrm{AC}} &= (1-p_e) \left|\phi^+\right\rangle\!\left\langle\phi^+\right| + p_e \left|\phi^-\right\rangle\!\left\langle\phi^-\right| \\ &= \frac{1}{2}\big(|00\rangle\langle 00| + (1-2p_e)\,|00\rangle\langle 11| + (1-2p_e)\,|11\rangle\langle 00| + |11\rangle\langle 11|\big).\end{aligned} \tag{C.3}$$

Therefore, the state received by Charlie from Alice and Bob can be expressed as $\rho_{\mathrm{AC}}^{\otimes 2}$, which takes the following form

$$\begin{aligned}\rho_{\mathrm{AC_1C_2B}} = \frac{1}{4}\big(&|0000\rangle\langle 0000| + (1-2p_e)\,|0000\rangle\langle 0011| + (1-2p_e)\,|0011\rangle\langle 0000| + |0011\rangle\langle 0011| + \\ &(1-2p_e)\,|0000\rangle\langle 1100| + (1-2p_e)^2\,|0000\rangle\langle 1111| + (1-2p_e)^2\,|0011\rangle\langle 1100| + \\ &(1-2p_e)\,|0011\rangle\langle 1111| + (1-2p_e)\,|1100\rangle\langle 0000| + (1-2p_e)^2\,|1100\rangle\langle 0011| + \\ &(1-2p_e)^2\,|1111\rangle\langle 0000| + (1-2p_e)\,|1111\rangle\langle 0011| + |1100\rangle\langle 1100| + \\ &(1-2p_e)\,|1100\rangle\langle 1111| + (1-2p_e)\,|1111\rangle\langle 1100| + |1111\rangle\langle 1111|\big).\end{aligned} \tag{C.4}$$

Charlie then performs a Bell-state measurement, enabling Alice and Bob to share an entangled state, as illustrated in Fig. C.1. For the purposes of this proof, assume Charlie uses the $|\phi^+\rangle$ state as the measurement operator. In this case, his measurement is represented by

$$\begin{aligned}\Pi_{\phi^+} =&(\mathbb{1}_2 \otimes \left|\phi^+\right\rangle\!\left\langle\phi^+\right| \otimes \mathbb{1}_2) \\ =&\frac{1}{2}\big(|0000\rangle\langle 0000| + |0000\rangle\langle 0110| + |0110\rangle\langle 0000| + |0110\rangle\langle 0110| + |1000\rangle\langle 1000| + \\ &|1000\rangle\langle 1110| + |1110\rangle\langle 1000| + |1110\rangle\langle 1110| + |0001\rangle\langle 0001| + |0001\rangle\langle 0111| + \\ &|0111\rangle\langle 0001| + |0111\rangle\langle 0111| + |1001\rangle\langle 1001| + |1001\rangle\langle 1111| + |1111\rangle\langle 1001| + |1111\rangle\langle 1111|\big).\end{aligned} \tag{C.5}$$

Thus, the state after Charlie's measurement becomes

$$\begin{aligned}\rho_{\mathrm{AB}} &= \mathrm{Tr}_{2,3}[\Pi_{\phi^+}\rho_{\mathrm{AC_1C_2B}}\Pi_{\phi^+}^\dagger] \\ &= \frac{1}{8}\big(|00\rangle\langle 00| + (1-2p_e)^2\,|00\rangle\langle 11| + (1-2p_e)^2\,|11\rangle\langle 00| + |11\rangle\langle 11|\big),\end{aligned} \tag{C.6}$$

where $\mathrm{Tr}_{2,3}[.]$ represents tracing out the modes 2 and 3 corresponding to $\mathrm{C_1}$ and $\mathrm{C_2}$. Nor-

malising the state by the success probability, $\mathrm{Tr}[\rho_{\mathrm{AB}}]$, gives

$$\begin{aligned}\tilde{\rho}_{\mathrm{AB}_{\phi^+}} &= \frac{\rho_{\mathrm{AB}}}{\mathrm{Tr}[\rho_{\mathrm{AB}}]} \\ &= \frac{1}{2}\big(\,|00\rangle\langle 00| + (1-2p_e)^2\,|00\rangle\langle 11| + (1-2p_e)^2\,|11\rangle\langle 00| + |11\rangle\langle 11|\,\big) \\ &= \frac{1}{2}\big(\,|00\rangle\langle 00| + (1-2p)\,|00\rangle\langle 11| + (1-2p)\,|11\rangle\langle 00| + |11\rangle\langle 11|\,\big) \\ &= (1-p)\left|\phi^+\right\rangle\!\left\langle\phi^+\right| + p\left|\phi^-\right\rangle\!\left\langle\phi^-\right|. \end{aligned} \tag{C.7}$$

This demonstrates that the resulting state after the BSM remains identical to the repeaterless case. Each BSM outcome projects the state between Alice and Bob onto a state that experiences the same level of noise as in the repeaterless scenario, with each outcome occurring with a probability of 0.25 as shown below

$$\tilde{\rho}_{\mathrm{AB}_{\phi^-}} = (1-p)\left|\phi^-\right\rangle\!\left\langle\phi^-\right| + p\left|\phi^+\right\rangle\!\left\langle\phi^+\right|, \tag{C.8a}$$

$$\tilde{\rho}_{\mathrm{AB}_{\psi^+}} = (1-p)\left|\psi^+\right\rangle\!\left\langle\psi^+\right| + p\left|\psi^-\right\rangle\!\left\langle\psi^-\right|, \tag{C.8b}$$

$$\tilde{\rho}_{\mathrm{AB}_{\psi^-}} = (1-p)\left|\psi^-\right\rangle\!\left\langle\psi^-\right| + p\left|\psi^+\right\rangle\!\left\langle\psi^+\right|. \tag{C.8c}$$

Therefore the average RCI becomes

$$\begin{aligned}\mathrm{RCI}_{\mathrm{BSM}} &= 0.25 \times \mathrm{RCI}(\tilde{\rho}_{\mathrm{AB}_{\phi^+}}) + 0.25 \times \mathrm{RCI}(\tilde{\rho}_{\mathrm{AB}_{\phi^-}}) + \\ &\quad 0.25 \times \mathrm{RCI}(\tilde{\rho}_{\mathrm{AB}_{\psi^+}}) + 0.25 \times \mathrm{RCI}(\tilde{\rho}_{\mathrm{AB}_{\psi^-}}) \\ &= 1 - \mathrm{H}_2(p), \end{aligned} \tag{C.9}$$

which is equal to the capacity of the repeaterless bound [93]. This highlights the importance of our protocol in achieving the capacity of the reperater bounds of the Pauli dephasing channel.

C.2 Probability of Success of the Second Stage

The probability of success of the second round given that the states were successful in the first round is given by

$$P_{s_1 s_2}(m) = \frac{2^{-(m-1)}}{P^m_{s_1}(m)} \sum_{r=0}^{\frac{m-1}{2}} \binom{m}{r} \left(1 + (1-2p)^{m-2r}\right)^m (1-2p)^{mr}, \tag{C.10}$$

for odd m and

$$P_{s_1s_2}(m)=\frac{2^{-(m-1)}}{P^m_{s_1}(m)}\left(\sum_{r=0}^{\frac{m}{2}-1}\binom{m}{r}\left(1+(1-2p)^{m-2r}\right)^m(1-2p)^{mr}+2^{m-1}(1-2p)^{\frac{m^2}{2}}\binom{m}{m/2}\right), \tag{C.11}$$

for even m. r represents half the number of errors of the first stage.

C.3 Eigenvalues of the Second Stage

As mentioned in Sec. 7.2.2, in order to saturate the channel capacity, we need to keep all the possible outcomes. Accordingly, we provide the eigenvalues of the remaining conditional states here. The eigenvalues of the successful state in the second round, given it failed the first round, $\lambda_{f_1s_2}(j)$, follow the same formula as Eq. (7.13) with $j=m,m+2,\ldots,m(m-1)$ for even m and $j=m,m+2,\ldots,m(m-1)+1$ for odd m. Similar to Eq. (7.15), these eigenvalues need to be normalised. The probability of success in the second round, $P_{f_1s_2}(m)$, given it failed in the first round, is computed using Eq. (7.14) with j values adjusted accordingly for the failed states and $\tilde{\lambda}_{s_1s_2}(j)$ is divided by $P^m_{f_1}(m)$ where $P^m_{f_1}(m)$ is obtained from Eq. (7.8). Therefore, the eigenvalues of the successful state of the second round given it fails the first round is given by $\lambda_{f_1s_2}(j)=\tilde{\lambda}_{s_1s_2}(j)/(P^m_{f_1}(m)P_{f_1s_2}(m))$.

The last set of eigenvalues we need to compute are for the states that failed in both the first and second rounds. These are derived from the relationship between the failed and successful states of the second round and the failed state from the first round, as shown below

$$\rho^{\otimes(m-1)}_{\mathrm{AB}_{f_1}}=P_{f_1s_2}(m)\times\rho_{\mathrm{AB}_{f_1s_2}}+P_{f_1f_2}(m)\times\rho_{\mathrm{AB}_{f_1f_2}}, \tag{C.12}$$

Here, $\rho_{\mathrm{AB}_{f_1}}$ represents the failed state from the first stage of the protocol. $P_{f_1s_2}(m)$ and $P_{f_1f_2}(m)$ are the probabilities of success and failure, respectively, in the second round given the state failed in the first round. Note that $P_{f_1f_2}(m)$ is equal to $1-P_{f_1s_2}(m)$. $\rho_{\mathrm{AB}_{f_1s_2}}$ and $\rho_{\mathrm{AB}_{f_1f_2}}$ are the conditional states of the second round that succeeded and failed, respectively, given they failed in the first round. Therefore the eigenvalues of the failed state of the second round given it also failed the first stage is given by

$$\lambda_{f_1f_2}(j_1,j_2)=\frac{1}{P_{f_1f_2}(m)}\left[\frac{(1-p)^{m(m-1)-j_1}p^{j_1}}{P^{m-1}_{f_1}(m)}-\frac{(1-p)^{m^2-j_2}p^{j_2}}{P^m_{f_1}(m)}\right], \tag{C.13}$$

where $j_1=m-1,m+1,\cdots,(m-1)^2$ and $j_2=j_1+1,j_1+3,\cdots,j_1+m-1$ for even m and $j_1=m-1,m+1,\cdots,m(m-1)$ and $j_2=j_1+1,j_1+3,\cdots,j_1+m$ for odd m.

C.4 Proof of the Capacity for the First Round of the Protocol

As stated in Eq. (7.20) when we add the successful and failed states up after the first round, they give the state of $m-1$ copies of Bell pairs as in average nothing changes but the state conditioned on a successful outcome individually purifies the Bell pairs. Note that the eigenvalues of the successful state is $\frac{(1-p)^{m-j_1}p^{j_1}}{P_{s_1}(m)}$ with a multiplicity of $\binom{m}{j_1}$ while the eigenvalues of the failed state is $\frac{(1-p)^{m-(j_1+1)}p^{j_1+1}}{P_{f_1}(m)}$ with a multiplicity of $\binom{m}{j_1+1}$ with $j_1 = 0, 2, \cdots, m$ if m is even. Therefore, when we add the successful and failed states up, the eigenvalues simply become $(1-p)^{(m-1)}p^{j_1}$ with $j_1 = 0, 1, \cdots, m-1$ with each eigenvalue having a multiplicity of $\binom{m-1}{j_1}$. Then the entropy of the combined state in the RHS of Eq. (7.20) becomes

$$
\begin{aligned}
\text{RHS} &= \frac{1}{m}\big(S(P_{s_1}(m)\rho_{\text{A}_{s_1}} + P_{f_1}(m)\rho_{\text{A}_{f_1}}) - S(P_{s_1}(m)\rho_{\text{AB}_{s_1}} + P_{f_1}(m)\rho_{\text{AB}_{f_1}})\big) \\
&= \frac{1}{m}\log_2(2^{m-1}) + \frac{1}{m}\sum_{j_1=0}^{m-1}\binom{m-1}{j_1}(1-p)^{(m-1)-j_1}p^{j_1}\log_2\big((1-p)^{(m-1)-j_1}p^{j_1}\big) \\
&= \frac{m-1}{m} + \frac{(1-p)^{m-1}}{m}\Bigg[\sum_{j_1=0}^{m-1}\binom{m-1}{j_1}(1-p)^{(m-1)-j_1}p^{j_1}\big((m-1-j_1)\log_2(1-p) + \\
&\quad j_1\log_2(p)\big)\Bigg] \\
&= \frac{m-1}{m} + \frac{(1-p)^{m-1}}{m}\Bigg[\sum_{j_1=0}^{m-1}\binom{m-1}{j_1}\left(\frac{p}{1-p}\right)^{j_1}(m-1)\log_2(1-p) + \\
&\quad \sum_{j_1=0}^{m-1}\binom{m-1}{j_1}\left(\frac{p}{1-p}\right)^{j_1} j_1\big(\log_2(p) - \log_2(1-p)\big)\Bigg].
\end{aligned}
\tag{C.14}
$$

Note that $S(P_{s_1}(m)\rho_{\text{A}_{s_1}} + P_{f_1}(m)\rho_{\text{A}_{f_1}}) = \log_2(2^{m-1})$ and using $\sum_{j=0}^{n}\binom{n}{k}x^j = (1+x)^n$ and $\sum_{j=0}^{n}\binom{n}{k}jx^j = nx(1+x)^{n-1}$, the expression in Eq. (C.14) can be further simplified to

$$
\begin{aligned}
\text{RHS} &= \frac{m-1}{m} + \frac{(1-p)^{m-1}(m-1)}{m}\Bigg[\left(1+\frac{p}{1-p}\right)^{m-1}\log_2(1-p) - \\
&\quad \left(\frac{p}{1-p}\right)\left(1+\frac{p}{1-p}\right)^{m-2}\log_2(1-p) + \left(\frac{p}{1-p}\right)\left(1+\frac{p}{1-p}\right)^{m-2}\log_2(p)\Bigg] \\
&= \frac{m-1}{m} + \frac{(1-p)^{m-1}(m-1)}{m}\left(1+\frac{p}{1-p}\right)^{m-2}\Bigg[\log_2(1-p) + \frac{p}{1-p}\log_2(p)\Bigg] \\
&= \frac{m-1}{m}\big[1 - \big(-(1-p)\log_2(1-p) - (p)\log_2(p)\big)\big] \\
&= \frac{m-1}{m}\big(1 - \text{H}_2(p)\big) \\
&= \frac{m-1}{m}C,
\end{aligned}
\tag{C.15}
$$

as $1 - \mathrm{H}_2(p)$ is equal to the capacity of the dephasing channel. Additionally, the LHS of Eq. (7.20) is already proven in Sec. 7.3.1.

Alternatively, we can use the following proof utilising the properties of von Neumann entropy which is also helpful for the proof of the second stage of the protocol. Recall Eq. (7.10) which presents the average RCI after the first round of the protocol. This equation can be expanded as

$$\mathrm{RCI}_1 = \frac{1}{m}\big[P_{s_1}(m)\, S(\rho_{\mathrm{A}_{s_1}}) + P_{f_1}(m)\, S(\rho_{\mathrm{A}_{f_1}}) - P_{s_1}(m)\, S(\rho_{\mathrm{AB}_{s_1}}) - P_{f_1}(m)\, S(\rho_{\mathrm{AB}_{f_1}})\big]. \quad \text{(C.16)}$$

As both $S(\rho_{\mathrm{A}_{s_1}})$ and $S(\rho_{\mathrm{A}_{f_1}})$ are equal to the dimensions of the state which is $\log_2(2^{m-1})$. Therefore, $P_{s_1}(m)\, S(\rho_{\mathrm{A}_{s_1}}) + P_{f_1}(m)\, S(\rho_{\mathrm{A}_{f_1}}) = \log_2(2^{m-1}) \times (P_{s_1}(m) + P_{f_1}(m)) = (m-1)$ as $P_{s_1}(m) + P_{f_1}(m) = 1$. Therefore,

$$\mathrm{RCI}_1 = \frac{1}{m}\big[(m-1) - P_{s_1}(m) S(\rho_{\mathrm{AB}_{s_1}}) - P_{f_1}(m) S(\rho_{\mathrm{AB}_{f_1}})\big]. \quad \text{(C.17)}$$

Using concavity of von Neumann entropy where $S(\sum_i \lambda_i \rho_i) \geq \sum_i \lambda_i\, S(\rho_i)$ for $\lambda_i \geq 0$ and $\sum_i \lambda_i = 1$,

$$P_{s_1}(m)\, S(\rho_{\mathrm{AB}_{s_1}}) + P_{f_1}(m)\, S(\rho_{\mathrm{AB}_{f_1}}) \leq S(P_{s_1}(m) \times \rho_{\mathrm{AB}_{s_1}} + P_{f_1}(m) \times \rho_{\mathrm{AB}_{f_1}}). \quad \text{(C.18)}$$

Therefore by substituting the above relation into Eq. (C.17) we can lower bound the actual RCI of this protocol by

$$\begin{aligned}
&\tfrac{1}{m}\big[(m-1) - S(P_{s_1}(m) \times \rho_{\mathrm{AB}_{s_1}} + P_{f_1}(m) \times \rho_{\mathrm{AB}_{f_1}})\big] \leq \tfrac{1}{m}\big[(m-1) - P_{s_1}(m)\, S(\rho_{\mathrm{AB}_{s_1}}) - P_{f_1}(m)\, S(\rho_{\mathrm{AB}_{f_1}})\big] \leq C \\
&\tfrac{m-1}{m}\, C \leq \tfrac{1}{m}\big[(m-1) - P_{s_1}(m)\, S(\rho_{\mathrm{AB}_{s_1}}) - P_{f_1}(m)\, S(\rho_{\mathrm{AB}_{f_1}})\big] \leq C \\
&\tfrac{m-1}{m}\, C \leq \mathrm{RCI}_1 \leq C
\end{aligned} \quad \text{(C.19)}$$

The proof of the lower bound in Eq. (C.19), follows the same steps as those in Eq. (C.14). Therefore, refer to Eq. (C.14) for the expansion of $S(P_{s_1}(m) \times \rho_{\mathrm{AB}_{s_1}} + P_{f_1}(m) \times \rho_{\mathrm{AB}_{f_1}})$. Notably, Eq. (C.19) becomes the capacity, C as $\lim_{m\to\infty} \frac{m-1}{m}\, C = C$.

C.5 Proof of the Capacity for the Second Round of the Protocol

Recall that Eq. (7.19) represents the average RCI for the second round of the protocol. However, unlike in the first stage, the eigenvalue multiplicities are not available in closed form, making it challenging to directly prove Eq. (7.19). To address this, we substitute $P_{s_1 s_2}(m) \times \mathrm{RCI}(\rho_{\mathrm{AB}_{s_1 s_2}}) + P_{s_1 f_2}(m) \times \mathrm{RCI}(\rho_{\mathrm{AB}_{s_1 f_2}})$ with $\mathrm{RCI}(\rho_{\mathrm{AB}_{s_1}}^{\otimes(m-1)})$, as averaging over the conditional states, whether successful or failed in the second round, given their success

in the first, yields $m-1$ copies of the successful state from the first round. Similarly, we replace $P_{f_1 s_2}(m) \times \mathrm{RCI}(\rho_{\mathrm{AB}_{f_1 s_2}}) + P_{f_1 f_2}(m) \times \mathrm{RCI}(\rho_{\mathrm{AB}_{f_1 f_2}})$ with $\mathrm{RCI}(\rho_{\mathrm{AB}_{f_1}}^{\otimes(m-1)})$, since these terms also sum to $m-1$ copies of the failed state from the first round, thereby conserving the reverse coherent information. However, computing the RCI of these states underestimates the key rates. Therefore, we demonstrate that Eq. (7.19) can be lower bounded by

$$\begin{aligned}
&\tfrac{1}{m^2}\big[P_{s_1}(m) \times \mathrm{RCI}(\rho_{\mathrm{AB}_{s_1}}^{\otimes(m-1)}) + P_{f_1}(m) \times \mathrm{RCI}(\rho_{\mathrm{AB}_{f_1}}^{\otimes(m-1)})\big] \leq \mathrm{RCI}_2 \leq C \\
&\tfrac{1}{m^2}\big[P_{s_1}(m)\, S(\rho_{\mathrm{A}_{s_1}}^{\otimes(m-1)}) + P_{f_1}(m)\, S(\rho_{\mathrm{A}_{f_1}}^{\otimes(m-1)}) - P_{s_1}(m)\, S(\rho_{\mathrm{AB}_{s_1}}^{\otimes(m-1)}) - P_{f_1}(m)\, S(\rho_{\mathrm{AB}_{f_1}}^{\otimes(m-1)})\big] \leq \mathrm{RCI}_2 \leq C \\
&\tfrac{1}{m^2}\big[(m-1)^2 - \big(P_{s_1}(m)\, S(\rho_{\mathrm{AB}_{s_1}}^{\otimes(m-1)}) + P_{f_1}(m)\, S(\rho_{\mathrm{AB}_{s_1}}^{\otimes(m-1)})\big)\big] \leq \mathrm{RCI}_2 \leq C, \qquad \text{(C.20)}
\end{aligned}$$

where both $S(\rho_{\mathrm{A}_{s_1}}^{\otimes(m-1)})$ and $S(\rho_{\mathrm{A}_{f_1}}^{\otimes(m-1)})$ are just equal to the dimensions of the state which is $\log_2(2^{(m-1)^2})$. Therefore, $P_{s_1}(m)\, S(\rho_{\mathrm{A}_{s_1}}^{\otimes(m-1)}) + P_{f_1}(m)\, S(\rho_{\mathrm{A}_{f_1}}^{\otimes(m-1)}) = \log_2(2^{(m-1)^2}) \times (P_{s_1}(m) + P_{f_1}(m)) = (m-1)^2$ as $P_{s_1}(m) + P_{f_1}(m) = 1$. As both $\rho_{\mathrm{AB}s1}^{\otimes(m-1)}$ and $\rho_{\mathrm{AB}f1}^{\otimes(m-1)}$ have no entanglement between each state, we can use $S(\rho^{\otimes n}) = n\, S(\rho)$, the relation becomes

$$\frac{1}{m^2}\big[(m-1)^2 - (m-1)\big(P_{s_1}(m)\, S(\rho_{\mathrm{AB}_{s_1}}) + P_{f_1}(m)\, S(\rho_{\mathrm{AB}_{s_1}})\big)\big] \leq \mathrm{RCI}_2 \leq C. \qquad \text{(C.21)}$$

Using the concavity of von Neumann entropy, the LHS of Eq. (C.21) can be lower bounded by

$$\begin{aligned}
&\frac{1}{m^2}\big[(m-1)^2 - (m-1) S\big(P_{s_1}(m)\rho_{\mathrm{AB}_{s_1}} + P_{f_1}(m)\rho_{\mathrm{AB}_{s_1}}\big)\big] \leq \frac{1}{m^2}\big[(m-1)^2 - \\
&\qquad (m-1)\big(P_{s_1}(m) S(\rho_{\mathrm{AB}_{s_1}}) + P_{f_1}(m) S(\rho_{\mathrm{AB}_{s_1}})\big)\big] \\
&\frac{1}{m^2}\big[(m-1)^2 - (m-1)^2\, \mathrm{H}_2(p)\big] \leq \frac{1}{m^2}\big[(m-1)^2 - (m-1)\big(P_{s_1}(m) S(\rho_{\mathrm{AB}_{s_1}}) + P_{f_1}(m) S(\rho_{\mathrm{AB}_{s_1}})\big)\big] \\
&\left(\frac{m-1}{m}\right)^2 \big[1 - \mathrm{H}_2(p)\big] \leq \frac{1}{m^2}\big[(m-1)^2 - (m-1)\big(P_{s_1}(m) S(\rho_{\mathrm{AB}_{s_1}}) + P_{f_1}(m) S(\rho_{\mathrm{AB}_{s_1}})\big)\big] \\
&\left(\frac{m-1}{m}\right)^2 C \leq \frac{1}{m^2}\big[(m-1)^2 - (m-1)\big(P_{s_1}(m) S(\rho_{\mathrm{AB}_{s_1}}) + P_{f_1}(m) S(\rho_{\mathrm{AB}_{s_1}})\big)\big]. \qquad \text{(C.22)}
\end{aligned}$$

Therefore, the RCI of the second round can be expressed as

$$\left(\frac{m-1}{m}\right)^2 C \leq \mathrm{RCI}_2 \leq C. \qquad \text{(C.23)}$$

C.6 Key Rate of the Protocol in Any Round

As the RCI of the first round is $\frac{m-1}{m}\, C$ and the RCI of the second stage is lower bounded by Eq. (C.23), the relationship between the RCI of any stage of the protocol versus capacity can

be gives as

$$\left(\frac{m-1}{m}\right)^n C \leq \mathrm{RCI}_n \leq C, \tag{C.24}$$

where n denotes the number of rounds. As mentioned in the main text, if $n = m$, as $m \to \infty$, the limit approaches C/e, which would cause the lower bound to fall below the capacity. However, the effective dephasing decreases with each round, resulting in higher distillable entanglement. As long as $n \ll m$, the protocol is able to reach the capacity of the dephasing channel.

C.7 Proof of Fidelity

Following the first round of the protocol, the reduced states in the alternative protocol have the same form as in the original protocol. However, in the second round, the form of the reduced state in the original protocol deviates from Eq (7.28). Nonetheless, since the fidelity of our actual protocol is higher than that of the alternative protocol, we use the alternative protocol as a lower bound to demonstrate that fidelity improves with each round, while the dephasing probability decreases.

Since the fidelity is defined as $F = 1 - p$ for the dephasing channel, demonstrating that p progressively decreases implies that the fidelity increases with each iteration. For this reason, the relationship between the dephasing probability for each round of protocol can be expressed as

$$p_{n+1} = \tilde{p}(p_n), \tag{C.25}$$

where the new probability of dephasing depends on the dephasing probability of the previous one. Therefore in reach round,

$$p_1 = \tilde{p}(p_0), \tag{C.26a}$$

$$p_2 = \tilde{p}(p_1) = \tilde{p}(\tilde{p}(p_0)), \tag{C.26b}$$

$$p_3 = \tilde{p}(p_2) = \tilde{p}(\tilde{p}(\tilde{p}(p_0))), \tag{C.26c}$$

where $\tilde{p}(p)$ is the new dephasing probability as a function of the previous dephasing probability which is given in Eq. (7.30). Based on this, let us prove that

$$p_1 = \tilde{p}(p_0) \leq p_0 = p. \tag{C.27}$$

Recall that for the dephasing channel, we have the constraint $0 \leq p_0 \leq \frac{1}{2}$. Using this range,

we can derive the following sequence of inequalities to show that $p_1 \leq p_0$.

$$\begin{aligned}
0 \leq p_0 \leq \frac{1}{2} \\
\Leftrightarrow 0 \leq 2p_0 \leq 1 \\
\Leftrightarrow 0 \leq 1 - 2p_0 \leq 1 \\
\Leftrightarrow 0 \leq (1-2p_0)^2 \leq 1 \\
\Leftrightarrow 0 \leq (1-2p_0)^2(1-2p_0)^m \leq (1-2p_0)^m \\
\Leftrightarrow (1-2p_0)^m \leq (1-2p_0)^{m-2} \\
\Leftrightarrow 1 + (1-2p_0)^m \leq 1 + (1-2p_0)^{m-2} \\
\Leftrightarrow (1-2p_0)(1+(1-2p_0)^m) \leq (1-2p_0)(1+(1-2p_0)^{m-2}) \\
\Leftrightarrow 1 - 2p_0 \leq \frac{(1-2p_0)+(1-2p_0)^{m-1}}{(1+(1-2p_0)^m)} \\
\Leftrightarrow 1 - \frac{(1-2p_0)+(1-2p_0)^{m-1}}{(1+(1-2p_0)^m)} \leq 2p_0 \\
\Leftrightarrow p_1 = \frac{1}{2}\left(1 - \frac{(1-2p_0)+(1-2p_0)^{m-1}}{(1+(1-2p_0)^m)}\right) \leq p_0. \qquad \text{(C.28)}
\end{aligned}$$

This final expression in Eq. (C.28) on the left-hand side matches Eq. (7.30) as a function of any Bell pair, m, which confirms that

$$p_1 \leq p_0. \qquad \text{(C.29)}$$

Note that the proof of $p_{n+1} \leq p_n$ for each round of the protocol follows from Eq. (C.28). For example, in the second round, each occurrence of p_0 is replaced by p_1, leading to $p_2 \leq p_1 \leq p_0$, which in turn implies $F_2 \geq F_1 \geq F_0$. To show that $\lim_{n\to\infty} \tilde{p}(p_n) = 0$ and $\lim_{n\to\infty} F = 1$, we apply fixed-point and stability analysis techniques from non-linear dynamics [338] to the iterative map function $\tilde{p}(p_n)$. We begin by computing the fixed points of $\tilde{p}(p_n) = p_n$,

$$\begin{aligned}
\frac{1}{2}\left(1 - \frac{(1-2p_n)+(1-2p_n)^{m-1}}{(1+(1-2p_n)^m)}\right) = p_n \\
p_n = 0, 1. \qquad \text{(C.30)}
\end{aligned}$$

We disregard $p_n = 1$ since, for the dephasing channel, p_n is always constrained to the range $0 \leq p_n \leq 1/2$. Next, we compute the derivative of $\tilde{p}(p_n)$ at the fixed point $p_n = 0$, given by $\frac{\mathrm{d}\tilde{p}}{\mathrm{d}p_n}\Big|_{p_n=0}$. In this case,

$$\frac{\mathrm{d}\tilde{p}}{\mathrm{d}p_n} = \frac{1-(1-2p_n)^{2m}+4p_n(p_n-1)(1-(m-1)(1-2p_n)^m)}{(1+(1-2p_n)^m)^2(1-2p_n)^2}, \qquad \text{(C.31)}$$

and substituting $p_n = 0$ into the expression above, we obtain

$$\left| \frac{\mathrm{d}\tilde{p}}{\mathrm{d}p_n}\bigg|_{p_n=0} \right| = 0. \tag{C.32}$$

Note that if $\left| \frac{\mathrm{d}\tilde{p}}{\mathrm{d}p_n}\big|_{p_n=0} \right| < 1$, the fixed point $p_n = 0$ is considered stable [338], meaning the iterative map converges to this fixed point. In our case, since the derivative at this fixed point is also zero, it is classified as super-stable [338]. This implies that p_n converges to zero very rapidly, leading to the fidelity approaching one as the number of rounds increases.

Bibliography

[1] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, vol. 9, no. 4, pp. 5–38, 1883.

[2] B. Schneier, "Applied cryptography, 2nd addition," *W iley*, 1997.

[3] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 2018.

[4] B. J. Copeland, J. Bowen, M. Sprevak, and R. Wilson, *The Turing Guide*. Oxford University Press, 2017.

[5] D. W. Davies, "The bombe a remarkable logic machine," *Cryptologia*, vol. 23, no. 2, pp. 108–138, 1999.

[6] 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.

[7] P. Benioff, "The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines," *Journal of Statistical Physics*, vol. 22, pp. 563–591, 1980.

[8] R. P. Feynman, "Simulating physics with computers," in *Feynman and computation*, pp. 133–153, cRc Press, 2018.

[9] D. G. Cory, A. F. Fahmy, and T. F. Havel, "Ensemble quantum computing by nmr spectroscopy," *Proceedings of the National Academy of Sciences*, vol. 94, no. 5, pp. 1634–1639, 1997.

[10] N. A. Gershenfeld and I. L. Chuang, "Bulk spin-resonance quantum computation," *Science*, vol. 275, no. 5298, pp. 350–356, 1997.

[11] S. Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, "Demonstration of a small programmable quantum computer with atomic qubits," *Nature*, vol. 536, no. 7614, pp. 63–66, 2016.

[12] R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Physical Review Letters*, vol. 86, no. 22, p. 5188, 2001.

[13] J. L. O'brien, "Optical quantum computing," *Science*, vol. 318, no. 5856, pp. 1567–1570, 2007.

[14] L. Gyongyosi and S. Imre, "A survey on quantum computing technology," *Computer Science Review*, vol. 31, pp. 51–71, 2019.

[15] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *Society for Industrial and Applied Mathematics Review*, vol. 41, no. 2, pp. 303–332, 1999.

[16] J. Proos and C. Zalka, "Shor's discrete logarithm quantum algorithm for elliptic curves," *arXiv preprint quant-ph/0301141*, 2003.

[17] C. Gidney and M. Ekerå, "How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, 2021.

[18] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[19] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, p. 175, IEEE, New York, 1984.

[20] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical Review Letters*, vol. 67, no. 6, p. 661, 1991.

[21] T. C. Ralph, "Continuous variable quantum cryptography," *Physical Review A*, vol. 61, p. 010303, Dec 1999.

[22] M. Hillery, "Quantum cryptography with squeezed states," *Physical Review A*, vol. 61, p. 022309, Jan 2000.

[23] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.

[24] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block," *Physical Review A*, vol. 68, no. 4, p. 042317, 2003.

[25] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 69, no. 5, p. 052319, 2004.

[26] J.-Y. Hu, B. Yu, M.-Y. Jing, L.-T. Xiao, S.-T. Jia, G.-Q. Qin, and G.-L. Long, "Experimental quantum secure direct communication with single photons," *Light: Science & Applications*, vol. 5, no. 9, pp. e16144–e16144, 2016.

[27] W. Zhang, D.-S. Ding, Y.-B. Sheng, L. Zhou, B.-S. Shi, and G.-C. Guo, "Quantum secure direct communication with quantum memory," *Physical Review Letters*, vol. 118, no. 22, p. 220501, 2017.

[28] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G.-L. Long, "Implementation and security analysis of practical quantum secure direct communication," *Light: Science & Applications*, vol. 8, no. 1, p. 22, 2019.

[29] D. Pan, Z. Lin, J. Wu, H. Zhang, Z. Sun, D. Ruan, L. Yin, and G. L. Long, "Experimental free-space quantum secure direct communication and its security analysis," *Photonics Research*, vol. 8, no. 9, pp. 1522–1531, 2020.

[30] T. Li and G.-L. Long, "Quantum secure direct communication based on single-photon bell-state measurement," *New Journal of Physics*, vol. 22, no. 6, p. 063017, 2020.

[31] Z. Qi, Y. Li, Y. Huang, J. Feng, Y. Zheng, and X. Chen, "A 15-user quantum secure direct communication network," *Light: Science & Applications*, vol. 10, no. 1, p. 183, 2021.

[32] H. Zhang, Z. Sun, R. Qi, L. Yin, G.-L. Long, and J. Lu, "Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states," *Light: Science & Applications*, vol. 11, no. 1, p. 83, 2022.

[33] L. Zhou, B.-W. Xu, W. Zhong, and Y.-B. Sheng, "Device-independent quantum secure direct communication with single-photon sources," *Physical Review Applied*, vol. 19, no. 1, p. 014036, 2023.

[34] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, no. 3, p. 1829, 1999.

[35] R. Cleve, D. Gottesman, and H.-K. Lo, "How to share a quantum secret," *Physical Review Letters*, vol. 83, no. 3, p. 648, 1999.

[36] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Physical Review A*, vol. 59, no. 1, p. 162, 1999.

[37] W. Tittel, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum secret sharing," *Physical Review A*, vol. 63, no. 4, p. 042301, 2001.

[38] T. Tyc and B. C. Sanders, "How to share a continuous-variable quantum secret by optical interferometry," *Physical Review A*, vol. 65, no. 4, p. 042310, 2002.

[39] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, "Tripartite quantum state sharing," *Physical Review Letters*, vol. 92, no. 17, p. 177903, 2004.

[40] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, "Experimental single qubit quantum secret sharing," *Physical Review Letters*, vol. 95, no. 23, p. 230505, 2005.

[41] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, T. Tyc, T. C. Ralph, and P. K. Lam, "Continuous-variable quantum-state sharing via quantum disentanglement," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 71, no. 3, p. 033814, 2005.

[42] T. Ogawa, A. Sasaki, M. Iwamoto, and H. Yamamoto, "Quantum secret sharing schemes and reversibility of quantum operations," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 72, no. 3, p. 032318, 2005.

[43] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, "Experimental demonstration of four-party quantum secret sharing," *Physical Review Letters*, vol. 98, no. 2, p. 020503, 2007.

[44] D. Markham and B. C. Sanders, "Graph states for quantum secret sharing," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 78, no. 4, p. 042309, 2008.

[45] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, "Quantum secret sharing with qudit graph states," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 82, no. 6, p. 062315, 2010.

[46] B. Bell, D. Markham, D. Herrera-Martí, A. Marin, W. Wadsworth, J. Rarity, and M. Tame, "Experimental demonstration of graph-state quantum secret sharing," *Nature Communications*, vol. 5, no. 1, pp. 1–12, 2014.

[47] I. Kogias, Y. Xiang, Q. He, and G. Adesso, "Unconditional security of entanglement-based continuous-variable quantum secret sharing," *Physical Review A*, vol. 95, no. 1, p. 012315, 2017.

[48] L. O. Conlon, B. Shajilal, A. Walsh, J. Zhao, J. Janousek, P. K. Lam, and S. M. Assad, "Verifying the security of a continuous variable quantum communication protocol via quantum metrology," *npj Quantum Information*, vol. 10, no. 1, p. 35, 2024.

[49] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical Review Letters*, vol. 70, no. 13, p. 1895, 1993.

[50] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature*, vol. 390, no. 6660, pp. 575–579, 1997.

[51] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, "Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels," *Physical Review Letters*, vol. 80, no. 6, p. 1121, 1998.

[52] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, "Unconditional quantum teleportation," *Science*, vol. 282, no. 5389, pp. 706–709, 1998.

[53] A. Furusawa and H. Kimble, "Experimental realization of continuous variable teleportation," in *Quantum Information with Continuous Variables*, pp. 77–93, Springer, 2003.

[54] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, *et al.*, "Quantum teleportation over 143 kilometres using active feed-forward," *Nature*, vol. 489, no. 7415, pp. 269–273, 2012.

[55] S. Takeda, T. Mizuta, M. Fuwa, P. Van Loock, and A. Furusawa, "Deterministic quantum teleportation of photonic quantum bits by a hybrid technique," *Nature*, vol. 500, no. 7462, pp. 315–318, 2013.

[56] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in quantum teleportation," *Nature Photonics*, vol. 9, no. 10, pp. 641–652, 2015.

[57] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, *et al.*, "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, no. 7670, pp. 70–73, 2017.

[58] X.-M. Hu, C. Zhang, B.-H. Liu, Y. Cai, X.-J. Ye, Y. Guo, W.-B. Xing, C.-X. Huang, Y.-F. Huang, C.-F. Li, *et al.*, "Experimental high-dimensional quantum teleportation," *Physical Review Letters*, vol. 125, no. 23, p. 230501, 2020.

[59] X.-M. Hu, Y. Guo, B.-H. Liu, C.-F. Li, and G.-C. Guo, "Progress in quantum teleportation," *Nature Reviews Physics*, vol. 5, no. 6, pp. 339–353, 2023.

[60] J. Zhao, H. Jeng, L. O. Conlon, S. Tserkis, B. Shajilal, K. Liu, T. C. Ralph, S. M. Assad, and P. K. Lam, "Enhancing quantum teleportation efficacy with noiseless linear amplification," *Nature Communications*, vol. 14, no. 1, p. 4745, 2023.

[61] S. Shen, C. Yuan, Z. Zhang, H. Yu, R. Zhang, C. Yang, H. Li, Z. Wang, Y. Wang, G. Deng, *et al.*, "Hertz-rate metropolitan quantum teleportation," *Light: Science & Applications*, vol. 12, no. 1, p. 115, 2023.

[62] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.

[63] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, "Quantum repeaters: From quantum networks to the quantum internet," *Review of Modern Physics*, vol. 95, no. 4, p. 045006, 2023.

[64] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.

[65] E. Schrödinger, "Die gegenwärtige situation in der quantenmechanik," *Naturwissenschaften*, vol. 23, no. 50, pp. 844–849, 1935.

[66] E. Schrödinger, "Quantisierung als eigenwertproblem," *Annalen der physik*, vol. 385, no. 13, pp. 437–490, 1926.

[67] W. Heisenberg, "Quantum-theoretical re-interpretation of kinematic and mechanical relations," *Z. Phys*, vol. 33, pp. 879–893, 1925.

[68] M. Born and P. Jordan, "Zur quantenmechanik," *Zeitschrift für Physik*, vol. 34, no. 1, pp. 858–888, 1925.

[69] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*. Cambridge university press, 2010.

[70] M. O. Scully and M. S. Zubairy, *Quantum optics*. Cambridge university press, 1997.

[71] P. A. M. Dirac, "The quantum theory of the emission and absorption of radiation," *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, vol. 114, no. 767, pp. 243–265, 1927.

[72] H.-A. Bachor and T. C. Ralph, *A Guide to Experiments in Quantum Optics*. Wiley Online Library, 1998.

[73] A. Furusawa and A. Furusawa, *Quantum states of light*. Springer, 2015.

[74] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Reviews of Modern Physics*, vol. 84, no. 2, pp. 621–669, 2012.

[75] H.-A. Bachor and T. C. Ralph, *A guide to experiments in quantum optics*. John Wiley & Sons, 2019.

[76] R. J. Glauber, "Coherent and incoherent states of the radiation field," *Physical Review*, vol. 131, no. 6, p. 2766, 1963.

[77] J. H. Shapiro, "The quantum theory of optical communications," *IEEE journal of selected topics in Quantum Electronics*, vol. 15, no. 6, pp. 1547–1569, 2009.

[78] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical Review Letters*, vol. 88, no. 5, p. 057902, 2002.

[79] J. Zhao, *Post-selection-based continuous variable quantum information processing*. PhD thesis, The Australian National University, 2019.

[80] B. Shajilal, *Experimental and Theoretical Investigation of Quantum Communication Resources A Study on Squeezing, Entanglement and Entropic Accord*. PhD thesis, The Australian National University (Australia), 2023.

[81] P. K. Lam, *Applications of quantum electro-optic control and squeezed light*. PhD thesis, The Australian National University, 1998.

[82] W. P. Bowen, *Experiments towards a quantum information network with squeezed light and entanglement*. PhD thesis, The Australian National University, 2003.

[83] J. Y. Haw *et al.*, *Continuous Variable Optimisation of Quantum Randomness and Probabilistic Linear Amplification*. PhD thesis, The Australian National University, 2018.

[84] D. Shaddock, *Advanced interferometry for gravitational wave detection*. PhD thesis, The Australian National University, 2000.

[85] E. D. Black, "An introduction to pound–drever–hall laser frequency stabilization," *American journal of physics*, vol. 69, no. 1, pp. 79–87, 2001.

[86] C. E. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.

[87] A. Leverrier, *Theoretical study of continuous-variable quantum key distribution*. PhD thesis, Télécom ParisTech, 2009.

[88] J. Von Neumann, *Mathematische grundlagen der quantenmechanik*, vol. 38. Springer-Verlag, 2013.

[89] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 269–273, 1998.

[90] J. Williamson, "On the algebraic problem concerning the normal forms of linear dynamical systems," *American Journal of Mathematics*, vol. 58, no. 1, pp. 141–163, 1936.

[91] A. Serafini, F. Illuminati, and S. De Siena, "Symplectic invariants, entropic measures and correlations of Gaussian states," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 37, no. 2, p. L21, 2003.

[92] L. Gyongyosi and S. Imre, "Properties of the quantum channel," *arXiv preprint arXiv:1208.1270*, 2012.

[93] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, no. 1, pp. 1–15, 2017.

[94] S. Pirandola, "End-to-end capacities of a quantum communication network," *Communications Physics*, vol. 2, no. 1, p. 51, 2019.

[95] I. L. Chuang, D. W. Leung, and Y. Yamamoto, "Bosonic quantum codes for amplitude damping," *Physical Review A*, vol. 56, no. 2, p. 1114, 1997.

[96] J. S. Ivan, K. K. Sabapathy, and R. Simon, "Operator-sum representation for bosonic Gaussian channels," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 84, no. 4, p. 042311, 2011.

[97] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Physical review letters*, vol. 85, no. 2, p. 441, 2000.

[98] H.-K. Lo, "Proof of unconditional security of six-state quantum key distribution scheme," *arXiv preprint quant-ph/0102138*, 2001.

[99] B. Kraus, N. Gisin, and R. Renner, "Lower and upper bounds on the secret-key rate for quantum key distribution protocols¡? format?¿ using one-way classical communication," *Physical review letters*, vol. 95, no. 8, p. 080501, 2005.

[100] 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.

[101] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Physical Review Letters*, vol. 93, no. 17, p. 170504, 2004.

[102] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, "No-switching quantum key distribution using broadband modulated coherent light," *Physical Review Letters*, vol. 95, no. 18, p. 180503, 2005.

[103] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," *Physical Review A*, vol. 76, no. 4, p. 042305, 2007.

[104] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states," *Nature Communications*, vol. 3, no. 1, p. 1083, 2012.

[105] 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.

[106] C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, "25 mhz clock continuous-variable quantum key distribution system over 50 km fiber channel," *Scientific Reports*, vol. 5, no. 1, p. 14607, 2015.

[107] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Physical Review Letters*, vol. 125, no. 1, p. 010502, 2020.

[108] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer, *et al.*, "Practical continuous-variable quantum key distribution with composable security," *Nature Communications*, vol. 13, no. 1, p. 4740, 2022.

[109] A. A. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, and T. Gehring, "Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator," *Science Advances*, vol. 10, no. 1, p. eadi9474, 2024.

[110] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, "Continuous variable quantum cryptography: Beating the 3 db loss limit," *Physical Review Letters*, vol. 89, no. 16, p. 167901, 2002.

[111] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," *Physical Review Letters*, vol. 102, no. 18, p. 180504, 2009.

[112] T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, R. Namiki, K. Kasai, R. Matsumoto, and T. Tsurumaru, "Implementation of continuous-variable quantum key distribution with discrete modulation," *Quantum Science and Technology*, vol. 2, no. 2, p. 024010, 2017.

[113] K. Brádler and C. Weedbrook, "Security proof of continuous-variable quantum key distribution using three coherent states," *Physical Review A*, vol. 97, no. 2, p. 022310, 2018.

[114] P. Papanastasiou, C. Lupo, C. Weedbrook, and S. Pirandola, "Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels," *Physical Review A*, vol. 98, no. 1, p. 012340, 2018.

[115] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation," *Physical Review X*, vol. 9, no. 2, p. 021059, 2019.

[116] Y. Pan, H. Wang, Y. Shao, Y. Pi, Y. Li, B. Liu, W. Huang, and B. Xu, "Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system," *Optics Letters*, vol. 47, no. 13, pp. 3307–3310, 2022.

[117] Y. Tian, Y. Zhang, S. Liu, P. Wang, Z. Lu, X. Wang, and Y. Li, "High-performance long-distance discrete-modulation continuous-variable quantum key distribution," *Optics Letters*, vol. 48, no. 11, pp. 2953–2956, 2023.

[118] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, "Advances in quantum cryptography," *Advances in Optics and Photonics*, vol. 12, no. 4, pp. 1012–1236, 2020.

[119] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," *arXiv preprint quant-ph/0306141*, 2003.

[120] M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations," *Physical Review A*, vol. 62, no. 6, p. 062308, 2000.

[121] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Physical Review A*, vol. 63, no. 5, p. 052311, 2001.

[122] V. C. Usenko, "Unidimensional continuous-variable quantum key distribution using squeezed states," *Physical Review A*, vol. 98, no. 3, p. 032321, 2018.

[123] I. Derkach, V. C. Usenko, and R. Filip, "Squeezing-enhanced quantum key distribution over atmospheric channels," *New Journal of Physics*, vol. 22, no. 5, p. 053006, 2020.

[124] R. Garcia-Patron Sanchez, *Quantum information with optical continuous variables: from Bell tests to key distribution*. PhD thesis, Université libre de Bruxelles, 2007.

[125] N. J. Cerf, S. Iblisdir, and G. Van Assche, "Cloning and cryptography with quantum continuous variables," *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics*, vol. 18, pp. 211–218, 2002.

[126] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, "Direct and reverse secret-key capacities of a quantum channel," *Physical Review Letters*, vol. 102, no. 5, p. 050503, 2009.

[127] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, "High-bit-rate continuous-variable quantum key distribution," *Physical Review A*, vol. 90, no. 4, p. 042329, 2014.

[128] H. Mani, T. Gehring, P. Grabenweger, B. Ömer, C. Pacher, and U. L. Andersen, "Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution," *Physical Review A*, vol. 103, no. 6, p. 062419, 2021.

[129] M. Sayat, B. Shajilal, S. P. Kish, S. M. Assad, T. Symul, P. K. Lam, N. Rattenbury, and J. Cater, "Satellite-to-ground continuous variable quantum key distribution: The Gaussian and discrete modulated protocols in low earth orbit," *IEEE Transactions on Communications*, 2024.

[130] N. Hosseinidehaj, N. Walk, and T. C. Ralph, "Optimal realistic attacks in continuous-variable quantum key distribution," *Physical Review A*, vol. 99, no. 5, p. 052336, 2019.

[131] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 86, no. 2, p. 022318, 2012.

[132] N. Gisin and R. Thew, "Quantum communication," *Nature Photonics*, vol. 1, no. 3, pp. 165–171, 2007.

[133] J. F. Dynes, H. Takesue, Z. L. Yuan, A. W. Sharpe, K. Harada, T. Honjo, H. Kamada, O. Tadanaga, Y. Nishida, M. Asobe, *et al.*, "Efficient entanglement distribution over 200 kilometers," *Optics Express*, vol. 17, no. 14, pp. 11440–11449, 2009.

[134] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, "Entanglement distribution over 300 km of fiber," *Optics Express*, vol. 21, no. 20, pp. 23241–23249, 2013.

[135] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Review of Modern Physics*, vol. 92, no. 2, p. 025002, 2020.

[136] M. M. Wilde, M. Tomamichel, and M. Berta, "Converse bounds for private communication over quantum channels," *IEEE Transactions on Information Theory*, vol. 63, no. 3, pp. 1792–1817, 2017.

[137] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: the role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.

[138] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Physical Review A*, vol. 59, no. 1, p. 169, 1999.

[139] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside quantum repeaters," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 21, no. 3, pp. 78–90, 2015.

[140] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, "Reverse coherent information," *Physical Review Letters*, vol. 102, no. 21, p. 210501, 2009.

[141] M. Horodecki, P. Horodecki, and R. Horodecki, "Unified approach to quantum capacities: towards quantum noisy coding theorem," *Physical Review Letters*, vol. 85, no. 2, p. 433, 2000.

[142] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. 461, no. 2053, pp. 207–235, 2005.

[143] I. Devetak, M. Junge, C. King, and M. B. Ruskai, "Multiplicativity of completely bounded p-norms implies a new additivity result," *Communications in Mathematical Physics*, vol. 266, pp. 37–63, 2006.

[144] M. S. Winnel, J. J. Guanzon, N. Hosseinidehaj, and T. C. Ralph, "Achieving the ultimate end-to-end rates of lossy quantum communication networks," *npj Quantum Information*, vol. 8, no. 1, p. 129, 2022.

[145] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, no. 6862, pp. 413–418, 2001.

[146] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Review of Modern Physics*, vol. 83, pp. 33–80, Mar 2011.

[147] A. M. Goebel, C. Wagenknecht, Q. Zhang, Y.-A. Chen, K. Chen, J. Schmiedmayer, and J.-W. Pan, "Multistage entanglement swapping," *Physical Review Letters*, vol. 101, no. 8, p. 080403, 2008.

[148] R. Kaltenbaek, R. Prevedel, M. Aspelmeyer, and A. Zeilinger, "High-fidelity entanglement swapping with fully independent sources," *Physical Review A*, vol. 79, no. 4, p. 040302, 2009.

[149] Z.-D. Li, R. Zhang, X.-F. Yin, L.-Z. Liu, Y. Hu, Y.-Q. Fang, Y.-Y. Fei, X. Jiang, J. Zhang, L. Li, *et al.*, "Experimental quantum repeater without quantum memory," *Nature Photonics*, vol. 13, no. 9, pp. 644–648, 2019.

[150] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," *Physical Review Letters*, vol. 76, no. 5, p. 722, 1996.

[151] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Physical Review A*, vol. 54, no. 5, p. 3824, 1996.

[152] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, "Quantum privacy amplification and the security of quantum cryptography over noisy channels," *Physical Review Letters*, vol. 77, no. 13, p. 2818, 1996.

[153] M. Horodecki, P. Horodecki, and R. Horodecki, "Inseparable two spin-1 2 density matrices can be distilled to a singlet form," *Physical Review Letters*, vol. 78, no. 4, p. 574, 1997.

[154] Z. Zhao, T. Yang, Y.-A. Chen, A.-N. Zhang, and J.-W. Pan, "Experimental realization of entanglement concentration and a quantum repeater," *Physical Review Letters*, vol. 90, no. 20, p. 207901, 2003.

[155] K. G. H. Vollbrecht, C. A. Muschik, and J. I. Cirac, "Entanglement distillation by dissipation and continuous quantum repeaters," *Physical Review Letters*, vol. 107, no. 12, p. 120502, 2011.

[156] S. Bratzik, S. Abruzzo, H. Kampermann, and D. Bruß, "Quantum repeaters and quantum key distribution: The impact of entanglement distillation on the secret key rate," *Physical Review A*, vol. 87, no. 6, p. 062335, 2013.

[157] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Optimal architectures for long distance quantum communication," *Scientific Reports*, vol. 6, no. 1, p. 20463, 2016.

[158] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," *Physical Review A*, vol. 52, no. 4, p. R2493, 1995.

[159] A. M. Steane, "Error correcting codes in quantum theory," *Physical Review Letters*, vol. 77, no. 5, p. 793, 1996.

[160] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Physical Review A*, vol. 54, no. 2, p. 1098, 1996.

[161] D. Gottesman, *Stabilizer codes and quantum error correction*. California Institute of Technology, 1997.

[162] E. Knill, R. Laflamme, R. Martinez, and C. Negrevergne, "Benchmarking quantum computers: the five-qubit error correcting code," *Physical Review Letters*, vol. 86, no. 25, p. 5811, 2001.

[163] M. S. Postol, "A proposed quantum low density parity check code," *arXiv preprint quant-ph/0108131*, 2001.

[164] D. J. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Transactions on Information Theory*, vol. 50, no. 10, pp. 2315–2330, 2004.

[165] D. Gottesman, "An introduction to quantum error correction and fault-tolerant quantum computation," in *Quantum information science and its contributions to mathematics, Proceedings of Symposia in Applied Mathematics*, vol. 68, pp. 13–58, 2010.

[166] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Quantum error correction beyond the bounded distance decoding limit," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 1223–1230, 2011.

[167] J. R. Wootton and D. Loss, "Repetition code of 15 qubits," *Physical Review A*, vol. 97, no. 5, p. 052313, 2018.

[168] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Physical Review Letters*, vol. 121, no. 19, p. 190502, 2018.

[169] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 ghz time-bin quantum key distribution," *Applied Physics Letters*, vol. 112, no. 17, 2018.

[170] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," *Physical Review Letters*, vol. 91, no. 5, p. 057901, 2003.

[171] S.-K. Liao, J. Lin, J.-G. Ren, W.-Y. Liu, J. Qiang, J. Yin, Y. Li, Q. Shen, L. Zhang, X.-F. Liang, *et al.*, "Space-to-ground quantum key distribution using a small-sized payload on tiangong-2 space lab," *Chinese Physics Letters*, vol. 34, no. 9, p. 090302, 2017.

[172] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Physical Review A*, vol. 51, no. 3, p. 1863, 1995.

[173] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Physical Review Letters*, vol. 85, no. 6, p. 1330, 2000.

[174] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Physical Review Letters*, vol. 89, no. 3, p. 037902, 2002.

[175] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, . A. s. p. l.-b. j. y. G.-C. Guo, and Z.-F. Han, "2 ghz clock quantum key distribution over 260 km of standard telecom fiber," *Optics Letters*, vol. 37, no. 6, pp. 1008–1010, 2012.

[176] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-frame-independent quantum key distribution," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 82, no. 1, p. 012304, 2010.

[177] X. Liu, D. Luo, Z. Luo, S. Li, Z. Zhang, and K. Wei, "Reference-frame-independent quantum key distribution over 250 km of optical fiber," *Physical Review Applied*, vol. 22, no. 6, p. 064018, 2024.

[178] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, "High-dimensional quantum key distribution using dispersive optics," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 87, no. 6, p. 062322, 2013.

[179] J. Liu, Z. Lin, D. Liu, X. Feng, F. Liu, K. Cui, Y. Huang, and W. Zhang, "High-dimensional quantum key distribution using energy-time entanglement over 242 km partially deployed fiber," *Quantum Science and Technology*, vol. 9, no. 1, p. 015003, 2023.

[180] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Physical Review Letters*, vol. 68, no. 5, p. 557, 1992.

[181] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, *et al.*, "High-rate quantum key distribution exceeding 110 mb s–1," *Nature Photonics*, vol. 17, no. 5, pp. 416–421, 2023.

[182] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, *et al.*, "Decoy-state quantum key distribution with polarized photons over 200 km," *Optics Express*, vol. 18, no. 8, pp. 8587–8594, 2010.

[183] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, *et al.*, "Satellite-to-ground entanglement-based quantum key distribution," *Physical Review Letters*, vol. 119, no. 20, p. 200501, 2017.

[184] S. Ecker, B. Liu, J. Handsteiner, M. Fink, D. Rauch, F. Steinlechner, T. Scheidl, A. Zeilinger, and R. Ursin, "Strategies for achieving high key rates in satellite-based qkd," *npj Quantum Information*, vol. 7, no. 1, p. 5, 2021.

[185] Y. Pan, M. Wu, H. Wang, J. Li, Y. Shao, Y. Li, W. Huang, S. Yu, Y. Zhang, and B. Xu, "Long-distance discrete-modulated continuous-variable quantum key distribution over 126.56 km of fiber," in *Optical Fiber Communication Conference*, pp. W1J–1, Optica Publishing Group, 2025.

[186] H. Wang, Y. Li, T. Ye, L. Ma, Y. Pan, M. Wu, J. Li, Y. Bian, Y. Pi, Y. Shao, *et al.*, "High-rate continuous-variable quantum key distribution over 100 km fiber with composable security," *arXiv preprint arXiv:2503.14843*, 2025.

[187] Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, J. Yang, Y. Zhang, W. Huang, and B. Xu, "Sub-mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber," *Optics Letters*, vol. 48, no. 7, pp. 1766–1769, 2023.

[188] L. Lydersen, J. Skaar, and V. Makarov, "Tailored bright illumination attack on distributed-phase-reference protocols," *Journal of Modern Optics*, vol. 58, no. 8, pp. 680–685, 2011.

[189] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Physical Review Letters*, vol. 108, no. 13, p. 130502, 2012.

[190] I. Derkach, V. C. Usenko, and R. Filip, "Preventing side-channel effects in continuous-variable quantum key distribution," *Physical Review A*, vol. 93, no. 3, p. 032309, 2016.

[191] A. Baliuka, M. Stöcker, M. Auer, P. Freiwang, H. Weinfurter, and L. Knips, "Deep-learning-based radio-frequency side-channel attack on quantum key distribution," *Physical Review Applied*, vol. 20, no. 5, p. 054040, 2023.

[192] S. P. Kish, C. Thapa, M. Sayat, H. Suzuki, J. Pieprzyk, and S. Camtepe, "Mitigation of channel tampering attacks in continuous-variable quantum key distribution," *Physical Review Research*, vol. 6, no. 2, p. 023301, 2024.

[193] F. Xu, M. Curty, B. Qi, L. Qian, and H.-K. Lo, "Discrete and continuous variables for measurement-device-independent quantum cryptography," *Nature Photonics*, vol. 9, no. 12, pp. 772–773, 2015.

[194] M. Lasota, O. Kovalenko, and V. C. Usenko, "Robustness of entanglement-based discrete-and continuous-variable quantum key distribution against channel noise," *New Journal of Physics*, vol. 25, no. 12, p. 123003, 2023.

[195] S. P. Kish, P. J. Gleeson, A. Walsh, P. K. Lam, and S. M. Assad, "Comparison of discrete variable and continuous variable quantum key distribution protocols with phase noise in the thermal-loss channel," *Quantum*, vol. 8, p. 1382, 2024.

[196] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, W.-Y. Liu, *et al.*, "Implementation of a 46-node quantum metropolitan area network," *npj Quantum Information*, vol. 7, no. 1, p. 134, 2021.

[197] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.

[198] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, *et al.*, "Long-term performance of the swissquantum quantum key distribution network in a field environment," *New Journal of Physics*, vol. 13, no. 12, p. 123001, 2011.

[199] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, *et al.*, "Field test of quantum key distribution in the tokyo qkd network," *Optics Express*, vol. 19, no. 11, pp. 10387–10409, 2011.

[200] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, *et al.*, "Field test of wavelength-saving quantum key distribution network," *Optics Letters*, vol. 35, no. 14, pp. 2454–2456, 2010.

[201] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, *et al.*, "Metropolitan all-pass and inter-city quantum communication network," *Optics Express*, vol. 18, no. 26, pp. 27217–27225, 2010.

[202] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, *et al.*, "The secoqc quantum key distribution network in vienna," *New Journal of Physics*, vol. 11, no. 7, p. 075001, 2009.

[203] T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, *et al.*, "Field test of a practical secure communication network with decoy-state quantum cryptography," *Optics Express*, vol. 17, no. 8, pp. 6540–6549, 2009.

[204] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Physical Review X*, vol. 6, no. 1, p. 011024, 2016.

[205] W. Yan, X. Zheng, W. Wen, L. Lu, Y. Du, Y.-Q. Lu, S. Zhu, and X.-S. Ma, "A measurement-device-independent quantum key distribution network using optical frequency comb," *npj Quantum Information*, vol. 11, no. 1, p. 97, 2025.

[206] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, *et al.*, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," *Physical Review X*, vol. 10, no. 3, p. 031030, 2020.

[207] A. A. Hajomer, U. L. Andersen, and T. Gehring, "High-rate continuous-variable measurement device-independent quantum key distribution with finite-size security," *Quantum Science and Technology*, vol. 10, no. 2, p. 025032, 2025.

[208] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate quantum cryptography in untrusted networks," *arXiv preprint arXiv:1312.4104*, 2013.

[209] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. Yuan, and A. J. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nature Photonics*, vol. 13, no. 5, pp. 334–338, 2019.

[210] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, *et al.*, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," *Physical Review Letters*, vol. 124, no. 7, p. 070501, 2020.

[211] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, *et al.*, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nature Photonics*, vol. 15, no. 8, pp. 570–575, 2021.

[212] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, "600-km repeater-like quantum communications with dual-band stabilization," *Nature Photonics*, vol. 15, no. 7, pp. 530–535, 2021.

[213] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, *et al.*, "Quantum key distribution over 658 km fiber with distributed vibration sensing," *Physical Review Letters*, vol. 128, no. 18, p. 180502, 2022.

[214] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, *et al.*, "Experimental twin-field quantum key distribution over 1000 km fiber distance," *Physical Review Letters*, vol. 130, no. 21, p. 210801, 2023.

[215] L. Zhou, J. Lin, C. Ge, Y. Fan, Z. Yuan, H. Dong, Y. Liu, D. Ma, J.-P. Chen, C. Jiang, *et al.*, "Independent-optical-frequency-comb-powered 546-km field test of twin-field quantum key distribution," *Physical Review Applied*, vol. 22, no. 6, p. 064057, 2024.

[216] C. Huang, R. Guan, X. Liu, W. He, S. Li, H. Liang, Z. Luo, Z. Zhang, W. Li, and K. Wei, "Scalable twin-field quantum key distribution network enabled by adaptable architecture," *arXiv preprint arXiv:2504.15137*, 2025.

[217] C. H. Park, M. K. Woo, B. K. Park, Y.-S. Kim, H. Baek, S.-W. Lee, H.-T. Lim, S.-W. Jeon, H. Jung, S. Kim, *et al.*, "2× n twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing," *npj Quantum Information*, vol. 8, no. 1, p. 48, 2022.

[218] G.-Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, "Heralded noiseless linear amplification and distillation of entanglement," *Nature Photonics*, vol. 4, no. 5, pp. 316–319, 2010.

[219] M. S. Winnel, N. Hosseinidehaj, and T. C. Ralph, "Generalized quantum scissors for noiseless linear amplification," *Physical Review A*, vol. 102, no. 6, p. 063715, 2020.

[220] K. Bencheikh, T. Symul, A. Jankovic, and J.-A. Levenson, "Quantum key distribution with continuous variables," *Journal of Modern Optics*, vol. 48, no. 13, pp. 1903–1920, 2001.

[221] P. Huang, G. He, J. Fang, and G. Zeng, "Performance improvement of continuous-variable quantum key distribution via photon subtraction," *Physical Review A*, vol. 87, no. 1, p. 012317, 2013.

[222] L. Hu, M. Al-Amri, Z. Liao, and M. Zubairy, "Continuous-variable quantum key distribution with non-Gaussian operations," *Physical Review A*, vol. 102, no. 1, p. 012608, 2020.

[223] W. Ye, H. Zhong, Q. Liao, D. Huang, L. Hu, and Y. Guo, "Improvement of self-referenced continuous-variable quantum key distribution with quantum photon catalysis," *Optics Express*, vol. 27, no. 12, pp. 17186–17198, 2019.

[224] J. Hu, Q. Liao, Y. Mao, and Y. Guo, "Performance improvement of unidimensional continuous-variable quantum key distribution using zero-photon quantum catalysis," *Quantum Information Processing*, vol. 20, pp. 1–20, 2021.

[225] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, "Security of continuous-variable quantum cryptography with Gaussian postselection," *Physical Review A*, vol. 87, no. 2, p. 020303, 2013.

[226] J. Fiurášek and N. J. Cerf, "Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution," *Physical Review A*, vol. 86, no. 6, p. 060302, 2012.

[227] N. Hosseinidehaj, A. M. Lance, T. Symul, N. Walk, and T. C. Ralph, "Finite-size effects in continuous-variable quantum key distribution with Gaussian postselection," *Physical Review A*, vol. 101, no. 5, p. 052335, 2020.

[228] H. M. Chrzanowski, N. Walk, S. M. Assad, J. Janousek, S. Hosseini, T. C. Ralph, T. Symul, and P. K. Lam, "Measurement-based noiseless linear amplification for quantum communication," *Nature Photonics*, vol. 8, no. 4, pp. 333–338, 2014.

[229] J. Zhao, J. Y. Haw, T. Symul, P. K. Lam, and S. M. Assad, "Characterization of a measurement-based noiseless linear amplifier and its applications," *Physical Review A*, vol. 96, no. 1, p. 012319, 2017.

[230] B. Shajilal, L. O. Conlon, A. Walsh, S. Tserkis, J. Zhao, J. Janousek, S. Assad, and P. K. Lam, "Improving Gaussian channel simulation using nonunity-gain heralded quantum teleportation," *Physical Review Applied*, vol. 22, no. 5, p. 054070, 2024.

[231] Z. Li, Y. Zhang, X. Wang, B. Xu, X. Peng, and H. Guo, "Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution," *Physical Review A*, vol. 93, no. 1, p. 012310, 2016.

[232] H. Zhong, Y. Wang, X. Wang, Q. Liao, X. Wu, and Y. Guo, "Enhancing of self-referenced continuous-variable quantum key distribution with virtual photon subtraction," *Entropy*, vol. 20, no. 8, p. 578, 2018.

[233] H. Zhong, Y. Guo, Y. Mao, W. Ye, and D. Huang, "Virtual zero-photon catalysis for improving continuous-variable quantum key distribution via Gaussian post-selection," *Scientific Reports*, vol. 10, no. 1, p. 17526, 2020.

[234] R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," *Physical Review Letters*, vol. 97, no. 19, p. 190503, 2006.

[235] M. M. Wolf, G. Giedke, and J. I. Cirac, "Extremality of Gaussian quantum states," *Physical Review Letters*, vol. 96, no. 8, p. 080502, 2006.

[236] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations," *Advanced Quantum Technologies*, vol. 1, no. 1, p. 1800011, 2018.

[237] F. Grosshans and P. Grangier, "Reverse reconciliation protocols for quantum cryptography with continuous variables," *arXiv preprint quant-ph/0204127*, 2002.

[238] G. Cariolaro and G. Pierobon, "Reexamination of bloch-messiah reduction," *Physical Review A*, vol. 93, no. 6, p. 062115, 2016.

[239] L. Li, T. Wang, X. Li, P. Huang, Y. Guo, L. Lu, L. Zhou, and G. Zeng, "Continuous-variable quantum key distribution with on-chip light sources," *Photonics Research*, vol. 11, no. 4, pp. 504–516, 2023.

[240] J. Eisert, S. Scheel, and M. B. Plenio, "Distilling Gaussian states with Gaussian operations is impossible," *Physical Review Letters*, vol. 89, no. 13, p. 137903, 2002.

[241] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," *Quantum*, vol. 5, p. 540, 2021.

[242] F. Kanitschar and C. Pacher, "Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection," *Physical Review Applied*, vol. 18, no. 3, p. 034073, 2022.

[243] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, "Quantum repeaters: From quantum networks to the quantum internet," *Reviews of Modern Physics*, vol. 95, no. 4, p. 045006, 2023.

[244] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: entangling photons that never interacted," *Physical Review Letters*, vol. 80, no. 18, p. 3891, 1998.

[245] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, "Quantum repeater with encoding," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 79, no. 3, p. 032325, 2009.

[246] W. Munro, K. Harrison, A. Stephens, S. Devitt, and K. Nemoto, "From quantum multiplexing to high-performance quantum networking," *Nature Photonics*, vol. 4, no. 11, pp. 792–796, 2010.

[247] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, "Long range failure-tolerant entanglement distribution," *New Journal of Physics*, vol. 15, no. 2, p. 023012, 2013.

[248] P. Mazurek, A. Grudka, M. Horodecki, P. Horodecki, J. Lodyga, L. Pankowski, and A. Przysiezna, "Long-distance quantum communication over noisy networks without long-time quantum memory," *Physical Review A*, vol. 90, no. 6, p. 062311, 2014.

[249] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, no. 6760, pp. 390–393, 1999.

[250] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, . f. R. Van Meter, and L. C. Hollenberg, "Surface code quantum communication," *Physical Review Letters*, vol. 104, no. 18, p. 180503, 2010.

[251] W. J. Munro, A. M. Stephens, S. J. Devitt, K. A. Harrison, and K. Nemoto, "Quantum communication without the necessity of quantum memories," *Nature Photonics*, vol. 6, no. 11, pp. 777–781, 2012.

[252] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, "Ultrafast and fault-tolerant quantum communication across long distances," *Physical review letters*, vol. 112, no. 25, p. 250501, 2014.

[253] E. Knill and R. Laflamme, "Concatenated quantum codes," *arXiv preprint quant-ph/9608012*, 1996.

[254] D. Gottesman, A. Kitaev, and J. Preskill, "Encoding a qubit in an oscillator," *Physical Review A*, vol. 64, no. 1, p. 012310, 2001.

[255] T. C. Ralph, A. Hayes, and A. Gilchrist, "Loss-tolerant optical qubits," *Physical Review Letters*, vol. 95, no. 10, p. 100501, 2005.

[256] M. Varnava, D. E. Browne, and T. Rudolph, "Loss tolerance in one-way quantum computation via counterfactual error correction," *Physical Review Letters*, vol. 97, no. 12, p. 120501, 2006.

[257] R. Raussendorf and J. Harrington, "Fault-tolerant quantum computation with high threshold in two dimensions," *Physical Review Letters*, vol. 98, no. 19, p. 190504, 2007.

[258] R. Raussendorf, J. Harrington, and K. Goyal, "Topological fault-tolerance in cluster state quantum computation," *New Journal of Physics*, vol. 9, no. 6, p. 199, 2007.

[259] Z. Li, L.-J. Xing, and X.-M. Wang, "Quantum generalized reed-solomon codes: Unified framework for quantum maximum-distance-separable codes," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 77, no. 1, p. 012308, 2008.

[260] M. Mirrahimi, Z. Leghtas, V. V. Albert, S. Touzard, R. J. Schoelkopf, L. Jiang, and M. H. Devoret, "Dynamically protected cat-qubits: a new paradigm for universal quantum computation," *New Journal of Physics*, vol. 16, no. 4, p. 045014, 2014.

[261] M. H. Michael, M. Silveri, R. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. M. Girvin, "New class of quantum error-correcting codes for a bosonic mode," *Physical Review X*, vol. 6, no. 3, p. 031006, 2016.

[262] S. Muralidharan, C.-L. Zou, L. Li, J. Wen, and L. Jiang, "Overcoming erasure errors with multilevel systems," *New Journal of Physics*, vol. 19, no. 1, p. 013026, 2017.

[263] S. Muralidharan, C.-L. Zou, L. Li, and L. Jiang, "One-way quantum repeaters with quantum reed-solomon codes," *Physical Review A*, vol. 97, no. 5, p. 052316, 2018.

[264] V. V. Albert, K. Noh, K. Duivenvoorden, D. J. Young, R. Brierley, P. Reinhold, C. Vuillot, L. Li, C. Shen, S. M. Girvin, *et al.*, "Performance and structure of single-mode bosonic codes," *Physical Review A*, vol. 97, no. 3, p. 032346, 2018.

[265] K. Noh, V. V. Albert, and L. Jiang, "Quantum capacity bounds of Gaussian thermal loss channels and achievable rates with gottesman-kitaev-preskill codes," *IEEE Transactions on Information Theory*, vol. 65, no. 4, pp. 2563–2582, 2018.

[266] C. Simon, H. De Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, "Quantum repeaters with photon pair sources and multimode memories," *Physical Review Letters*, vol. 98, no. 19, p. 190503, 2007.

[267] J. Dias, M. S. Winnel, N. Hosseinidehaj, and T. C. Ralph, "Quantum repeater for continuous-variable entanglement distribution," *Physical Review A*, vol. 102, p. 052425, Nov 2020.

[268] C. Liu, M. Wang, S. A. Stein, Y. Ding, and A. Li, "Quantum memory: A missing piece in quantum computing units," *arXiv preprint arXiv:2309.14432*, 2023.

[269] Y.-W. Cho, G. Campbell, J. Everett, J. Bernu, D. Higginbottom, M. Cao, J. Geng, N. Robins, P. Lam, and B. Buchler, "Highly efficient optical quantum memory with long coherence time in cold atoms," *Optica*, vol. 3, no. 1, pp. 100–107, 2016.

[270] M. Cao, F. Hoffet, S. Qiu, A. S. Sheremet, and J. Laurat, "Efficient reversible entanglement transfer between light and quantum memories," *Optica*, vol. 7, no. 10, pp. 1440–1444, 2020.

[271] Y.-F. Hsiao, P.-J. Tsai, H.-S. Chen, S.-X. Lin, C.-C. Hung, C.-H. Lee, Y.-H. Chen, Y.-F. Chen, A. Y. Ite, and Y.-C. Chen, "Highly efficient coherent optical memory based on electromagnetically induced transparency," *Physical Review Letters*, vol. 120, no. 18, p. 183602, 2018.

[272] Y. Ma, Y.-Z. Ma, Z.-Q. Zhou, C.-F. Li, and G.-C. Guo, "One-hour coherent optical storage in an atomic frequency comb memory," *Nature Communications*, vol. 12, no. 1, p. 2381, 2021.

[273] M. Hain, N. Stewen, and T. Halfmann, "Light storage by electromagnetically induced transparency for one second at the level of a single photon inpr3+: Y2sio5 prepared with multiple frequency ensembles," *New Journal of Physics*, 2025.

[274] M. P. Hedges, J. J. Longdell, Y. Li, and M. J. Sellars, "Efficient quantum memory for light," *Nature*, vol. 465, no. 7301, pp. 1052–1056, 2010.

[275] F. Bussières, C. Clausen, A. Tiranov, B. Korzh, V. B. Verma, S. W. Nam, F. Marsili, A. Ferrier, P. Goldner, H. Herrmann, *et al.*, "Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory," *Nature Photonics*, vol. 8, no. 10, pp. 775–778, 2014.

[276] J. S. Stuart, M. Hedges, R. Ahlefeldt, and M. Sellars, "Initialization protocol for efficient quantum memories using resolved hyperfine structure," *Physical Review Research*, vol. 3, no. 3, p. L032054, 2021.

[277] J. Chen and M. Afzelius, "Efficient and reversible optical-to-spin conversion for solid-state quantum memories," *Quantum Science and Technology*, vol. 10, no. 2, p. 025060, 2025.

[278] N. Maring, K. Kutluer, J. Cohen, M. Cristiani, M. Mazzera, P. M. Ledingham, and H. de Riedmatten, "Storage of up-converted telecom photons in a doped crystal," *New Journal of Physics*, vol. 16, no. 11, p. 113021, 2014.

[279] W.-H. Zhang, Y.-H. Ye, L. Zeng, M.-X. Dong, E.-Z. Li, J.-Y. Peng, Y. Li, D.-S. Ding, and B.-S. Shi, "Telecom-wavelength conversion in a high optical depth cold atomic system," *Optics Express*, vol. 31, no. 5, pp. 8042–8048, 2023.

[280] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, no. 13, p. 130503, 2012.

[281] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," *Nature Photonics*, vol. 9, no. 6, pp. 397–402, 2015.

[282] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, *et al.*, "Experimental measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 111, no. 13, p. 130502, 2013.

[283] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 112, no. 19, p. 190503, 2014.

[284] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, *et al.*, "Measurement-device-independent quantum key distribution over 200 km," *Physical Review Letters*, vol. 113, no. 19, p. 190501, 2014.

[285] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Physical Review Letters*, vol. 117, no. 19, p. 190501, 2016.

[286] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, "Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference," *PRX Quantum*, vol. 3, no. 2, p. 020315, 2022.

[287] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, 2018.

[288] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution," *Physical Review Letters*, vol. 123, no. 10, p. 100506, 2019.

[289] H. Liu, C. Jiang, H.-T. Zhu, M. Zou, Z.-W. Yu, X.-L. Hu, H. Xu, S. Ma, Z. Han, J.-P. Chen, *et al.*, "Field test of twin-field quantum key distribution through sending-or-not-sending over 428 km," *Physical Review Letters*, vol. 126, no. 25, p. 250502, 2021.

[290] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, *et al.*, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nature Photonics*, vol. 15, no. 8, pp. 570–575, 2021.

[291] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, *et al.*, "Quantum key distribution over 658 km fiber with distributed vibration sensing," *Physical Review Letters*, vol. 128, no. 18, p. 180502, 2022.

[292] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, *et al.*, "Twin-field quantum key distribution over 830-km fibre," *Nature Photonics*, vol. 16, no. 2, pp. 154–161, 2022.

[293] P. Wang, X. Wang, and Y. Li, "Continuous-variable measurement-device-independent quantum key distribution using modulated squeezed states and optical amplifiers," *Physical Review A*, vol. 99, no. 4, p. 042309, 2019.

[294] H.-X. Ma, P. Huang, D.-Y. Bai, T. Wang, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, "Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation," *Physical Review A*, vol. 99, no. 2, p. 022322, 2019.

[295] W. Asavanant, K. Takase, K. Fukui, M. Endo, J.-i. Yoshikawa, and A. Furusawa, "Wave-function engineering via conditional quantum teleportation with a non-Gaussian entanglement resource," *Physical Review A*, vol. 103, no. 4, p. 043701, 2021.

[296] J. Fiurášek, R. García-Patrón, and N. J. Cerf, "Conditional generation of arbitrary single-mode quantum states of light by repeated photon subtractions," *Physical Review A*, vol. 72, no. 3, p. 033822, 2005.

[297] J. Clausen, H. Hansen, L. Knöll, J. Mlynek, and D.-G. Welsch, "Conditional quantum-state engineering in repeated 2-photon down-conversion," *Applied Physics B*, vol. 72, no. 1, pp. 43–50, 2001.

[298] E. Bimbard, N. Jain, A. MacRae, and A. Lvovsky, "Quantum-optical state engineering up to the two-photon level," *Nature Photonics*, vol. 4, no. 4, pp. 243–247, 2010.

[299] A. Luis and L. Sánchez-Soto, "Phase-difference operator," *Physical Review A*, vol. 48, no. 6, p. 4702, 1993.

[300] P. Cochrane, G. J. Milburn, and W. Munro, "Teleportation using coupled oscillator states," *Physical Review A*, vol. 62, no. 6, p. 062307, 2000.

[301] N.-K. Tran and O. Pfister, "Quantum teleportation with close-to-maximal entanglement from a beam splitter," *Physical Review A*, vol. 65, no. 5, p. 052313, 2002.

[302] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, no. 14, p. 3018, 1998.

[303] W.-Y. Liang, H. Wen, Z.-Q. Yin, H. Chen, H.-W. Li, W. Chen, and Z.-F. Han, "Tomographic approach in three-orthogonal-basis quantum key distribution," *Communications in Theoretical Physics*, vol. 64, no. 3, p. 295, 2015.

[304] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Tomography increases key rates of quantum-key-distribution protocols," *Physical Review A*, vol. 78, no. 4, p. 042316, 2008.

[305] J. Schwinger, "Unitary operator bases," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 46, no. 4, pp. 570–579, 1960.

[306] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Annals of Physics*, vol. 191, no. 2, pp. 363–381, 1989.

[307] P. Horodecki, Ł. Rudnicki, and K. Życzkowski, "Five open problems in quantum information theory," *PRX Quantum*, vol. 3, no. 1, p. 010101, 2022.

[308] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution without phase postselection," *Physical Review Applied*, vol. 11, no. 3, p. 034053, 2019.

[309] F.-Y. Lu, Z.-Q. Yin, C.-H. Cui, G.-J. Fan-Yuan, R. Wang, S. Wang, W. Chen, D.-Y. He, W. Huang, B.-J. Xu, *et al.*, "Improving the performance of twin-field quantum key distribution," *Physical Review A*, vol. 100, no. 2, p. 022306, 2019.

[310] M. Curty, K. Azuma, and H.-K. Lo, "Simple security proof of twin-field type quantum key distribution protocol," *npj Quantum Information*, vol. 5, no. 1, pp. 1–6, 2019.

[311] H.-L. Yin and Y. Fu, "Measurement-device-independent twin-field quantum key distribution," *Scientific Reports*, vol. 9, no. 1, pp. 1–13, 2019.

[312] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, "Twin-field quantum key distribution with large misalignment error," *Physical Review A*, vol. 98, no. 6, p. 062323, 2018.

[313] M. S. Winnel, J. J. Guanzon, N. Hosseinidehaj, and T. C. Ralph, "Overcoming the repeaterless bound in continuous-variable quantum communication without quantum memories," *arXiv preprint arXiv:2105.03586*, 2021.

[314] Ö. Erkılıç, L. Conlon, B. Shajilal, S. Kish, S. Tserkis, Y.-S. Kim, P. K. Lam, and S. M. Assad, "Surpassing the repeaterless bound with a photon-number encoded measurement-device-independent quantum key distribution protocol," *npj Quantum Information*, vol. 9, no. 1, p. 29, 2023.

[315] Y.-B. Sheng and F.-G. Deng, "Deterministic entanglement purification and complete nonlocal bell-state analysis with hyperentanglement," *Physical Review A*, vol. 81, no. 3, p. 032307, 2010.

[316] Y.-B. Sheng and F.-G. Deng, "One-step deterministic polarization-entanglement purification using spatial entanglement," *Physical Review A*, vol. 82, no. 4, p. 044305, 2010.

[317] Y.-B. Sheng, L. Zhou, and G.-L. Long, "Hybrid entanglement purification for quantum repeaters," *Physical Review A*, vol. 88, no. 2, p. 022302, 2013.

[318] X.-M. Hu, C.-X. Huang, Y.-B. Sheng, L. Zhou, B.-H. Liu, Y. Guo, C. Zhang, W.-B. Xing, Y.-F. Huang, C.-F. Li, *et al.*, "Long-distance entanglement purification for quantum communication," *Physical Review Letters*, vol. 126, no. 1, p. 010503, 2021.

[319] C.-X. Huang, X.-M. Hu, B.-H. Liu, L. Zhou, Y.-B. Sheng, C.-F. Li, and G.-C. Guo, "Experimental one-step deterministic polarization entanglement purification," *Science Bulletin*, vol. 67, no. 6, pp. 593–597, 2022.

[320] W. Dür and H. J. Briegel, "Entanglement purification and quantum error correction," *Reports on Progress in Physics*, vol. 70, no. 8, p. 1381, 2007.

[321] F. Verstraete, J. Dehaene, and B. DeMoor, "Local filtering operations on two qubits," *Physical Review A*, vol. 64, no. 1, p. 010101, 2001.

[322] W. Dür and H.-J. Briegel, "Entanglement purification for quantum computation," *Physical Review Letters*, vol. 90, no. 6, p. 067901, 2003.

[323] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, "Local permutations of products of bell states and entanglement distillation," *Physical Review A*, vol. 67, no. 2, p. 022310, 2003.

[324] S. J. Devitt, W. J. Munro, and K. Nemoto, "Quantum error correction for beginners," *Reports on Progress in Physics*, vol. 76, no. 7, p. 076001, 2013.

[325] R. Matsumoto, "Conversion of a general quantum stabilizer code to an entanglement distillation protocol," *Journal of Physics A: Mathematical and General*, vol. 36, no. 29, p. 8113, 2003.

[326] H. Aschauer, *Quantum communication in noisy environments*. PhD thesis, Ludwig–Maximilians–Universität, 2005.

[327] A. Ambainis and D. Gottesman, "The minimum distance problem for two-way entanglement purification," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 748–753, 2006.

[328] L. Zhou, W. Zhong, and Y.-B. Sheng, "Purification of the residual entanglement," *Optics Express*, vol. 28, no. 2, pp. 2291–2301, 2020.

[329] G. Lindblad, "Completely positive maps and entropy inequalities," *Communications in Mathematical Physics*, vol. 40, pp. 147–151, 1975.

[330] T. M. Cover, *Elements of information theory*. John Wiley & Sons, 1999.

[331] N. J. Beaudry and R. Renner, "An intuitive proof of the data processing inequality," *arXiv preprint arXiv:1107.0740*, 2011.

[332] S. Beigi, "A new quantum data processing inequality," *Journal of Mathematical Physics*, vol. 54, no. 8, 2013.

[333] F. Riera-Sàbat, P. Sekatski, A. Pirker, and W. Dür, "Entanglement-assisted entanglement purification," *Physical Review Letters*, vol. 127, no. 4, p. 040502, 2021.

[334] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang, "A survey of post-quantum cryptography: Start of a new race," *Cryptography*, vol. 7, no. 3, p. 40, 2023.

[335] R. Bavdekar, E. J. Chopde, A. Agrawal, A. Bhatia, and K. Tiwari, "Post quantum cryptography: a review of techniques, challenges and standardizations," in *2023 International Conference on Information Networking (ICOIN)*, pp. 146–151, IEEE, 2023.

[336] M. Stanley, Y. Gui, D. Unnikrishnan, S. Hall, and I. Fatadin, "Recent progress in quantum key distribution network deployments and standards," in *Journal of Physics: Conference Series*, vol. 2416, p. 012001, IOP Publishing, 2022.

[337] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, "Micius quantum experiments in space," *Reviews of Modern Physics*, vol. 94, no. 3, p. 035001, 2022.

[338] H. G. Schuster and W. Just, *Deterministic chaos: an introduction*. John Wiley & Sons, 2006.